WANs and Routers

Objectives

Upon completion of this chapter, you should be able to answer the following questions:

- Which four groups of industry professionals create the rules and standards that allow wide-area networks (WANs) to work together?

- How do WANs and LANs differ?

- What is the main purpose of a LAN?

- Why were WANs developed?

- What are three types of WAN connections (encapsulations)?

- Where do WANs and LANs operate on the OSI model?

- What devices are used in LANs? In WANs?

- Why is a LAN faster than a WAN?

- How do routers work in LANs and WANs?

- What are the main components of a router, and what tasks do they perform?

- What are the most common interface connections on routers, and how are they used?

- What are six types of serial encapsulations used on routers?

- What kinds of cables are used to connect routers to other routers on serial and Ethernet links?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary:

continued

This chapter begins the Cisco Networking Academy Program's CCNA 2 curriculum. The CCNA 2 course and book focus almost entirely on routers—what they are, what they are capable of doing, how to tell them specifically what to do, and how to find out if they are doing their jobs correctly.

This chapter introduces routers, focusing on how routers forward packets between different LANs by using wide-area networks (WANs). The first section of this chapter begins with a review of the basics of how routers route IP packets. As the chapter continues, the text takes a closer look at the WAN links used by routers to forward packets. The second major section of this chapter then moves the focus to the physical components of an internetwork with routers and WAN links, taking a look at the internal and external components of routers, and some details about how to connect cables to routers.

Introduction to Routing Over WANs

The most important function of a *router* is simply put:

> Routers route packets.

This one seemingly simple statement summarizes the most important function of a router—namely, the routing, or forwarding, of IP packets. Although Chapter 10, "Routing Fundamentals and Subnets," of *Networking Basics CCNA 1 Companion Guide* (and the corresponding module of the Networking Basics CCNA 1 online curriculum) covered IP routing in some detail, a brief review of routing is helpful as you begin to learn more about router hardware and software.

From the perspective of the OSI network layer—Layer 3—hosts (computers) and routers work together to deliver packets from one host to another. To do so, the host that creates the packet sends the packet to a nearby router. That router might send the packet to a second router, with that second router forwarding the packet to a third router, and so on, until the packet is delivered to a router that is connected to the same LAN as the destination computer. That last router then sends the packet to the final destination. Figure 1-1 shows just such an example, with the web server on the left sending a packet back to the PC on the right.

Figure 1-1 shows three main steps, all from the perspective of the Internet Protocol (IP):

1. The web server needs to send a packet to the computer on the right (172.16.3.3), so the web server sends the packet to its *default gateway* router—namely, R1.

2. R1 decides to forward the packet to R2 next, based on R1's routing table.

3. R2's routing table shows that 172.16.3.3 should be on a subnet directly connected to R2, so R2 knows to send the packet directly to the destination (172.16.3.3).

Figure 1-1   IP Routing, from a Layer 3 Perspective

Subnet 172.16.1.0, 255.255.255.0   Subnet 172.16.4.0, 255.255.255.0   Subnet 172.16.3.0, 255.255.255.0
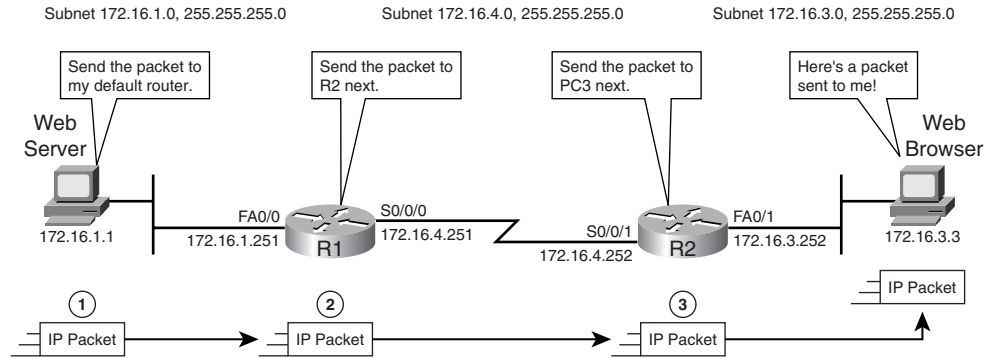
This description focuses on the OSI Layer 3 (network layer) details of how hosts and routers forward packets in an IP network. However, both the hosts and the routers must also be aware of how to use Layer 1 and Layer 2 standards and protocols to send the packets over the various types of physical networks. For example, Figure 1-2 and the descriptions that follow it explain some of the Layer 2 details of the process. Specifically, the example shows the data-link headers and trailers, along with the encapsulation process.

Figure 1-2   IP Routing, Including Layer 2 Encapsulation and De-encapsulation

Subnet 172.16.1.0, 255.255.255.0   Subnet 172.16.4.0, 255.255.255.0   Subnet 172.16.3.0, 255.255.255.0
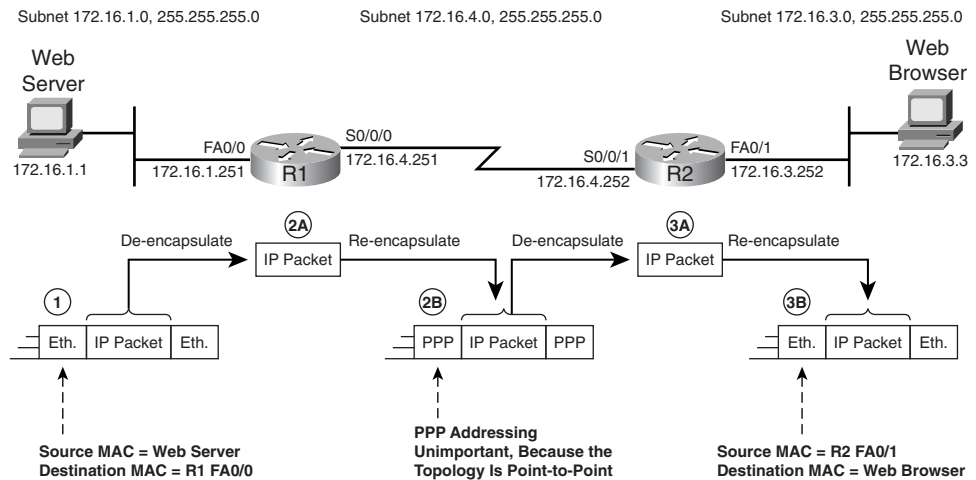
Figure 1-2 focuses on how the hosts and routers need to encapsulate the packet before sending anything over the LAN and WAN links. Hosts and routers must use data-link protocols, such as Ethernet on the LAN and Point-to-Point Protocol (PPP) on WAN links, to forward the packets over the physical links. To use the data links, a router encapsulates the packet into a data-link frame by putting the packet between a data-link header and trailer. The receiving router

removes, or de-encapsulates, the packet. Figure 1-2 shows the same three steps as Figure 1-1, but focuses on the encapsulation and de-encapsulation process at Layer 2:

1. The web server encapsulates the IP packet in an Ethernet frame to send the packet to its default gateway (R1).

2. R1 processes and routes the packet as follows:

   A. R1 de-encapsulates the packet by extracting the packet from the received Ethernet frame.

   B. After R1 has decided to forward the packet out interface S0/0/0, R1 must encapsulate the packet in the correct data-link frame for that link—in this case, a PPP frame.

3. R1 processes and routes the packet as follows:

   A. R2 de-encapsulates (removes) the IP packet from the PPP frame.

   B. After R2 knows that it needs to forward the packet over an Ethernet LAN out interface Fa0/0, R2 encapsulates the IP packet in a new Ethernet frame before sending the data over the Ethernet on the right.

Routers must use OSI Layer 1, 2, and 3 standards and protocols to perform one of the most basic functions of routers: the end-to-end routing of packets across an internetwork. The explanations of Figure 1-1 describe some of the Layer 3 logic, while the explanations of Figure 1-2 describe some of the OSI Layer 2 logic. The routing process includes many other small details, including physical layer details.

Packet Tracer	Packet Tracer configuration file NA02-0102 uses a configuration that mostly matches Figure 1-2. Simulation scenario 1 shows the packet flow shown in the figure.

This first major section of the chapter describes some of the more important basic features of how routers can be used to create a *wide-area network (WAN)*. First, this section describes how to create WAN links between two remote sites, and then it shows how to create the equivalent of a WAN link in a lab, which allows engineers to test WAN concepts for the cost of a few inexpensive cables. This section goes on to cover a little more information about routing over WANs and router WAN hardware.

Connecting Routers to WAN Links

Many network diagrams purposefully ignore the physical details of how a router connects to a WAN link. For example, Figure 1-1 and Figure 1-2 show a lightning-bolt line between R1 and R2, meaning that a point-to-point WAN link exists, but the cabling details are unimportant to the discussion for those diagrams. This section takes a closer look at WAN links, particularly the cabling and devices that connect to a router to create a WAN link.

This chapter focuses on the simplest type of WAN link, called a ***point-to-point WAN link***. A point-to-point WAN link, also called a ***leased line***, leased circuit, or WAN link, connects two devices over a WAN. Leased lines give the devices on each end (typically routers) the ability to send data to each other at the same time. Leased lines are also permanently installed, meaning that the devices can send data to each other at any time.

To create a point-to-point WAN link, a company must use the services of a ***telephone company (telco)*** or other company that sells WAN services. To install a new leased line, a company must order the leased line from a telco or other company that sells such services. The order form for the leased line lists the street address of each site, the exact location inside the building to which the telco should install its cables, and the speed at which the leased line should run. The telco then can physically install cables into the buildings, to the correct floor and room, to provide a physical link over which bits can be sent between the two devices.

Additionally, the telco requires a special type of networking device to be attached to the end of the leased line. This device, called a ***channel service unit/data service unit (CSU/DSU)***, helps protect the telco's equipment electrically and provides many other functions to make the leased line work.

Note

You can think of LANs as using cables that you own, and WAN links as using cables that you lease or rent.

How To ⌕   The following list outlines the steps a network engineer could use to install a point-to-point WAN link:

Step 1   Order the leased line from a telco or other company that sells such services.

Step 2   Order a router and a CSU/DSU for each of the two sites.

Step 3   Physically install the router and CSU/DSU at each site.

Step 4   Connect the router and CSU/DSU to the line from the telco, at each site.

Figure 1-3 shows the resulting leased line.

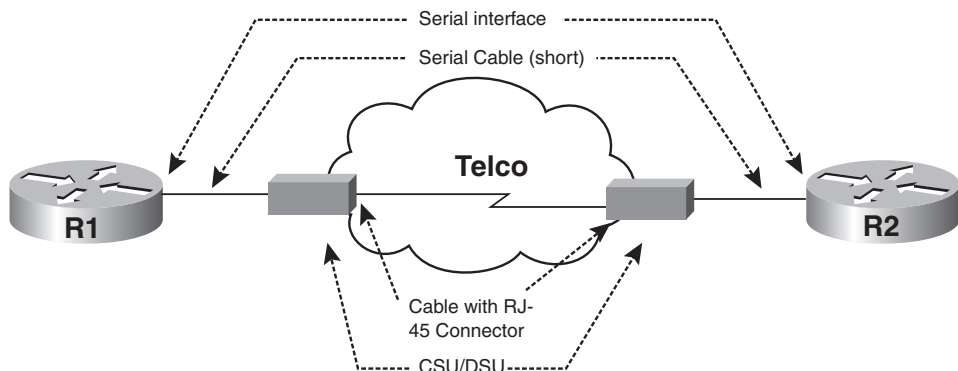**Figure 1-3**   WAN Link Showing the Serial Cables, CSU/DSUs, and Telco

Figure 1-3 shows many of the details of a WAN link. The figure shows two *serial cables*, whose job is to connect a router's serial interface to a CSU/DSU. The leased line from the telco acts as if it were a single cable, with two twisted pairs: one for transmission in each direction. However, the telco does not actually run a cable between the two routers, but instead uses other technology that is beyond the scope of this book and the related course. So, the telco cloud and lightning-bolt line represent the fact that the details are hidden and unimportant for this discussion.

Figure 1-3 cannot really show the length of the cables very well. The serial cables are typically very short, usually less than 50 feet in length, and often only a few feet in length. The router and CSU/DSU at each site typically sit in the same room, often next to each other. However, the line from the telco may be a few miles long, or it may be thousands of miles long, depending on the distance between the sites.

This book often uses the term telco to refer to any company that sells WAN services, but many other terms can be used as well. For example, up until the early 1980s, the United States used a single large monopoly telco (AT&T), but then the U.S. Department of Justice decided to break up that monopoly to increase competition. As a result, some of the old parts of AT&T that provided local telephone services became separate companies, with these companies often being called regional Bell operating companies (RBOC). (The "Bell" in the name refers to Alexander Graham Bell, who both invented the telephone and started the company that became AT&T.) Over time, telcos came to be known by the more generic name of *service provider*. In some parts of the world, telcos are called Post, Telephone, and Telegraph (PTT) companies, with a single government-controlled company providing postal services and telephone services throughout a single country. Regardless of which term you use, these companies provide services such as the point-to-point WAN link shown in Figure 1-3.

The routers and CSU/DSUs in Figure 1-3 are collectively referred to by the telco as *customer premises equipment (CPE)*, because from the telco's perspective, the router and CSU/DSU are equipment that sits at the telco customer's site.

Next, the text takes a closer look at two more detailed topics related to WAN links. The first, clocking and synchronization, is very important to how WAN links work. Following that, a few of the more important WAN standards are covered.

WAN Clocking on DTE and DCE Devices

The routers and CSU/DSUs in a typical leased line play the role of either data circuit-terminating equipment (DCE) or data terminal equipment (DTE). In normal circumstances, the router acts as the DTE, and the CSU/DSU as the DCE, which are defined as follows:

- *Data circuit-terminating equipment (DCE)*—A device that connects to the leased line provided by the telco. The term *circuit-terminating* refers to the fact that a leased line is sometimes called a data circuit, or simply a circuit, and the CSU/DSU sits at the end of the circuit. The DCE also provides clocking to the DTE.

Note

Cisco Systems gives its customers the option to buy router serial interfaces either with or without built-in CSU/DSUs. Interfaces with built-in CSU/DSUs connect the telco's cable directly to the router, with no need for an external CSU/DSU or serial cable.

Note

Some networking texts use the term *data communications equipment* to mean the same thing as data circuit-terminating equipment.

■ *Data terminal equipment (DTE)*—A device that sends data over a circuit. Routers act as DTEs because they send IP packets, encapsulated in data-link frames, over WAN links. DTEs also expect to receive clocking from the DCE.

The definitions of DCE and DTE both bring up the topic of *clocking*, which is also known as *synchronization*. The *serial links* used between two routers typically use synchronous communication, which means that both routers on the ends of the leased line must use the exact same speed for sending and receiving bits. Building hardware that uses the exact same speed is expensive, because creating clocks that run at the exact same speed is expensive. For example, if you go to the store and buy two wristwatches, and let them run for a few months, it would not be surprising if one watch runs a few seconds faster than the other watch. The same kind of thing happens with networking devices. With WAN links, the clocks need to match exactly, so the two routers synchronize their clocks continually to make sure their clocks run at the same speed.

For example, assume that a leased line has been installed, and the line should run at a speed of 64 Kbps. The routers need to send a new bit every 1/64,000th of a second. To do that, the routers have a chip that acts as a clock. However, one router's clock may run a little slower or faster than the other router's clock. Synchronization, or clocking, is a method by which the routers are made to adjust their clock rates continually so that they both run at the same speed.

To synchronize the clocks on the *serial interfaces* of both routers on the ends of a serial link, a couple of things must happen. First, the telco uses a clock, typically an atomic clock, which is a precise method of keeping time. The CSU/DSUs can adjust their internal clocks based on the electrical signals coming over the leased line from the telco. Then, the CSU/DSUs, acting as DCE, provide a clocking signal to the routers (acting as DTEs) over the serial cables. The routers then adjust their clocks so that they continuously run at the same speed. It is like the scene in spy movies where all the spies synchronize their wristwatches to the same time before starting some amazing timed-to-the-second trickery. On a WAN link, the synchronization occurs continually, based on one master clock source inside the telco.

Now that you have seen the basics of WAN link cabling, the next section looks at some of the standards bodies and standards that define more of the details about how different WAN links work.

WAN Standards

The term *WAN* refers to Layer 1 and Layer 2 standards from many organizations. The reasons for the large variety of standards are varied. WANs have existed for more than 50 years, predating LAN standards by a few decades. Similar to how computers keep getting faster and cheaper, the speed of WANs has continually improved, while the cost per kbps has decreased. Each new advance in speed and technology has required a new set of standards. To make all this work, over a long period of time, a large number of WAN standards have been created.

Today, most WAN standards are created by one of many standards bodies listed in Table 1-1. Regardless of their reason for existence, these organizations play a role in the development of WAN standards, oftentimes sharing or referring to standards from other organizations.

Table 1-1   Popular WAN Standards Organizations

Standards Body	General Purpose
International Organization for Standardization (ISO)	An international standards body composed of delegates from each equally participating country. It develops a very wide range of international standards.
Internet Engineering Task Force (IETF)	An open international networking organization that develops the protocols of the TCP/IP networking model.
Electronic Industries Alliance (EIA)	A trade association that works closely with the Telecommunications Industry Association (TIA) on cabling standards.
International Telecommunication Union (ITU)	An international standards organization, under the control of the United Nations, for the purpose of developing world-wide telecommunications standards.

Unlike Ethernet LAN standards, which define both Layer 1 and Layer 2 details, most WAN standards focus on either Layer 1 or Layer 2. For example, on the leased line shown in Figure 1-1 and Figure 1-2, the *Point-to-Point Protocol (PPP)* data link layer protocol, defined by IETF, can be used. Alternatively, ITU's *High-Level Data Link Control (HDLC)* protocol can be used. Other WAN data link layer protocols, such as *Frame Relay*, allow more than two routers to connect to a WAN and communicate with each other, unlike leased lines, which allow only two routers to communicate. However, none of these standards defines the physical layer details of transmitting bits over a WAN link.

At Layer 1, the leased lines shown in Figure 1-1 and Figure 1-2 could be T1 lines, as used in North America, or E1 lines, as used in Europe. Or, instead of leased lines, those lines could use a switched service standard such as *Integrated Services Digital Network (ISDN)*, which allows a temporary point-to-point link to be created by doing the equivalent of making a phone call.

Table 1-2 lists some of the more popular standards used at Layer 1 and Layer 2 for WANs. The names shown in the table are the commonly used names for the WAN standards rather than the formal names, because most people do not use the formal names.

Note

Table 1-2 is included for reference, but you do not need to memorize the details listed. The CCNA 4 course covers the more commonly used standards in more detail.

Table 1-2   Popular WAN Standards at Layers 1 and 2

Layer 1 Standards	Layer 2 Standards
EIA/TIA-232	HDLC
EIA/TIA-449	Frame Relay
V.24	PPP
V.35	Synchronous Data Link Control (SDLC)
X.21	Serial Line Internet Protocol (SLIP)
G.703	X.25
EIA-530	Asynchronous Transfer Mode (ATM)
ISDN	Link Access Procedure, Balanced (LAPB)
T1, T3, E1, and E3	Link Access Procedure on the D channel (LAPD)
xDSL	Link Access Procedure Frame (LAPF)
SONET (OC-3, OC-12, OC-48, OC-192)	

Although the number of different standards may be a bit overwhelming at first glance, you can learn most of the details of how routers use WANs by working with simple point-to-point leased lines, so most of the rest of the book uses leased lines in its examples.

Creating Inexpensive Leased Lines in a Lab

Leased lines and other WAN services that connect two sites cost money. Typically, the telcos and other WAN service providers charge a fee to install a new leased line, and then they charge a monthly charge for use of the line as well. In fact, the "leased" part of the term "leased line" comes from the fact that the pricing works much like a lease on a car or an apartment, with some small fee up front and an ongoing monthly fee as well.

Two routers can be made to think they have a leased line between them—without having an actual leased line from the telco—as long as the routers sit relatively close to each other. For example, when building a lab to use for this course, the routers typically sit in the same room. To install the equivalent of a WAN leased line between two routers' serial interfaces, without having to pay any money to a telco, you can follow these steps:

How To

Step 1   Buy two routers, each with a serial interface.

Step 2   For one router, buy a serial *DTE cable*. The connector on one end of the cable should be connected to one of the router's serial interfaces.

Step 3   For the other router, buy a serial *DCE cable*. The connector on one end of the cable should connect to the second router's serial interface.

Step 4   Connect the DTE and DCE cables together. The DTE cable has a male connector, and the DCE cable has a female connector. (When purchasing the cables, make sure that both the DTE and DCE cables have the same type of connector so that they will connect to each other.)

Step 5   Enable clocking on the router that is connected to the DCE cable so that the router takes the place of the telco and CSU/DSU by providing clocking to the other router.
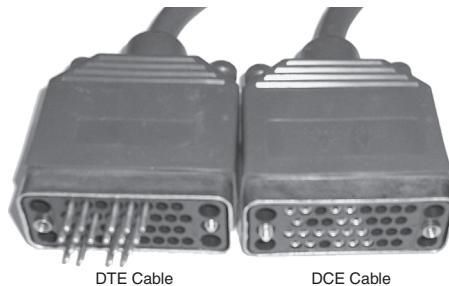
Figure 1-4 shows an example of how to connect the DCE and DTE cables to create a WAN link. Such links, called *back-to-back* WAN links due to the connection of the two cables together, are widely popular. Most networking labs used for network testing before deploying a new site, and most labs used for teaching classes, use these back-to-back WAN links.

Figure 1-4   Router as DCE: Back-to-Back Serial Links
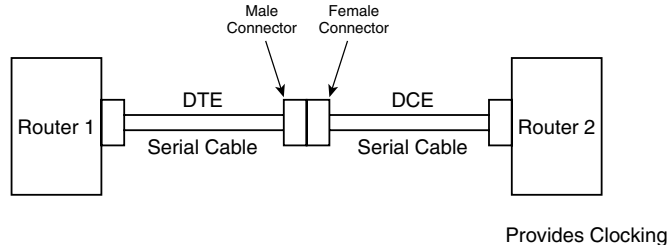
For two cables to connect correctly, one cable must use a male connector (the DTE cable) and the other must use a female connector (the DCE cable). Figure 1-5 shows a picture of the ends of two V.35 serial cables, one a DTE cable with a male connector, and the other a DCE cable with a female connector. V.35 is one of the more popular types of connectors for serial cables.

> **Note**
>
> Unlike the cables shown in Figure 1-5, DTE and DCE cables from most cable suppliers have the word "DTE" or "DCE" printed on them to help identify the cable as a DTE or DCE cable.

Figure 1-5   V.35 DTE and DCE Cable Connectors

Besides ordering and installing the correct cables, you must configure one router to provide clocking, as mentioned in Step 5 of the process. If there is no telco, and no CSU/DSUs, the routers do not have any device that provides the clocking and synchronization function. Conveniently, you can make one of the router serial interfaces supply that clocking by using the **clock rate** command. The router serial interface that acts as the DCE (the router serial interface that is cabled to the DCE cable) can provide the clocking function.

> **Note**
>
> Any of a router's serial interfaces can provide clocking, as shown in Figure 1-4.

Overview of Routing Over WANs

Any time you see a drawing of a network that uses routers, the routers seem to always be connected to at least one WAN. Why is that? Well, routers route packets based on Layer 3, oftentimes routing based on the IP protocol. The IP protocol, being a network layer protocol, was purposefully designed to allow packets to be forwarded over most any type of physical network. So, routers can connect to Ethernet LANs, Token Ring LANs, point-to-point WANs, Frame Relay WANs, cable networks, DSL lines, dialed lines using modems, ISDN, and most any kind of physical network that people will create in the future. In short, routers are designed to give network engineers a wide variety of options for the types of physical networks used, with routers being able to route packets over any and every type of media.

The beginning of this chapter reviewed the basics of one of the most important functions of routers: the routing of packets from one host (computer) to another. The following list summarizes some of the key functions performed by routers:

- **Routing**—The process of forwarding packets, as reviewed in Figure 1-1 and Figure 1-2.

- **Path selection**—When multiple possible routes to reach a subnet exist, routers must choose the best route or path over which to reach the subnet. This process can be referred to as path determination or *path selection*.

- **Dynamic and static routes**—Routers may learn or select routes either dynamically, using routing protocols, or statically, with the engineer configuring the routers with routing information.

- **Logical addressing**—Routers rely on the logical addressing defined by Layer 3 protocols. Layer 3 addressing (for example, IP addressing) allows addresses to be grouped for easier routing, which aids the process of end-to-end packet delivery by routers.

Path selection is one of the more interesting features of routers. When a router learns about multiple paths to reach a particular subnet, the router must pick the best route, typically based on the routing protocol *metric* for each router.

Figure 1-6 shows an example in which router R1 learns two possible routes, one from router R2 and one from router R3. The routers use the RIP routing protocol to advertise routes in this case, with RIP using hop count as the metric. The figure shows the process of how R1 learns a route to reach subnet 172.16.3.0/24, as follows:

1. R2 advertises a route to reach 172.16.3.0/24, using routing protocol messages sent out both of its serial interfaces. The advertisements list a metric of 1 in each case.

2. After learning about the metric 1 route to 172.16.3.0/24 from R2, R3 then advertises about the same route in a routing protocol message sent to R1, but with a metric of 2.

3. As a result, R1 has learned of two routes to reach 172.16.3.0, but the route learned from R2 has the lower metric, so R1 chooses that route.

4. R1 adds a route for 172.16.3.0/24 to its IP routing table— a route referencing router R2 as the next-hop router to which packets should be forwarded.

Figure 1-6   Redundant Routes Learned by R1 in a WAN
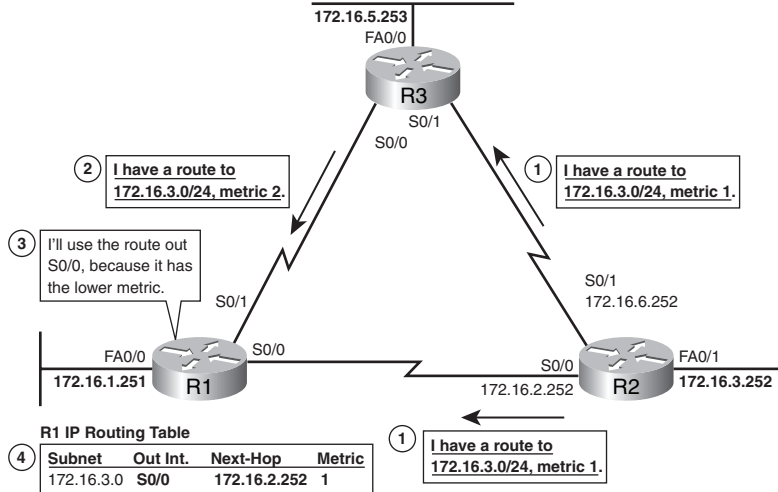
Both R1 and R3 could have been configured with the static routes shown in their respective routing tables, or they could have learned the routes using a dynamic routing protocol. With statically configured routes, the router does not need to use a routing protocol to learn about the routes in the network.

> **Packet Tracer**   Packet Tracer configuration file NA02-0106 shows an internetwork that closely matches Figure 1-6. By clicking a router icon in real-time mode, you can see the routing table on that router.

Router Hardware and Software Components

Routers have to do a lot of work, including forwarding potentially large numbers of packets per second and performing many important overhead functions such as learning and maintaining good IP routes. For example, a router in the core of a large enterprise network might route hundreds of thousands of packets per second, and a router in the core of the Internet might route millions of packets per second. To do that work, a router has many of the same components as a PC. In fact, a router is actually a computer that is designed for the specialized purpose of routing packets. In contrast, PCs are general-purpose computers, designed to perform many different tasks.

Each router has some hardware and software that essentially work just like a typical PC. Like PCs, each router has a central processing unit (CPU), *random-access memory (RAM)*, and read-only memory (ROM). For example, R1 in Figure 1-6 may receive a packet whose destination is 172.16.3.2, which is an address in subnet 172.16.3.0. To forward the packet, the router needs to look at its routing table, which is stored in RAM. To make the decision about which

route to use, R1 needs to process the packet, which involves comparing the destination IP address with R1's routing table—work that can be done by the CPU. The router's ROM holds some of the basic diagnostic software that runs when the router is first powered on.

The logic used to route packets is a part of the router's operating system, which on Cisco routers is called *Cisco IOS*. (*IOS* is short for Internetwork Operating System.) Cisco IOS is software that includes all the specialized features needed by routers, including routing protocols, basic routing logic, and support for allowing network engineers to log in to the router.

Additionally, just like PCs have network interface cards (NIC), routers have physical network interfaces. Because routers are designed to connect to many different kinds of physical networks, routers have a large variety of types of network interfaces. For example, in Figure 1-6, R1 has one Fast Ethernet interface, labeled Fa0/0, and two serial interfaces, labeled S0/0 and S0/1.

Routers also have a few important types of memory that are not typically used on PCs. Unlike PCs, routers typically do not have a disk drive. Instead, routers use the following two different types of memory that can permanently store data:

- *Nonvolatile RAM (NVRAM)*—Where the router stores its configuration, including its IP addresses and masks, the routing protocol to use, and other related information.

- *Flash memory*—Where the router stores the OS (Cisco IOS) and other files.

Table 1-3 summarizes these components of routers. The section "Internal Router Components" on the next page covers a little more detail about these and other components of routers. Also, Chapters 2, 3, and 5 cover in more depth the features supported by NVRAM, RAM, and flash memory.

Table 1-3   Overview of the Main Use of Router Internal Hardware Components

Internal Component	Characteristics
Random-access memory (RAM)	▪ Stores routing tables ▪ Holds ARP cache ▪ Performs packet buffering ▪ Provides temporary memory for a router's configuration file while the router is powered on ▪ Loses content when a router is powered down or restarted
NVRAM	▪ Stores the backup/startup configuration file for the router ▪ Retains content when the router is powered down or restarted
Read-only memory (ROM)	▪ Maintains instructions for power-on self test (POST) diagnostics ▪ Requires replacing pluggable chips on the motherboard for software upgrades ▪ Stores bootstrap program and basic operating system software

Table 1-3   Overview of the Main Use of Router Internal Hardware Components   *(continued)*

Internal Component	Characteristics
Flash memory	▪ Holds the Cisco IOS software image ▪ Allows software to be updated without removing and replacing chips on the processor ▪ Retains content when a router is powered down or restarted ▪ Can store multiple versions of Cisco IOS software ▪ Is a type of electrically erasable programmable read-only memory (EEPROM)
Interfaces	▪ Physical network connection through which packets enter and exit a router ▪ Located on the motherboard or on a separate interface module

Router Components and Cabling

The main purpose of a router is to route packets. To do so, a router must have physical interfaces with which to connect to physical networks. Internally, a router must be able to receive the bits on one interface, process the received bits, store the bits in memory, move the bits to the outbound interface, and send the bits. The router also needs to support some method for humans to examine how the router is working, and to tell the router any important parameters it should be using when routing packets. This second major section of this chapter covers the details of the internal and external components of routers that support all these functions.

Internal Router Components

You may work with routers on a regular basis and never have to look at all the electronics inside the router. In fact, to work with routers at a general level, you really only need to know the basic facts about router internals that have already been covered, such as that NVRAM holds the configuration, that flash memory holds the Cisco IOS software, and that the router has a CPU and RAM that it uses when processing packets. However, to work with routers at a more detailed level (and to achieve certification), you need to understand more about the internal components.

Each model of router has the same general types of hardware components, but, depending on the model, those components are located at different places inside the router. To show just one example, Figure 1-7 shows a picture of the inside of a Cisco 2600 series router. The figure views the router with the top cover removed, looking down into the router.
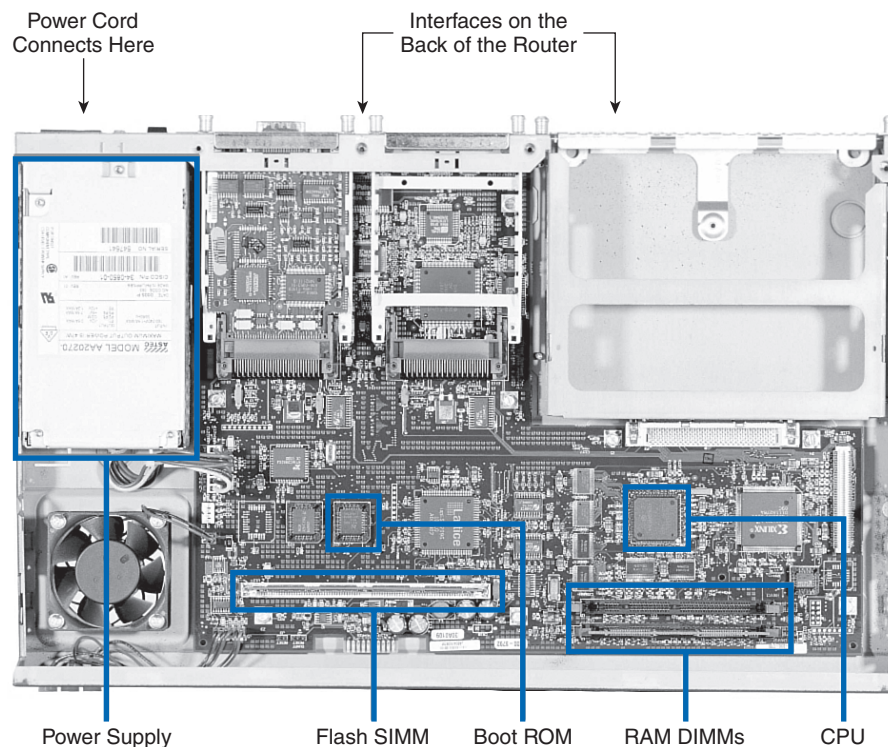
Figure 1-7   Inside of a Cisco 2600 Router

Figure 1-7 shows some of the main components, most of which are on the motherboard of the router. The RAM is typically composed of chips attached to a small removable circuit board, called a dual in-line memory module (DIMM). Flash memory also consists of chips on a circuit board, using a similar type of technology called a single in-line memory module (SIMM). ROM is often called boot ROM, because when any computer is first turned on, the computer "boots" itself up to a working state. A router uses the software in boot ROM to boot itself into a working state.

Whereas Figure 1-7 shows a picture of the inside of a Cisco 2600 series router, Figure 1-8 shows a logic diagram of how some of the internal components work together. Like Figure 1-7, the actual location of the components in Figure 1-8 is not very important, but the figure provides some perspectives on how the components may be connected.

Figure 1-8 shows a lot of words inside small boxes, with lines connecting the boxes. The words inside the boxes represent different components inside the router, with the lines representing the *buses*. Computers use buses to move data internally, much like cities use buses to move people around the city. In this particular logic diagram, the memory is shown on the left, and the interfaces on the right. The CPU chip is shown in the text box labeled M68030, which is a CPU chip made by the Motorola corporation. Although the details in operation are not important, it

is important to see that the router's different internal components—the different types of memory, the CPU, and the interfaces—are all connected via buses. The buses then allow the router to move bits around internally.

Figure 1-8   Logic Diagram of the Internal Components of a Cisco 2600 Series Router
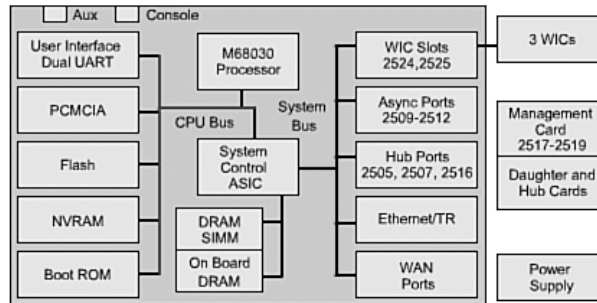
From a practical perspective, knowing the function of a router's main internal components is more important than knowing the locations of the physical components inside a particular model of router. Table 1-4 lists internal components and includes comments about how each is used.

Table 1-4   Key Internal Router Components

Component	Description
CPU	Executes the operating system's instructions. Among these functions are system initialization, routing functions, and network interface control.
RAM	Used to store the Cisco IOS software and the working memory that it needs. This includes the routing table, running configurations, and packet queues, which hold packets until the interface can be used to forward the packet. The contents of RAM are lost when the router loses power.
Flash memory	Used to store a full Cisco IOS software image. In most routers a copy of the Cisco IOS software image is transferred to RAM from flash memory during the boot process. Physically, flash memory consists of SIMMs or PCMCIA cards, which can be upgraded to increase the amount of flash memory. Flash memory does not lose its contents when the router loses power.
NVRAM	NVRAM is used to store the startup configuration. As described in Chapter 2, "Introduction to Routers," a router copies the startup configuration from NVRAM into RAM when the router is initialized and uses the running configuration in RAM for normal router operation. NVRAM retains its contents when the router loses power.

Table 1-4   Key Internal Router Components   *(continued)*

Component	Description
Buses	Buses provide a physical means for the router to move bits between the router's different components. Most routers contain a system bus and a CPU bus. The system bus is used to communicate between the CPU and the interfaces; for example, this bus transfers the packets to and from the interfaces. The CPU uses the CPU bus to access router storage devices, such as NVRAM and flash memory.
ROM	Holds the bootstrap program, the ROM monitor software, and optionally a scaled-down version of the Cisco IOS software. (Chapter 2 covers these types of software.) ROM is not erasable, and can be upgraded only by replacing the ROM chips, but ROM does retain its contents when the router loses power.
Power supply	Converts the voltage and current of a standard power source to the voltage and current required by the devices in the router. The power supplies may be internal or external to the router chassis (the metal box that holds the router's components), and some routers have multiple power supplies for redundancy.

To see the internal router components of Figure 1-7, you must use a screwdriver to take the metal cover off the router. Typically, you do not need to open the router unless you are upgrading memory—for example, when adding or replacing a flash memory SIMM. However, some components do need to be accessed on a somewhat regular basis, so Cisco makes those components available as physical connectors that are easily accessed from the back of a router. These physical connectors fall into two major categories—interfaces and management ports—and are covered in the remainder of this chapter.
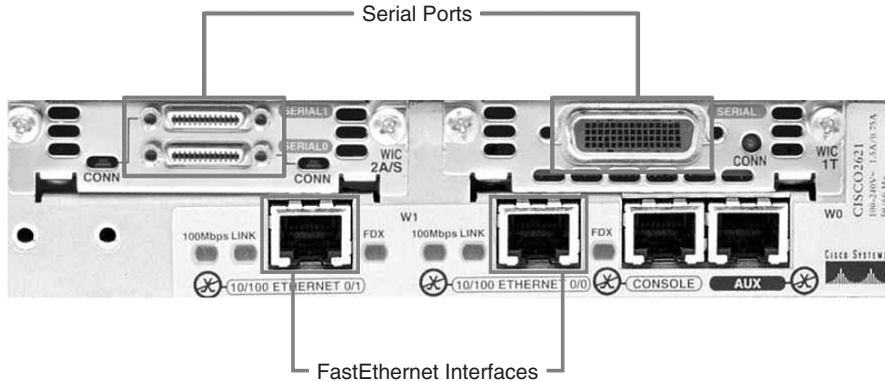
External Router Interfaces

Although the term *interface* may seem generic, when speaking of Cisco routers, the term interface has a very specific meaning. In particular, interface refers to a physical connector on the router whose intended purpose is to receive and forward packets. These interfaces consist of a socket or jack into which a cable can be easily connected. The interfaces are not inside the router, but outside, typically in the back of the router. Figure 1-9 shows a picture of the back of a Cisco 2600 series router, with several LAN and WAN interfaces shown.

Routers support a wide variety of different types of interfaces because routers need to be able to forward packets over many kinds of physical networks. For example, some routers may have serial interfaces, DSL interfaces, ISDN, cable TV, or other types of WAN interfaces, and the list goes on. Figure 1-9 shows a typical router, with some LAN interfaces and some WAN interfaces. The left side of the figure shows the interfaces, with the bottom-left showing two 10/100

Fast Ethernet interfaces with RJ-45 jacks. The upper part of the figure shows three serial inter-faces. The two serial interfaces on the left use a connector called a ***smart serial interface***, which is smaller than the DB-60 connector on the right.

**Figure 1-9**   Interfaces on a Cisco 2600 Series Router

To be useful, most router interfaces need to be connected to a cable. (The notable exception to that rule is a wireless interface, which uses an antenna instead of a cable.) The next two sec-tions examine cabling for both LANs and WANs.

Cabling Ethernet LAN Interfaces

In most cases, the LAN cabling required for a router's Ethernet LAN interfaces is very straight-forward. Many router Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces come with RJ-45 jacks that support unshielded twisted-pair (UTP) cabling, as was covered extensively in the Networking Basics CCNA 1 course. For these interfaces, the only possibly tricky part is to remember that as far as Ethernet UTP cabling pinouts are concerned, routers act like PCs. (This is just another example of the similarities between a PC Ethernet NIC and a router Ethernet interface.) So, routers use a straight-through cable to connect to a switch, just as a straight-through cable should be used to connect a PC NIC to a switch. Figure 1-10 shows an example.

Figure 1-10   Interfaces on a Cisco 2600 Series Router
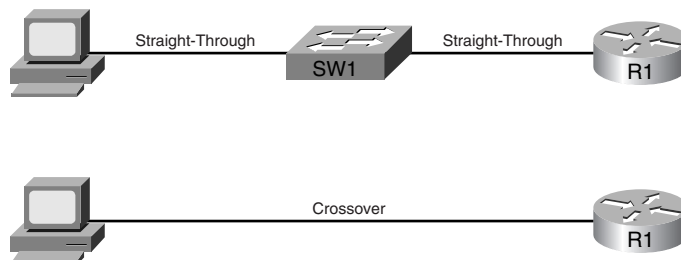
The bottom half of Figure 1-10 shows another common choice for router LAN cabling used in labs. When creating a network in a lab, often only one PC is needed on the LAN connected to a router. In such cases, the router can be cabled directly to that one PC, creating an Ethernet segment with the router and the PC. To make it work, an Ethernet crossover cable must be used.

Connecting Ethernet cables to a router's RJ-45 jacks is simple and easy, but a little extra care must be taken as compared to cabling PCs. Other router interfaces, such as non-Ethernet interfaces, use an RJ-45 jack as well. For example, most router console and auxiliary ports use an RJ-45 jack (see Figure 1-9 for an example). Also, routers' ISDN Basic Rate Interface (BRI) interfaces use a jack called an RJ-48 jack, which is the exact same size and shape as an RJ-45 jack, so an Ethernet cable with an RJ-45 connector can be plugged into a BRI interface. Also, some router serial interfaces have a built-in CSU/DSU; in those cases, the physical interface is again an RJ-48 jack.

To help combat this problem, Cisco labels all interfaces and ports with a text description and uses a different background color behind the text for each type of interface. Table 1-5 lists the interfaces that can accept a cable with an RJ-45 connector, along with the color codes used on the back of the router.

Table 1-5   Router Interfaces and Ports into Which an RJ-45 Connector Fits

Interface or Port	Type of Jack	Background Color
Ethernet	RJ-45	Yellow
Console port	RJ-45	Light blue
Auxiliary port	RJ-45	Black
BRI with S/T interface	RJ-48C	Orange
BRI with U interface	RJ-49C	Orange
T1/E1 with built-in CSU/DSU	RJ-48C	Light green

Caution

In some cases, connecting the wrong equipment to the wrong router interface or port can damage the equipment.

Whereas the figures in this book are black and white, the online curriculum has several color pictures that show the color schemes listed in Table 1-5. Memorizing the colors in the table is probably not all that important, but it is useful to look for the colors when looking at routers in the lab or when looking at the online curriculum. Also note that cables supplied by Cisco also match this color scheme, making it a little easier to make sure you use the right cable on the right interfaces.

Lab 1.2.6   Connecting Router LAN Interfaces

In this activity, you identify the Ethernet and Fast Ethernet interfaces on the router. You then identify and locate the proper cables to connect the router. Finally, you use the cables to connect the router and computer to a hub or switch.

Cabling WAN Interfaces for Leased Lines

As mentioned earlier, in the section "Connecting Routers to WAN Links," around Figure 1-3, a single WAN leased line connects two sites, and two sites only. The equipment at each site consists of a router with a serial interface, and a CSU/DSU. Together, the equipment at a single site is called the customer premises equipment (CPE), which is a term using the telco's perspective, because this equipment sits at the telco customer's site, not at the telco's site.

Figure 1-3 earlier in the chapter shows the general concept of how each router connects via a serial cable to the CSU/DSU, with the CSU/DSU then connecting to the leased line installed by the telco. As a reminder, Figure 1-11 shows the cabling between the router and an external CSU/DSU, showing the shapes of several of the more popular connectors used on serial cables to connect to the CSU/DSUs.

Figure 1-11   Serial Cables
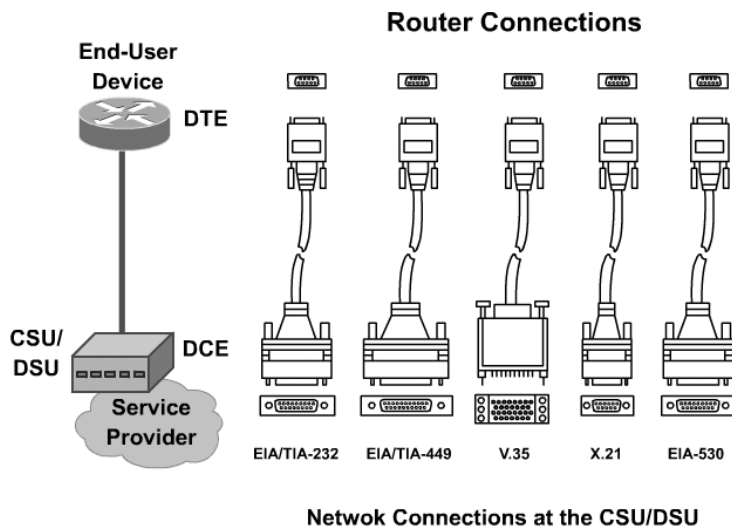
Even from Figure 1-11, you can see that many different types of serial cables exist. Picking the right serial cable requires more thought than does picking the right Ethernet UTP cable. Network engineers must consider three main points when ordering serial cables:

- The serial cable must have a connector that matches the type of serial connector on the router. Routers support several styles of serial interface connectors, with the most popular being the smart serial connector and DB-60 connectors shown in Figure 1-9.

- The serial cable's other end must have a connector that matches the connector on the CSU/DSU that will be used. Even more standards exist for these connectors, with five different styles shown in Figure 1-11.

- Serial cables typically use one of two different pinouts, based on whether the router is acting as DTE or DCE. The engineer must determine the role of the router (typically DTE), and then choose a DTE cable or DCE cable.

(Note that the online curriculum includes a similar list, but with one additional step, which points out that the cables must have the correct gender [male or female]. However, by making sure that you correctly choose either a DTE or DCE cable, you coincidentally ensure that you are using the right connector gender.)
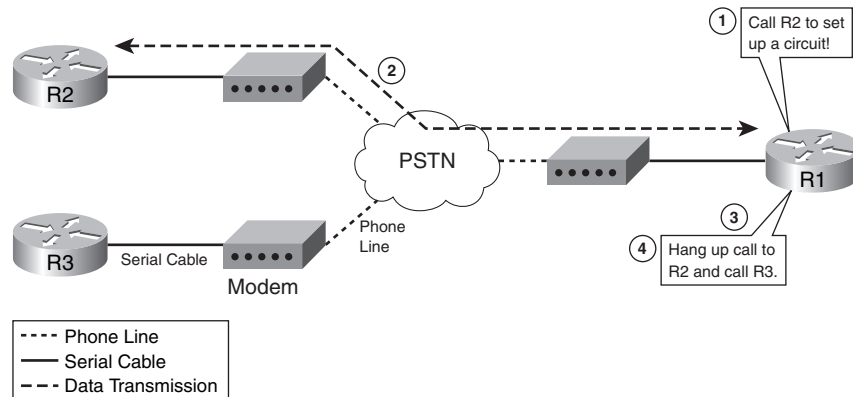
Lab 1.2.7   Connecting WAN Interfaces

In this activity, you identify the serial interfaces on the router. You then identify and locate the proper cables to interconnect the routers. Finally, you use the cables to con-nect the routers.

Cabling Other Types of WANs

As mentioned earlier in the "WAN Standards" section, this book uses point-to-point leased lines for WAN links to keep things simple, with the WAN Technologies CCNA 4 course cover-ing more details about other types of WANs. However, it is useful to know a little about two other general types of WANs: *circuit switching* and *packet switching*.

A single point-to-point leased line allows two routers to communicate with each other. Circuit switching and packet switching, however, allow more than two routers to communicate. For example, Figure 1-12 shows a typical circuit-switched WAN, with three routers.

Figure 1-12   Circuit-Switched WAN Using Modems

Figure 1-12 shows a circuit-switched WAN using phone lines and routers with asynchronous serial interfaces. The routers' *asynchronous serial interfaces* connect to *external modems* using short serial cables like those shown in Figure 1-11. The modem then connects to the phone line from the phone company.

To send data over a circuit-switched WAN, a router creates the equivalent of a phone call to one other router. While the phone call is active, the two routers send packets to each other. Figure 1-12 shows two routers with asynchronous serial interfaces, external modems, and a phone line connected to each of the three modems in the figure. The following process matches that shown in Figure 1-12:

1. Router R1 places a phone call to router R2, creating a circuit between R1 and R2.

2. R1 and R2 exchange packets over the circuit.

3. When R1 has finished sending all the data it wants to send, R1 does the equivalent of hanging up the phone by terminating the call.

4. R1 can then call R3 to send data.

The term *circuit switching* is actually very descriptive in this case. Using telco terminology, the word ***circuit*** refers to the transmission path between two phones during a phone call. So, routers such as R1 set up a circuit to another router such as R2 to send data back and forth. Those same routers can switch between circuits to different sites, sending to one remote site at a time.

The term *packet switching* is also very descriptive, because a router can change, or switch, the interfaces out which it forwards data for each different packet. Instead of having to do the equivalent of calling and hanging up the phone to each site when sending a packet, the router stays permanently connected to a ***packet-switched network (PSN)***. The PSN forwards the packets sent by the router based on an address inside the packet. The router can send multiple packets into the PSN, each with different addresses. The PSN in turn forwards the packets to the correct destinations. As a result, the routers can stay connected to the PSN, and not have to create and tear down circuits—a much more efficient process for the routers.

Figure 1-13 shows a sample of how a Frame Relay network works. Frame Relay is one type of packet-switching technology, with X.25 and Asynchronous Transfer Mode (ATM) being two others.

Figure 1-13   Packet-Switched WAN Example: Frame Relay
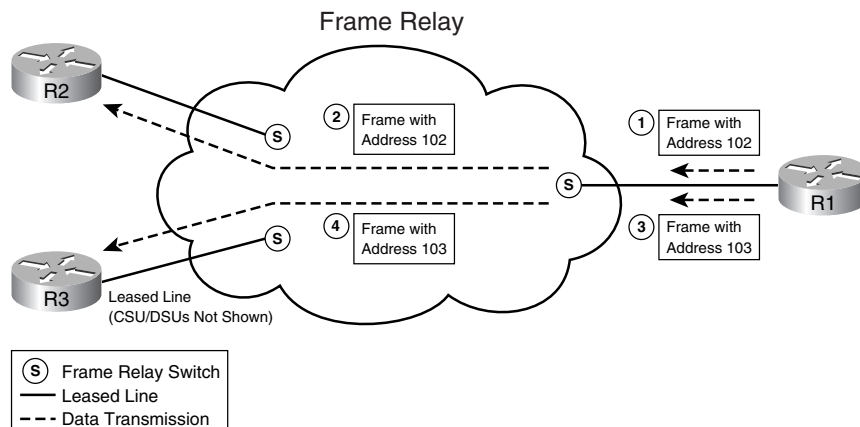
In a Frame Relay network, each router essentially has a leased line connecting it to a device, called a Frame Relay switch, in the Frame Relay network. Once connected, routers can send Frame Relay frames, placing a Frame Relay address in the header. The Frame Relay address tells the Frame Relay network which remote router needs to receive the frame. The process steps shown in Figure 1-13 are explained by the following list:

1. R1 sends a frame with address 102 to the Frame Relay network.

2. The switches in the Frame Relay network know that address 102 means that the frame should be sent to router R2, so the switches forward the frame correctly.

3. R1 now needs to send data to R3, so R1 sends a frame into the Frame Relay network, this time with address 103 in the frame header.

4. The switches in the Frame Relay network know that address 103 means that the frame should be sent to router R3, so the switches forward the frame correctly.

A router's interfaces are used to forward packets over WAN packet-switched services, such as the network in Figure 1-13, and over other types of WAN and LAN links. For example, routers use serial interfaces to connect to the Frame Relay service in Figure 1-13. The next section looks at another type of physical connector on routers, called management ports, and how they are used to log in to, configure, and troubleshoot a router.

Router Management Ports

When talking about routers, the term *interface* specifically refers to physical connectors used for the purpose of forwarding packets. In contrast, the term *port* refers to a physical connector used for managing and controlling a router.

Most routers have two management ports: the *console port* and the *auxiliary port (aux port)*. (Some routers do not have aux ports.) Both ports are meant to allow a terminal, or more likely a PC with a *terminal emulator*, to log in to the router to issue commands on the router. These commands may be used to troubleshoot problems or to configure the router to tell it how to act.

A terminal emulator is software that acts like a terminal. That, of course, creates another question—what is a terminal? A *terminal* is a device with a display screen, much like one used with a PC today, and a keyboard, but a terminal is not a PC. Terminals are simple devices that connect to a computer via a cable. The person using the terminal can type on the keyboard, and the terminal sends the text to the computer. The computer responds to what was typed—typically a command to tell the computer to do something—by sending some text back to the terminal screen so the person knows the results of the command.

Terminal emulator software creates a window on the screen of a PC. When you use that window, any text you type on the keyboard (typically a command) is displayed in the window and sent to some other computer, such as a router. The other computer then executes the command and sends some text messages back to the terminal emulator. Figure 1-14 shows such an example, with the command **show version** being typed by the user, and some text being returned from a

router. Note that the figure shows the results, with the **show version** command sitting near the top of the window.

Figure 1-14   Using a Terminal Emulator and a Router

To use a terminal emulator to send commands to a router, you can connect the PC to the router's console port or aux port, or use Telnet. The next two sections show how to connect to the console and aux ports. To connect using Telnet, the emulator can be told to use Telnet to connect to a given IP address or hostname, and the PC uses its connection to an IP network, typically through its NIC, to connect to the router.

Cabling and Accessing a Router Console Port

To successfully log in to a router via its console, you must install the correct cabling and then configure the terminal emulator correctly. The trickiest part of the cabling is that the terminal emulator typically uses a PC serial port to communicate with the router. (A PC's serial port is often referred to as a *COM port*, which is short for serial communications port.) The serial port is oftentimes either a nine-pin connector, called a *DB-9 connector*, or a *Universal Serial Bus (USB) connector*. The console cable supplied by Cisco—a *rollover cable*—typically has RJ-45 connectors on the ends. So, you have to make sure that you have a small piece of hardware called a converter that attaches to the end of the RJ-45 rollover cable, providing either a DB-9 or USB connector as needed.

After you have the right cables and connector converters available, however, the process is relatively simple. You can use the following steps to correctly install the cabling, with the details related to the PC serial port at Step 2:

How To

Step 1   Connect a rollover cable to the console port. (The console port is typically an RJ-45 jack, and the rollover cable also has RJ-45 connectors.)

Step 2   Connect a converter to the other end of the rollover cable to match the type of connector on the PC's serial port.

Step 3   Connect the cable (or the converter that is on the end of the cable) to the serial port on the PC.

Figure 1-15 shows a picture of the cabling components.

**Figure 1-15**   Console Cabling
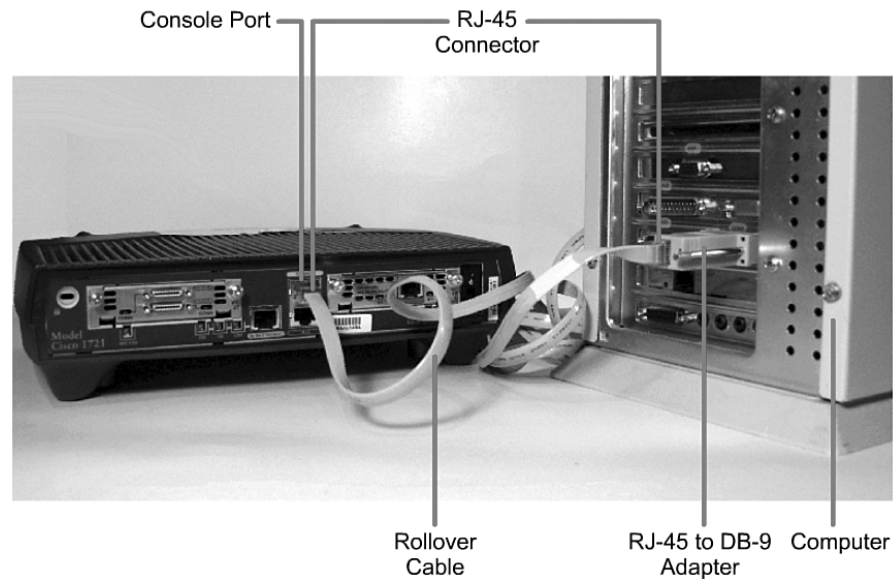
Besides connecting the console rollover cable as shown in Figure 1-15, a terminal emulator must be installed and configured to use the proper settings. These settings make the terminal emulator software act like one of the terminal models that used to be sold as standalone pieces of hardware. (The online curriculum states that the emulator must act like an old terminal type called a VT-100 terminal, but many terminal types actually work.) Most any terminal emulator can be used, with an emulator called HyperTerminal being relatively popular. HyperTerminal is included with some Microsoft OSs, and it can be downloaded for free from

http://www.hilgraeve.com. Figure 1-16 shows the HyperTerminal configuration screen, reflecting the correct default terminal settings for using the console port of a router, as follows:

- 9600 bps

- 8 data bits

- No parity

- 1 stop bit

- No flow control

Figure 1-16   HyperTerminal Configuration Settings
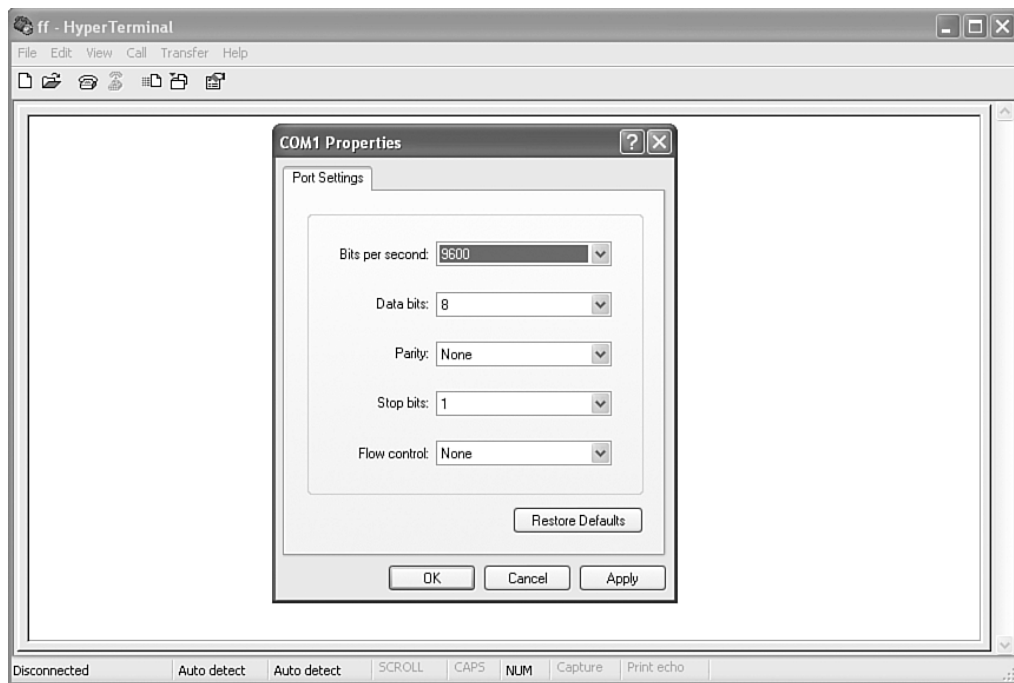
The speed setting of 9600 bps (default) brings up an interesting point about how the console and aux ports work. Both ports are considered to be asynchronous ports. *Asynchronous communications* means that both devices on each end of the cable (the PC and console port in this case) must use the same speed—in this case, 9600 bps. However, an asynchronous device does not attempt to adjust its clock based on what the other device is doing. In contrast, you may recall that the section titled "WAN Clocking on DTE and DCE Devices" earlier in this chapter explained a concept of clocking and synchronization by which the DTEs (routers) adjusted their clocks. In that case, the router's serial interfaces use synchronous communications, because they synchronize their clock speeds, whereas the console and aux ports use asynchronous communications, because they do not synchronize their clock speeds.

Note

The online curriculum also uses the term *RS-232* when referring to the console and aux ports. RS-232 is an old-style connector used on some early models of routers, but routers mainly use RJ-45 instead of RS-232 for the console connectors today.

Lab 1.2.5   Connecting Console Interfaces

In this lab, you connect a PC to a router using a console or rollover cable.

Cabling a Router Auxiliary Port

Cabling a router's aux port requires slightly more effort than cabling the console port. The router must have an external modem connected, with the modem typically using a different connector than the typical RJ-45 connector on the rollover cable. However, after the router aux port is cabled to a modem, the PC is cabled to a modem, and the terminal emulator is configured correctly, the PC can use the terminal emulator to call the remote router and log in. Figure 1-17 shows a picture of the cabling for the aux port.

Figure 1-17   Router Aux Cabling
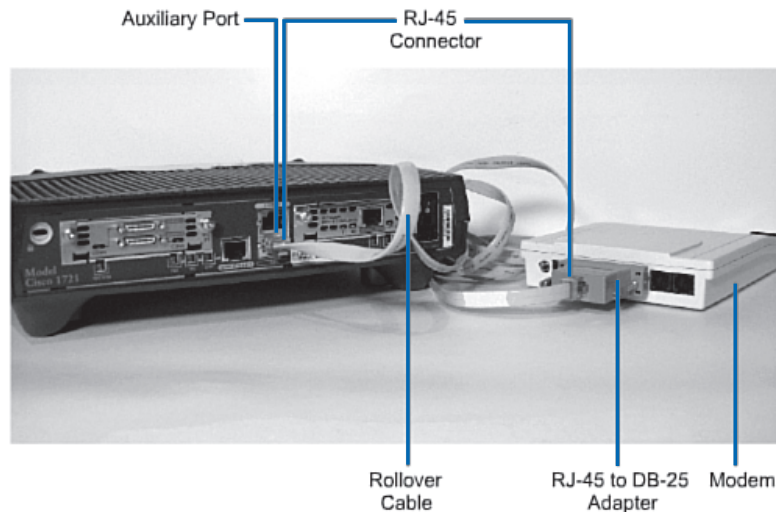
Comparing the Console and Auxiliary Ports

One of the main benefits of the console and aux ports is that both allow ***out-of-band management*** of routers. Most of the time, when a network engineer needs to execute commands on a router, the engineer telnets to the router. However, Telnet sends IP packets, with those IP packets going over the IP network. In some cases, the problem may be that packets cannot reach the remote router, so telnetting to that remote router will not work. The engineer then needs a way to log in to a router using a communications link that is outside the IP network, like a console cable or a phone call between two modems and the aux port. The term *out-of-band* simply refers to the fact that the communications link is "outside the bandwidth" used for sending IP packets.

Figure 1-18 shows the main benefit of the two out-of-band management ports of a router.

Figure 1-18   Out-of-Band Access to a Remote Router
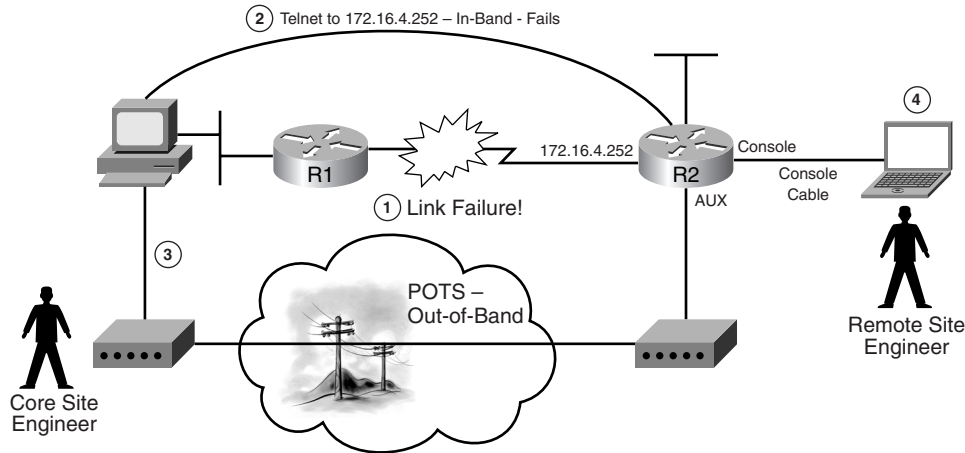
Note

The term POTS stands for plain old telephone system, which is just a reference to the worldwide network that allows a typical phone call to be made. It is also called the public switched tele-phone network (PSTN).

Figure 1-18 begins with the core site network engineer, on the left, logged in to remote router R2 using Telnet. The figure shows the following steps:

1. The link between R1 and R2 fails.

2. The telnet from the core engineer's PC fails.

3. The core site engineer can use a modem to call the remote router (R2) via the remote router's aux port.

4. Alternatively, if an engineer is at the remote site, the remote site engineer can access R2 via the console port.

Both the console and aux ports were designed to be used for out-of-band management of a router. The main difference is that the console is meant for local access when the engineer is next to the router, and the aux port is intended for remote access when the engineer is not even at the same site as the router. Beyond that basic difference, however, some functions are best performed at the console port and others can be performed only at the console port. For that reason, the console port is used more often than the aux port when the engineer is close to the router. Table 1-6 summarizes some of the key comparison points between these two manage-ment ports.

Table 1-6   Comparison of Router Console and Auxiliary Ports

Feature	Console	Auxiliary
Uses short cable, requiring the terminal to be close to the router	Yes	No
Intended for use as a remote-access method using modems and the PSTN	No	Yes
Router sends error messages to this port by default	Yes	No
Password recovery can be performed from this port	Yes	No
Sends router boot messages to this port	Yes	No

Summary

This chapter introduced a large variety of topics related to computer networking.

The major difference between a WAN and a LAN is the geographic area that is covered. A LAN connects workstations, printers, servers, and other devices within a building or other small area. A WAN is used to connect multiple LANs, typically over a large geographic area. The primary characteristics of a WAN include the ability to connect devices separated by wide geographic areas, the use of service providers to make these connections, and the serial connections used to access bandwidth.

WANs operate at the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2). Several organizations define WAN Layer 1 and 2 standards, including ITU, ISO, IETF, and EIA. Routers understand the Layer 1 and 2 details of both LANs and WANs, plus they use Layer 3 routing logic. The Layer 3 logic allows the routers to send packets over any type of LAN or WAN link, making good use of the different types of physical networks.

Routers are specialized computers whose primary purpose is to forward packets. Routers include the following components that help the router forward packets:

- **Cisco IOS**—The OS that runs on Cisco routers

- **CPU**—Executes instructions in the OS

- **RAM or DRAM**—Stores items used for the router's work, such as the routing table

- **NVRAM**—Stores the initial (startup) configuration file

- **Flash memory**—Acts as permanent memory, typically holding the Cisco IOS software

- **ROM**—Holds the bootstrap program and POST diagnostic programs

- **LAN interfaces**—Can be used to receive and forward packets

- **WAN interfaces**—Can be used to receive and forward packets

- **Management ports**—Include the router's console and auxiliary ports and can be used to access the router's CLI

A router's LAN interfaces typically connect to a LAN switch via a straight-through cable. A router's serial interface may connect to a WAN link via a serial cable, connected to a router serial port on one end and an external CSU/DSU on the other end of the cable. The CSU/DSU connects to the leased-line cable from the telco. For WAN links, the router acts as DTE, accepting clocking and synchronization from the CSU/DSU, acting as the DCE.

Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. Answers are listed in Appendix A, "Answers to Check Your Understanding and Challenge Questions."

1. Which of the following statements accurately describe differences between a LAN and a WAN? (Choose two)

   A. A LAN makes data connections across a broad geographic area, and a WAN makes a local connection in a building.

   B. Companies can use a WAN to connect remote locations, and a LAN can make a local connection in a building.

   C. WANs are usually faster than LANs.

   D. Only WANs require a CSU/DSU to be used on the ends of the cable.

2. Network professionals belong to organizations that plan and define standards used in networking. Which of the following are recognized industry organizations? (Choose two.)

   A. IETF

   B. UAS-K

   C. ISO

   D. EIA

   E. OSI-N

   F. ITU

3. Which of the following are true about a router? (Choose three.)

   A. Routers enable different IP networks or IP subnets to communicate with each other.

   B. Routers choose paths between networks using MAC address information.

   C. Path selection is one of the main functions of a router.

   D. Protocols are specialized chips on a router's motherboard to store routing tables.

   E. Routers have a central processing unit and memory.

   F. Only one network can be connected to a router at a time.

4. Which of the following are main components of a router? (Choose three.)

   A. ROM

   B. Flash memory

   C. CTG interfaces

   D. NV-ROM

   E. RAM

5. Which of the following statements describe the function of RAM in a router? (Choose two.)

   A. RAM stores the necessary Cisco IOS software for the router to begin booting.

   B. RAM is not necessary if extra NVRAM is available.

   C. RAM stores the current configuration information.

   D. RAM is maintained when the router is turned off.

   E. RAM stores routing tables for the router.

6. Which of the following statements are true about DTE? (Choose two.)

   A. DTE is an acronym for digital transfer enhancement.

   B. DTE provides clocking information to the provider.

   C. DTE usually resides on the customer's premises.

   D. DTE is an acronym for data terminal equipment.

   E. DTE is always connected to the first serial interface on a router.

7. Which of the following statements are true about DCE? (Choose two.)

   A. DCE is an acronym for digital clocking equipment.

   B. DCE provides clocking to the DTE.

   C. DCE is an acronym for data circuit-terminating equipment.

   D. DCE can be connected to the aux port on a router.

8. The term WAN refers to which layers of the OSI model? (Choose two.)

   A. Transport

   B. Data link

   C. Network

   D. Physical

   E. Session

   F. Presentation

9. Which of the following physical ports and/or cables on a router require clocking to be configured in a back-to-back connection? (Choose one.)

   A. Serial port with DTE cable

   B. Console

   C. Aux port

   D. Ethernet

   E. Serial port with DCE cable

10. Which of the following statements are true about router interfaces? (Choose two.)

   A. Interfaces must be connected to serial cables.

   B. LAN interfaces can work with straight-through or rollover cables.

   C. Ethernet interfaces usually use RJ-45 connectors.

   D. Interfaces can accept smart serial connectors.

11. What are possible functions of a console port? (Choose two.)

   A. Storing routing information

   B. Accessing the router to change configurations

   C. Telnet access to the router

   D. Password recovery

   E. Backup to the smart serial connections

12. In the following figure, which setting is different from the default for connecting to a Cisco router?

   A. Bits per second

   B. Data bits

   C. Parity

   D. Flow control
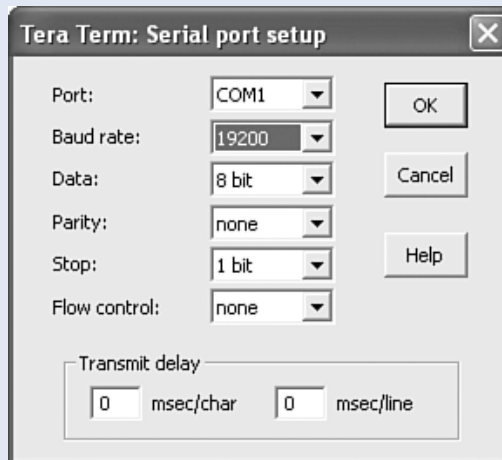
13. Which of the following are data-link encapsulations for WAN? (Choose three.)

   A. Frame Relay

   B. RIP

   C. IETF

   D. High-Level Data Link Control (HDLC)

14. Which of the following are used in WANs? (Choose two.)

   A. Hub

   B. Router

   C. Modem

   D. Multiport repeaters

   E. Bridges

15. Which of the following describe the function of flash memory in a router? (Choose three.)

   A. Holds the Cisco IOS software image

   B. Replaces the need for RAM chips

   C. Keeps its contents when a router is rebooted

   D. Can store multiple versions of Cisco IOS software

   E. Backs up configuration files

16. Which of the following are true about out-of-band router management? (Choose three.)

   A. Can be performed using the console port with a rollover cable

   B. Can be performed using Ethernet interfaces

   C. Provides access to Telnet services

   D. Can allow troubleshooting when a link is down

   E. Can be performed using a dialup connection

17. Which of the following are true about the items shown in the following figure? (Choose three.)

   A. Item B contains serial interfaces.

   B. Items C and D can be used for router management.

   C. Item C can use a crossover cable.

   D. Item B can accept either DTE or DCE cables.

   E. Item A can be used for a DCE.
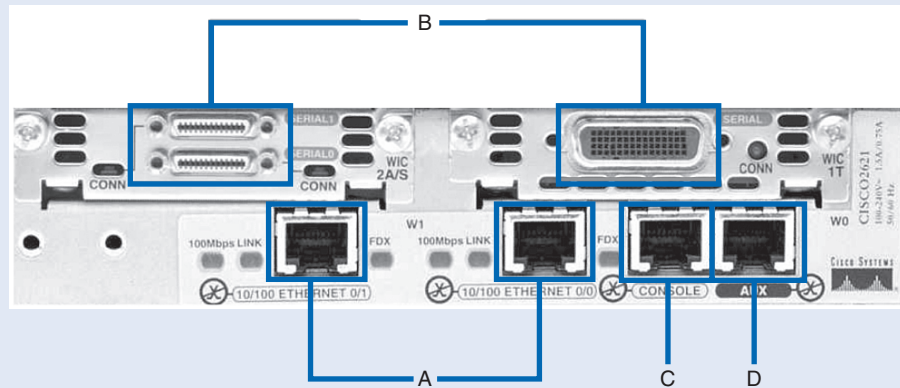
**18.** Which statement is true about a router? (Choose one.)

    A. The running configuration is stored in ROM, and flash memory holds the Cisco IOS software.

    B. NVRAM stores the startup configuration file, and RAM stores the running configuration.

    C. RAM stores the startup configuration file, and NVRAM stores the running configuration.

    D. Flash memory stores the running configuration, and ROM stores the Cisco IOS software.

Challenge Questions and Activities

These questions require a deeper application of the concepts covered in this chapter and are similar to the style of questions you might see on a CCNA certification exam. You can find the answers in Appendix A.

1. Which type of cable is used in the connections marked in the following figure?
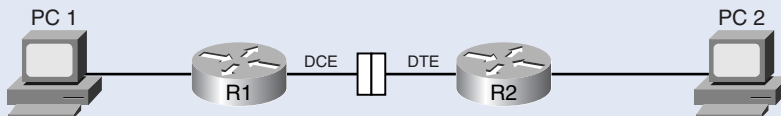
    A. PC1 to R1: _____

    B. R1 to R2: _____

    C. R2 to SW2: _____

    D. R2 to PC2: _____
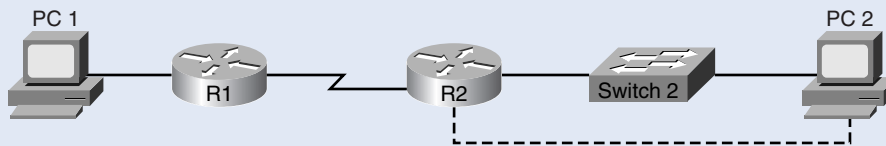
2. Router R1 has been used in a lab for the last several years. R1 connects to router R2 using a back-to-back serial connection, using its serial interface that does not have a built-in CSU/DSU. R1 also has a single Ethernet interface connected to a single PC without using a hub or switch. To save money, the IT manager has decided to use R1 for a new site being installed into the network, as shown in the bottom half of the following figure. Which of the following answers is true regarding other opportunities to save money with this new installation?

    A. R1 can use the serial cable that was formerly attached to R2, but not the serial cable that was formerly attached to R1.

    B. R1 can use the same Ethernet cable that it formerly used.

    C. If R1 changed its serial interface to use an integrated CSU/DSU, R1 could use the same serial cable as before.