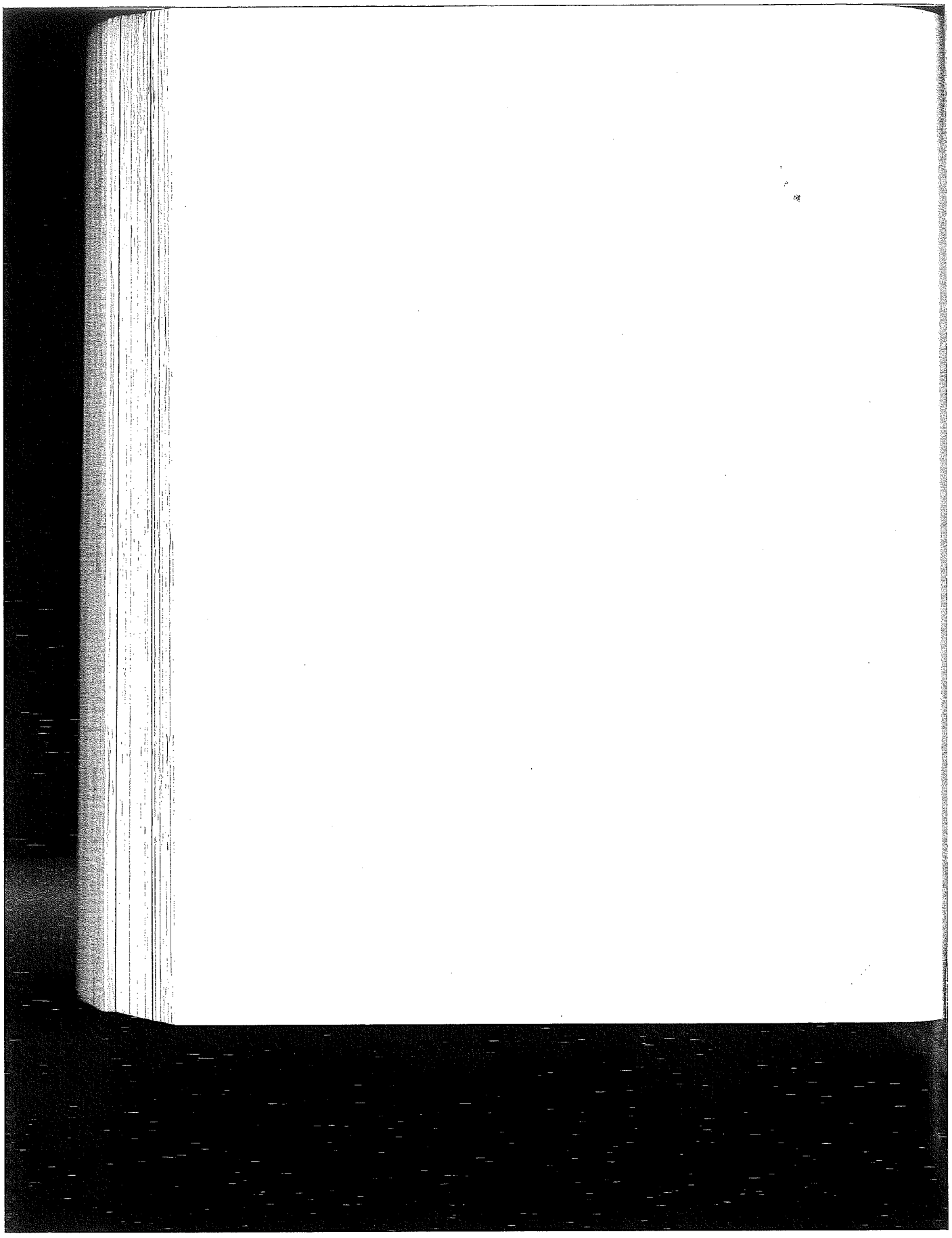
To exit ConfigMaker, click the **File** menu, and then click **Exit**. ConfigMaker is a pretty cool piece of software. Use it to learn more about the hardware and software configurations of the various routers and devices that Cisco manufactures. It's not bad at all for free.

SEE ALSO

➢ *For a review of connecting a PC console to the router, see page 115.*

Getting help in ConfigMaker

ConfigMaker is a typical Windows program. Click the **Help** menu, and then click Cisco **ConfigMaker Help Topics** to open the Help dialog box. You can use the **Contents**, **Index**, and **Find** tabs to get help on the various ConfigMaker features.



chapter

17

Using a TFTP Server for Router Configuration Storage

What Is a TFTP Server?

Installing the Cisco TFTP Server Software

Copying to the TFTP Server

Copying from the TFTP Server

Loading a New IOS from the TFTP Server

What Is a TFTP Server?

Saving router configurations to a location other than the router's own NVRAM is a way to protect the time and effort that you have put in configuring a particular router. When all is said and done the router configuration becomes the main factor in how the router actually gets its job done. So being able to back up the configuration file is a vital part of building some fault tolerance into your internetworking. You already know that when you reconfigure a router you must use the **Copy** command to move the new configuration parameters from the running configuration to the startup configuration in NVRAM. There is also a way to copy a running configuration or startup configuration to a computer that is on the network.

Trivial File Transfer Protocol (TFTP) is a TCP/IP transport protocol that can be used to move files from the router to a PC running TFTP server software. TFTP is actually very similar to the *File Transfer Protocol (FTP)* that is used for uploading and downloading files on the Internet (your Web browser supports FTP). FTP requires a username and password when you log on to an FTP server.

TFTP doesn't require a username or password (hence the "trivial" notation). All you need to know is the IP address of the computer that is running the TFTP server software and you can copy your configuration file to the server. You can also use TFTP servers to copy a configuration file to your router or upgrade (or change) your router IOS image by copying a new IOS file to the router's flash RAM. Because most routers don't have disk drives, TFTP servers provide you with an alternative location for backup files related to the router (such as a copy of the configuration or alternative configurations). Figure 17.1 depicts the different file manipulations that can take place between a router and a TFTP server.

So, a TFTP server is a PC that is running TFTP server software and is accessible on the network. Because neither login nor password is required, all you need to know to connect to the TFTP server is its IP address.

SEE ALSO

➤ *For information on using the* **Copy** *command with configuration files, see page 154.*

FTP and the Web

You probably have access to FTP sites on the World Wide Web, and have downloaded files from them. And you are probably thinking that you don't remember providing a username and password. Many of the FTP sites available on the Web are anonymous FTP sites. You log in as anonymous with no password (or your IP address or email address sometimes serves as the password). When you log on to a secure FTP site, you have to provide an appropriate username and password.

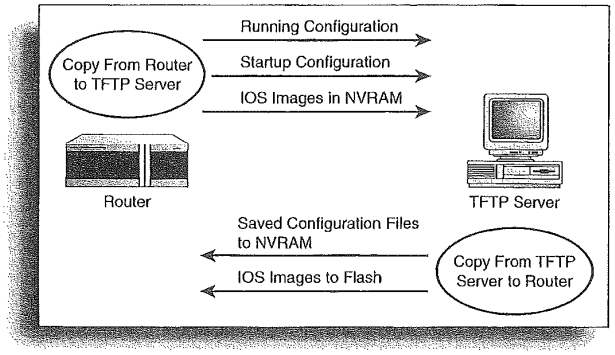


FIGURE 17.1
You can copy files from the router to the TFTP server and vice versa.

Obtaining TFTP Software

Several different TFTP server software packages are available. Cisco provides a free TFTP server application for registered Cisco product users. The TFTP server software can be downloaded from the Cisco site at `www.cisco.com`.

If you don't have access to the Cisco TFTP server software or would like to try other TFTP server software, you can find it on the Web. Use your favorite search engine and search for the keywords **TFTP server**. One shareware TFTP server is the SolarWinds TFTP server available at `http://www.solarwinds.net/`. SolarWinds makes a number of add-on tools for Cisco routers. You will find that most of the TFTP server software packages work pretty much the same. You start the server software and then execute the appropriate commands on the router. The TFTP server is pretty passive throughout the entire process but most TFTP server applications will have a window that shows you the status of a copy to or from the server.

If you want to use the Cisco TFTP server software, all you need to do is log on to the Cisco site (`www.cisco.com`) using your customer username and password (provided to you by the Cisco reseller that sold you your router). Then click the **Software Center** link on the Cisco Home Page.

On the Software Center page, click the link for **Other Software**. You will be taken to the page that provides the link for downloading the Cisco TFTP server (see Figure 17.2). Click the link and then

choose an appropriate folder on your computer where the server software can be placed during the download. After the download is complete, you can install the Cisco TFTP server software as outlined in the next section.

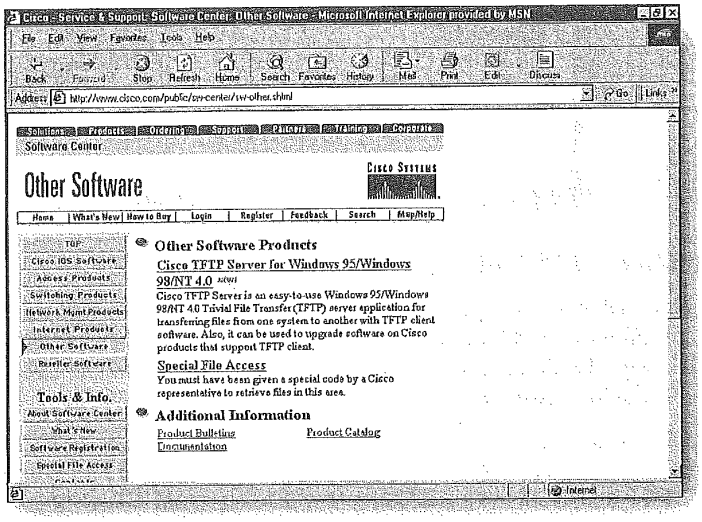


FIGURE 17.2
Cisco's TFTP server can be downloaded from the Cisco software center on the Web.

Installing the Cisco TFTP Server Software

You can install the Cisco TFTP server software on a Windows 95/98 workstation that is on the same network as the router (this means that the router is the default gateway for the TFTP server). For example if the router's Ethernet 0 port is configured with the IP number 10.16.0.1, this number should be entered as the workstation's default gateway. The IP address for the workstation also needs to be in the same subnet range as the Ethernet 0 port. Because I've divided a Class A network (you should be able to tell this by the first Octet of the default gateway IP address, if not, go back and take another look at Chapter 11) into 14 subnets, and used the first subnet on the Ethernet network connected to the router's E0 port, the range of IP addresses available would be 10.16.0.1 to 10.32.255.254. Because my workstation serves as the TFTP server, I made sure its IP address was in this range. I chose 10.16.0.4 in the TCP/IP Properties dialog box, as shown in Figure 17.3.

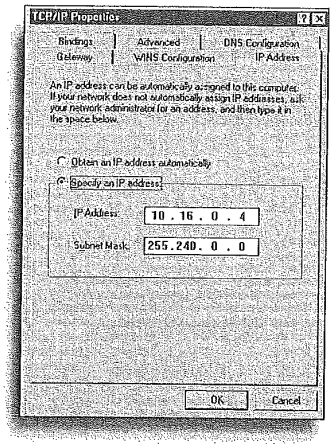


FIGURE 17.3
Make sure the workstation that will serve as the TFTP server is configured with an appropriate IP number.

After you've got the IP addressing squared away, you can set up the TFTP server software on the workstation. The installation process is very straightforward.

Setting up the Cisco TFTP server software

1. Use the Windows Explorer to locate the folder where you downloaded the Cisco TFTP server software.
2. Double-click the **Cisco TFTP** icon. The installation program for the software will load.
3. Click **Next** after reading the opening Installation. You will be asked to choose a location for the installation of the TFTP server software or allow it to be installed to a default folder.
4. Choose a different folder using the **Browse** button or go with the default. Click **Next** to continue.
5. A Default Icons folder will be created for the TFTP program. You can choose to have the icon placed in another folder by selecting the folder list provided on this screen. Click **Next** to continue.
6. The software will be installed. Click **Finish** to complete the process.

DHCP servers automatically assign IP addresses

If you use a DHCP server, such as an NT 4 server with DHCP enabled, IP addresses are automatically assigned to the workstations on the network. You might want to block out an address for the workstation that will serve as the TFTP server and manually assign the address in the TCP/IP properties box (see Figure 17.3).

Now that the software is installed on the workstation that will serve as the TFTP server, you are ready to copy files to and from the router. The next section discusses copying a configuration file to the TFTP server.

Copying to the TFTP Server

As you learned previously, you can copy startup configuration files from NVRAM or the running configuration file from RAM to the TFTP server. For example, let's say that you have a solid startup configuration saved in NVRAM and you want to save it to the TFTP server before you make any changes to it. This would enable you to restore the original startup configuration file to the router from the TFTP server, if your configuration changes turn out to affect network operations negatively.

Copying the startup configuration to the TFTP server

1. Start the TFTP server software on the workstation: select the **Start** menu, choose **Programs**, and then click **Cisco TFTP Server**. The TFTP Server window will open. The window is really just a gray, empty box that displays the IP address of the TFTP server (the computer you are running the software on) on the Title bar.
2. On your router console, enter the Privileged mode using the `enable` command and the enable password.
3. At the router prompt, type `copy startup-config tftp`, and then press **Enter**.
4. You are asked to provide the IP address of the remote host. Enter the IP address of the TFTP server (in this case my IP address was `10.16.0.4`). Then press the **Enter** key.
5. You will be asked to supply the name of the file you would like to write to the server. The default is the router's name followed by config (such as cisco2505-config). Press **Enter** to accept the default or enter the name of the configuration file you want to copy and then press **Enter**.
6. You will be asked to confirm the procedure (see Figure 17.4). Press **Enter** to confirm (if you don't want to confirm, type `n` for no and you will be returned to the Privileged prompt).

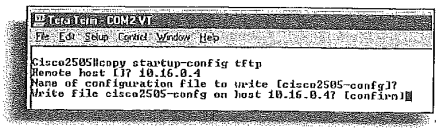


FIGURE 17.4
After you've specified the IP address of the TFTP server and the file to be copied, you are asked to confirm the process.

The file will be written to the TFTP server. A prompt reading `Writing router name-config. !! [OK]` means that the copy was a success. If you return to the TFTP Server workstation and look at the server window, you will find that a record of the copy job has been recorded, as shown in Figure 17.5. The TFTP server window also confirms that the copy job was a success.

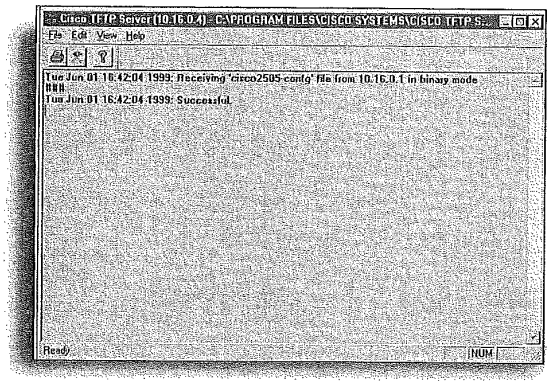


FIGURE 17.5
The TFTP server window provides an acknowledgement of the copy process that took place.

You can also copy the running-config from RAM using the procedure outlined. The only difference is that the command in step 3 would read `copy running-config tftp`.

Copying from the TFTP Server

The reverse operation—copying a file from the TFTP server to the router—is as straightforward as the process outlined in the previous section. You can copy a configuration file from the TFTP server into the router's NVRAM or you can copy the configuration from the server directly into RAM as a new running-configuration. If you copy the file into NVRAM it not only becomes the new running configuration for the router but it also will be the startup configuration when you reboot the router. Let's take a look at how to copy the

configuration file from the server into the NVRAM where it becomes the new startup configuration for the router.

Copying the startup configuration to router

1. Start the TFTP server software on the server workstation.
2. On your router console, enter the Privileged mode using the `enable` command and the enable password.
3. At the router prompt, type `copy tftp startup-config`, and then press **Enter**.
4. You are asked to provide the IP address of the remote host. Enter the IP address of the TFTP server (in this case my IP address was 10.16.0.4). Then press the **Enter** key.
5. You are asked to provide the name of the configuration file on the TFTP server you want to copy. Type the name at the prompt (if you use the default name when you copied the file to the server, you don't need to enter a new name). Press **Enter** to continue.
6. You will be asked to confirm the procedure (see Figure 17.6). Press **Enter** to confirm.

Viewing the copied file

You can take a look at the configuration file that was copied using the Window Explorer on the TFTP server workstation. Right-click the ***My Computer*** icon and choose ***Explore*** from the shortcut menu. The default location for the TFTP server folder is C:\Cisco Systems\Cisco TFTP Server. Check out this folder in Explorer and you should see the copy of the configuration file that was placed there during the copy process.

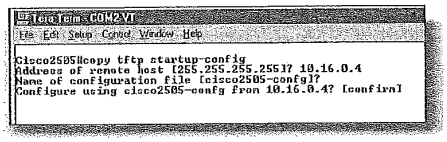


FIGURE 17.6
After you've entered the IP address for the server and the filename, press Enter to confirm the process.

The file will be loaded to the router and will become the active configuration (and will be saved in NVRAM). Again you will receive an `[OK]` message on the router that the procedure was a success. You can return to the TFTP server where the process will also be confirmed as a success.

Loading a New IOS from the TFTP Server

As you can see, copying to and from the TFTP server is a pretty easy process (when you compare it to creating IP subnets or doing some of the other configuration chores required by the router). You can also use the TFTP server to copy various versions of the IOS to the Flash RAM on the router. This makes it very easy to update the operating system on the router.

Cisco is constantly fine-tuning the IOS available for their routers. A number of different release versions are available. At the time this book was being written a new release, version 12, became available. Of course, as with any new operating system, bugs are found and fixes are programmed so a number of service releases are also made available for new IOS versions. In Cisco's case, upgrade versions of even what would be considered an older IOS such as 11 are still being fine-tuned, as well. You can view all the most recent IOS versions available on the Cisco Web site at `www.cisco.com`.

To download operating system images (files), you must have the appropriate service agreement with the Cisco reseller who sold you your router. A valid service contract number is required and you must register on the Cisco site to download IOS files. Figure 17.7 shows the Web page that provides the links to the various IOS images. This page also provides a convenient IOS planner that enables you to choose new IOS versions by your router (for example, I would click my Cisco 2505 router and only the IOS images appropriate for that model of router would appear on the Planner page.

To load a new IOS into a router's Flash RAM, download an appropriate IOS image from the Cisco Web site (if you purchased an IOS update from your Cisco reseller, you might also have the IOS files on a CD). Place the IOS file in the TFTP server's root folder. The default for this folder is C:\Cisco Systems\Cisco TFTP Server and you can use the Windows Explorer to copy or move the file to the appropriate folder.

Copy not working?

If the copy doesn't work, it typically means that the TFTP server cannot be found on the network. Make sure that the workstation is connected to the network and that the IP address for the workstation/TFTP server is in the same subnet range as the Ethernet port on the router that serves that particular subnet. If you think you have everything set up correctly, ping the TFTP server. At the router console prompt type `ping IP Address`, and then press ***Enter*** (where the IP address is that of the server/workstation). If you get a positive result, reinstall the TFTP software and try the process again.

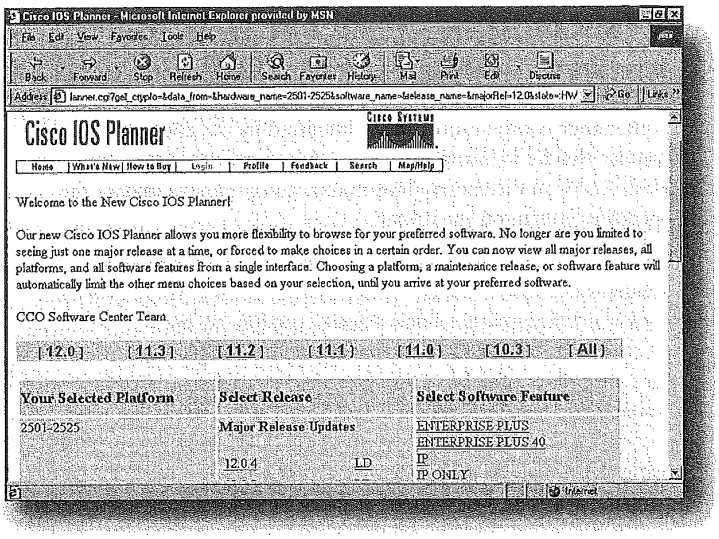


FIGURE 17.7
Cisco provides a convenient IOS Planner page on the Web that you can use to identify router IOS updates available for your router.

Now you are ready to copy the new IOS into the router's Flash. Be advised that this version of the IOS will replace the previous version. You can choose to not have the Flash RAM erased during the copy process, but that means you will have multiple copies of the IOS in Flash; in the case of the 2505 router with only 8MB of Flash, there is only enough room for one IOS image, anyhow.

After the IOS file is on the TFTP Server, you are ready to begin the process that will move the IOS file onto the router.

Copying a New IOS to the Router's Flash RAM

1. Start the TFTP server software on the server workstation.
2. On your router console, enter the Privileged mode using the `enable` command and the enable password.
3. At the router prompt, type `copy tftp flash`, and then press **Enter**.
4. You are notified that the router will proceed with the copy, but that router functions will be stopped while the IOS image is updated. To proceed, press **Enter**.

5. You are asked to provide the IP address of the remote host. Enter the IP address of the TFTP server (in this case my IP address was 10.16.0.4). Then press the **Enter** key.
6. You are asked to provide the name of the IOS file on the TFTP server you want to copy. Type the name at the prompt. Make sure the file is an IOS Image; in your example I used 80114109.bin, which is the image for IOS 11.2. Press **Enter** to continue.
7. You will then be asked for the destination filename. Go with the default name of the IOS (as entered in step 6). Press **Enter** to continue.
8. You will be asked to confirm that the flash RAM will be erased before the new IOS is written to it. Press **Enter** to confirm. Because Flash contains the current IOS, you will be asked to confirm a second time. Press **Enter** to confirm.
9. You will be asked whether you want to save the modified system configuration. Type `yes`, and then press **Enter**. Figure 17.8 shows my entries on the 2505 router for the upgrade of the IOS.
10. You will be asked for a final confirmation to proceed with the Flash erase. Type `yes` and press **Enter**.

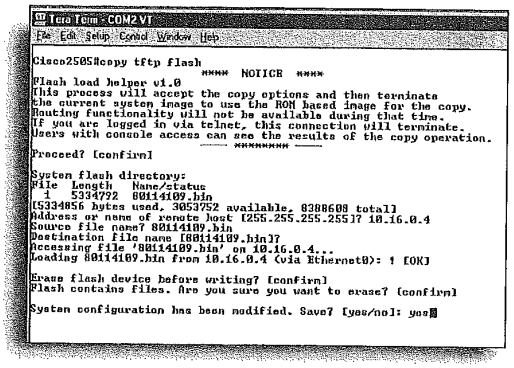


FIGURE 17.8
The writing of a new IOS to Flash RAM requires a number of confirmation steps.

The current IOS image will be erased and replaced by the new IOS image. A series of exclamation points appear on the router as the process takes place. This process may take a couple of minutes because the IOS images can be quite large (the 11.2 IOS is over 6MB). If you take a peek at the Cisco TFTP server window, a series of number symbols (#) repeat across the screen as the process takes place.

The router will reboot after the new IOS file is copied. You can now press **Enter** and enter the console password (if required) to place yourself at the user prompt. To check your new IOS image, type `show flash` at the prompt, and then press **Enter**. The new IOS image (the filename you entered in step 6) should now reside in the router's Flash.

You can also copy the current IOS image to a TFTP server if you want. This gives you a backup if the Flash RAM on the router goes bad or you just like having a copy of the IOS safely filed away in a secondary location. The command at the Privileged prompt would be `copy flash tftp`. You then provide the IP address of the server and other information as requested in the steps already discussed.

TFTP servers make an excellent repository for alternative configuration files and IOS updates. They supply you with the backup storage space that the router itself doesn't have.

chapter

18

Basic Router Troubleshooting

Troubleshooting Hardware Problems

Troubleshooting LAN Interfaces

Troubleshooting WAN Interfaces

Troubleshooting TCP/IP

Troubleshooting IPX

Troubleshooting AppleTalk

A Final Word on Troubleshooting

Troubleshooting Hardware Problems

Although the subject of troubleshooting your router connections and configurations would certainly fill an entire book (or books), it probably makes sense to finish up a primer book on internetworking and Cisco routers with a basic overview of troubleshooting techniques. Hardware problems that you could face can include a failed router interface controller, making an interface or interfaces inoperable, or a router that has just rolled over and died completely.

Other problems on your internetwork will most likely boil down to two categories such as physical connection problems and router configuration problems. Some physical connection problems you have control over such as a bad router serial cable or a hardware problem with a hub or a stretch of network cabling. Other events such as an out-of-control Jeep Cherokee crashing into the phone company's switching equipment is just a little beyond your control. Some hardware problems you can fix; others you just have to sit and wait (which is difficult when your users can't access the resources that they need to do their jobs).

As far as configuration problems go, some adjustments to a configuration might be necessary if there are radical changes to the network topology (such as a downed connection). In other cases, your original configuration might not be up snuff and you need to edit it to resolve issues that are affecting the internetwork negatively. You will look at configuration issues and the troubleshooting of specific protocols later in this chapter.

Router Problems

Router hardware problems can revolve around interface controllers, RAM modules, the router's processor, and even the router's fan. And although it might sound silly, the first thing you should check on a router that is down is whether the router has been turned off or the power cord has been kicked out of the wall socket.

You learned the basics of router interfaces in Chapter 6, "Understanding Router Interfaces." The various network and WAN interfaces on the router are each connected to a controller. The interface controller is either hardwired to the router's motherboard

(as is the case with the 2500 series) or contained on the interface card that you placed in one of the slots available on the router (as is the case with Cisco's higher end routers like the 4500 series).

One way to check a particular interface on the router is using the `show interfaces` command. If the interface is up and the line protocol is up (as shown in Figure 18.1), you don't have a problem with that interface. If the interface controller no longer functions, the interface won't register as an available interface when you use the `show interfaces` command. If the interface is up and the line protocol is down, your problem is a configuration issue, not a hardware problem.

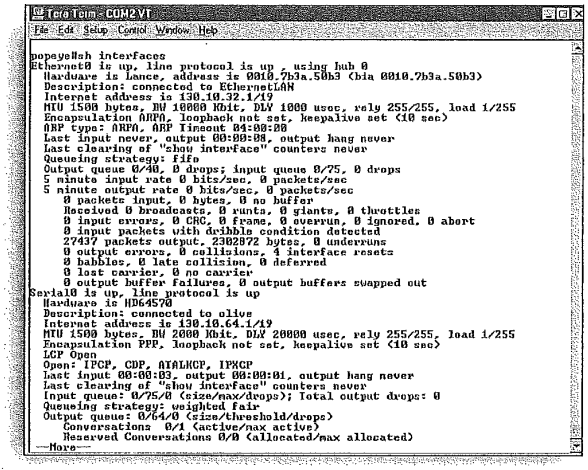


FIGURE 18.1
The `show interfaces` command can be used to quickly check the interface status on a router.

You can also check the controllers on your router. The `show controllers` command provides statistics for interface controller cards. Figure 18.2 shows the results of the `show controller ethernet` command.

Another component on the router that is of vital importance is the router's fan (it's one of the cheapest parts but also one of the most important). If the fan doesn't work, the router will overheat (just like a PC with a broken fan). It will reboot. So, if you have a router that seems to reboot after only being on for a short period of time, power up the router and listen carefully to see if the fan is working.

Check LAN and WAN connections

If a particular interface is down, such as a serial interface, the V.35 cable might have become disconnected. Always check the various LAN and WAN connections to the router. Loose cables can make it appear as if there is a hardware problem with the router itself.

(Some of the high-end Cisco routers actually have complex cooling systems and also enable you to monitor the temperature of the device.)

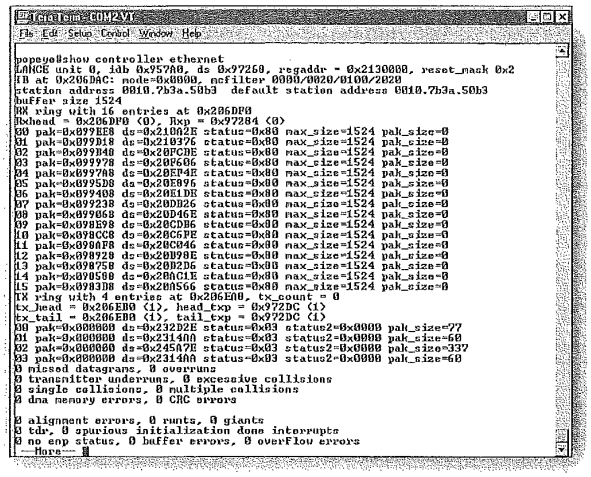


FIGURE 18.2
The `show controller` command can be used to view statistics related to the controllers installed on the router.

In cases where the router crashes, it can be tough to determine if the problem was hardware- or software-related. You can use the `show stacks` command to retrieve error messages that were saved by the ROM monitor at the time of the crash. (Cisco technical support representatives can use the `show stacks` information to pinpoint the software or hardware problem that caused the crash).

Besides the physical failure of router components, you might also run into situations where the router doesn't have enough RAM (or processor speed) to really handle all the traffic that you have flowing through it. You might need to add additional routers to the internetwork to lighten the load or upgrade existing router hardware components (such as RAM). In some cases you might want to upgrade from the existing router to a higher-end router.

One way that network administrators identify bottlenecks on their networks (a *bottleneck* is a device that is slowing network traffic) is to use some type of network management software package that allows the monitoring of devices, protocols, and other aspects of the network and enables you to view the current health of your internetwork. CiscoWorks is an example of a network management software

package that provides a number of tools for monitoring and troubleshooting internetworks. On large internetworks some sort of network management software is vital for keeping tabs on the network and its various devices.

Other Hardware Problems

Other hardware problems that will affect the job that your router is doing relate to devices that are directly connected to the router.

On Ethernet networks, hubs are typically attached to an Ethernet port on the router. If the hub goes down, the LAN's connection to the router also goes down, making node addresses on the LAN unavailable to other nodes on the internetwork.

Hubs typically have a power on LED somewhere on the unit that makes it easy for you to determine whether the hub is on or off. If the hub is plugged in and turned on and still provides no indication that the unit has powered up, replace the hub.

If you are having trouble with individual nodes on a LAN, hubs typically have an LED that lights when a particular port on the hub is connected to a node via a twisted-pair cable. If the display light isn't on, you either have a bad cable (see the next section concerning cabling and LAN connections) or the port on the hub is bad.

The same types of problems can be associated with router connections to Token Ring networks. A Token Ring Multi-Station Access Unit will be attached to the router providing the connection between the nodes on the LAN and the router. If the Access Unit goes down, the LAN's connection to the router will be disrupted.

WAN connectivity devices can also pose potential problems to the internetwork. Routers are often connected to CSU/DSUs that provide connectivity to certain WAN technologies such as leased lines and packet-switching network. If the CSU/DSU goes down, the WAN connection between the router and the rest of the internetwork also goes down.

If the hardware problem is related to your service provider's switching equipment there is little that you can do to fix the problem yourself. You have to sit and wait for the connection to come back up. In many cases, network administrators will build fault tolerance into an

Approach your troubleshooting systematically

Whether you are troubleshooting hardware or software problems, approach the problem systematically. First identify the problem, and then gather facts related to the problem. You can use various router commands to help you gather facts. After you have some information to work with, take each parameter that might be the cause of the problem and test it individually until you find the cause of the problem. Changing a lot of different parameters all at once isn't going to let you identify the root cause of a particular problem.

internetwork by providing redundant connections (backup connections) between certain routers. For example, you might have a Frame Relay connection between two routers. As a backup, you configure the router so that it can also connect to the remote router using a dial-up connection over a modem if necessary. The modem line won't give you the speed that the Frame-Relay connection will, but if you have to move time-sensitive data, you at least have a backup route for the packets.

Cabling Problems

Connectivity problems on a LAN related to physical cabling on the LAN can be due to shorts, breaks, and other problems. In cases where physical connections (that you have control over) are suspect, a variety of tools are available for checking cabling ranging from voltmeters to time domain reflectometers (TDR).

A digital *voltmeter* is a simple device that can be connected to a cable and test the cable for a break or a short. Basically, the voltmeter can tell you if the cable is bad or not and whether you are looking at a short or break. If the cable has a short, replace it. If there is a break, you must trace the cable (have fun standing on a ladder with your head stuck up in the drop-ceiling) to find where the break has occurred.

A *TDR* is a more sophisticated device that can diagnose shorts and breaks in a cable but it can also provide you with information on where the short or break exists on the cable. The TDR actually emits short pulses down the cable and is able to use a timing mechanism that estimates the distance that the pulse has traveled.

Network cabling is always suspect. People move furniture and disrupt cable connections, a leaky roof allows cabling in the ceiling to become soaked with water (sometimes leading to shorts)—all sorts of weird things can happen to cables that sever the connection that they were providing. Always check cables first. Then move on to some of the other devices you've discussed.

SEE ALSO

For a review of network cabling, see page 17.

A Final Word on Hardware

When troubleshooting hardware problems, don't immediately assume that the connection problem lies with the router's hardware. Make sure that you systematically check the other devices discussed in this section and their connective media to the router. Because routers usually live out their lives powered on (you aren't constantly turning them on and off), the hardware does seem to last forever (as long at the fan doesn't go down or you place it in a closed closet where the temperature is about 100 degrees).

You can protect the router itself against power problems using a couple of different devices. Uninterruptible Power Supplies (*UPS*) will supply power to the router using a battery if the electricity is cut. You can protect the router against power surges using some sort of surge suppressor. The router isn't unlike a computer, so place it in an environment that is favorable to a valuable electronic device.

Troubleshooting LAN Interfaces

Another aspect of troubleshooting the router's connection to LANs is becoming familiar with the output that appears on the router console when you use certain IOS commands to diagnose problems. One of the most powerful diagnostic tools on the router is the `show` command. You will take a look at the `show` command and how the information that it provides is related to two popular LAN types: Ethernet and Token Ring.

SEE ALSO

➢ *For a review of Ethernet and Token Ring, see page 25.*

Troubleshooting Ethernet with Show

Ethernet is a passive network architecture that uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as its strategy for network access. Problems related to Ethernet can revolve around excess collisions on the network due to cable breaks, cable runs that exceed the maximum length allowed, and malfunctioning network cards that can cause excessive broadcast traffic.

The `show interfaces ethernet [interface number]` command enables you to view statistics related to a particular Ethernet interface. Figure 18.3 shows the results of this command on an Ethernet 0 interface on a Cisco 2505 router.

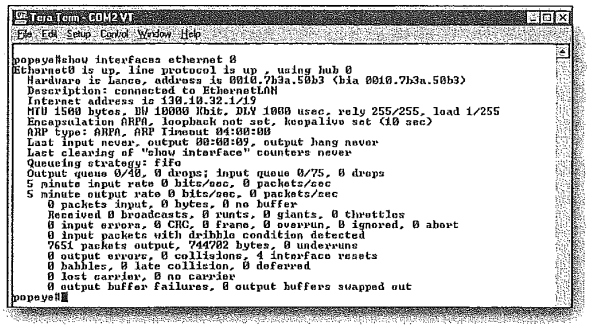


FIGURE 18.3
The `show interfaces ethernet` command can be used to view statistics related to the Ethernet interfaces installed on the router.

Although the statistics provided might seem rather cryptic at first examination, they actually provide a great deal of information that can help you troubleshoot problems related to an Ethernet interface. Some of these statistics also provide insight into the use of other hardware resources on the router such as RAM. The list that follows highlights some of the statistics found in response to the `show interfaces ethernet [interface number]` command.

- Ethernet 0 is Up, Line Protocol is Up—This lets you know that the interface is active and that the Ethernet protocols believe that the line is usable. If the interface is down, check the LAN connection to the interface. You can also try to bring up the interface in the Configuration mode (if the LAN connection is okay). Enter the configuration-if mode for the interface and "bounce" the interface. Use the `shut` command (to down the interface), and then use the `no shut` command to up the interface. This might bring the interface back up.
- Hardware Address—This is the hexadecimal MAC address for the interface.
- Internet Address—This is the IP address and subnet mask assigned to the interface (you will learn IP addressing in the "Troubleshooting TCP/IP" section).

- MTU—This is the maximum transmission unit for the interface in bytes.
- BW—This is the bandwidth for the interface in kilobits/second.
- Rely—This is a measurement of the reliability of the line with 255/255 being 100 percent reliable. The lower the first number in the reliability measurement, the less reliable the interface connection (due to downed lines or other problems).
- Load—This measures the current load on the interface. The measurement 255/255 would be a totally saturated interface (meaning too much traffic, you might need to add another interface or router to service the network).
- Encapsulation—This is the Ethernet frame type assigned to the interface. ARPA is the default and is the 802.2 Ethernet frame type. If the frame type doesn't match the frame type used on your network (such as an older NetWare network using 802.3 raw frames, you must reset the frame type. Use the `arp` command at the config-if prompt for the interface and assign the correct Ethernet encapsulation type (such as arpa, or snap).
- Collisions—This shows the number of collisions monitored by the interface. A large number of collisions means that there might be some physical problem on the network such as a break in a cable or a malfunctioning network interface card that is generating a large amount of broadcast traffic. This could also mean that cables are too long on the LAN.

As you can see, this one IOS command provides a lot of information related to the health of a particular interface and the traffic that it is experiencing. And as you also can see, problems with an Ethernet interface might be core problems with the LAN that it is servicing (such as excessive collisions).

Troubleshooting Token Ring with Show

Token Ring uses token passing as its method of access to the LAN. The device with the token can transmit. Other devices must wait until they take possession of the token so that they can transmit. So problems with Token Ring networks don't revolve around packet collision issues as Ethernet does.

The command to view the statistics related to a Token Ring interface is `show interfaces tokenring [interface number]`. And as with the `show interfaces` command on Ethernet interfaces, this command shows the status of the interface and information on the hardware and protocol addresses of the interface as well as information on the interface's reliability. A number of the parameters shown in the statistics are the same as those shown for an Ethernet port (such as Hardware Address, Internet Address, MTU, BW, and Rely). Other settings have to do with Token Ring LAN functionality such as ring speed.

- Token Ring is Up—This lets you know that the interface is currently active. If the interface is down, you can try to bounce the interface in the configuration-if mode to get it back online.
- Hardware Address—This is the hexadecimal MAC address for the interface.
- Internet Address—This is the IP address and subnet mask assigned to the interface (you will learn IP addressing in the "Troubleshooting TCP/IP" section).
- MTU—This is the maximum transmission unit for the interface in bytes.
- BW—This is the bandwidth for the interface in kilobits/second.
- Rely—This is a measurement of the reliability of the line with 255/255 being 100 percent reliable. This measurement is averaged for the interface over a period of five minutes.
- Load—This measures the current load on the interface. The measurement 255/255 would be a totally saturated interface and again means that you might have too large of a Token Ring LAN being serviced by the one interface on the router.
- Ring Speed—This is setting for the speed of the Token Ring LAN that the router is connected to. All devices on the Token Ring network, including the router, must be using the same ring speed (either 4Mbps or 16Mbps). Any mismatches will result in an interruption in the flow of data. To check the ring speed set on the router use the `show running-config` command. If you need to reset the ring speed enter the config-if mode on the router console for the interface. Then use the `ring-speed` command to reset the ring speed.

- Restarts—On Token Ring Interfaces this value should always be 0. If it is other than 0, the interface has been restarted because of some problem on the Token Ring LAN.

Troubleshooting Token Ring interfaces on routers requires a very good understanding of how Token Ring LANs operate. Problems such as congested rings, for example, require that you further segment the Token Ring LAN. And although this section provides some primer information on Token Ring interface settings, you should learn a lot more about Token Ring itself than can be provided in this book. A very good source for Token Ring related information is `www.ibm.com`. They are the architects of Token Ring and provide a number of white papers and other resources related to Token Ring LANs.

Troubleshooting WAN Interfaces

Basic troubleshooting of WAN interfaces is very similar to troubleshooting LAN interfaces. You can use the `show interface serial [interface number]` to view the statistics related to a particular interface. However, more precise troubleshooting of WAN interfaces is much more complex than LAN interfaces because of the different WAN protocols (such as PPP or Frame Relay) that you might be using on your serial connection between routers. Also thrown into this mix is the state of your service provider's leased lines or packet switched network connections.

Let's take a look at the show interface serial command and how some of the statistics related to a serial interface can provide insight into potential problems. Figure 18.4 shows the results of the `show interface serial 0` command on a 2505 router.

- Serial 0 is Up—This lets you know that the interface is active. If the interface is down, there might be a problem with the connection from the router to the CSU/DSU. Check the cable. Or there might be a problem with the telephone company line that you are connected to (if the CSU/DSU is okay, call your service provider to see if the line is down—first check the status of the

router on the other end of the connection). You can also try to bounce the interface to bring it back up (as discussed in the Ethernet section).

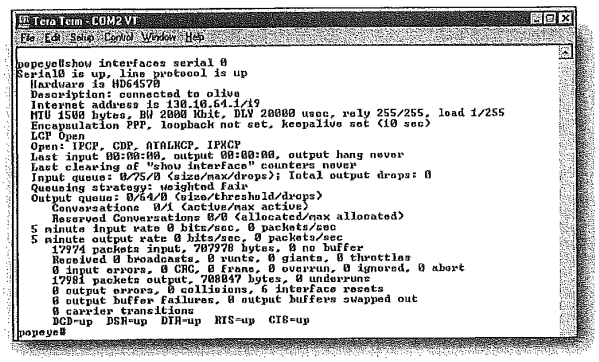


FIGURE 18.4
The `show interfaces serial` command can be used to view statistics for a serial interface on a router.

Check the CSU/DSU signal

You can use a monitoring device called a *breakout box* to determine whether you are getting a signal from the CSU/DSU. Disconnect the CSU/DSU from the router and connect it to the breakout box. If you don't get a signal, the leased line might not be connected to the CSU/DSU or the line is down.

- Line Protocol is Up—This lets you know that the WAN protocols in use believe that the line is usable. If the line protocol is down, your router might not be configured correctly (use the `show running-config` command to check this). Or the router that you are attempting to connect to isn't configured with the appropriate protocol (check it too). You might also be experiencing a problem due to the service provider's line or switching equipment.
- Internet Address—This is the IP address and subnet mask assigned to the interface (you will learn IP addressing in the "Troubleshooting TCP/IP" section).
- MTU—This is the maximum transmission unit for the interface in bytes.
- BW—This is the bandwidth for the interface in kilobits/second. This is set for the interface at the config-if prompt using the `bandwidth` command. The bandwidth must be set to a value that coincides with the speed of the line that the router's serial interface is connected to.

- Rely—This is a measurement of the reliability of the line with 255/255 being 100 percent reliable. The lower the first number in the reliability measurement the less reliable the interface connection (due to downed lines or other problems).
- Load—This measures the current load on the interface. The measurement 255/255 would be a totally saturated interface (meaning too much traffic, you might need to add another interface or router to service the LAN).
- Encapsulation—This is the WAN protocol assigned to the interface. It must match the WAN protocol on the router that is at the other end of the connection. The WAN protocol must also be set for the type of service you are being provided from your service provider (don't set it for PPP if you are connecting to a Frame-Relay switch).
- CRC—This shows the number of cyclical redundancy checks that have failed on incoming packets. This is usually an indication that the line provided by the phone company is experiencing a great deal of noise or that your serial cable from the router to the CSU/DSU is too long.

Again, this is only an overview of the information provided by the `show` command for a serial interface on a router and how it relates to potential problems. Troubleshooting WAN connection demands that you have a great deal of experience configuring and working with WAN connections on an internetwork. For example, troubleshooting dial-up connections and ISDN connections are really a science unto themselves. As with any discipline, the more time you spend working with WAN issues on internetworks the better you become at diagnosing problems relating to them.

Routers configured as a DCE must provide a clock rate

If you have configured your router as a DCE, the router must provide a clock rate for the serial connection. At the config-if prompt for the interface, use the `clock rate` command to set the appropriate clock rate. Legal clock rates range from 1200 to 800,000,000 bits per second. To see if an interface has been configured as a DCE, run the `show controllers serial [interface number]` command. This will show you the clock rate set for the line and the type of cable connected to the interface (DCE or DTE).

Troubleshooting TCP/IP

TCP/IP is a large routable protocol stack that can present a number of interesting problems to router administrators. You've already seen in Chapter 10 that subnetting IP networks can be a mathematical nightmare in and of itself. And you will find that when you work with IP networks, a number of the problems that you face have to do with improper configurations on a router or node on the network.

A duplicated IP address on a workstation will take that workstation offline and the workstation that also has been configured with the duplicate IP address.

Let's take a look at some of the common IP network–related problems first. Then you will look at the `ping` and `trace` commands and how you can use them to help troubleshoot IP–related problems. The list that follows provides some basic IP related problems and how you would fix them:

- Default Gateway Improperly Configured—When you set up the workstations and servers on a LAN that connects to a router, the default gateway for the LAN (and all the computers on it) is the IP address of the router interface directly connected to the LAN. If a workstation cannot communicate with the network, check the default gateway (or even more basic—check the IP address).
- Routing Not Enabled On One of the Routers—Use the `show ip route` command to see whether the router has been enabled for routing. If the routing table doesn't have any learned entries in it, the router has not been enabled for routing.
- Routing Protocol Has Not Been Enabled—You must enable a routing protocol, if you want the router to build a routing table. Use the `show running-config` command to see whether a routing protocol has been enabled (which should match the routing protocol you are using on the other routers on your network).
- No IP Address Configured on an Interface—You will have problems if the router interface has not been configured with an IP address. Use `the show ip interfaces` command to make sure your interfaces have been configured with an IP address (except in the cases of serial connections which can be configured IP unnumbered).

Watch those Access lists

I discussed standard IP Access lists in Chapter 14, "Routing AppleTalk." Grouping Access lists to router interfaces without a good understanding on how those lists will affect network traffic is a big mistake. Don't use Access Control lists unless you are sure that it will filter traffic that you don't want, not traffic that you require to be passed through the router interface.

Using *ping*

A great tool for checking the physical network connection between two routers on the internetwork (or any two nodes) is the `ping` command. `ping` sends an ICMP echo packet to the noted IP address and if the address received the packet it echoes the packet back to the

source. The time that the echo packet takes to go the roundtrip is measured in milliseconds.

To use the `ping` command, type `ping [ip address]`, where you supply the IP address of the destination router interface or node on the network. Figure 18.5 shows the results of a `ping` command between two routers.

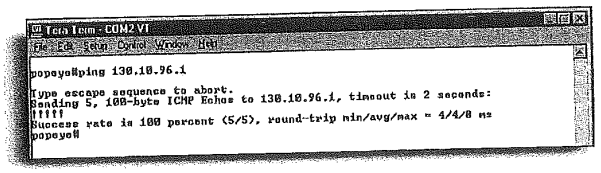


FIGURE 18.5
The show `ping` command can be used to check the connection between a router and other nodes on the internetwork.

An extended `ping` command also exists that enables you to set the protocol type for the echo packet (`ping` can be used with IPX and AppleTalk), the size of the packet, and the timeout for the response. Type `ping` and then press **Enter**. Supply the information requested by each step in the extended `ping` command, followed by **Enter**, (just press **Enter** to accept the defaults). Figure 18.6 shows the results of an extended `ping` command.

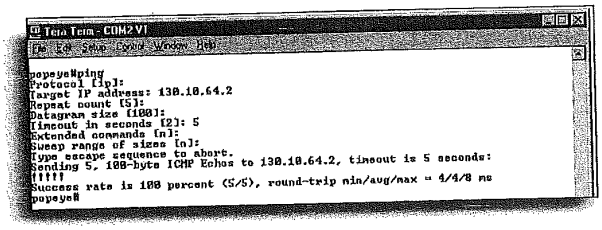


FIGURE 18.6
The extended `ping` command enables you to set parameters such as protocol type and timeout for the ping packet.

Using *trace*

Another command that you can use to troubleshoot connectivity problems is the `trace` command. It enables you to see the route that the packets take from source to destination. This enables you to determine if routers that would normally participate in the path between a particular router and node or router and router is currently down. To use the trace command, type `trace [ip address]`.

Using `ping` and `trace`
`ping` and `trace` can both be used at the user prompt or the privileged prompt.

The results of the `trace` command shown in Figure 18.7 show that the route determined by trace consisted of one directly connected router with the IP address of 130.10.64.2. The trace took four milliseconds.

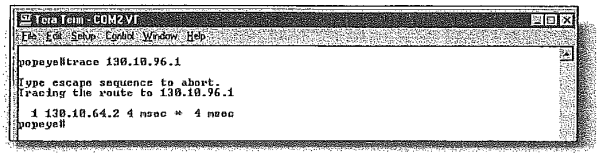


FIGURE 18.7
The `trace` command can show the route between two routers on the internetwork.

Troubleshooting IPX

Networking with IPX poses some of the same problems that you face when working with IP. Incorrectly entered IPX network numbers on router interfaces can cause problems just as incorrectly configured IP addresses on interfaces do. Let's take a look at some of the basic troubleshooting issues you might face when working with IPX networks:

- Incorrectly Configured Clients—Novell Networks are very server-centric and so the hosts on the network must have their client software configured to correctly communicate with the NetWare server. It is the server that verifies the user to the network, so make sure that you are using the appropriate version of the client software for the version of server software that you are using.
- Too Many Clients—When you install a NetWare server you must provide a disk that shows the server how many licenses you have purchased for client machines. If you try to add more clients than you have licenses for, the server will not let the user on the network. Use the `Load Monitor` command on the NetWare server to check the number of client spots available on the server.
- Problems with Ethernet Encapsulation—NetWare supports several different Ethernet frame types—such as Ethernet 802.2 and Ethernet 802.3 (raw Ethernet) If you inadvertently mismatch the frame type on a router LAN interface with the frame type used

by NetWare hosts and servers, the router is going to have problems routing packets. Check the frame type (encapsulation) of all your router interfaces using the `show ipx interface brief` command (the results of this command on a 2505 router appear in Figure 18.8).

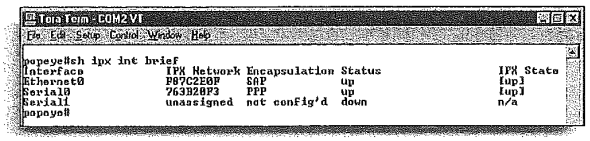


FIGURE 18.8
Quickly check the Encapsulation type of IPX-enabled interfaces on the router.

Obviously, one of the first things that you should do when you experience problems on a router is check your configuration and the settings on the interfaces. Other troubleshooting issues revolve around hardware and cabling issues. Because IPX is typically found on LANs, make sure that the LAN is working correctly before connecting to the router. Then if you have problems you know that they are on the router not the network.

Using extended `ping`
You can use extended `ping` to check nodes on the network (or router interfaces) using their IPX address in the form network number.node number.

SEE ALSO

➢ *For a review of IPX addressing, see page 214.*

Troubleshooting AppleTalk

AppleTalk LANs are typically small (when compared to corporate IP or IPX networks); it is somewhat simpler to deal with physical cabling problems and hardware problems (because you are typically dealing with fewer computers). Dealing with configuration and software problems is another issue.

When Apple Macintosh users looks for a particular service on the AppleTalk network, they employ the Chooser on the Macintosh. If the user can't find a particular service or zone, you've got a problem. And you will find that most of the problems with AppleTalk networks typically revolve around cable ranges and zone names. If a router's configuration doesn't agree with the cable ranges and zone names used on the AppleTalk internetwork that it is connected to, routing problems will occur and Mac clients won't find what they're looking for in the computer's Chooser.

AppleTalk phases

AppleTalk actually exists in two different phases: 1 and 2. Phase 1 didn't allow cable ranges but required a single network address for a network segment. If you are trying to route traffic through an AppleTalk internetwork where both AppleTalk Phase 1 and Phase 2 are in use, you might experience routing problems. It is a good idea to upgrade routers and other devices to support AppleTalk Phase 2.

Another thing to keep in mind, because the administrator assigns cable ranges, is that you don't want to inadvertently configure two LAN segments with the same network number or cable range. This will obviously cause routing problems.

Two router commands that are useful for troubleshooting in AppleTalk environments are `ping` and the `debug appletalk routing` command. `ping`, as you know, enables you to check the connection to a particular node on the network or check whether or not a router interface is up. The `debug` command enables you to view advertisements of routes on the AppleTalk internetwork and reports of conflicting network numbers on the network.

To use the `ping` command for AppleTalk addresses, type `ping appletalk [network number.node address]`. For example, on my router I want to ping the Ethernet 0 port on another router that has been configured for AppleTalk. The command is `ping appletalk 12.176` (you can also use the extended `ping` command for AppleTalk). Figure 18.9 shows the result of this command.

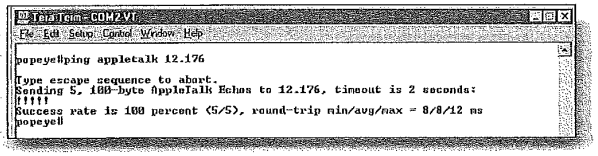


FIGURE 18.9
Check the status of a node on the AppleTalk network using the `ping` command.

The `debug` command (a Privileged command) is simple to use, but it requires a lot of the router's resources, such as memory, so you don't want to leave it on forever (use `no debug all`, to quickly turn it off). The command is entered as `debug apple routing`. Figure 18.10 shows some of the information that the command provides.

A Final Word on Troubleshooting

In this chapter you have taken a look at some of the basic troubleshooting techniques for hardware, network architectures (such as Ethernet), and network protocols (such as IP). One thing that I haven't talked about is a network map. Any network administrator worth his salt will be sure to have an up-to-date map of the entire network including the addressing scheme and the location of devices such as routers, bridges, and servers.

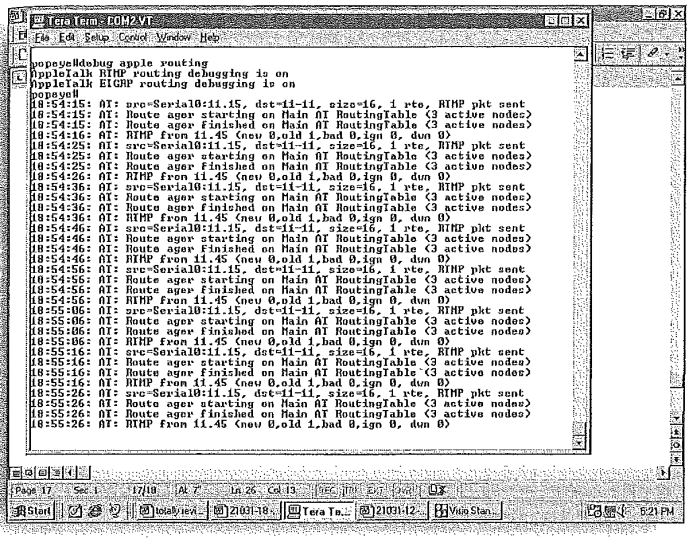


FIGURE 18.10
Use debug to monitor AppleTalk routing updates.

A map (or diagram if you want) of your internetwork can be used to find node addresses when you need them for commands like Ping or Telnet. The map also provides you with a complete overview of the topology of the network. You really can't run the network efficiently without a map.

And creating a network map is easy. Network diagramming tools such as Visio Standard (from Visio Corporation) make it easy to build simple and complex network diagrams. Other versions of Visio such as the Enterprise version supply all the icons that you need for just about every networking device manufactured, enabling you to create diagrams that can be understood by any network administrator.

Even if you don't use a network-diagramming tool, use some sort of graphics package and get a network map on to your computer, so that you can upgrade it as the network topology changes or grows. You won't be sorry that you have it when trouble rears its ugly head. Good luck!

part V

APPENDIXES

Basic Command Summary 323 A

Selected Cisco Router Specifications 337 B

Glossary 343

Appendix

A

Basic Router Command Summary

Router Examination Commands

Router Memory Commands

Password and Router Name Configuration Commands

Interface Configuration Commands

IP-Related Commands

IPX-Related Commands

AppleTalk-Related Commands

WAN-Related Commands

Troubleshooting Commands

Miscellaneous Commands

Cisco IOS Command Summary

This appendix provides a summary of the Cisco IOS commands covered in this book. The commands are broken down into tables; each table contains a list of associated commands. Commands in each table are listed alphabetically. For example, router examination commands are contained in Table A.1. This resource is best used after you have completed reading the entire book. You will then understand the context of each command and its use.

Because some root commands overlap—for example, show is used as a general examination command and as a troubleshooting command—you might find variations of the same command in more than one table. The fact that commands are grouped by their typical usage, however, should make the tables an easy way to reference a particular group of related commands.

For example, you can go to a particular table category, such as IP-related commands or AppleTalk-related commands, and find the specific IP or AppleTalk IOS command you are looking for. It is understood that each command is executed by typing the command at the appropriate prompt (noted in the results of the command) and then pressing **Enter**.

Router Examination Commands

Router examination commands enable you to quickly check the status of the router's interfaces and other parameters. Table A.1 summarizes these commands. These commands can be used at both the user and privileged prompts unless otherwise noted.

Table A.1 Router Examination Commands

Command	Results
`show CDP Neighbor`	Shows the routers that are directly connected to your router by LAN or serial connections.
`show clock`	Shows the time and date settings for the router.
`show flash`	Shows the IOS file or files contained in the router's Flash RAM and the amount of total Flash RAM and used Flash RAM.

Command	Results
`show history`	Shows a list of your last 10 commands.
`show hub`	Shows information on the status of the hub ports of a 2505 router.
`show interface ethernet [interface number]`	Shows the current configuration of a specified Ethernet interface.
`show interface serial [interface number]`	Shows the current configuration of a specified serial interface.
`show interfaces`	Lists all the interfaces on the router and statistics related to the interface such as their current configuration and encapsulation. Also tells you if the interface is active.
`show processes`	Shows CPU utilization information.
`show protocol`	Lists the routing protocols configured on the router.
`show version`	Shows the version of the IOS currently running on the router.

Router Memory Commands

Router memory commands enable you to check information such as the current running configuration or the startup-configuration stored in NVRAM. These commands also enable you to copy or erase configuration files from the router's memory. Commands for saving and retrieving router configurations or IOS files to and from an FTP server are also included in this list. These commands can be used at the user and privileged prompt unless otherwise noted (see Table A.2).

Table A.2 Router Memory–Related Commands

Command	Results
`copy flash tftp`	Privileged command to copy an IOS file from Flash to the TFTP server
`copy running-config startup-config`	Copies the currently running configuration to the router's NVRAM.

continues...

Table A.2 Continued

Command	Results
`copy startup-config tftp`	Privileged command to copy the startup configuration from NVRAM to a TFTP server.
`copy tftp flash`	Privileged command to copy an IOS file from a TFTP server to the router's Flash RAM.
`copy tftp startup-config`	Privileged command to copy a startup configuration file from a TFTP server to the router's NVRAM.
`erase startup-config`	Erases the startup-configuration from the router's NVRAM.
`show running-config`	Privileged command that shows the router configuration currently running in RAM.
`show startup-config`	Privileged command that shows the router configuration stored in the router's NVRAM. Loaded by the router when the router is rebooted.

Password and Router Name Configuration Commands

Password and router name commands enable you to change the various passwords on the router including the router login password and the secret enable password for the Privileged mode (see Table A.3). This list also contains the command for changing the router's name. Each of these commands is used in the Configuration mode.

Table A.3 Password and Router Name Commands

Command	Results
`enable secret password [password]`	Global configuration command that enables you to change the secret Privileged mode password on the router.
`hostname [name]`	Global configuration command that changes the name of the router.

Command	Results
`line console 0`	Enables you to enter the Line Configuration mode to set the login password for the router.
`line vty 0 4`	Enables you to enter the virtual terminal Configuration mode to set the virtual terminal password for the router.
`password [password]`	Used in the line console 0 Configuration mode to set the login password for the router; also used in the line vty 0 4 Configuration mode to set the virtual terminal password for the router.

SEE ALSO

➤ *For help recovering forgotten passwords, see page 137.*

Interface Configuration Commands

Interface configuration commands relate to configuring interfaces on the router (see Table A.4). The general configuration command, `config` (the Privileged command to enter the configuration mode), is included among the commands. For interface configuration related to a specific network or WAN protocol, see the appropriate table (such as WAN-Related Commands).

Table A.4 Interface Configuration Commands

Command	Results
`config`	Privileged command that enables you to enter the Global Configuration mode.
Ctrl+Z	While not an actual interface configuration command, it is the command used to end a router configuration session.
`enable cdp`	Enables a particular interface (you must be in the config-if Configuration mode) to show connected neighbor routers (you can then use the show cdp neighbor command on the router).

continues...

Table A.4 Continued

Command	Results
`encapsulation [encapsulation type]`	Interface-specific configuration command that enables you to set the encapsulation type for a LAN or serial interface on the router.
`interface ethernet [interface number]`	Global Configuration command that enables you to configure parameters related to a particular Ethernet interface.
`interface serial [interface number]`	Global configuration command that enables you to configure parameters related to a particular serial interface.

IP-Related Commands

IP commands are related to configuring IP addressing on interfaces and enabling IP routing on the router (see Table A.5). Commands related to RIP and IGRP are also included.

Table A.5 IP-Related Commands

Command	Results
`access-list [list #] permit or deny [ip address] [wildcard mask]`	Global configuration command for creating an IP Access list. The network or node address that will be permitted or denied must be included and the wildcard mask must be provided. Repeat this command for each line that will appear in the Access list. The `list #` range for IP lists is 1–99.
`debug ip igrp transaction`	Privileged command that enables you to view statistics related to IGRP update messages on the router.
`debug ip rip`	Privileged command that enables you to view the RIP update messages sent and received by the router.

Command	Results
`ip access-group [list number] out or in`	Interface configuration command where you group a particular IP Access list to an interface. The `out` or `in` parameter is used to filter traffic going either out or in the specified interface.
`ip address [ip address] [subnet mask]`	Used in the config-if mode to assign an IP address to a router interface. The *`ip address`* command is followed by the *`ip address`* and *`subnet`* you are assigning to the interface.
`ip routing`	Global configuration command that enables IP routing on the router.
`ip unnumbered [interface or logical interface]`	Config-if prompt command enables you to designate a serial interface as not having its own IP address. The interface or logical interface parameter must designate a router interface (such as an Ethernet port) on the router that does have an IP address.
`network [major network number]`	Used with the `router rip` and `router igrp` commands to specify the major IP networks that the router is directly connected to.
`no debug all`	Turns off debugging (Privileged mode command).
`no ip routing`	Global configuration command that disables IP routing on the router.
`router igrp [autonomous system number]`	Global configuration command that turns on IGRP routing. The autonomous number is the AS number for the routing domain that the router belongs to (if an AS exists).
`router rip`	Global configuration command the turns on RIP routing.
`show access-list [list number]`	Enables you to view a particular Access list. The list number is the number you assigned to the list when you created it.

continues...

Table A.5 Continued

Command	Results
`show ip interface [interface type and number]`	Command enables you to view the IP related configuration settings for a particular router interface.
`show ip protocol`	Provides information related to the routing protocol updates sent and received by the router (such as RIP broadcasts).
`show ip route`	Shows the RIP or IGRP routing table for the router.
`telnet [ip address]`	A user and Privileged command that enables you to log in to a router remotely.

IPX-Related Commands

These commands are related to the configuration of IPX addressing on interfaces and enabling IPX routing on the router (see Table A.6). Commands related to IPX RIP also included.

Table A.6 IPX-Related Commands

Command	Results
`access list [list #] permit or deny [source network address] [destination network address].`	Access list creation command (a Global Configuration command) that enables you to create IPX Access lists. The list numbers available for IPX are 800 to 899.
`access-list [list #] permit or deny -1 -1`	IPX Access list creation statement that enables you to permit or deny all networks and nodes not specified in other statements in the Access list.
`debug ipx routing activity`	Privileged command that enables you to view the IPX routing updates coming in and going out of the router.
`ipx access-group [list #] in or out`	Config-if configuration command that enables you to group an IPX access list to a router interface. `in` or `out` the interface must be specified.

Command	Results
`ipx network : ipx network [network number] encapsulation [frame type]`	Interface configuration command (config-if prompt) that enables you to set the IPX network address for a router Ethernet interface and set the Ethernet frame type for the interface.
`ipx routing`	Global configuration command that enables IPX routing on the router.
`no debug ipx routing activity`	Turns off IPX debugging.
`show access-list [list #]`	View an IPX or other type of Access list.
`show ipx interface`	View the settings for IPX enabled router interfaces (a User and Privileged command).
`show ipx route`	View the IPX routing table on a router.
`show ipx traffic`	View statistics related to the IPX packets sent and received.

AppleTalk-Related Commands

These commands are related to the configuration of AppleTalk and the viewing of AppleTalk configuration settings (see Table A.7).

Table A.7 AppleTalk-Related Commands

Command	Results
`access-list [list #] deny or permit zone [zone name]`	Global configuration command that enables you to build Access list lines based on zone names. AppleTalk Access lists can have a list number range of 600 to 699.
`access-list [list #] permit or deny cable-range [cable range]`	Global configuration command that enables you to build an AppleTalk Access list.
`appletalk access-group [list #]`	Config-if command that groups an AppleTalk Access list to a specified router interface.

continues...

Table A.7 Continued

Command	Results
`appletalk cable-range [cable-range number]`	Interface configuration command where you set the AppleTalk cable-range for a selected interface.
`appletalk routing`	Global configuration command that enables AppleTalk routing.
`appletalk zone [zone name]`	Interface configuration command that enables you to set the AppleTalk zone name for a particular interface.
`show appletalk global`	Provides information on the number of networks and zone available on the internetwork and the time interval for ZIP queries and RTMP updates.
`show appletalk interface`	Provides more detailed information on the router interfaces and their AppleTalk configurations.
`show appletalk interface brief`	Provides a short summary of all the interfaces on the router and their AppleTalk configurations.
`show appletalk interface e0`	Enables you to view detailed AppleTalk configuration information for a specified router interface.
`show appletalk zone`	Provides zone and network information for the zone available on the internetwork.

WAN-Related Commands

These commands are related to the configuration of WAN protocols on router serial interfaces (see Table A.8). Command for configuring Frame-Relay and X.25 on a router are included in this list.

Table A.8 WAN-Related Commands

Command	Results
`bandwidth [bandwidth]`	A `config-if` command for setting the bandwidth of a serial interface.
`clock rate [clockrate]`	`config-if` command used to set the clock rate on a serial interface when the router is used as a DCE device.
`encapsulation [WAN protocol]`	`config-if` command for setting the WAN encapsulation type for a serial interface (such as PPP, HDLC, and so on).
`frame-relay interface-dlci [dlci #]`	`config-if` command to set the DLCI number for a Frame-Relay configured interface.
`frame-relay lmi-type [LMI type]`	`config-if` command to set the LMI type for a Frame-Relay configured interface.
`isdn spid[spid channel designation] [SPID #]`	Global configuration command for entering the unique SPID number for each ISDN channel.
`isdn switch type basic-[switch identifier]`	Global configuration command that sets the ISDN switch type that your router is connected to.
`show frame-relay lmi`	Shows invalid messages sent or received via the router's Frame-Relay connection.
`show frame-relay map`	Shows the DLCI mapping to the router's interfaces.
`x25 address [data link address]`	`config-if` command used to set the data link address for X.25, when X.25 is set as the encapsulation type.
`x25 ips [bits]`	`config-if` command used to set the input packet size for an X.25 interface.
`x25 ops [bits]`	`config-if` command used to set the output packet size for an X.25 interface.
`x25 win [number of packets]`	`config-if` command to set the input window size for an X.25 interface.
`x25 wout [number of packets]`	`config-if` command to set the output window size for an X.25 interface.

Troubleshooting Commands

The commands in this table are related to troubleshooting the router (see Table A.9). The `ping` and `trace` command are included in this list.

Table A.9 Troubleshooting Commands

Command	Results
`ping [node address]`	Used to check the connection between two different router's (`ping` followed by the IP address or AppleTalk node address) on the remote router's interface. This command can also be used to check the connection between nodes on the network.
`show controller`	Lets you take a look at the status of interface controllers on the router.
`show interface [interface type] [interface number]`	An excellent command for viewing all the parameters related to a specific interface on the router.
`show stacks`	Provides error messages related to the crashing of a router when the router is restarted.
`trace [ip address]`	Shows the path between your router and another router or node on the internetwork. This command can also be used with AppleTalk addresses.

Miscellaneous Commands

This table contains some miscellaneous router commands such as the banner creation command and the command for setting the time and date on the router (see Table A.10).

Table A.10 Miscellaneous IOS Commands

Command	Results
`banner motd [banner end character]`	Global configuration command that enables you to create a banner for the router login screen. The banner end character is any non-alphanumeric

Command	Results
	character that tells the configuration mode that you are signaling the end of the banner text.
Ctrl+Z	While not an actual interface configuration command it is the command used to end a router configuration session.
disable	Exits the Privileged mode and returns to the User mode.
enable	Enter the Privileged mode. You must supply the Privileged password to enter the Privileged mode using this command.
quit	User and Privileged command that enables you to exit the router.
reload	Privileged command that reboots the router.
set clock	Privileged command that enables you to set the time and the date on the router.

Appendix B

Selected Cisco Router Specifications

Router Selection

Cisco 7500 Routers

Cisco 4500 Routers

Cisco 2500 Routers

Cisco 1000 Routers

A Final Note

How this appendix is structured

Cisco manufactures several different internetworking hardware devices (routers, switches, hubs, and so on)—too many to describe in this appendix. We will concentrate on Cisco routers, in particular routers that would typically be used in a small- to medium-sized internetwork (you could consider this one campus of an internetwork). Figure B.1 is a diagram of an internetwork that is a composite of several real-world internetworks that are actually used by several companies and one municipality. Each router type used in this internetwork diagram will be described briefly in this appendix.

Router Selection

When planning any enterprisewide internetwork (or even a campus network that is only a portion of the enterprise), the hardware that will be implemented as part of the plan must be capable of performing its intended function and imparting some scalability and flexibility to the network in case of future growth or the possible need for topology changes. Scalability and flexibility have really become industry buzzwords and in the final analysis really boil down to purchasing hardware. In this case, routers must not only serve the current situation but also enable you to upgrade or reconfigure the equipment if necessary without throwing everything out and starting over.

Cisco 7500 Routers

The Cisco 7500 routers are high-end routers that typically serve as border routers (also called *core routers*) and provide the routing of packets between routing domains. The 7513 router shown in Figure B.1 serves as a border router between the corporate network and the Internet (notice also that a firewall is installed between the internetwork and the border router).

The 7513 comes with 11 slots that are hot-swappable (interface cards can be swapped or inserted even while the router is running). The 7513 can provide several different interfaces including Ethernet, Fast-Ethernet, Token Ring, FDDI, T-1, Synchronous serial, and primary ISDN.

The 7513 router can also be configured with dual redundant power supplies and dual route switch processors. Table B.1 summarizes the hardware configuration for a basic 7513.

Table B.1 Cisco 7513 Specifications

Power supplies	2
Flash RAM	16MB standard, expandable to 220MB
Standard RAM	32MB, expandable to 128MB
Interface slots	11
Processor slots and type	2 slots/MIPS RISC processor
Weight	75 pounds

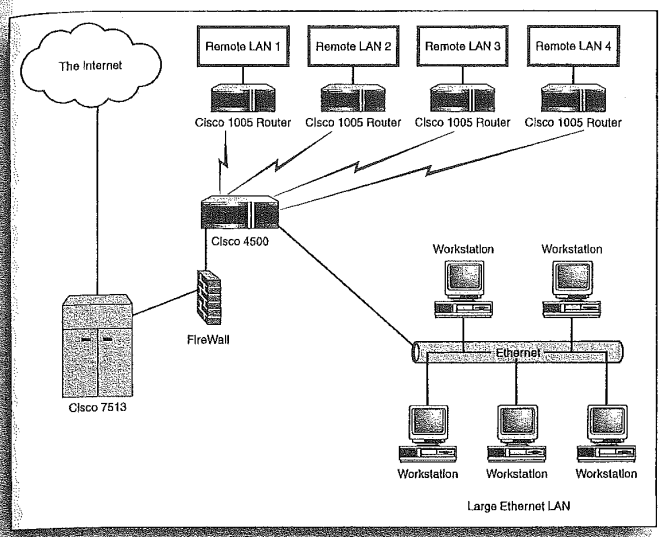


FIGURE B.1
This internetwork uses several different types of Cisco routers to connect various LANs.

Cisco 4500 Routers

The Cisco 4500 routers are considered distribution-level routers and are used as the central connection point for small LANs and remote sites on the internetwork. Notice in Figure B.1 the 4500 router is used as a sort of central distribution point for the remote offices (which are connected to the 4500 by access routers) and the main LAN (which is directly connected to the 4500 via a LAN interface).

The Cisco 4500 routers are modular, so their interface slots can be customized with particular types of interface cards with varying numbers of ports. The Cisco 4500 router, although considered a medium-capacity router, has a broad range of interface cards available and can support Ethernet, Fast-Ethernet, Token-Ring, FDDI, serial, and ISDN to name a few.

The 4500 series does not support hot swappable interface cards (like the 7000 series) nor do they have the capacity for redundant power supplies. Table B.2 shows the basic specifications for a 4500 router.

Why include the router weight?
I included weight as a specification to give you an idea of how the different router families differ in size. A 7513 router weighs 75 pounds while one of the Series 2500 routers weighing in at only 10 pounds can be carried under your arm like a notebook.

Table B.2 Cisco 4500 Specifications

Power supplies	1 internal power supply
Flash RAM	4MB standard expandable to 16
Standard RAM	4MB standard expandable to 16
Interface slots	3 slots
Processor slots and type	1 slot 100-MHz IDT Orion RISC
Weight	14 pounds

Cisco 2500 Routers

The Cisco 2500 series routers are inexpensive routers and are considered access-level routers. Figure B.2 shows the 2505 router, and Table B.3 explains the 2505 specifications. 2500 series routers provide more ports than other branch-office routers such as the 1000 series. They support synchronous and asynchronous serial interfaces, Ethernet interface, Token Ring interfaces, and ISDN interfaces.

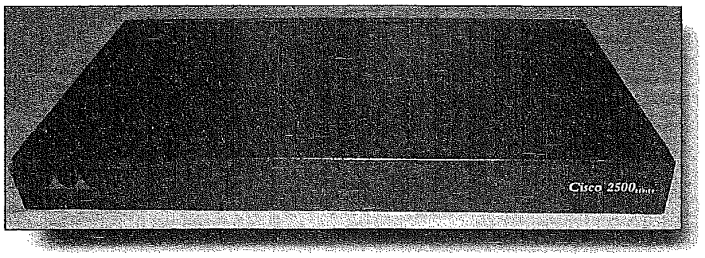


FIGURE B.2
Over a million 2500 series routers have been sold by Cisco, making it the most popular router in the world.

Table B.3 Cisco 2505 Specifications

Power supplies	1 internal power supply
Flash RAM	8MB
Standard RAM	4MB expandable to 16
Interface slots	No slots/2 serial interfaces, 1 Ethernet interface in the form of an 8-port hub
Processor slots and type	1 processor 20MHz 68030
Weight	10 pounds

Cisco 1000 Routers

The Cisco 1000 series routers are small routers designed to connect remote LANs to the overall WAN (or internetwork). In Figure B.1, Cisco 1005 routers are used by remote sites to connect to the 4500 distribution router. The 1005 routers would be connected to the 4500 using a serial interface and a particular WAN technology. Because the primary job of the 1000 series is accessing the internetwork, these routers are often referred to as access-class routers.

The Cisco 1005 router only comes with one serial interface (with a 60-pin serial port, which is typical of Cisco routers—see Figure B.3). This serial interface supports both synchronous and asynchronous communication, so several different WAN protocols could be used to connect to the 4500 router including PPP, Frame Relay, or HDLC.

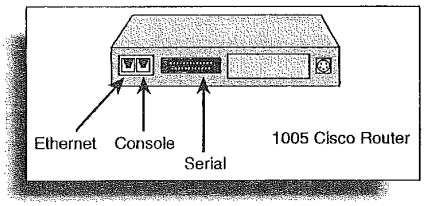


FIGURE B.3
The Cisco 1005 router supplies one Ethernet and one serial interface.

Because the Cisco 1005 is designed to support a remote site, it contains only one Ethernet port, which can be hooked to the hub that connects the Ethernet workstations to the network. Table B.4 details some of the specifications of the 1005 router.

Table B.4 Cisco 1005 Specifications

Power supplies	1 external power supply
Flash RAM	None, PCMCIA slot provides option of a Flash card
Standard RAM	8MB
Interface slots	No slots/2 interfaces
Processor slots and type	1 processor MC68360
Weight	6 pounds

A Final Note

Probably the most amazing thing about all these routers is that, although they differ a great deal in processor power and the number of interfaces they provide, each of these routers uses the same operating system—the Cisco IOS. This makes it extremely easy for a network administrator to configure several different router types without really missing a beat. The fact that the command set is consistent across the routers means you must learn only one operating system to work with many different internetworking devices.

As a final word of advice, you should definitely make the time to explore Cisco's Web site at `www.cisco.com`. It not only provides specifications for all of Cisco's products, but it also provides white papers, manuals, and even free software that you can download. Although you might find the site somewhat difficult to navigate at first, you will find that it provides a real wealth of knowledge related to internetworking technologies.

GLOSSARY

AARP (AppleTalk Address Resolution Protocol) A Network layer protocol that resolves AppleTalk network addresses to hardware addresses. AARP sends broadcasts to all stations on the network to match hardware addresses to logical destination addresses for packets.

AARP broadcast Broadcasts to all stations on an AppleTalk network to match hardware addresses to logical destination addresses for packets.

Access list A list of conditions called `permit` and `deny` statements that help regulate traffic flow into and out of a router.

agents Software watchdogs used by SNMP to keep an eye on network processes. See also *SNMP*

anding A method used by the router in which it compares or "ands" an IP address with its subnet mask to determine the network address.

AppleTalk A routable networking architecture developed by Apple that provides network services to Apple Macintosh computers.

area A subset of an internetwork containing several member routers. When several areas are grouped into a higher-level subset this organizational level is called a routing domain.

ARP (Address Resolution Protocol) A TCP/IP protocol used to map IP addresses to node hardware addresses.

asynchronous communication Serial data transfer connections that rely on start and stop bits to make sure that the data is completely received by the destination device.

ATM (Asynchronous Transfer Mode) An advanced packet-switching protocol that uses fixed packet sizes (53 bytes) called cells to increase the throughput of the data transfer. Typically run over high-speed fiber optic networks. See also *cells* and *SONET*

attenuation The degradation of the data signal over the run of the cable.

autonomous system In cases where link-state routing protocols are used that require greater memory and processing capabilities from the routers on the network, it isn't uncommon to divide the internetwork into routing domains. In IP networks, a routing domain is referred to as an autonomous system. See also *border router*

bandwidth The capacity of a medium to conduct data.

banner A message that appears on the login screen of a router on a router console or virtual terminal.

baseband A transmission that uses a single bit stream over the entire bandwidth available.

beaconing A Token Ring fault tolerance strategy where nodes on the ring can determine the state of the network in cases where cable failure has taken place or there is a problem with a down stream neighbor on the ring.

BGP (Border Gateway Protocol) A commonly used routing protocol for interdomain routing. It is the standard EGP for the Internet. BGP handles the routing between two or more routers that serve as the border routers for particular autonomous systems.

border router A high-end router used to connect autonomous systems. Also known as core routers.

bottleneck A device that is slowing network traffic.

breakout box A device used to determine whether you are getting a signal from the CSU/DSU connected to a router.

BRI See *ISDN*

bridges Internetworking devices that operate at the Data Link layer of the OSI model. Bridges are used to segment networks that have grown to a point where the amount of data traffic on the network media is slowing the overall transfer of information.

broadcast storms A condition caused when broadcast traffic from devices on an Ethernet network overwhelms it with messages bringing down the network.

bus network A network topology characterized by a main trunk or backbone line with the networked computers attached at intervals along the line.

cable range A network designation for an AppleTalk network segment assigned by the network administrator. Cable ranges can consist of a single number designating one network on the network wire or it can be a range of network numbers specifying a number of networks on the same wire.

campus A portion of an internetwork that is made up of several connected LANs as one location. See also *internetwork*

CDP (Cisco Discovery Protocol) A Cisco proprietary protocol that provides you with the ability to access information related to neighboring routers. See also *Neighbors*

cells Packets of fixed size used by Asynchronous Transfer Mode. See also *ATM*

circuit switching A connectivity strategy where a dedicated connection is established between the sender and receiver on a switched network (such as the Public Switched Telephone Network). Data moves from the source to the destination along the circuit (the lines) that has been established for the particular session.

Class A Large IP networks that supply over 16 million node addresses for the network.

Class B Large- to medium-sized IP networks that supply over 65,000 node addresses.

Class C Small IP networks that only provide 254 node addresses.

Class D A class of IP network addresses used by multicast groups receiving data on an internetwork from a particular application or server service. An example of a multicast use of Class D addresses is Microsoft NetShow, which can broadcast the same content to a group of users at one time.

Class E IP addresses that belong to an experimental class and are unavailable for general use.

CLI (Command-Line Interface) The interface provided by the Cisco IOS on a router console or virtual terminal that allows you to enter the various IOS commands.

clients A computer on the network that is logged in by and receives services from (such as printing or file access) a server computer.

clock ticks A metric used by the IPX Routing Information protocol. A tick is 1/18 of a second.

Configuration mode The router mode that enables you to configure the router configuration using global commands and specific interface-related commands.

convergence The time it takes for all the routers on the network to be up-to-date in terms of the changes that have taken place in the network topology. The longer it takes for all the routers on the internetwork to converge the greater the possibility that packets will be routed to routes that are no longer available on the network.

CRC (Cyclical Redundancy Check) The Data Link layer makes sure that frames sent over the physical link are received error free.

Protocols operating at this layer will add a trailer on each frame called a CRC check. Basically this is a mathematical calculation that takes place on the sending computer and then on the receiving computer. If the two CRCs match up then the frame was received in total and its integrity was maintained during transfer.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) A network access strategy used by AppleTalk. A device that is ready to send data out onto the network will notify the other network nodes of its intention to place data on the network.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) A network access strategy used by Ethernet networks. If a node sending data detects that there has been a collision, it will wait to resend the data until the line is determined to be free of other data.

CSU/DSU (Channel Service Unit/Digital Service Unit) A device that connects LAN equipment such as a router to digital phone lines.

data link broadcasts Broadcast messages used by CDP to discover neighboring Cisco routers that are also running CDP. See also *CDP*

datagrams Grouping of information in the data bit stream, datagrams are also referred to as packets or frames.

DCE (Data Circuit Terminating Equipment) Equipment that provides a connection between the network and the switched network. The DCE often provides clocking information to synchronize the communication between the network termination equipment (such as a DTE) and the switched network. See also *DTE* and *PDN*

DDP (Datagram Delivery Protocol) An AppleTalk Network layer protocol that provides a connectionless datagram delivery system (similar to UDP in the TCP/IP stack).

DDS Digital Data Service Leased digital lines used for data communications. DDS lines include the T-Carrier system, which provides a range of line types and data transfer rates.

DECnet A network protocol stack developed by the Digital Equipment Corporation.

default gateway The address of the router interface to which a particular LAN is connected. Every device on the LAN uses that connected router interface address as its default gateway.

delay The amount of time it takes to move a packet from the interface to the intended destination. Delay is measured in microseconds.

deny statements Statements in an Access list that deny traffic from certain networks or nodes to enter or exit a particular router interface.

dial-up connection The simplest and least expensive type of data transfer connection uses a modem to connect two computers or other devices over a regular analog voice-grade telephone line.

distance-vector routing algorithms Routing algorithms that require the router to pass their entire routing table to their nearest router neighbors (routers that they are directly connected to). This basically sets up an update system that reacts to a change in the network like a line of dominos falling.

DLCI (Data Link Connection Identifier) A reference or pointing device that makes sure that packets sent over a switched network, such as Frame Relay, end up at the proper destination. This is done by mapping the logical addresses (IP addresses, for example) of the sending and receiving routers to the DLCI of the virtual circuit that they use to communicate. See also *Frame Relay*

DOD model When TCP/IP was developed, the Department of Defense (DOD) developed their own conceptual model—the DOD model—(also known as the DARPA model) for how the various protocols in the TCP/IP stack operate.

DTE (Digital Terminal Device) The termination device for a data network and connects to DCE device, which provides a connection to a switched network. See also *DCE* and *PDN*

dynamic algorithms Routing tables that are built dynamically by a routing protocol.

EGP (Exterior Gateway Protocol) A routing protocol that provides the mechanism for the routing of data between routing domains. Border Gateway Protocol (BGP) is an example of an EGP. See also *BGP*

encapsulation The packaging of data in a particular protocol header. For example Ethernet data is encapsulated in an Ethernet header before being placed on the network.

Ethernet The most commonly deployed network architecture; it provides access to the network using CSMA/CD (carrier sense multiple access with collision detection).

Exec The Cisco IOS uses a command interpreter to execute your commands (it interprets the command and then executes it). The User mode and the Privileged mode are considered different levels of the Exec.

extended segment An AppleTalk network segment that has been assigned a range of network numbers.

FDDI (Fiber Distributed Data Interface) An architecture that provides high-speed network backbones that can be used to connect a number of different network types. FDDI uses fiber-optic cable, wired in a ring topology, using token passing as its media access method, operating at a data rate of at least 100Mbps and allowing long cable distances.

Flash RAM A special kind of ROM that you can erase and reprogram. Flash is used to store the Cisco IOS that runs on your router. You can also store alternative versions of the Cisco IOS on the Flash (such as an upgrade of your current IOS), which makes it very easy for you to upgrade the router.

Frame Relay A packet-switching WAN protocol that uses permanent virtual circuits for communication sessions between points on the WAN. These virtual circuits are identified by a DLCI (Data Link connection identifier)—a value provided by the frame relay service provider. See also *DLCI*

FTP (File Transfer Protocol) TCP/IP Application protocol that provides the ability to transfer files between two computers.

gateways Used to connect networks that don't embrace the same network protocol and so protocol translation is necessary between the two disparate networks. For example, a gateway can be used as the connection between an IBM AS400 miniframe and a PC-based LAN.

global commands Self-contained, one-line configuration commands that affect the overall global configuration of the router. Examples are hostname and enable secret.

HDLC (High Level Data Link Control) A synchronous Layer 2 WAN transport protocol. The HDLC used on Cisco routers is a Cisco proprietary version.

high-order bits The first four bits in any octet of an IP address (on the far left of the octet) are referred to as the high-order bits.

hop count A metric used by RIP. A hop is the movement of the packets from one router to another router. See also *RIP*

hub A centralized connectivity device, especially in a star topology. The computers on the network connect to the hub.

hubs Devices operating at the Physical layer of the OSI model that provide the central connection point for networks arranged in a star topology.

ICMP (Internet Control Message Protocol) A message service provider and management protocol used by routers to send messages to host computers that are sending data that must be routed.

IGP (Interior Gateway Protocol) A routing protocol that provides the mechanisms for the routing of packets within the routing domain. IGPs such as RIP or IGRP would be configured on each of the routers in the router domain. See also *RIP*, *IGRP*, and *OSPF*

IGRP (Interior Gateway Routing Protocol) A distance-vector routing protocol developed by Cisco in the 1980s. IGRP uses a composite metric that takes into account several variables; it also overcomes certain limitations of RIP, such as the hop count metric and the inability of RIP to route packets on networks that require more than 15 hops.

Interface The physical connection between the router and a particular network medium type; interfaces are also referred to as ports.

International Data Numbers See X.121

internetwork When several LANs are connected. This is really a network of networks (this type of network can also be referred to as a campus).

intranet A corporate network that is internal to the enterprise (not connected to the global Internet) but uses Internet protocols such as Simple Mail Transport Protocol and Hypertext Transport Protocol (the protocol used by Web Browsers) to share information among corporate users.

IOS (Internetworking Operating System) The Cisco proprietary operating system software that provides the router hardware with the ability to route packets on an internetwork. The IOS provides the command sets and software functionality that you use to monitor and configure the router.

IP unnumbered Serial interfaces on a router configured without IP addresses (they will still route IP packets even though they are designated as IP unnumbered).

IPX (Internet Package Exchange Protocol) A connectionless oriented transport protocol that provides the addressing system for the IPX/SPX stack. Operating at the Network and Transport layers of the OSI model, IPX directs the movement of packets on the internetwork using information that it gains from the IPX Routing Information Protocol (RIP).

IPX network number The first part of the IPX address, which can be up to 16 hexadecimal characters in length (this part of the network.node address is 32-bits. The remaining 12 hexadecimal digits in the address make up the node address (which makes up the remaining 48 bits of the address).

IPX RIP (Routing Information Protocol) A routing protocol that uses two metrics: clock ticks (1/18 of a second) and hop count—to route packets through an IPX internetwork.

IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) The NetWare proprietary network protocol stack for LAN connectivity. IPX is similar to TCP/IP in that the protocols that make up the IPX/SPX stack don't directly map to the layers of the OSI model. IPX/SPX gained a strong foothold in early local area networking because IPX/SPX was strong on performance and didn't require the overhead that is needed to run TCP/IP.

IRQ (Interrupt ReQuest) A unique request line that allows a device to alert the computer's processor that the device connected to that IRQ requires processing services.

ISDN (Integrated Services Digital Network) Is digital connectivity technology used over regular phone lines. A device called an ISDN modem is used to connect a device to the telephone network. ISDN is available in Basic Rate ISDN (BRI) and primary Rate ISDN (PRI).

ISDN modem See *terminal adapter*

ISO (International Standards Organization) This global standard organization develops sets of rules and models for everything from technical standards for networking to how companies do business in the new global market. They are responsible for the OSI conceptual model of networking. See also *OSI*

keepalives Messages sent by network devices to let other network devices know that a link between them exists

LAN (Local Area Network) A server-based network of computers that is limited to a fairly small geographical area, such as a particular building.

LAN interface A router interface providing a connection port for a particular LAN architecture such as Ethernet or Token Ring.

leading bits The first three bits in an IP network address. Rules have been established for the leading bits in the first octet of each of the classes (A, B, and C). Class A addresses must have 0 as the first bit. In Class B addresses the first bit of the first octet is set to 1, and the second bit is set to 0. In Class C addresses the first two bits of the first octet are set to 1 and the third bit is set to 0.

lease lines Dedicated phone providing a full-time connection between two networks through the PSTN or another service provider. Leased lines are typically digital lines.

LLC (Logical Link Control) A sublayer of the Data Link layer that establishes and maintains the link between the sending and receiving computer as data moves across the network's physical media.

LMI (Local Management Interface) The signaling standard used between a router and a Frame Relay switch. Cisco routers support three LMI types: Cisco, ANSI, and q933a.

Load The current amount of data traffic on a particular interface. Load is measured dynamically and is represented as a fraction of 255, with 255/255 showing the saturation point.

LocalTalk The cabling system used to connect Macintosh computers (it uses shielded twisted-pair cables with a special Macintosh adapter).

logical interface A software-only interface that is created using the router's IOS. Logical interfaces are also referred to as virtual interfaces. See also *loopback interface*, *null interface*, and *tunnel interface*

loopback interface A software-only interface that emulates an actual physical interface and can be used to keep data traffic local that is intended for a hardware interface that is nonfunctioning. See also *logical interface*

lower-order bits The first four bits in any octet (counting from right to left) are referred to as the lower-order bits.

MAC (Addresses Media Access Control) MAC addresses are burned on to ROM chips on network interface cards, giving each of them a unique address.

MAU (Multistation Access Unit) Token Ring networks are wired in a star configuration with a MAU providing the central connection for the nodes. The MAU itself also provides the logical ring that the network operates on.

mesh topology A network design where devices use redundant connections as a fault tolerance strategy.

metric The method routing algorithms use to determine the suitability of one path over another. The metric can be a number of different things such as the path length, the actual cost of sending the packets over a certain route, or the reliability of a particular route between the sending and receiving computers.

NADN (Nearest Downstream Neighbor) On a Token Ring network, a NADN would be the active node directly downstream from a particular node. See also *NAUN*

NAUN (Nearest Upstream Neighbor) In Token Ring network a computer that passes the token to the next computer on the logical ring would be called the nearest active upstream neighbor or NAUN.

NBP (Name Binding Protocol) A Transport layer protocol that maps lower-layer addresses to AppleTalk names that identify a particular network resource such as a printer server that is accessible over the internetwork.

NCP (Netware Core Protocol) An IPX/SPX protocol that handles network functions at the Application, Presentation, and Session layers of the OSI model.

neighbors Routers that are directly connected to a particular router by LAN or WAN connections.

NetBEUI (NetBIOS Extended User Interface) A simple and fast network protocol that was designed to be used with Microsoft's and IBM's NetBIOS (Network Basic Input Output System) protocol in small networks.

network A group of computers and related hardware that are joined together so that they can communicate.

NIC (Network Interface Card) A hardware device that provides the connection between a computer and the physical media of a network. The NIC provides the translation of data into a bit; sometimes referred to as an adapter.

NLSP (NetWare Link Services Protocol) A Novell developed link-state routing protocol that can be used to replace RIP as the configured routing protocol for IPX routing.

node Any device on the network (such as a computer, router, or server).

nonextended segment An AppleTalk network segment that is assigned only one network number.

NOS (Network Operating System) Any number of server-based software products, such as Windows NT, Novell NetWare, and AppleTalk, that provides the software functionality for LAN connectivity.

NT domain A network managed by an NT server called the Primary Domain Controller.

null interface A software only interface that drops all packets that it receives. See also *logical interface*

NVRAM Nonvolatile RAM RAM that can be used to store the startup configuration file for the router. NVRAM can be erased and you can copy the running configuration on the router to NVRAM. NVRAM does not lose its contents when the router is rebooted.

octet Eight bits of information; one portion of the four octet IP address used on IP networks.

OSI (Open Systems Interconnection Model) A conceptual model for networking developed in the late 1970s by the International Standards Organization (ISO). In 1984 the model became the international standard for network communications. It provides a conceptual framework (based upon seven layers called protocol stacks) that helps explain how data gets from one place to another on a network.

OSPF (Open Shortest Path First) A link state protocol developed by the Internet Engineering Task Force (IETF) as a replacement for RIP. Basically, OSPF uses a shortest-path-first algorithm that allows it to compute the shortest path from source to destination when it determines the route for a specific group of packets. See also *IGP*

packet switching A Wide Area Networking strategy where the bit stream of data is divided into packets. Each packet has its own control information and is switched through the network independently.

PDN (Public Data Network or Private Data Network) A packet switching network operated by a service provider. PDNs provide WAN connectivity avenues for the connecting of LANs at remote sites.

peer-to-peer network A local area network that operates without a server but allows connected computers to access shared resources such as files and printers.

permit statements Statements in an Access list that permit traffic from certain networks or nodes to enter or exit a particular router interface.

Ping (Packet InterNet Groper) An IP protocol used to test the connection between two or more nodes on a network. These nodes can be host computers, servers, or routers.

port commands A set of commands that enable you to specify a particular interface or controller for configuration; these commands must be followed by subcommands that provide additional configuration information. See also *subcommands*

Port See *interface*

PPP (Point-to-Point Protocol) A synchronous and asynchronous protocol that can provide WAN connections over a number of different connection types.

PRI See *ISDN*

privileged mode A complete access level to the router that enables you to view, save and erase router configuration parameters and enter the Configuration mode for the router. See also *Configuration mode*

Protocols The software-based rules that define how networked computers send and receive data.

PSTN (Public Switched Telephone Network) The telephone communication infrastructure provided by the Baby Bells.

RAM (Random Access Memory) Similar to the dynamic memory you use on your PC, RAM provides the temporary storage of information (packets are held in RAM when their addressing information is examined by the router) and holds information such as the current routing table.

reliability The ratio of expected-to-received keepalives. See also *keepalives*

repeaters Physical devices that take the signal received from network devices and regenerates the signal so that it maintains its integrity along a longer media run than is normally possible. Repeaters are also referred to as concentrators.

ring topology Networked computers connected one after the other on the wire in a physical circle. Ring topology moves information on the wire in one direction with each networked computer actually resending the information it receives onto the next computer in the ring.

RIP (Routing Information Protocol) A distance-vector routing protocol that uses hop count as its metric. RIP summarizes the information in the routing table by IP network numbers (also referred to as major network numbers).

roll-over cable The cable used to connect the console computer and the router.

ROM (Read Only Memory) Memory chips that contain burned-in software instructions. Router ROM contains the Power-on Self-Test (POST) and the bootstrap program for the router.

routable protocol A networking protocol that provides the necessary Layer 3 protocols for the routing of packets.

router An internetworking device used to connect LANs via LAN and WAN connections. The router uses a combination of software and hardware to route packets between networks.

router console The computer serving as the router's dumb terminal. Used to view and enter configuration settings on the router.

routers Internetworking devices that operate at the Network layer (Layer 3) of the OSI model. Using a combination of hardware and software (Cisco Routers use the Cisco IOS—Internetwork Operating System), routers are used to connect networks.

routing protocol Protocols that provide the mechanism for a router to build a routing table and share the routing information with other connected routers.

RTMP (Routing Table Maintenance Protocol) A Transport layer protocol that is responsible for establishing and maintaining routing tables on routers that have been enabled to route AppleTalk.

running configuration The router configuration currently running in the router's RAM.

SAP (Service Access Point) The LLC sublayer provides these reference points so that a computer sending data can refer to the SAPs when communicating with the upper-layer protocols of the OSI stack on a receiving node.

SAP (Service Advertisement Protocol) A protocol that advertises the availability of various resources on the NetWare network.

serial adapters Adapters provided with the router used to connect the rollover cable to the COM port on a computer.

serial interfaces A router interface providing a connection port for various WAN technologies. A router port would typically be attached to a cable such as a V.35 cable that then attaches to a WAN DCE device. See also *DCE*

server The provider of data communications resources to client machines on the network.

server-based network A network where client computers are authenticated on the network by a server computer. The server provides centralized file storage and other centralized services such as printing and other resources.

session A transaction between networked nodes.

share-level security Typically used in Peer-to-Peer networks, each shared resource requires a password for access. See also *peer-to-peer network*

SMTP (Simple Mail Transport Protocol) TCP/IP Application layer protocol that provides mail delivery between two computers.

SNMP (Simple Network Management Protocol) A TCP/IP Application layer protocol that can be used to monitor the health of an internetwork. SNMP uses software agents that report back on a particular measured parameter related to the network.

SONET (Synchronous Optical Network) a Fiber Optic network developed by Bell Communications Research that provides voice, data, and video at high speeds.

SPID (Service Profile Identifier) A number used to authenticate an ISDN channel to the switch that connects the ISDN–enabled device to the phone system. Each channel must have a different SPID number.

SPX (Sequence Packet Exchange) A connection–oriented transport protocol in the IPX/SPX stack that provides the upper layer protocols with a direct connection between the sending and receiving machines.

star topology A network design where all the computers connect together at a central hub, each with its own cable.

static algorithms Internetwork mapping information that a network administrator enters into the router's routing table.

static routing Routing where the routing tables have been entered and updated manually by the network administrator.

subcommands Commands that provide specific configuration information for the interface or controller that you specify with a particular port command. See also *port commands*

subnet mask A four-octet mask that is used to determine which bits in the IP address refer to the network address, which bits in the IP address refer to the subnet address, and which bits in the IP address refer to the node address.

switches A Layer 2 internetworking device that can be used to preserve the bandwidth on your network using segmentation. Switches are used to forward packets to a particular segment using MAC hardware addressing (the same as bridges). Because switches are hardware-based, they can actually switch packets faster than a bridge.

switching The routing of packets on a router from an incoming interface to an outgoing interface.

synchronous communication Serial connections that use a clocking device that provides the precise timing of the data as it moves from sending to receiving computer across a serial connection.

TCP (Transport Control Protocol) A connection-oriented protocol that provides a virtual circuit between user applications on the sending and receiving machines on a TCP/IP network.

TCP/IP (Transmission Control Protocol/Internet Protocol) A routable protocol stack that can be run on a number of different software platforms (Windows, UNIX, and so on) and is embraced by most network operating systems as the default network protocol.

TDR (Time Domain Reflectometer) A device that can diagnose shorts and breaks in a cable and can also provide information on where the short or break exists on the cable.

Telnet A terminal emulation protocol (part of the TCP/IP stack) that enables you to connect a local computer with a remote computer (or other device such as a router).

terminal adapter Also known as an ISDN modem, used to connect a node configured for ISDN to the phone system. See also *ISDN*

TFTP server A computer running TFTP software that can be used for the saving of router configuration files. Files can be copied from the router to the TFTP server, or from the TFTP server to the router.

TFTP (Trivial File Transfer Protocol) A stripped-down version of FTP that provides a way to move files without any type of authentication (meaning no username or password).

Token Ring A network architecture developed by IBM that is arranged in a logical ring and uses a token passing strategy for network access. Token Ring can run at 4 or 16Mbps. IBM developed and supports token-passing LANs.

topology Networks have a physical layout or topology that will reflect, for instance, the cable type used and the actual architecture of the network (such as ring, bus, mesh, or star topology).

tunnel interface A logical interface that can be used to move packets of a particular network architecture type over a connection that doesn't typically support these types of packets. See also *logical interface*

UDP (User Datagram Protocol) A connectionless-oriented TCP/IP stack transport protocol that provides a connection between application layer protocols that don't require the acknowledgements and synchronization provided by TCP. See also *TCP*

UPS (Uninterruptible Power Supply) A device that will supply power to a computer device such as a router using a battery if the electricity is cut.

User mode The basic access level to the router, User mode commands allow you to examine the router's configuration but don't allow you to change any configuration parameters. See also *Privileged mode* and *Configuration mode*

virtual circuit A defined route established across a WAN cloud so that all the data packets move to the destination along the same route. The use of virtual circuits in packet switching networks can improve the overall performance of data transfers.

virtual interfaces See *logical interface*

virtual terminal A computer or router that uses Telnet to access another router.

VLMs (Virtual Loadable Modules Netware) Software modules that establish and maintain network sessions between the client and server on an IPX/SPX network.

voltmeter A device that can be connected to a cable to test the cable for a break or a short.

WAN (Wide Area Network) A group of connected campuses or internetworks that span large geographical areas.

WAN interfaces Serial interfaces or special interfaces such as ISDN interfaces that are used for WAN connectivity. See also *serial interfaces*

wildcard mask 32-bit mask used with IP addresses to determine which portion of the IP address should be ignored in Access list `deny` and `permit` statements.

X.121 A telephone standards addressing scheme (also known as International Data Numbers) used by the X.25 WAN protocol that is comprised of one to 14 decimal digits. This number identifies the local X.121 address for your serial interface and must be configured on the router that is being enabled for X.25.

XNS (Xerox Network Systems) In the 1960s a bunch of geniuses at the Xerox Palo Alto Research Center developed the XNS (Xerox Network Systems) network operating system. NetWare is based heavily on this early networking protocol stack.

ZIP (Zone Information Protocol) A Network and Transport layer protocol that is used to assign logical network addresses to nodes on the network.

Zone A logical grouping of different AppleTalk physical network segments. Zones are logical groupings of users (similar to the concept of workgroups in Microsoft peer-to-peer networking).

INDEX

Symbols

56K modems, 56

A

Access lists, 244
- AppleTalk Access lists, 256-258
- building, 246-247, 252-253
- deleting, 254
- deny statements, 244-247
- grouping to an interface, 253-254
- IP Access lists, 247-254, 314
- IPX Access lists, 254-256
- operation of, 244-246
- permit statements, 244-247
- wildcard masks, 248-252

access-list [list #] deny or permit zone [zone name] command, 331

access-list [list #] permit or deny -1 -1 command, 330

access-list [list #] permit or deny cable-range [cable range] command, 331

access-list [list #] permit or deny [ip address] [wildcard mask] command, 328

access-list [list #] permit or deny [source network address] [destination network address] command, 330

active hubs, 72

Address Resolution Protocol (ARP), 47, 172

addresses
- AppleTalk, 229-232
- hardware addresses, 45
- IP addresses, 47, 174
  - *classes, 175-177*
  - *cost, 176*
  - *DHCP servers, 293*
  - *obtaining, 176*
  - *purpose of, 174-175*
  - *router interfaces, 196-201*
  - *subnet masks, 178-181*
  - *subnetting, 180-194*
  - *TFTP servers, 290*
  - *written forms, 174, 177-179*
- IPX addresses, 214-216
- MAC addresses, 45
  - *finding, 43*
  - *router LAN interfaces, 104*
  - *routing, 175*
- major network addresses, 192
- network addresses, 192

administration of peer-to-peer networks, 10

algorithms for routing, 87
- distance vector, 88-90
- dynamic, 88-89
- link state, 88-89
- metrics, 89-91
- static, 87, 89

American Registry for Internet Numbers, 176

Apple Macintosh networks
- AppleTalk, 30-31, 228
  - *addressing, 229-232*
  - *as a routable protocol, 85*
  - *configuring, 232-236*
  - *monitoring, 237-240*
  - *network interface cards, 228*
  - *phases, 230, 318*
  - *protocols, 49-51, 228-229*
  - *resources, 232*
  - *troubleshooting, 317-319*
  - *zones, 232-233*
- LocalTalk, 30

AppleTalk, 30-31, 228
- addressing, 229-232
- as a routable protocol, 85
- configuring, 232-235
  - *LAN interfaces, 235-236*
  - *WAN interfaces, 236*
- monitoring, 237-240
- network interface cards, 228
- phases, 230, 318
- protocols, 49-51, 228-229
  - *AARP, 50, 228*
  - *AFP, 50*
  - *AppleShare, 50*
  - *ATP, 50*
  - *DDP, 51, 228*
  - *NBP, 50, 229*
  - *RTMP, 229*
  - *ZIP, 50, 228*
- resources, 232
- troubleshooting, 317-319
- zones, 232-233

AppleTalk Access lists
creating, 256-258
grouping, 257-258
appletalk access-group [list #] command, 331
appletalk cable-range [cable-range number] command, 332
AppleTalk commands, 331-332
appletalk routing command, 332
appletalk zone [zone name] command, 332
Application layer (OSI model), 35, 38, 40
application servers, 11
APR (Address Resolution Protocol), 47
architectures (networks), 25
AppleTalk, 30-31
Ethernet, 26-27
advantages, 28
disadvantages, 28
Fast Ethernet, 28, 103
frame types, 27-28
Gigabit Ethernet, 28
IEEE 802.3 specification, 27
implementations, 27
router interfaces, 103
FDDI, 29-30, 104
IBM Token Ring, 28-29
beaconing, 29
IEEE 802.5 specification, 28
router interfaces, 103-104
troubleshooting, 309-311
network interface cards (NICs), 14
ARP (Address Resolution Protocol), 172
Asynchronous Transfer Mode (ATM), 64-65
asynchronous serial communications, 106
ATM (Asynchronous Transfer Mode), 64-65

B

bandwidth [bandwidth] command, 333
banner motd end character command, 162-163
banner motd [banner end character] command, 334
banners (routers), 161-163
baud rate (serial communications), 119
BGP (Border Gateway Protocol), 95-96
boot sequence or routers, 126-128
Border Gateway Protocol (BGP), 95-96
border routers, 96
bridges
broadcast storms, 74
internetworking, 68, 71-72
source-routing bridges, 73
transparent bridges, 73
broadcast storms, 12, 73-74
broadcasts
messages, 81
SAP announcements, 216-217
building Access lists, 246-247, 252-253
bus topology (networks), 21-22

C

cables
category 5 twisted pair cable, 17, 19
coaxial cable, 17-19
copper cable, 17-19
DCE cables, 260-261
DTE cables, 260-261
fiber-optic cable, 17-19
guidelines for selecting, 18
pin configurations, 122
roll-over cable, 116
testing, 306
Thicknet cable, 17-19
Thinnet cable, 18-19
troubleshooting, 306
campus networks, 75
campuses, 11
cards
network cards, 41, 43
NICs (network interface cards), 12-13
addresses, 13
AppleTalk, 228
I/O ports, 17
installing, 13-15
IRQs, 15-16
network architectures, 14
problems with, 14
slots, 13
VIP (Versatile Interface Processor) cards, 102
category 5 twisted pair cable, 17, 19

CDP (Cisco Discovery Protocol), 157
Data Link broadcasts, 157
disabling, 160
enabling, 157-160
holdtime, 158
platform independence, 158
viewing CDP neighbors, 159-160

checking router memory, 154-156, 158

circuit switching WANs, 60-61

Cisco, 338
1-800 number, 115
TFTP server software, 291-294
Web address, 104, 113, 273, 342

Cisco Certified Internetworking Engineers, 126

Cisco ConfigMaker, 125, 272
Cisco IOS version requirements, 272
delivering configurations to routers, 284-287
downloading, 272-273
exiting, 287
Help, 287
installing, 273-274
internetwork diagrams, 274-276
adding devices, 276-279
connecting LANs to routers, 278-281
connecting routers to routers, 281-284
deleting devices, 278
saving, 286
starting, 274
system requirements, 273
windows
Connection window, 275
Devices window, 275
Network Diagram window, 275
Status bar, 276
Task list, 276
wizards
Address Network Wizard, 274
Deliver Configuration Wizard, 274, 285
Ethernet Wizard, 280

Cisco Discovery Protocol (CDP), 157
Data Link broadcasts, 157
disabling, 160
enabling, 157-160
holdtime, 158
platform independence, 158
viewing CDP neighbors, 159-160

Cisco IOS, 115, 142, 342
checking version, 272
command set, 142-144
abbreviating commands, 153
configuration commands, 145-147
Exec commands, 144-145
router examination commands, 149, 151-153
command summary, 324
AppleTalk commands, 331-332
interface configuration commands, 327-328
IP commands, 328-330
IPX commands, 330-331
miscellaneous commands, 334-335
password configuration commands, 326-327
router examination commands, 324-325
router memory commands, 325-326
router name configuration commands, 326-327
troubleshooting commands, 334
WAN commands, 332-333
Command-Line Interface (CLI), 143, 151
ConfigMaker, 272
copying to Flash RAM, 298-300
Help system, 147-150
loading from TFTP server, 297-298

Cisco routers
assembling, 115
checking your purchase, 115
Cisco 1000 routers, 341
Cisco 2500 routers, 340
Cisco 2505 routers, 112
Cisco 4500 routers, 339-340
Cisco 7500 routers, 338
Cisco IOS, 115, 342
console
connecting, 116-117
terminal emulation, 117-119
CPUs, 113
design, 113
installing, 116
interfaces, 113
memory, 113-114
networks connections, 119-122
ports, 112-113
roll-over cable, 116
selecting, 113, 338
serial adapters, 116
weight, 339

CiscoWorks, 125

CLI (Command-Line Interface), 143, 151

clock, 154

clock rate [clockrate] command, 333

clock set command, 154

coaxial cable, 17-19

command summary, 324
- AppleTalk commands, 331-332
- interface configuration commands, 327-328
- IP commands, 328-330
- IPX commands, 330-331
- miscellaneous commands, 334-335
- password configuration commands, 326-327
- router examination commands, 324-325
- router memory commands, 325-326
- router name configuration commands, 326-327
- troubleshooting commands, 334
- WAN commands, 332-333

Command-Line Interface (CLI), 143, 151

commands, 142-144
- abbreviating, 153
- access-list [list #] deny or permit zone [zone name] command, 331
- access-list [list #] permit or deny -1 -1 command, 330
- access-list [list #] permit or deny cable-range [cable range] command, 331
- access-list [list #] permit or deny [ip address] [wildcard mask] command, 328
- access-list [list #] permit or deny [source network address] [destination network address] command, 330
- appletalk access-group [list #] command, 331
- appletalk cable-range [cable-range number] command, 332
- AppleTalk commands, 331-332
- appletalk routing command, 332
- appletalk zone [zone name] command, 332
- bandwidth [bandwidth] command, 333
- banner motd end character command, 162-163
- banner motd [banner end character] command, 334
- clock rate [clockrate] command, 333
- clock set command, 154
- config command, 136-137, 327
- configuration commands, 145-146
  - *global commands, 146*
  - *port commands, 147*
  - *subcommands, 147*
- copy flash tftp command, 325
- copy running-config startup-config command, 325
- copy startup-config tftp command, 326
- copy tftp flash command, 326
- copy tftp startup-config command, 326
- Ctrl+Z command, 327, 335
- debug appletalk routing command, 318-319
- debug ip igrp events command, 206-207
- debug ip igrp transaction command, 206-207, 328
- debug ip rip command, 204, 328
- debug ipx routing activity command, 224-225, 330
- disable command, 335
- enable command, 335
- enable cdp command, 327
- enable secret password [password] command, 146, 326
- encapsulation [encapsulation type] command, 328
- encapsulation [WAN protocol] command, 333
- erase startup-config command, 128, 326
- Exec commands, 144-145
- frame-relay interface-dlci [dlci #] command, 333
- frame-relay lmi-type [LMI type] command, 333
- Help, 147-150
- history, 156
- hostname [name] command, 146, 326
- interface configuration commands, 327-328
- interface ethernet [interface number] command, 328
- interface serial [interface number] command, 328
- ip access-group [list number] out or in command, 329
- ip address [ip address] [subnet mask] command, 329
- IP commands, 328-330
- ip ospf hello-interval command, 95
- ip routing command, 202, 329

ip subnet-zero command, 192
ip unnumbered [interface or logical interface] command, 329
ipx access-group [list #] in or out command, 330
IPX commands, 330-331
ipx network:ipx network [network number] encapsulation [frame type] command, 331
ipx routing command, 218, 331
isdn spid [spid channel designation] [SPID #] command, 333
isdn switch type basic-[switch identifier] command, 333
line console 0 command, 327
line vty 0 4 command, 327
network [major network number] command, 329
no debug all command, 329
no debug ip rip command, 204
no debug ipx routing activity command, 225, 331
no ip routing command, 202, 329
password configuration commands, 326-327
password [password] command, 327
ping command, 160-161, 314-315, 317-319, 334
quit command, 335
reload command, 128, 335
router examination commands, 324-325
router igrp [autonomous system number] command, 329
router memory commands, 325-326
router name configuration commands, 326-327
router rip command, 329
set clock command, 335
show command, 149-150, 153, 238
show access-list [list #] command, 253, 329, 331
show appletalk commands, 238-240
show appletalk global command, 332
show appletalk interface brief command, 332
show appletalk interface command, 332
show appletalk interface e0 command, 332
show appletalk zone command, 332
show cdp interface command, 157
show cdp neighbor command, 159-160, 324
show cdp neighbor details command, 160
show clock command, 153-154, 324
show controller command, 303-304, 334
show flash command, 156, 324
show frame-relay lmi command, 268, 333
show frame-relay map command, 268, 333
show history command, 153, 325
show hub command, 153, 325
show interface command, 94-95, 101-102, 151-152, 303, 325
show interface ethernet [interface number] command, 325
show interface serial 0 command, 311-313
show interface serial [interface number] command, 260-261, 325
show interface [interface type] [interface number] command, 334
show interfaces ethernet [interface number] command, 308-309
show interfaces tokenring [interface number] command, 310-311
show ip interface [interface type and number] command, 199, 314, 330
show ip protocol command, 204, 330
show ip route command, 203, 206, 314, 330
show ipx interface brief command, 317
show ipx interface command, 222, 331
show ipx route command, 223, 225, 331
show ipx traffic command, 224-225, 331
show processes command, 153, 325
show protocol command, 153, 325
show running-config command, 136, 155-156, 314, 326
show stacks command, 304, 334

show startup-config command, 326
show version command, 153, 272, 325
telnet [ip address] command, 330
trace [ip address] command, 315-316, 334
troubleshooting commands, 334
WAN commands, 332-333
x25 address [data link address] command, 333
x25 ips [bits] command, 333
x25 ops [bits] command, 333
x25 win [number of packets] command, 333
x25 wout [number of packets] command, 333

communication (networks)
connection-oriented communication, 39, 41
connectionless communication, 39, 41
OSI model, 34-35

Communication servers, 11

communications
serial communications
asynchronous, 106
baud rate, 119
data bits, 119
parity, 119
stop bits, 119
synchronous, 106
terminal emulation, 118-119
subnets
between subnets, 81
on the same subnet, 80-81

computers
mainframes
dumb terminals, 8
history of, 8
PCs
history of, 8
IBM Personal Computer, 8
networking, 8-26

concentrators. *See* repeaters.

config command, 136-137, 327

ConfigMaker, 125, 272
Cisco IOS version requirements, 272
delivering configurations to routers, 284-287
downloading, 272-273
exiting, 287
Help, 287
installing, 273-274
internetwork diagrams, 274-276
adding devices, 276-279
connecting LANs to routers, 278-281
connecting routers to routers, 281-284
deleting devices, 278
saving, 286
starting, 274
system requirements, 273
windows
Connection window, 275
Devices window, 275
Network Diagram window, 275
Status bar, 276
Task list, 276
wizards
Address Network Wizard, 274
Deliver Configuration Wizard, 274, 285
Ethernet Wizard, 280

configuration commands, 145-146
global commands, 146
port commands, 147
subcommands, 147

Configuration mode (routers), 134-135, 137-139, 144-147

configurations (routers)
copying, 294-296
saving, 290-291
viewing, 296

configuring
AppleTalk, 232-235
LAN interfaces, 235-236
WAN interfaces, 236
routable protocols, 87
router interfaces, 102
routers, 124
access, 134-139
boot sequence, 126-128
commands, 124
from network management workstation, 125
from router console, 124, 126
from scratch, 128
from TFTP Server, 125
from virtual terminal, 124
importance of correct configuration, 126
interfaces, 132-134
routed protocols, 131-132
routing protocols, 87, 131-132
Setup dialog, 128-134
System Configuration dialog, 127-128
virtual terminal, 124
with Cisco ConfigMaker, 125, 284-287
WAN protocols
Frame Relay, 265-269
HDLC, 261-262

ISDN, 268-270
PPP, 262-263
X.25, 263-265
connecting
routers
to console, 116-117
to network, 119-122
Telnet, 209-210
TFTP servers, 290
WANs, 55
dedicated leased lines, 56-59
dial-up connections, 55
switched networks, 59-62
connection-oriented communication, 39, 41
connectionless communication, 39, 41
connections (networks), 12
cables
copper cables, 17-19
fiber-optic cables, 17-19
guidelines for selecting, 18
hubs, 19-20
MAUs, 20
NICs (network interface cards), 12-13
addresses, 13
I/O ports, 17
installing, 13-15
IRQs, 15-16
network architectures, 14
problems with, 14
slots, 13
repeaters, 20
connections (routers)
checking, 314-316
troubleshooting, 303, 306
console
connecting, 116-117
terminal emulation, 117-119
copper cable, 17-19
copy flash tftp command, 325
copy running-config startup-config command, 325
copy startup-config tftp command, 326
copy tftp flash command, 326
copy tftp startup-config command, 326
copying
IOS to Flash RAM, 298-300
router configurations, 294-296
running configuration, 156
core routers, 96
CPUs, 113
CRC (Cyclical Redundancy Check), 41
Ctrl+Z command, 327, 335
Cyclical Redundancy Check (CRC), 41

D

DARPA (Defense Advanced Research Projects Agency), 48
data bits (serial communications), 119
Data-Link layer (OSI model), 41-43, 45
Logical Link Control (LLC), 43-44
Media Access Control (MAC), 43-44
date (routers), setting, 154
DDS lines, 56-58
debug appletalk routing command, 318-319
debug ip igrp events command, 206-207
debug ip igrp transaction command, 206-207, 328
debug ip rip command, 204, 328
debug ipx routing activity command, 224-225, 330
DECnet, 131
dedicated leased lines, 56
DDS lines, 56-58
T-carrier lines, 56-59
Defense Advanced Research Projects Agency (DARPA), 48
deleting Access lists, 254
deny statements (Access lists), 244-247
designing internetworks
with ConfigMaker, 274-284
with Visio Standard, 319
DHCP servers, 293
diagrams (internetworks), 274-276
adding devices, 276-279
as a troubleshooting tool, 318-319
connections
LANs to routers, 278-281
routers to routers, 281-284
deleting devices, 278
saving, 286
dial-up connections, 55
dialogs
Setup, 128-134
System Configuration, 127-128

Digital Communication Equipment (DCE), 260-261
Digital Equipment Corporation DECnet, 131
Digital Subscriber Line (DSL), 61
Digital Terminal Equipment (DTE), 260-261
disable command, 335
DOS and IRQs, 15
downloading ConfigMaker, 272-273
DSL (Digital Subscriber Line), 61
dumb terminals, 8

E

EGPs (Exterior Gateway Protocols), 93, 95-96
EIGRP (Enhanced Interior Gateway Routing Protocol), 85, 94
email (gateways), 74
enable command, 335
enable cdp command, 327
enable secret password [password] command, 146, 326
Enabled mode (routers). *See* Privileged mode (routers).
encapsulation, 146, 260
encapsulation [encapsulation type] command, 328
encapsulation [WAN protocol] command, 333
Enhanced Interior Gateway Routing Protocol (EIGRP), 85, 94
erase startup-config command, 128, 326
Ethernet, 26-27
  advantages, 28
  disadvantages, 28
  Fast Ethernet, 28, 103
  frame types, 27-28
  Gigabit Ethernet, 28
  IEEE 802.3 specification, 27
  implementations, 27
  router interfaces, 103
  troubleshooting, 307-309
Ethernet frame, 42
  IEEE specifications, 45
  internetworking, 71
  segments, 42
Exec commands, 144-145
exiting ConfigMaker, 287
Exterior Gateway Protocols (EGPs), 93, 95-96
extranets, 50

F

Fast Ethernet, 28, 103
FDDI, 29-30
  router interfaces, 104
  tutorial, 71
Fiber Distributed Data Interface. *See* FDDI.
fiber-optic cables, 17-19
file servers, 11
File Transfer Protocol (FTP), 47, 170, 290
filtering packets with Access lists, 244
  AppleTalk Access lists, 256-258
  building, 246-247, 252-253
  deleting Access lists, 254
  deny statements, 244-247
  grouping to an interface, 253-254
  IP Access lists, 247-254
  IPX Access lists, 254-256
  operation of, 244-246
  permit statements, 244-247
  wildcard masks, 248-252
finding IRQs, 15-16
Flash RAM, 156, 158, 298-300
Frame Relay, 64
  configuring, 265-269
  cost effectiveness of, 260
  serial router interfaces, 107
frame-relay interface-dlci [dlci #] command, 333
frame-relay lmi-type [LMI type] command, 333
FTP (File Transfer Protocol), 47, 170, 290

G-H

gateways
  email, 74
  internetworking, 68-69, 74-75
Global Configuration mode (routers). *See* Configuration mode (routers).
grouping Access lists to interfaces, 253-254

hardware addresses, 45
hardware problems, 302-307

HDLC (High-Level Data Link Control), 65
configuring, 261-262
serial router interfaces, 105-106
Help
Cisco IOS, 147-150
ConfigMaker, 287
Hewlett Packard and HP OpenView, 125
High-Level Data Link Control (HDLC), 65
configuring, 261-262
serial router interfaces, 105-106
history of commands, 156
hostname [name] command, 146, 326
HP OpenView, 125
hubs, 19-20
hybrid topologies (networks), 26
Hyper-RFC Web site, 172
HyperTerminal, 117

I-J

I/O ports (NICs), 17
IBM
Personal Computer, 8
Web address, 71, 311
IBM Token Ring, 28-29
beaconing, 29
IEEE 802.5 specification, 28
router interfaces, 103-104
troubleshooting, 309-311
ICMP (Internet Control Message Protocol), 172
IEEE (Institute for Electrical and Electronic Engineers), 45
802 specifications, 43-44, 47
Ethernet frame specifications, 45
IETF (Internet Engineering Task Force), 95
IGPs (Interior Gateway Protocols), 92-95
IGRP (Interior Gateway Routing Protocol), 93-95, 204-207
installing
Cisco TFTP server software, 292-294
ConfigMaker, 273-274
network interface cards (NICs), 13-15
routers, 116
Institute for Electrical and Electronic Engineers (IEEE), 45
802 specifications, 43-44, 47
Ethernet frame specifications, 45
Integrated Services Digital Network (ISDN), 60
basic rate ISDN, 61
configuring, 268-270
primary rate ISDN, 61
serial router interfaces, 107-108
interface configuration commands, 327-328
interface ethernet [interface number] command, 328
interface serial [interface number] command, 328
interfaces
Command-Line Interface (IOS), 143, 151
LAN interfaces, 102-105, 307-311
router interfaces, 100-101, 113
Access lists, 246-247, 253-254
configuration commands, 327-328
configuring, 102
IP addresses, 196-201
IPX routing, 219-223
LAN interfaces, 102-105
logical interfaces, 108-110
MAC addresses, 104
router configuration, 132-134
serial interfaces, 104-108
viewing, 101-102
serial interfaces, 260
encapsulation, 260
Frame Relay, 260, 265-269
HDLC, 261-262
ISDN, 268-270
PPP, 262-263
X.25, 263-265
WAN interfaces, 260
tips for selecting, 260
troubleshooting, 311-313
Interior Gateway Protocols (IGPs), 92-95
Interior Gateway Routing Protocol (IGRP), 93-95, 204-207
International Standards Organization (ISO)
ISO 9002, 34
ISO 9660, 34
Open Systems Interconnection Reference Model, 34

Internet, 50, 68

Internet Control Message Protocol (ICMP), 172

Internet Engineering Task Force (IETF), 95

Internet Protocol (IP), 47, 172

Internetwork, 50

Internetwork Packet Exchange Protocol (IPX), 49, 213, 316-317

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX), 48-49

internetworking, 68-69
- bridges, 68, 71-72
- campus networks, 75
- cost-saving tips, 55
- Ethernet frame, 71
- expansion, 68
- gateways, 68-69, 74-75
- Internet, 68
- repeaters, 68-70, 72
- routers, 68, 73-74
- segmentation, 68
- switches, 68, 73

Internetworking Operating System (IOS), 142
- command set, 142-144
  - *abbreviating commands, 153*
  - *configuration commands, 145-147*
  - *Exec commands, 144-145*
  - *router examination commands, 149, 151-153*
- Command-Line Interface (CLI), 143, 151
- Help, 147-150

internetworks, 11
- designing
  - *with ConfigMaker, 274-284*
  - *with Visio Standard, 319*
- neighbors, 157-160
  - *pinging, 160-161*
  - *viewing, 159-160*

Interrupt ReQuests (IRQs), 15
- finding, 15-16
- settings, 16

intranets, 50

IOS, 142
- checking version, 272
- command set, 142-144
  - *abbreviating commands, 153*
  - *configuration commands, 145-147*
  - *Exec commands, 144-145*
  - *router examination commands, 149, 151-153*
- command summary, 324
  - *AppleTalk commands, 331-332*
  - *interface configuration commands, 327-328*
  - *IP commands, 328-330*
  - *IPX commands, 330-331*
  - *miscellaneous commands, 334-335*
  - *password configuration commands, 326-327*
  - *router examination commands, 324-325*
  - *router memory commands, 325-326*
  - *router name configuration commands, 326-327*
  - *troubleshooting commands, 334*
  - *WAN commands, 332-333*
- Command-Line Interface (CLI), 143, 151
- ConfigMaker, 272
- copying to Flash RAM, 298-300
- Help system, 147-150
- loading from TFTP server, 297-298

IP (Internet Protocol), 47, 172

IP Access lists, 247-249, 314
- creating, 252-253
- deleting, 254
- grouping to an interface, 253-254
- wildcard masks, 249-252

ip access-group [list number] out or in command, 329

ip address [ip address] [subnet mask] command, 329

IP addresses, 47, 174
- classes, 175-177
- cost, 176
- DHCP servers, 293
- obtaining, 176
- purpose of, 174-175
- router interfaces, 196-198
  - *LAN interfaces, 198-200*
  - *viewing, 199*
  - *WAN interfaces, 200-201*
- subnet masks, 178-181
- subnetting, 180-181
  - *binary and decimal conversions, 181-182*
  - *calculating available node addresses, 188*
  - *calculating IP subnet ranges, 186-188*
  - *Class A subnets, 182-188, 194*
  - *Class B subnets, 188-190, 194*
  - *Class C subnets, 190-193*

network subnet mask creation, 184-186
subnet creation, 182-184
subnet O, 192-193
TFTP servers, 290
written forms, 174, 177-179

IP commands, 328-330

IP datagrams, 171

ip ospf hello-interval command, 95

IP routing, 196-197
configuring routing protocols, 201-207
disabling, 202
dynamic routing, 207-209
enabling, 202
LANs, 198-200
static routing, 207-209
Telnet, 209-210
WANs, 200-201

ip routing command, 202, 329

ip subnet-zero command, 192

ip unnumbered [interface or logical interface] command, 329

IPX (Internetwork Packet Exchange), 49, 213, 316-317

IPX Access lists
creating, 254-256
grouping, 255-256

ipx access-group [list #] in or out command, 330

IPX addresses, 214-216

IPX commands, 330-331

ipx network:ipx network [network number] encapsulation [frame type] command, 331

IPX routing
configuring, 217-219
monitoring, 223-225
router interfaces, 219-223

ipx routing command, 218, 331

IPX/SPX, 212
as a routable protocol, 85
protocol stack, 48-49
protocols
IPX (Internetwork Packet Exchange), 213
NetWare Core Protocol (NCP), 213
NetWare VLMs (Virtual Loadable Modules), 213
NLSP (NetWare Link Services Protocol), 214
RIP (Routing Information Protocol), 213
SAP (Service Advertisement Protocol), 213-214, 216-217
SPX (Sequence Packet Exchange), 213

IRQs, 15
finding, 15-16
settings, 16

ISDN (Integrated Services Digital Network), 60
basic rate ISDN, 61
configuring, 268-270
primary rate ISDN, 61
serial router interfaces, 107-108

isdn spid [spid channel designation] [SPID #] command, 333

isdn switch type basic-[switch identifier] command, 333

ISO (International Standards Organization)
ISO 9002, 34
ISO 9660, 34
Open Systems Interconnection Reference Model, 34

K-L

LAN interfaces, 102-105
AppleTalk, 235-236
IP addresses, 198-200
troubleshooting, 307-311

LANs, 11
campuses, 11
internetworking, 68-69
bridges, 68, 71-72
Ethernet frame, 71
expansion, 68
gateways, 68-69, 74-75
repeaters, 68-70, 72
routers, 68, 73-74
segmentation, 68
switches, 68, 73
internetworks, 11

layers
NetBEUI, 45
OSI model, 34-35
Application layer, 35, 38, 40
data movement through, 36-39
Data-Link layer, 41-45
mnemonic, 36
Network layer, 40
numbering of, 36
Physical layer, 35, 43
Presentation layer, 38, 40
Session layer, 38-39, 41
Transport layer, 40

TCP/IP, 45-46, 49
ARP, 47
FTP, 47
IP, 47
IP addresses, 47
SMTP, 47
TCP, 47
UDP, 47

layers. *See also* protocol stack.

leased lines, 56
DDS lines, 56-58
T-carrier lines, 56-59

line console 0 command, 327

line vty 0 4 command, 327

loading Cisco IOS from a TFTP server, 297-298

local area networks (LANs), 11
campuses, 11
internetworking, 68-69
bridges, 68, 71-72
Ethernet frame, 71
expansion, 68
gateways, 68-69, 74-75
repeaters, 68-70, 72
routers, 68, 73-74
segmentation, 68
switches, 68, 73
internetworks, 11

LocalTalk, 30

logical router interfaces, 108
Loopback interface, 108-109
Null interface, 109
Tunnel interface, 109-110

Loopback logical router interface, 108-109

M

MAC addresses, 45
finding, 43
router LAN interfaces, 104
routing, 175

Macintosh networks
AppleTalk, 30-31, 228
addressing, 229-232
configuring, 232-236
monitoring, 237-240
network interface cards, 228
phases of, 230
protocols, 49-51, 228-229
resources, 232
zones, 232-233
LocalTalk, 30

mainframes
dumb terminals, 8
history of, 8

major network addresses, 192

maps (internetworks), 274-276
adding devices, 276-279
as a troubleshooting tool, 318-319
connections
LANs to routers, 278-281
routers to routers, 281-284
deleting devices, 278
saving, 286

MAUs, 20

Media Access Control (MAC) addresses, 43, 45

memory, 113-114
checking, 154-156, 158
Flash RAM, 114, 156, 158
NVRAM, 114
RAM, 114
role of, 114
ROM, 114
router memory commands, 325-326

mesh topology (networks), 25

Microsoft Windows 3.11
IRQs, 15
peer-to-peer networking capabilities, 9

Microsoft Windows 95/98
IRQs, 15
peer-to-peer networking capabilities, 9

Microsoft Windows NT Server, 11, 16

Microsoft Windows NT Workstation
IRQs, 16
peer-to-peer networking capabilities, 90

model network (OSI), 34
layers, 34-45
network communication, 34-35
protocol stacks, 34-35

modems, 56

modes (routers), 134
Configuration mode, 134-135, 137-139, 144-147
Privileged mode, 134-137, 144, 153-154
ROM Monitor mode, 134
RXBoot mode, 134
User mode, 134-136, 144

monitoring
AppleTalk routing, 237-240
IPX routing, 223-225

multiport repeaters, 72

multistation access units (MAUs), 20

N

naming routers, 129
NCP (NetWare Core Protocol) (IPX/SPX), 49, 213
neighbors, 157-160
pinging, 160-161
viewing, 159-160
NetBEUI
as a routable protocol, 85
protocol stack, 45
NetBIOS Extended User Interface. *See* NetBEUI.
NetWare (Novell), 212
Ethernet frame, 45
IPX/SPX, 48-49, 212
IPX, 49
NCP, 49
SAP, 49
SPX, 49
NetWare Core Protocol (NCP) (IPX/SPX), 49, 213
NetWare Link Services Protocol (NLSP), 214
NetWare VLMs (Virtual Loadable Modules), 213
network addresses, 192
network cards, 41, 43
network communication
connection-oriented communication, 39, 41
connectionless communication, 39, 41
OSI model, 34-35
network interface cards (NICs), 12-13
addresses, 13, 41, 43
AppleTalk, 228
I/O ports, 17
installing, 13-15
IRQs, 15-16
network architectures, 14
problems with, 14
slots, 13
Network layer (OSI model), 40
network operating systems (NOS), 11, 168
network protocols
AppleTalk, 85, 228-240
IPX/SPX, 85, 212-214, 216-217
NetBEUI, 85
routing, 103
TCP/IP, 85
network [major network number] command, 329
networks
architectures, 25
AppleTalk, 30-31
Ethernet, 26-28, 103
Fast Ethernet, 103
FDDI, 29-30, 104
IBM Token Ring, 28-29, 103-104
NICs (network interface cards), 14
campus networks, 75
connections, 12
cables, 17-19
hubs, 19-20
I/O ports, 17
IRQs, 15-16
MAUs, 20
NICs (network interface cards), 12-15
repeaters, 20
extranets, 50
Internet, 50
Internetwork, 50
intranets, 50
LANs, 11
campuses, 11
internetworking, 68-75
internetworks, 11
Macintosh networks, 49-51
PC networks, 9
benefits, 8
connections, 12-20
models, 8-12
topologies, 20-26
peer-to-peer networks, 8-9
administration, 10
drawbacks, 10
security, 10
protocol stacks, 34-35, 168-173
routers, 78
connecting, 119-122
interfaces, 100-110
network protocols, 103
routing data, 78
AppleTalk. See AppleTalk.
IP routing, 196-210
IPX routing, 217-225
packet switching, 81-82
packets, 78
path determination, 78-80
subnet communication, 80-81
subnets, 78-81
server-based networks, 9-11
drawbacks, 12
LANs, 11
server types, 11
WANs, 11
subnets, 78-81
topologies, 20-21
bus topology, 21-22
hybrid topologies, 26
mesh topology, 25
ring topology, 23-25
star topology, 22-23

WANs, 11, 54
connections, 55-62
cost-saving tips, 55
wireless technologies, 54

NICs (network interface cards), 12-13
addresses, 13, 41, 43
AppleTalk, 228
I/O ports, 17
installing, 13-15
IRQs, 15-16
network architectures, 14
problems with, 14
slots, 13

NLSP (NetWare Link Services Protocol), 214

no debug all command, 329

no debug ip rip command, 204

no debug ipx routing activity command, 225, 331

no ip routing command, 202, 329

NOS (network operating systems), 11, 168

Novell NetWare, 11, 212
Ethernet frame, 45
IPX/SPX, 48-49, 212

Null logical router interface, 109

O

Ohio State RFC Repository Web site, 172

Open Shortest Path First (OSPF), 85, 95

Open Systems Interconnection Reference Model, 34
layers, 34-35
Application layer, 35, 38, 40
data movement through, 36-39
Data-Link layer, 41-45
mnemonic, 36
Network layer, 40
numbering of, 36
Physical layer, 35, 43
Presentation layer, 38, 40
Session layer, 38-39, 41
Transport layer, 40
network communication, 34-35
protocol stacks, 34-35

OSI model, 34
layers, 34-35
Application layer, 35, 38, 40
data movement through, 36-39
Data-Link layer, 41-45
mnemonic, 36
Network layer, 40
numbering of, 36
Physical layer, 35, 43
Presentation layer, 38, 40
Session layer, 38-39, 41
Transport layer, 40
network communication, 34-35
protocol stacks, 34-35
TCP/IP, 168-169, 173

OSPF (Open Shortest Path First), 85, 95

P

Packet InterNet Groper (Ping), 160-161

packet switching WANs, 61-62
ATM (Asynchronous Transfer Mode), 64-65
frame relay, 64
HDLC, 65
PPP, 65
X.25, 62-64

packets
filtering with Access lists, 244
AppleTalk Access lists, 256-258
building, 246-247, 252-253
deleting Access lists, 254
deny statements, 244-247
grouping to an interface, 253-254
IP Access lists, 247-254
IPX Access lists, 254-256
operation, 244-246
permit statements, 244-247
wildcard masks, 248-252
routing, 78
path determination, 78-80
subnet communication, 80-81
switching, 78, 81-82

parity (serial communications), 119

password configuration commands, 326-327

password [password] command, 327

passwords
configuration commands, 326-327
routers, 130
enable password, 138
login password, 138

lost passwords, 139
virtual terminal password, 139
history of, 8
IBM Personal Computer, 8
networking
benefits, 8
connections, 12-20
models, 8-12
topologies, 20-26

peer-to-peer networks, 8-9
administration, 10
drawbacks, 10
security, 10

permit statements (Access list), 244-247

personal computers. ***See*** **PCs.**

Physical layer (OSI model), 35, 43

ping command, 160-161, 314-315, 317-319, 334

Plain Old Telephone System (POTS), 57

Point to Point Protocol (PPP)
configuring, 262-263
serial router interfaces, 106

ports
I/O ports (NICs), 17
routers, 100-101, 112-113
configuring, 102
viewing, 101-102

POTS (Plain Old Telephone System), 57

PPP (Point to Point Protocol), 65
configuring, 262-263
serial router interfaces, 106

Presentation layer (OSI model), 38, 40

print servers, 11

Privileged mode (routers), 134-137, 144, 153-154

ProComm Plus, 117

protocol stacks, 34-35, 44
AppleTalk, 49-50
AARP, 50
AFP, 50
AppleShare, 50
ATP, 50
DDP, 51
NBP, 50
ZIP, 50
ATM (Asynchronous Transfer Mode), 64-65
frame relay, 64
HDLC, 65
IPX/SPX, 48-49
NetBEUI, 45
OSI protocol stack, 35
PPP, 65
TCP/IP, 45-46, 49
ARP, 47
FTP, 47
Internet, 50
IP, 47
IP addresses, 47
SMTP, 47
TCP, 47
UDP, 47
X.25, 62-64
LAP/B, 63
PLP, 62-63
virtual circuits, 64
x.21bis, 63
See also layers.

protocols
network protocols
AppleTalk, 85, 228-240
IPX/SPX, 85, 212-214, 216-217
NetBEUI, 85
routing, 103
TCP/IP, 85, 168-173
routable protocols, 84-85
AppleTalk, 228-240
configuring, 87, 131-132
routing protocols, 84-85
algorithms, 87-91
areas, 91
Border Gateway Protocol (BGP), 95-96
configuring, 87
EIGRP (Enhanced Interior Gateway Routing Protocol), 85, 94
hybrid routing protocols, 90
IGRP (Interior Gateway Routing Protocol), 93-95
Interior Gateway Protocols (IGPs), 92-95
IP routing, 201-207
operation of, 85-86
OSPF (Open Shortest Path First), 85, 95
purpose of, 85, 87
RIP (Routing Information Protocol), 85, 93
router configuration, 131-132
routing domain, 91-92
WAN protocols
configuring, 261-270
Frame Relay, 107, 260, 265-269
HDLC, 105-106, 261-262
ISDN, 107-108, 268-270
PPP, 106, 262-263
X.25, 106-107, 263-265

PSTN (Public Switched Telephone Network), 57

Public Switched Telephone Network. ***See*** **PSTN.**

Q-R

quit command, 335

reload command, 128, 335

renaming routers, 138

repeaters, 20, 68-70, 72

ring topology (networks), 23-25

RIP (Routing Information Protocol), 85, 93, 202-204, 213

ROM Monitor mode (routers), 134

routable protocols, 84-85
AppleTalk, 228-240
configuring, 87, 131-132

router console, 124, 126

router examination commands, 149, 151-153, 324-325

router igrp [autonomous system number] command, 329

router interfaces, 75

router memory commands, 325-326

router name configuration commands, 326-327

router rip command, 329

routers, 78
assembling, 115
banners, 161-163
boot sequence, 126-128
border routers, 96
broadcast storms, 73
Cisco routers
checking your purchase, 115
Cisco 1000 routers, 341
Cisco 2500 routers, 340
Cisco 2505 routers, 112
Cisco 4500 routers, 339-340
Cisco 7500 routers, 338
Cisco IOS, 115, 342
selecting, 338
weight, 339
clock, 154
configurations
copying, 294-296
saving, 290-291
viewing, 296
configuring, 124
access, 134-139
boot sequence, 126-128
commands, 124
from network management workstation, 125
from router console, 124, 126
from scratch, 128
from TFTP Server, 125
from virtual terminal, 124
importance of correct configuration, 126
interfaces, 132-134
routed protocols, 131-132
routing protocols, 131-132
Setup dialog, 128-134
System Configuration dialog, 127-128
virtual terminal, 124
with Cisco ConfigMaker, 125, 284-287
connections, 116-122
checking, 314-316
Telnet, 209-210
terminal emulation, 117-119
convergence, 88
core routers, 96
CPUs, 113
date settings, 154
design, 113
Digital Communication Equipment (DCE), 261
Digital Terminal Equipment (DTE), 260-261
installing, 116
interfaces, 100-101, 113
Access lists, 246-247, 253-254
configuration commands, 327-328
configuring, 102
IP addresses, 196-201
IPX routing, 219-223
LAN interfaces, 102-105
logical interfaces, 108-110
MAC addresses, 104
router configuration, 132-134
serial interfaces, 104-108
viewing, 101-102
internetworking, 68, 73-74
memory, 113-114
checking, 154-156, 158
Flash RAM, 114, 156, 158
NVRAM, 114
RAM, 114
role of, 114
ROM, 114
modes, 134
Configuration mode, 134-135, 137-139, 144-147
Privileged mode, 134-137, 144, 153-154
ROM Monitor mode, 134
RXBoot mode, 134
User mode, 134-136, 144
naming, 129
neighbors, 157-160
pinging, 160-161
viewing, 159-160
network protocols, 103
networks connections, 119-122

passwords, 130
enable password, 138
login password, 138
lost passwords, 139
virtual terminal password, 139
ports, 100-101, 112-113
configuring, 102
viewing, 101-102
renaming, 138
roll-over cable, 116
routing tables, 82-84
running configuration
copying, 156
purpose of, 155
saving, 200
testing, 157
viewing, 155
selecting, 113
serial adapters, 116
slots, 262
time settings, 154
traffic flow, 244-258
troubleshooting
AppleTalk, 317-319
cable problems, 306
connections, 303, 306
hardware problems, 302-307
IPX, 316-317
LAN interfaces, 307-311
network maps, 318-319
TCP/IP, 313-316
tips for approaching, 305
WAN interfaces, 311-313
VIP cards, 102

routing data, 78
AppleTalk. *See* AppleTalk.
IP routing, 196-197
configuring routing protocols, 201-207
disabling, 202
dynamic routing, 207-209
enabling, 202
LANs, 198-200
static routing, 207-209
Telnet, 209-210
WANs, 200-201
IPX routing
configuring, 217-219
monitoring, 223-225
router interfaces, 219-223
switching, 81-82
MAC addresses, 175
path determination, 78-80
subnet communication, 80-81
subnets, 78-81

Routing Information Protocol (RIP), 85, 93, 213

routing protocols, 84-85
algorithms, 87
distance vector, 88-90
dynamic, 88-89
link state, 88-89
metrics, 89-91
static, 87, 89
areas, 91
Border Gateway Protocol (BGP), 95-96
configuring, 87
EIGRP (Enhanced Interior Gateway Routing Protocol), 85, 94
Exterior Gateway Protocols (EGPs), 93, 95-96
hybrid routing protocols, 90
IGRP (Interior Gateway Routing Protocol), 93-95
Interior Gateway Protocols (IGPs), 92-95
IP routing, 201-207
operation of, 85-86
OSPF (Open Shortest Path First), 85, 95
purpose of, 85, 87
RIP (Routing Information Protocol), 85, 93
router configuration, 131-132
routing domain, 91-92

routing tables, 82-84

running configurations
copying, 156
purpose of, 155
saving, 200
testing, 157
viewing, 155

RXBoot mode (routers), 134

S

SAP (Service Advertisement Protocol) (IPX/SPX), 49, 213-214, 216-217

saving
internetwork diagrams, 286
router configurations, 290-291
running configurations, 200

security
networks, 10
share-level security, 10

Sequenced Packet Exchange (SPX) (IPX/SPX), 49, 213

serial communications
asynchronous, 106
baud rate, 119
data bits, 119
parity, 119
stop bits, 119
synchronous, 106
terminal emulation, 119
terminal emulation software, 118

serial interfaces, 104-108, 260
encapsulation, 260
Frame Relay, 260, 265-269
HDLC, 261-262
ISDN, 268-270
PPP, 262-263
X.25, 263-265
server-based networks, 9-11
drawbacks, 12
LANs, 11
server types, 11
WANs, 11
servers
application servers, 11
Communication servers, 11
DHCP servers, 293
file servers, 11
print servers, 11
TFTP servers
connecting, 290
copying a new IOS to Flash RAM, 298-300
copying router configurations from, 295-296
copying router configurations to, 294-295
IP addresses, 290
loading a new IOS from, 297-298
locating on network, 297
router configuration, 125
saving router configurations to, 290-291
software, 291-294
viewing router configurations, 296
Service Advertisement Protocol (SAP) (IPX/SPX), 49, 213-214, 216-217
Session layer (OSI model), 38-39, 41
set clock command, 335
share-level security, 10
show command, 149-150, 153, 238
show access-list [list #] command, 253, 329, 331
show appletalk commands, 238-240
show appletalk global command, 332
show appletalk interface brief command, 332
show appletalk interface command, 332
show appletalk interface e0 command, 332
show appletalk zone command, 332
show cdp interface command, 157
show cdp neighbor command, 159-160, 324
show cdp neighbor details command, 160
show clock command, 153-154, 324
show controller command, 303-304, 334
show flash command, 156, 324
show frame-relay lmi command, 268, 333
show frame-relay map command, 268, 333
show history command, 153, 325
show hub command, 153, 325
show interface command, 94-95, 101-102, 151-152, 303, 325
show interface ethernet [interface number] command, 325
show interface serial 0 command, 311-313
show interface serial [interface number] command, 260-261, 325
show interface [interface type] [interface number] command, 334
show interfaces ethernet [interface number] command, 308-309
show interfaces tokenring [interface number] command, 310-311
show ip interface [interface type and number] command, 199, 314, 330
show ip protocol command, 204, 330
show ip route command, 203, 206, 314, 330
show ipx interface brief command, 317
show ipx interface command, 222, 331
show ipx route command, 223, 225, 331
show ipx traffic command, 224-225, 331
show processes command, 153, 325
show protocol command, 153, 325

show running-config command, 136, 155-156, 314, 326
show stacks command, 304, 334
show startup-config command, 326
show version command, 153, 272, 325
Simple Mail Transport Protocol (SMTP), 47, 170
Simple Network Management Protocol (SNMP), 130, 170
slots, 262
SMTP (Simple Mail Transport Protocol), 47, 170
SNMP (Simple Network Management Protocol), 130, 170
software
terminal emulation software, 116
HyperTerminal, 117
ProComm Plus, 117
serial communications, 118
Tera Term Pro, 117-119
TFTP servers
installing, 292-294
sources, 291-292
SolarWinds, 291
SPX (Sequenced Packet Exchange) (IPX/SPX), 49, 213
star topology (networks), 22-23
starting ConfigMaker, 274
statements (Access lists)
deny statements, 244-247
permit statements, 244-247
stop bits (serial communications), 119
subnet masks (IP addresses), 178-181
subnets, 78-81
subnetting IP addresses, 180-181
binary and decimal conversions, 181-182
calculations
available node addresses, 188
IP subnet ranges, 186-188
Class A subnets, 182-188, 194
Class B subnets, 188-190, 194
Class C subnets, 190-193
network subnet mask creation, 184-186
subnet creation, 182-184
subnet O, 192-193
suites. *See* protocol stacks.
switched networks (WANs), 59-60
circuit switching, 60-61
packet switching, 61-65
cut-through switches, 73
internetworking, 68, 73
store-and-forward switches, 73
switching packets, 78, 81-82
synchronous serial communications, 106
System Configuration dialog, 127-128

T

T-1 lines, 56-59
T-carrier lines, 56-59
TCP (Transport Control Protocol), 47, 171
TCP/IP, 168
Application layer, 170
FTP (File Transfer Protocol), 47, 170
SMTP (Simple Mail Transport Protocol), 47, 170
SNMP (Simple Network Management Protocol), 130, 170
Telnet, 170, 209-210
TFTP (Trivial File Transfer Protocol), 170
as a routable protocol, 85
DOD model, 168-169, 173
history, 48
Host-to-Host layer, 171
TCP (Transport Control Protocol), 47, 171
UDP (User Datagram Protocol), 47, 171
Internet, 50
Internet layer, 171
ARP (Address Resolution Protocol), 47, 172
ICMP (Internet Control Message Protocol), 172
IP (Internet Protocol), 47, 172
Network Access layer, 172-173
OSI Model, 168-169, 173
protocol stack, 45-47, 49
RFC (Request for Comments, 172
software platforms, 46
troubleshooting, 313-316

Telnet, 170, 209-210

telnet [ip address] command, 330

Tera Term Pro, 117-119

terminal emulation (serial communications), 119

terminal emulation software, 116
- HyperTerminal, 117
- ProComm Plus, 117
- serial communications, 118
- Tera Term Pro, 117-119

testing
- cables
  - *time domain reflectometer (TDR), 306*
  - *voltmeter, 306*
- running configurations, 157

TFTP (Trivial File Transfer Protocol), 170, 290

TFTP servers
- connecting, 290
- copying
  - *a new IOS to Flash RAM, 298-300*
  - *router configurations from, 295-296*
  - *router configurations to, 294-295*
- IP addresses, 290
- loading a new IOS from, 297-298
- locating on network, 297
- router configuration, 125
- saving router configurations to, 290-291
- software
  - *installing, 292-294*
  - *sources, 291-292*
- viewing copied router configurations, 296

Thicknet cable, 17-19

Thinnet cable, 18-19

time, setting, 154

Token Ring, 28-29
- beaconing, 29
- IEEE 802.5 specification, 28
- router interfaces, 103-104
- troubleshooting, 309-311

topologies of networks, 20-21
- bus topology, 21-22
- hybrid topologies, 26
- mesh topology, 25
- ring topology, 23-25
- star topology, 22-23

trace [ip address] command, 315-316, 334

traffic flow (Access lists), 244
- AppleTalk Access lists, 256-258
- building, 246-247, 252-253
- deleting, 254
- deny statements, 244-247
- grouping to an interface, 253-254
- IP Access lists, 247-254
- IPX Access lists, 254-256
- permit statements, 244-247
- wild card masks, 248-252

Transmission Control Protocol/Internet Protocol. ***See*** **TCP/IP.**

Transport Control Protocol (TCP), 47, 171

Transport layer (OSI model), 40

Trivial File Transfer Protocol (TFTP), 170, 290

troubleshooting
- AppleTalk, 317-319
- cable problems, 306
- commands, 334
- connections, 303, 306
- hardware problems, 302-307
- IPX, 316-317
- LAN interfaces, 307-311
- network interface cards (NICs), 14
- network maps, 318-319
- TCP/IP, 313-316
- tips for approaching, 305
- WAN interfaces, 311-313

Tunnel logical router interface, 109-110

U

UDP (User Datagram Protocol), 47, 171

User Datagram Protocol. ***See*** **UDP.**

User mode (routers), 134-136, 144

V

Versatile Interface Processor (VIP) cards, 102

viewing
- neighbors, 159-160
- router configurations, 296
- router interfaces, 101-102
- running configuration, 155

VIP (Versatile Interface Processor) cards, 102

Visio Standard, 319

W

WAN commands, 332-333
WANs, 11, 54
connections, 55
dedicated leased lines, 56-59
dial-up connections, 55
switched networks, 59-62
cost-saving tips, 55
interfaces, 260
AppleTalk, 236
IP addresses, 200-201
tips for selecting, 260
troubleshooting, 311-313
protocols
Frame Relay, 107, 260, 265-269
HDLC, 105-106, 261-262
ISDN, 107-108, 268-270
PPP, 106, 262-263
X.25, 106-107, 263-265
wireless technologies, 54
Web sites
American Registry for Internet Numbers, 176
Cisco, 104, 113, 273, 342
FTP sites, 290
Hyper-RFC, 172
IBM, 71, 311
Ohio State RFC Repository, 172
SolarWinds, 291
Wide Area Networks. ***See*** **WANs.**
wildcard masks (Access lists), 249-252
Windows 3.11. ***See*** **Microsoft Windows 3.11.**
Windows 95/98. ***See*** **Microsoft Windows 95/98.**
Windows NT Server. ***See*** **Microsoft Windows NT Server.**
Windows NT Workstation. ***See*** **Microsoft Windows NT Workstation.**
wireless technologies and WANs, 54
workstation and router configurations, 125

X-Y-Z

X.25
configuring, 263-265
protocol stack, 62-64
LAP/B (Link Access Procedure/Balanced Protocol), 63
PLP (Packet Layer Protocol), 62-63
virtual circuits, 64
X.21bis, 63
serial router interfaces, 106-107
x25 address [data link address] command, 333
x25 ips [bits] command, 333
x25 ops [bits] command, 333
x25 win [number of packets] command, 333
x25 wout [number of packets] command, 333
Xerox, 213
XNS (Xerox Network Systems), 213

Other Related Titles

Practical Network Cabling
Frank Derfler and Les Freed
ISBN: 0-7897-2247-X
$29.99 US/$44.95 CAN

Upgrading and Repairing PCs, Eleventh Edition
Scott Mueller
ISBN: 0-7897-1903-7
$59.99 US/$89.95 CAN

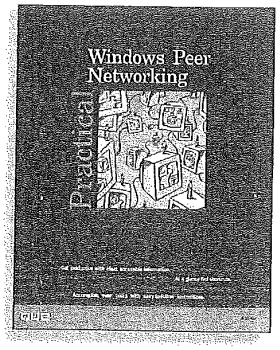
Terabit Networks: The Next Infrastructure
Marcus Goncalves
ISBN: 0-7897-2139-2
$39.99 US/$59.95 CAN

Deploying and Supporting Internetworking Services in Windows 2000
James Ramsey
ISBN: 0-7897-2230-5
$39.99 US/$59.95 CAN

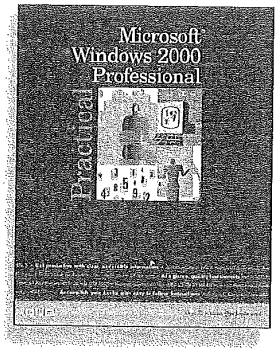
Upgrading and Repairing Networks, Second Edition
Terry Ogletree
ISBN: 0-7897-2034-5
$49.99 US/$74.95 CAN

que®

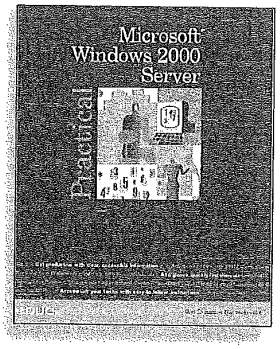
www.quecorp.com



Practical Windows Peer Networking
Jerry Ford
ISBN: 0-7897-2233-X
$29.99 US/
$44.95 CAN



Practical Microsoft Windows 2000 Professional
Ed Bott
ISBN: 0-7897-2124-4
$24.99 US/
$37.95 CAN



Practical Microsoft Windows 2000 Server
Robert Reinstein
ISBN: 0-7897-2141-4
$29.99 US/
$44.95 CAN

All prices are subject to change.

Cisco Routers

Practical

Practical Cisco Routers is an excellent primer and useful reference that tells you only what you need to know about a number of networking technologies that are making their mark on the information technology world. This book provides the basics of LANs, WANs, and routing technology and helps you understand how Cisco routers and the Cisco Internetworking Operating System (IOS) fit into the picture. Using a conversational approach that includes step-by-step instruction for the most commonly used features, easy-to-implement tips, and task-based solutions, *Practical Cisco Routers* is an indispensable tool for those new to internetworking technology and those who wish to review the different aspects of working with Cisco routers.

- Review the basics of LANs, WANs, and internetworking technology
- Learn how routers work and explore Cisco router hardware
- Configure a router using the Cisco IOS
- Learn how to route popular LAN protocols such as TCP/IP, IPX/SPX, and AppleTalk®
- Work with Cisco's ConfigMaker software to configure a new router
- Learn basic troubleshooting techniques and commands to keep your routed networks up and running
- Learn about the Open Systems Interconnection (OSI) Reference Model and how it relates to real-world networking protocols such as TCP/IP and IPX/SPX

Joe Habraken is an information technology professional with more than 15 years experience as an author, consultant, and instructor. A Microsoft® Certified Professional, he currently provides consulting services in the networking arena to various companies and organizations. Joe serves as the lead instructor for the Networking Technologies program at Globe College in St. Paul, Minnesota, where his Windows NT® Server courses and popular Cisco Routers courses are highly attended by both networking students and IT professionals.

$29.99 USA / $44.95 CAN / £21.99 Net UK

ISBN 0-7897-2100-1

Category	Networking
Covers	Cisco Routers
User Level	Beginning-Intermediate

que®

www.quecorp.com