Chapter 6

Connectivity Devices

People sometimes think of a network as a single, local cabling system that enables any device on the network to communicate directly with any other device on the same network. A network by this definition, however, has no connections to other remote networks.

An *internetwork* consists of multiple independent networks that are connected and can share remote resources. These logically separate but physically connected networks can be dissimilar in type. The device that connects the independent networks together may need a degree of "intelligence" because it may need to determine when packets will stay on the local network or when they will be forwarded to a remote network.

This chapter examines some important connectivity devices. In the following sections, you learn about modems, repeaters, bridges, routers, brouters, and gateways. (Some of this material also appears in Chapter 2, "Networking Standards," in the discussion of communication devices and OSI.)

Chapter 6 targets the following objective in the Planning section of the Networking Essentials exam:

Test Objectives

- Select the appropriate connectivity devices for various Token Ring and Ethernet networks. Connectivity devices include repeaters, bridges, routers, brouters, and gateways

Test Yourself

Stop! Before reading this chapter, test yourself to determine how much study time you will need to devote to this section.

1. Which of the following connectivity devices is the least expensive?

   A. Repeater

   B. Bridge

   C. Router

   D. Gateway

2. Which of the following connectivity devices uses logical addresses?

   A. Repeater

   B. Bridge

   C. Router

   D. None of the above

3. Which of the following connectivity devices connects dissimilar networking protocol environments?

   A. Repeater

   B. Bridge

   C. Router

   D. Gateway

4. A router that requires a human-configured routing table is called a(n) __________.

   A. explicit router

   B. static router

   C. simple router

   D. bridge

Modems

Standard telephone lines can transmit only analog signals. Computers, however, store and transmit data digitally. Modems can transmit digital computer signals over telephone lines by converting them to analog form.

Converting one signal form to another (digital to analog in this case) is called *modulation*. Recovering the original signal is called *demodulation*. The word "modem" derives from the terms modulation/demodulation.

Modems can be used to connect computer devices or entire networks that are at distant locations. (Before digital telephone lines existed, modems were about the only way to link distant devices.) Some modems operate constantly over dedicated phone lines. Others use standard public switched-telephone network (PSTN) dial-up lines and make a connection only when one is required.

Modems enable networks to exchange e-mail and to perform limited data transfers, but the connectivity made possible is extremely limited. By themselves, modems don't enable remote networks to connect to each other and directly exchange data. In other words, a modem is not an internetwork device. Nevertheless, modems can be used in conjunction with an internetwork device, such as a router, to connect remote networks through the PSTN or through an analog service, such as a 56 KB line.

note

Modems don't necessarily need to connect through the PSTN. Short-haul modems frequently are used to connect devices in the same building. A standard serial connection is limited to 50 feet, but short-haul modems can be used to extend the range of a serial connection to any required distance.

Many devices are designed to operate with modems. When you want to connect such devices without using modems, you can use a null-modem cable, which connects the transmitter of one device to the receiver of the other device.

Until recently, modem manufacturers used a parameter called *baud rate* to gauge modem performance. The baud rate is the oscillation speed of the sound wave transmitted or received by the modem. Although baud rate is still an important parameter, recent advances in compression technology have made it less meaningful. Some modems now provide a data transfer rate (in bits per second—a more meaningful measure of network performance) that exceeds the baud rate. In other words, you can no longer assume the baud rate and the data transfer rate are equal.

Modems are classified according to the transmission method they use for sending and receiving data. The two basic types of modems are as follows:

- Asynchronous modems
- Synchronous modems

The following sections describe asynchronous and synchronous transmission.

Asynchronous Transmission

Asynchronous transmission does not use a clocking mechanism to keep the sending and receiving devices synchronized. Instead, this type of transmission uses *bit synchronization* to synchronize the devices for each frame that is transmitted.

In bit synchronization, each frame begins with a start bit that enables the receiving device to adjust to the timing of the transmitted signal. Messages are kept short so that the sending and receiving devices do not drift out of synchronization for the duration of the message. Asynchronous transmission is most frequently used to transmit character data and is ideally suited to environments in which characters are transmitted at irregular intervals, such as when users enter character data.

Figure 6.1 illustrates the structure of a typical frame used to transmit character data. This frame has four components:

- **A Start bit.** This component signals that a frame is starting and enables the receiving device to synchronize itself with the message.
- **Data bits.** This component consists of a group of seven or eight bits when character data is being transmitted.
- **A parity bit.** This component is optionally used as a crude method of detecting transmission errors.
- **A stop bit or bits.** This component signals the end of the data frame.

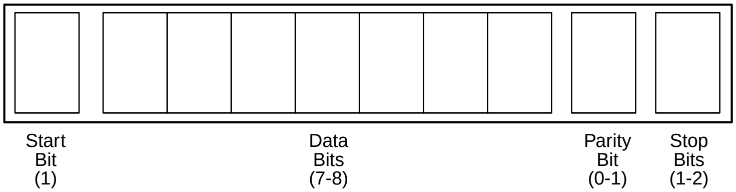


Figure 6.1

The structure of an asynchronous frame consists of four key bit components.

Asynchronous transmission is a simple, inexpensive technology ideally suited for transmitting small frames at irregular intervals. Because start, stop, and parity bits must be added to each character being transmitted, however, overhead for asynchronous transmission is high—often in the neighborhood of nearly 20 to 30 percent. This high overhead wastes bandwidth and makes asynchronous transmission undesirable for transmitting large amounts of data.

Asynchronous transmission is frequently used for PC-to-PC and terminal-to-host communication. Data in these environments is often of the bursty, character-oriented nature that is ideal for asynchronous communication. Asynchronous transmission generally requires less expensive hardware than synchronous transmission.

Synchronous Transmission

Synchronous transmission eliminates the need for start and stop bits by synchronizing the clocks on the transmitting and receiving devices. This synchronization is accomplished in two ways:

- **By transmitting synchronization signals with data.** Some data encoding techniques, by guaranteeing a signal transition with each bit transmitted, are inherently self-clocking.
- **By using a separate communication channel to carry clock signals.** This technique can function with any signal-encoding technique.

Figure 6.2 illustrates the two possible structures of messages associated with synchronous transmission.

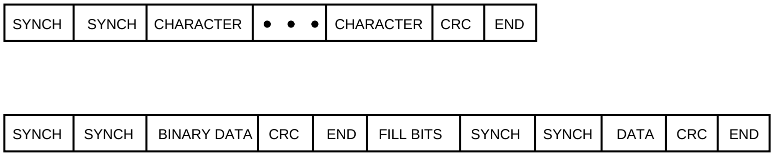


Figure 6.2

Structures of synchronous transmissions.

Both synchronous transmission methods begin with a series of *synch signals*, which notify the receiver of the beginning of a frame. Synch signals generally utilize a bit pattern that cannot appear elsewhere in messages, ensuring that the signals always are distinct and easily recognizable by the receiver.

A wide variety of data types can be transmitted. Figure 6.2 illustrates both character-oriented and bit-oriented data. Notice that under synchronous transmission, multiple characters or long series of bits can be transmitted in a single data frame. Because the transmitter and receiver remain in synchronization for the duration of the transmission, frames may be very long.

When frames are long, parity is no longer a suitable method for detecting errors. If errors occur, multiple bits are more likely to be affected, and parity techniques are less likely to report an error. A more appropriate error-control technique for synchronous transmission is the *cyclic redundancy check (CRC)*. In this technique, the transmitter uses an algorithm to calculate a CRC value that summarizes the entire value of the data bits. This value is then appended to the data frame. The receiver uses the same algorithm, recalculates the CRC, and compares the CRC in the frame to the CRC value it has calculated. If the values match, the frame almost definitely was transmitted without error.

When synchronous transmission links are idle, communicating devices generally send *fill bits* to the devices synchronized.

Synchronous transmission offers many advantages over asynchronous transmission. The overhead bits (synch, CRC, and end) comprise a smaller portion of the overall data frame, which provides for more efficient use of available bandwidth. Synchronization improves error detection and enables the devices to operate at higher speeds.

The disadvantage of synchronous transmission is that the more complex circuitry necessary for synchronous communication is more expensive.

Hubs

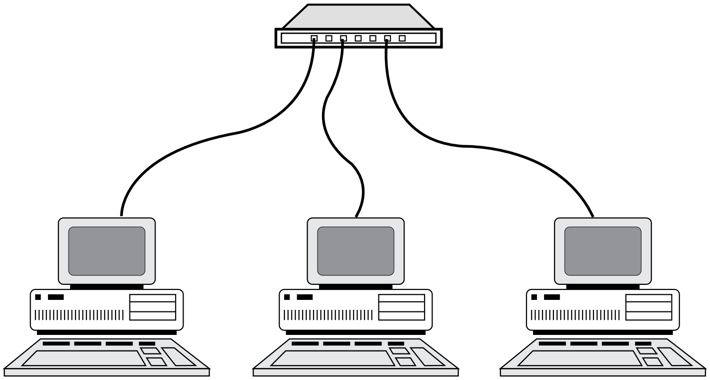
Hubs, also called *wiring concentrators*, provide a central attachment point for network cabling (see fig. 6.3). Coaxial cable Ethernet is the only LAN standard that doesn't use hubs. Hubs come in three types:

- Passive
- Active
- Intelligent

The following sections describe each of these types in more detail.

Figure 6.3

A network wired to a central hub.



Passive Hubs

Passive hubs do not contain any electronic components and do not process the data signal in any way. The only purpose of a passive hub is to combine the signals from several network cable segments. All devices attached to a passive hub receive all the packets that pass through the hub.

Because the hub doesn't clean up or amplify the signals (in fact, the hub absorbs a small part of the signal), the distance between a computer and the hub can be no more than half the maximum permissible distance between two computers on the network. For example, if the network design limits the distance between two computers to 200 meters, the maximum distance between a computer and the hub is 100 meters.

As you might guess, the limited functionality of passive hubs makes them inexpensive and easy to configure. That limited functionality, however, is also the biggest disadvantage of passive hubs. ARCnet networks commonly use passive hubs. Token Ring networks also can use passive hubs, although the industry trend is to utilize active hubs to obtain the advantages cited in the following section.

Active Hubs

Active hubs incorporate electronic components that can amplify and clean up the electronic signals that flow between devices on the network. This process of cleaning up the signals is called *signal regeneration.* Signal regeneration has the following benefits:

- The network is more robust (less sensitive to errors).
- Distances between devices can be increased.

These advantages generally outweigh the fact that active hubs cost considerably more than passive hubs.

Later in this chapter, you learn about *repeaters,* devices that amplify and regenerate network signals. Because active hubs function in part as repeaters, they occasionally are called *multiport repeaters.*

Intelligent Hubs

Intelligent hubs are enhanced active hubs. Several functions can add intelligence to a hub:

- **Hub management.** Hubs now support network management protocols that enable the hub to send packets to a central network console. These protocols also enable the console to control the hub; for example, a network administrator can order the hub to shut down a connection that is generating network errors.
- **Switching hubs.** The latest development in hubs is the switching hub, which includes circuitry that very quickly routes signals between ports on the hub. Instead of repeating a packet to all ports on the hub, a switching hub repeats a packet only to the port that connects to the destination computer for the packet. Many switching hubs have the capability of switching packets to the fastest of several alternative paths. Switching hubs are replacing bridges and routers on many networks.

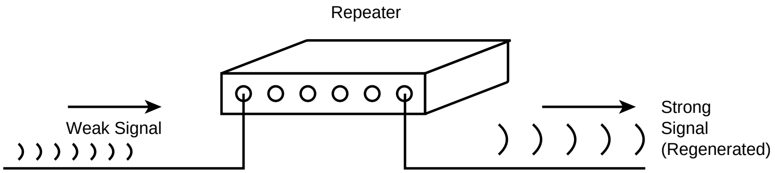
Repeaters

As you learned in Chapter 3, “Transmission Media,” all media attenuate the signals they carry. Each media type, therefore, has a maximum range that it can reliably carry data. The purpose of a repeater is to extend the maximum range for the network cabling.

A *repeater* is a network device that repeats a signal from one port onto the other ports to which it is connected (see fig. 6.4). Repeaters operate at the OSI Physical layer. (Refer to “The OSI Reference Model” section in Chapter 2.) A repeater does not filter or interpret—it merely repeats (regenerates) a signal, passing all network traffic in all directions.

Figure 6.4

A repeater regenerates a weak signal.



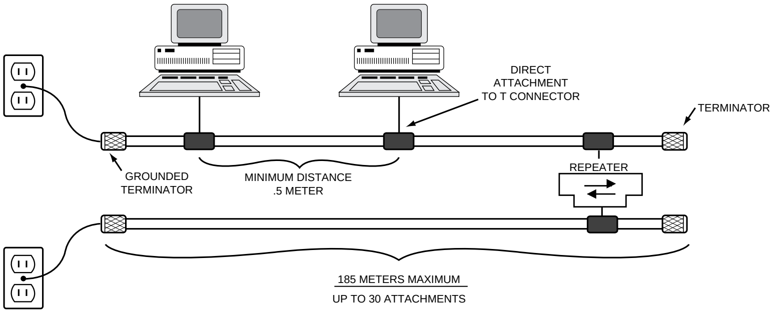
A repeater doesn't require any addressing information from the data frame because a repeater merely repeats bits of data. This means that if data is corrupt, a repeater will repeat it anyway. A repeater will even repeat a broadcast storm caused by a malfunctioning adapter (see Chapter 13, "Troubleshooting").

The advantages of repeaters are that they are inexpensive and simple. Also, although they cannot connect networks with dissimilar data frames (such as a Token Ring network and an Ethernet network), some repeaters can connect segments with similar frame types but dissimilar cabling.

Figure 6.5 shows the use of a repeater to connect two Ethernet cable segments. The result of adding the repeater is that the potential length of the overall network is doubled.

Figure 6.5

Using a repeater to extend an Ethernet LAN.



Some repeaters simply amplify signals. Although this increases the strength of the data signal, it also amplifies any noise on the network. In addition, if the original signal has been distorted in any way, an amplifying repeater cannot clean up the distortion.

Certainly, it would be nice if repeaters could be used to extend networks indefinitely, but all network designs limit the size of the network. The most important reason for this limitation is signal propagation. Networks must work with reasonable expectations about the maximum time a signal might be in transit. This is known as *propagation delay*—the time it takes for a signal to reach the farthest point on the network. If this maximum propagation delay interval expires and no signals are encountered, a network error condition is assumed. Given the maximum propagation delay allowed, it is possible to calculate the maximum permissible cable length for the network. Even though repeaters enable signals to travel farther, the maximum propagation delay still sets a limit to the maximum size of the network.

Bridges

Bridges, on the other hand, can extend the maximum size of a network. Although the bridged network in figure 6.6 looks much like the earlier example of a network with a repeater, the bridge is a much more flexible device. Bridges operate at the MAC sublayer of the OSI Data Link layer (see Chapter 2).

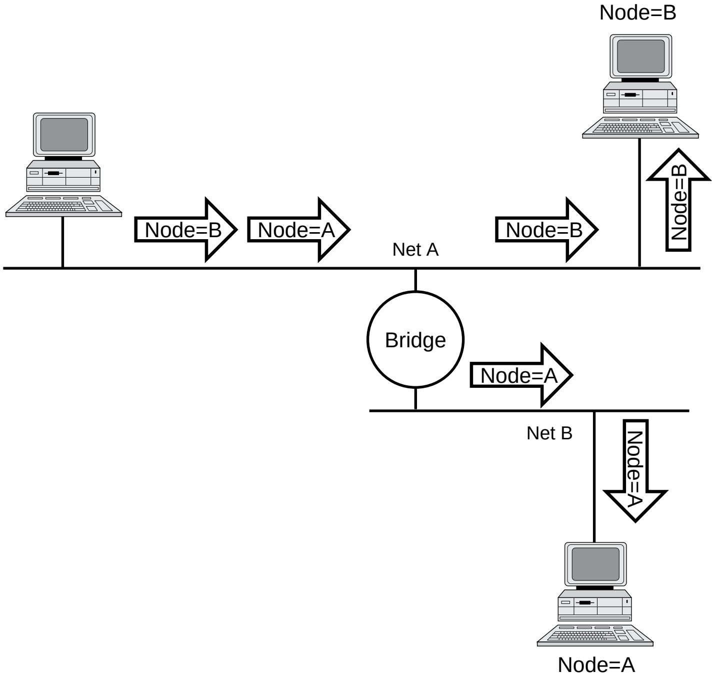


Figure 6.6

Extending a network with a bridge.

A repeater passes on all signals that it receives. A bridge, on the other hand, is more selective and passes only those signals targeted for a computer on the other side. A bridge can make this determination because each device on the network is identified by a unique address. Each packet that is transmitted bears the address of the device to which it should be delivered. The process works as follows:

1. The bridge receives every packet on LAN A and LAN B.
2. The bridge learns from the packets which device addresses are located on LAN A and which are on LAN B. The bridge then builds a table with this information.
3. Packets on LAN A that are addressed to devices on LAN A are discarded, as are packets on LAN B that are addressed to devices on LAN B. These packets can be delivered without the help of the bridge.
4. Packets on LAN A addressed to devices on LAN B are retransmitted to LAN B for delivery. Similarly, the appropriate packets on LAN B are retransmitted to LAN A.

On older bridges, the network administrator had to manually configure the address tables. Newer bridges are called *learning bridges.* Learning bridges function as described in step 2, automatically updating their address tables as devices are added to or removed from the network.

Bridges accomplish several things. First, they divide busy networks into smaller segments. If the network is designed so that most packets can be delivered without crossing a bridge, traffic on the individual network segments can be reduced. If the Accounting and Sales departments are overloading the LAN, for example, you might divide the network so that Accounting is on one segment and Sales on another. Only when Accounting and Sales must exchange packets does a packet need to cross the bridge between the segments.

Bridges also can extend the physical size of a network. Although the individual segments still are restricted by the maximum size imposed by the network design limits, bridges enable network designers to stretch the distances between segments and extend the overall size of the network.

Bridges, however, cannot join dissimilar types of LANs. This is because bridges depend on the physical addresses of devices. Physical device addresses are functions of the Data Link layer, and different Data Link layer protocols are used for each type of network. A bridge, therefore, cannot be used to join an Ethernet segment to a Token Ring segment.

Bridges sometimes are also used to link a LAN segment through a synchronous modem connection to another LAN segment at a remote location. A so-called *remote bridge* minimizes modem traffic by filtering signals that won't need to cross the modem line (see fig. 6.7).

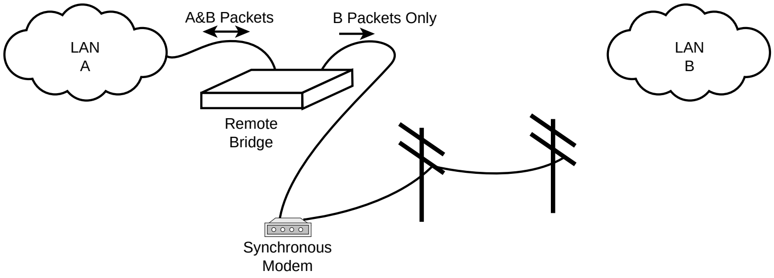


Figure 6.7

A remote bridge acts as a filter for a synchronous modem.

Routing

An internetwork consists of two or more physically connected independent networks that are able to communicate. The networks that make up an internetwork can be of very different types. For example, an internetwork can include Ethernet and Token Ring networks.

Because each network in an internetwork is assigned an address, each network can be considered logically separate; that is, each network functions independently of other networks on the internetwork. Internetwork connectivity devices, such as routers, can use network address information to assist in the efficient delivery of messages. Using network address information to deliver messages is called *routing*. The common feature that unites internetwork connectivity devices (routers and brouters) is that these devices can perform routing. The following list details some common internetwork connectivity devices:

- Routers
- Brouters
- Gateways

Each of these devices is discussed in the following sections.

Routers

Bridges are suitable for relatively simple networks, but bridges have certain limitations that become more significant in complex network situations. One limitation of bridges is that a network with bridges generally cannot include redundant paths. (Redundant paths are desirable because they enable the network to continue functioning when one path goes down.)

Consider the network in figure 6.8. Both bridges are aware of the existence of Node B, and both can pick up the packet from Net A and forward it. At the very least, the same packet can arrive twice at Node B.

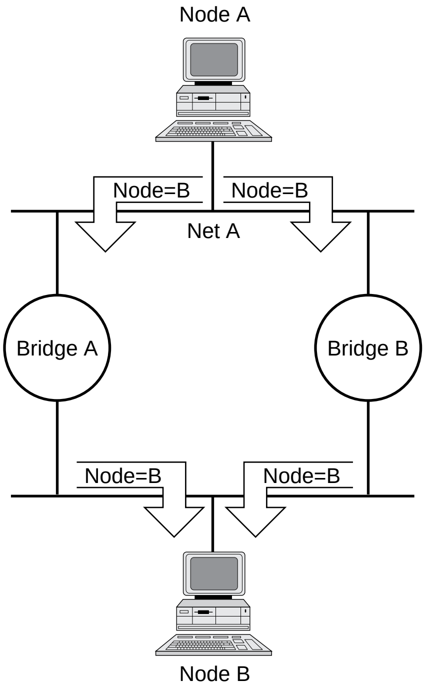
A worse case, however, is that these relatively unintelligent bridges can start passing packets around in loops, which results in an ever-increasing number of packets that circulate on the network and never reach their destinations. Ultimately, such activity can (and will) saturate the network.

note

An algorithm, called the *spanning tree algorithm*, enables complex Ethernet networks to use bridges while redundant routes exist. The algorithm enables the bridges to communicate and construct a logical network without redundant paths. The logical network is reconfigured if one of the paths fails.

Figure 6.8

A complex network with bridges.



Another problem is that the bridges cannot analyze the network to determine the fastest route over which to forward a packet. When multiple routes exist, this is a desirable capability, particularly in wide area networks (WANs), where some routes are often considerably slower than others.

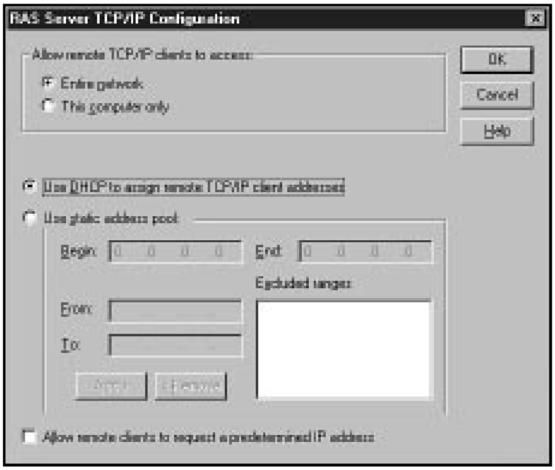
Routers organize the large network in terms of logical network segments. Each network segment is assigned an address so that every packet has both a destination network address and a destination device address.

note

Recall that an internetwork consists of two or more logically separate but physically connected networks. By this definition, any network segmented with routers is an internetwork.

Routing in Windows NT

The word “router” evokes the image of a screenless, box-shaped device—and many routers fit that image—but the tasks performed by a router can be (and sometimes are) performed by a PC. Many situations exist in which it is useful to configure a PC for routing functions, and one of the most important is when the PC serves as a remote access server. *Windows NT 4.0 Remote Access Service (RAS)*, for example, is capable of acting as an IP or an IPX router or a NetBIOS Gateway. (More on the NetBIOS Gateway in the next sidebar.) Modem connections used to enable only point-to-point communications (from one computer to another computer). Under Windows NT, the connection is still a point-to-point connection (from the remote client computer to the RAS server on the local LAN), but the RAS server can route packets to other computers, thus providing the remote client with access to the entire network (see fig. 6.9).



RAS Server TCP/IP Configuration

Allow remote TCP/IP clients to access:

● Entire network
○ This computer only

● Use DHCP to assign remote TCP/IP client addresses
○ Use static address pool

Begin: 0 0 0 0 End: 0 0 0 0

From:
To:

Excluded ranges:

□ Allow remote clients to request a predetermined IP address

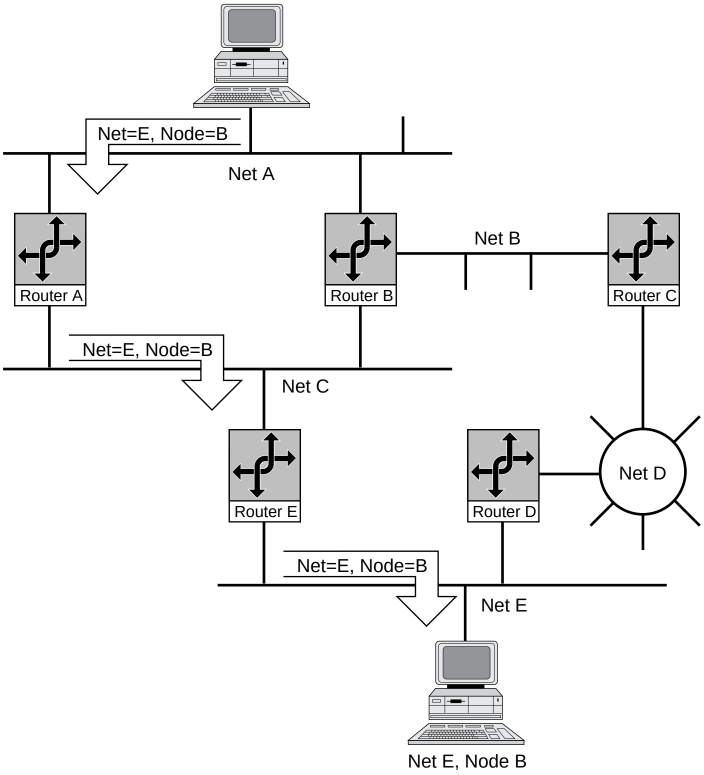
Figure 6.9

In the Windows NT RAS Server TCP/IP Configuration dialog box, you can access to either the entire network or to the RAS server machine only.

Figure 6.10 shows a complex network based on routers.

Figure 6.10

An internetwork with routers.



Routers are more "intelligent" than bridges. Not only do routers build tables of network locations, but they also use algorithms to determine the most efficient path for sending a packet to any given network. Even if a particular network segment isn't directly attached to the router, the router knows the best way to send a packet to a device on that network. In figure 6.10, for example, Router A knows that the most efficient step is to send the packet to Router C, not Router B.

Notice that Router B presents a redundant path to the path Router A provides. Routers can cope with this situation because they exchange routing information to ensure that packet loops don't occur. In figure 6.10, if Router A fails, Router B provides a backup message path, thus making this network more robust.

note

One consequence of all the processing a router performs on a packet is that routers generally are slower than bridges.

You can use routers to divide large, busy LANs into smaller segments, much as you can use bridges. But that's not the only reason to select a router. Routers also can connect different network types. Notice that the network in figure 6.10 includes a Token Ring segment with the Ethernet segments. On such networks, a router is the device of choice.

note

The protocols used to send data through a router must be specifically designed to support routing functions. IP, IPX, and DDP (the AppleTalk Network-layer protocol) are routable protocols. NetBEUI is a nonroutable protocol.

Because routers can determine route efficiencies, they usually are employed to connect a LAN to a wide area network (WAN). WANs frequently are designed with multiple paths, and routers can ensure that the various paths are used most efficiently.

note

The Network layer functions independently of the physical cabling system and the cabling system protocols—independently, that is, of the Physical and Data Link layers. This is the reason that routers easily can translate packets between different cabling systems. Bridges, on the other hand, cannot translate packets in this way because they function at the Data Link layer, which is closely tied to physical specifications.

Routers come in two types:

- **Static Routers.** These routers do not determine paths. Instead, you must configure the routing table, specifying potential routes for packets.
- **Dynamic Routers.** These routers have the capability to determine routes (and to find the optimum path among redundant routes) based on packet information and information obtained from other routers.

To determine the best path for a packet, routers employ some form of routing algorithm. Some common routing algorithms are discussed in the following sections.

Routing Algorithms

Routing refers to the process of forwarding messages through switching networks. In some cases, routing information is programmed into the switching devices. However, preprogrammed switches cannot adjust to changing network conditions. Most routing devices, therefore, are dynamic, which means that they have the capability of discovering routes through the internetwork and then storing the route information in route tables.

Route tables do not store only path information. They also store estimates of the time taken to send a message through a given route. This time estimate is known as the cost of a particular path. Some of the methods of estimating routing costs are as follows:

- **Hop count.** This method describes the number of routers that a message might cross before it reaches its destination. If all hops are assumed to take the same amount of time, the optimum path is the path with the smallest hop count.
- **Tic count.** This method provides an actual time estimate, where a *tic* is a time unit as defined by the routing implementation.
- **Relative expense.** This method calculates any defined measure of the cost (including the monetary cost) to use a given link.

After costs are established, routers can select routes, either statically or dynamically, as follows:

- **Static route selection.** This selection method uses routes that have been programmed by the network administrator.
- **Dynamic route selection.** Under this selection method, routing cost information is used to select the most cost-effective route for a given packet. As network conditions change and are reflected in routing tables, the router can select different paths to maintain low costs.

Two common methods of discovering routes are *distance vector routing* and *link-state routing*. Both are discussed in the following sections.

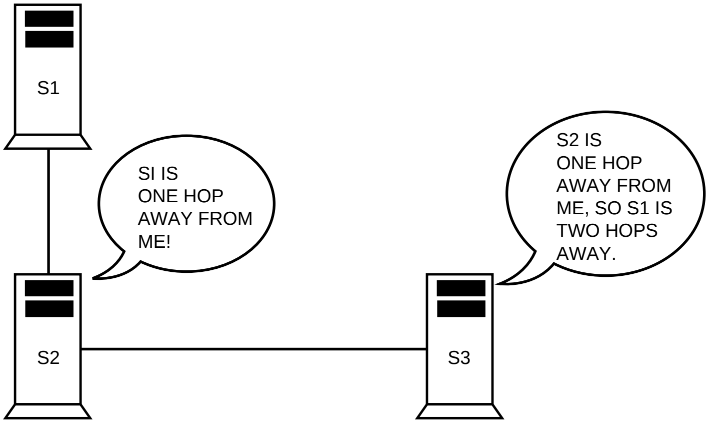
Distance Vector Routing

Distance vector routers advertise their presence to other routers on the network. Periodically, each router on the network broadcasts the information in its routing table. Other routers can use this information to update their own router tables.

Figure 6.11 illustrates how the process works. In the figure, Server S3 learns that Server S2 can reach Server S1 in three hops. Because S3 knows that S2 is one hop away, S3 knows that its cost to reach S1 through S2 is two hops.

Figure 6.11

Distance vector routing.


S1
SI IS ONE HOP AWAY FROM ME!
S2 IS ONE HOP AWAY FROM ME, SO S1 IS TWO HOPS AWAY.
S2
S3

Distance vector routing is an effective algorithm, but it can be fairly inefficient. Because changes must ripple through the network from router to router, it might take a while for a change to become known to all routers on the network. In addition, the frequent broadcasts of routing information produce high levels of network traffic that can hurt performance on larger networks.

Link-State Routing

Link-state routing reduces the network traffic required to update routing tables. Routers that are newly attached to the network can request routing information from a nearby router.

After routers have exchanged routing information about the network, routers broadcast messages only when something changes.

These messages contain information about the state of each link the router maintains with other routers on the network. Because routers keep each other updated, complete network routing updates are not needed often.

Brouters

A *brouter* is a router that also can act as a bridge. A brouter attempts to deliver packets based on network protocol information, but if a particular Network layer protocol isn't supported, the brouter bridges the packet using device addresses.

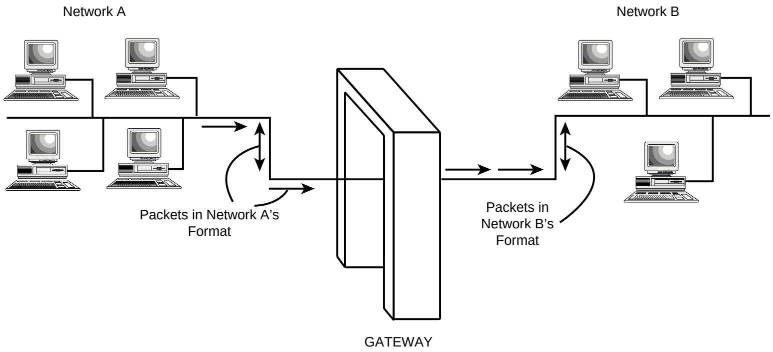
Gateways

The term "gateway" originally was used in the Internet protocol suite to refer to a router. Today, the term "gateway" more commonly refers to a system functioning at the top levels of the OSI model that enables communication between dissimilar protocol systems. A gateway generally is dedicated to a specific conversion, and the exact functioning of the gateway depends on the protocol translations it must perform. Gateways commonly function at the OSI Application layer.

Gateways connect dissimilar environments by removing the layered protocol information of incoming packets and replacing it with the packet information necessary for the dissimilar environment (see fig. 6.12).

Figure 6.12

Gateways convert packet protocol information to connect dissimilar environments.



Gateways can be implemented as software, hardware, or a combination of both.

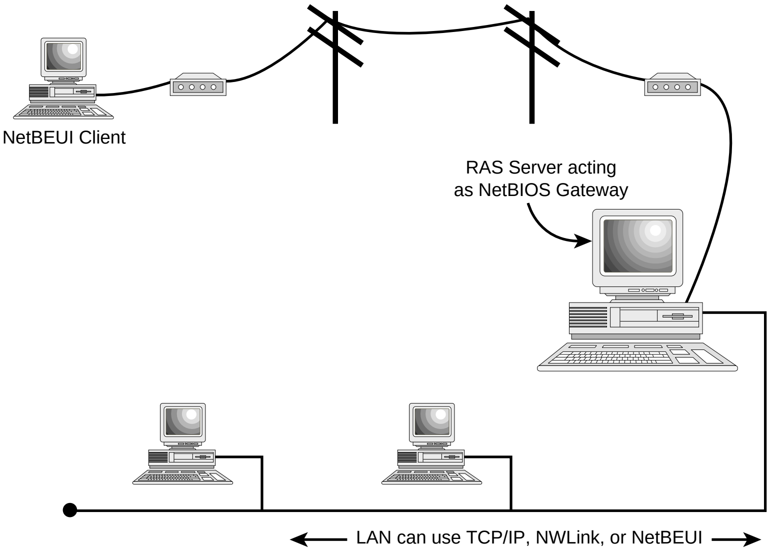
The NetBIOS Gateway

A previous sidebar described how Windows NT 4.0 RAS can act as an IP or an IPX router. RAS's NetBIOS gateway is an even more powerful feature. Not only does the NetBIOS gateway forward remote packets to the LAN, but it also acts as a gateway, providing NetBEUI clients with access to the LAN even if the LAN uses only TCP/IP or IPX/SPX.

The NetBIOS gateway (see fig. 6.13) is very much like the gateways described in this section. The NetBIOS gateway accepts a packet from the remote computer using one protocol (NetBEUI) and converts the packet, stripping incompatible protocol headers and replacing them with the headers the packet will need to circulate under a different protocol.

Figure 6.13

The Windows NT NetBIOS Gateway.


NetBEUI Client
RAS Server acting as NetBIOS Gateway
LAN can use TCP/IP, NWLink, or NetBEUI

Summary

This chapter examined some of the connectivity devices that network engineers use to expand, optimize, and interconnect networks. These devices have some similarities, but each is designed for a specific task, as described in the following list:

- **Repeaters.** Repeaters regenerate a signal and are used to expand LANs beyond cabling limits.
- **Bridges.** Bridges know the side of the bridge on which a node is located. A bridge passes only packets addressed to computers across the bridge, so a bridge can thus filter traffic, reducing the load on the transmission medium.
- **Routers.** Routers forward packets based on a logical (as opposed to a physical) address. Some routers can determine the best path for a packet based on routing algorithms.
- **Gateways.** Gateways function under a process similar to routers except that gateways can connect dissimilar network environments. A gateway replaces the necessary protocol layers of a packet so that the packet can circulate in the destination environment.

You should be familiar with the features of these connectivity devices and with their relative advantages and disadvantages for the Networking Essentials exam.

Exercises

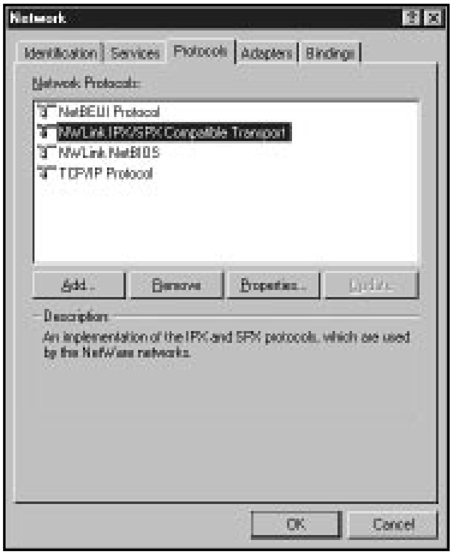
Exercise 6.1: Enabling IPX Routing

Objective: Learn to configure Windows NT Server's NWLink properties so that your Windows NT Server system can act as an IPX router.

Time estimate: 10 minutes

To configure Windows NT Server for IPX routing, you must install the NWLink protocol and add the RIP for NWLink IPX service.

1. Click the Start button and choose Settings/Control Panel.
2. In the Windows NT Control Panel, double-click the Network application and select the Protocols tab (see fig. 6.14).



An implementation of the IPX and SPX protocols, which are used by the NetWare networks.

Figure 6.14

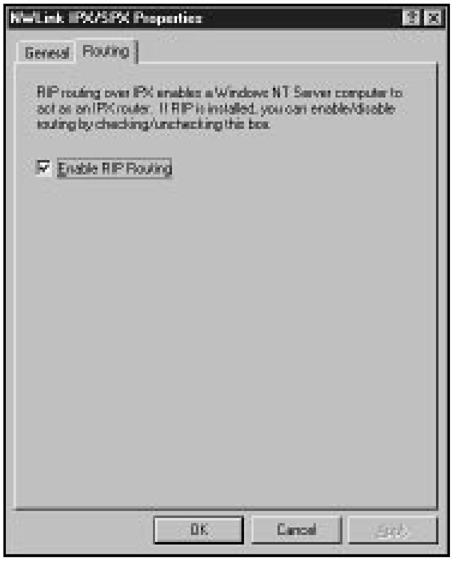
The Network application's Protocols tab.

3. Make sure that the NWLink IPX/SPX Compatible Transport is installed. If it isn't, click the Add button and choose NWLink Compatible Transport from the protocols list. Windows NT asks for the Windows NT installation disk and prompts you for NWLink configuration information. (You can let it default if you're just doing this as a test.) Don't shut down your system yet.

continues

Exercise 6.1: Continued

4. Select the Network application's Services tab. Make sure that the RIP for NWLink IPX service is installed. If it isn't, click the Add button and select RIP for NWLink IPX from the Services list. RIP enables routing on IPX/SPX (and NWLink) networks. Windows NT asks for the Windows NT installation disk.
5. Restart your computer. Return to the Network application and select the Protocols tab.
6. Select NWLink IPX/SPX Compatible Transport and click the Properties button.
7. In the NWLink IPX/SPX Properties dialog box, select the Routing tab. A check box lets you enable/disable RIP routing (see fig. 6.15). (If you just installed RIP, RIP routing will be enabled by default.)



RIP routing over IPX enables a Windows NT Server computer to act as an IPX router. If RIP is installed, you can enable/disable routing by checking/unchecking this box.

☑ Enable RIP Routing

Figure 6.15

The Routing tab of the NWLink IPX/SPX Properties dialog box enables you to enable or disable routing.

Warning

Both the TCP/IP suite and the IPX/SPX suite have protocols called RIP (refer to Chapter 5, "Transport Protocols"). These protocols have similar functions, but they are unrelated. Make sure you install the RIP for NWLink IPX service in this exercise and not the RIP for Internet Protocol service.

Review Questions

The following questions test your knowledge of the information in this chapter. For additional exam help, visit Microsoft's site at www.microsoft.com/train_cert/cert/Mcpsteps.htm.

1. Your LAN includes computers in two rooms at different ends of the company office. The cables connecting the rooms exceed the maximum cabling distance for the transmission medium, and the network is experiencing problems due to signal loss in the long cables. The cheapest and simplest solutions would be to add a __________.

   A. router

   B. repeater

   C. bridge

   D. brouter

2. Your Ethernet LAN is experiencing performance problems due to heavy traffic. A simple solution would be to add a __________.

   A. gateway

   B. repeater

   C. bridge

   D. router

3. The __________ algorithm enables bridges to operate on a network with redundant routes.

   A. distance vector

   B. link-state

   C. spanning tree

   D. learning tree

4. You need to connect a Windows NT LAN with a Unix network. To do so, you will need a __________.

   A. bridge

   B. gateway

   C. brouter

   D. router

5. You need to connect a Token Ring and an Ethernet LAN segment. To do so, you will need a __________.

   A. repeater

   B. bridge

   C. remote bridge

   D. router

6. A __________ uses a routing table to determine where to send a packet.

   A. bridge

   B. router

   C. both A and B

   D. none of the above

7. Which three of the following are advantages of active hubs?

   A. They can regenerate network signals.

   B. LAN ranges can be extended.

   C. They are inexpensive.

   D. They function as repeaters.

8. Which two networks can use passive hubs?

   A. Ethernet

   B. ARCnet

   C. Token Ring

   D. All the above

9. Which two of the following features can add intelligence to a hub?

   A. Signal regeneration

   B. Network-management protocols

   C. Multiport repeaters

   D. Switching circuitry

10. Which two statements are true of repeaters?

    A. Repeaters filter network traffic.

    B. Repeaters extend network distances.

    C. Repeaters regenerate signals.

    D. Repeaters operate at the OSI Data Link layer.

11. Which three statements are true of bridges?

    A. Bridges amplify and regenerate signals.

    B. Bridges can connect logically separate networks.

    C. Bridges use device address tables to route messages.

    D. Bridges divide networks into smaller segments.