Network Hardware And Topologies

Terms you'll need to understand:

- √ Network interface card (NIC)
- √ Interrupt request line (IRQ)
- √ Base memory address
- √ Transceiver
- √ Repeater
- √ Amplifier
- √ Hub
- √ Bridge
- √ Router
- √ Brouter
- √ Gateway
- √ Bus
- √ Ring
- √ Star
- √ Mesh

Techniques you'll need to master:

- √ Installing and configuring a network interface card
- √ Understanding and configuring IRQs
- √ Understanding hubs, bridges, routers, brouters, and gateways and their uses
- √ Knowing the features, advantages, and disadvantages of the bus, ring, star, and mesh topologies

In the previous chapter, you learned about network cables and connectors. This chapter continues the discussion of the physical network by explaining network adapter configuration. We also cover the various methods and standards related to configuring a network and the devices used to connect separate networks.

Networking Components

There are many networking devices that you can use to create, segment, and enhance networks. In this section, we discuss several networking devices, such as network adapter cards, repeaters, amplifiers, bridges, routers, and gateways.

Adapters

The network adapter, or NIC (network interface card), is the piece of hardware that physically connects a computer to the network. Before you make this connection, you must successfully install and configure this card. The simplicity or complexity of this installation and configuration depends on the type of network adapter you decide to use. For some configurations, you may not have to do anything other than install the network card in the appropriate slot in your computer. Self-configuring and Plug and Play adapters automatically configure themselves appropriately. If you don't have a Plug and Play adapter, or are using an OS that doesn't support Plug and Play, you must configure the interrupt request line (IRQ, or interrupt) and the Input/Output (I/O) address. The IRQ is the logical communication line that the device uses to communicate with the processor. The I/O address is a three-digit hexadecimal number that identifies a communication channel between hardware devices and the CPU. Both the IRQ and I/O address must be appropriately configured for the network card to function correctly.

You should know the common interrupts and I/O addresses so that you can configure the network card to operate without conflict. Usually, if two devices have the same resources (I/O address or IRQ) assigned, there will be a conflict. Therefore, your goal is to find and set a unique IRQ and I/O address for the network card to use. The interrupts, I/O addresses, and related devices that you should know are described in Table 5.1.

Table 5.1 Vital statistics for common interrupts and I/O addresses.

Common Use	IRQ	I/O Addresses
System timer	0	N/A
Keyboard	1	N/A
Secondary IRQ controller or video adapter	2	N/A
COM 2 or COM 4	3	2F0 to 2FF
COM 1 or COM 3	4	3F0 to 3FF
Usually unassigned (may be used by LPT 2 or sound card)	5	N/A
Floppy disk controller	6	N/A
LPT 1	7	N/A
Realtime clock	8	N/A
Usually unassigned (may cascade from IRQ 2)	9	370 to 37F
Usually unassigned (may be a primary SCSI controller)	10	N/A
Usually unassigned (may be a secondary SCSI controller)	11	N/A
PS/2 Mouse	12	N/A
Math coprocessor	13	N/A
Primary hard disk controller	14	N/A
Unassigned (may be a secondary hard disk controller)	15	N/A

IRQ 2 cascades to IRQ 9 because there were only eight IRQ options originally. To create 15 IRQ options, IRQ 2 was used to create a second set of IRQs starting at IRQ 9. This means that IRQ 2 is actually an indicator between the first set of IRQs (0 through 8) and the second set (9 through 15).

Base Memory Address

Some NICs have the capability to use the computer's memory (RAM) as a buffer to store incoming and outgoing data frames. The base memory address is a hexadecimal value that represents a location in RAM where

this buffer resides. Because other devices also use base memory addresses in RAM, it's important to remember to select a base memory address that does not conflict with other devices. The Windows 95 or 98 Device Manager reports the settings for individual devices and determines if there are any conflicts in the system (see Figure 5.1). If you have Windows NT, use Windows NT Diagnostics (WINMSD.EXE) to determine which system resources are being utilized.

Transceiver Settings

Network cards support various types of network connections. On a NIC, the physical interface between itself and the network is called a transceiver—a term used to refer to a device that both transmits and receives data. Transceivers on network cards can receive and transmit digital or analog signals. The type of interface that the network adapter uses can often be defined on the physical network adapter. Jumpers (small connectors that create a circuit between two pins on the physical card) can usually be set to specify the type of transceiver the adapter should use, according to the networking scheme. For example, a jumper set in one position may enable the RJ-45 connector to support a twisted-pair network; in another position, the same jumper might enable an external transceiver to be used in a 10Base5 (Thicknet) network. (This option may be selected by setup software in newer NICs.)

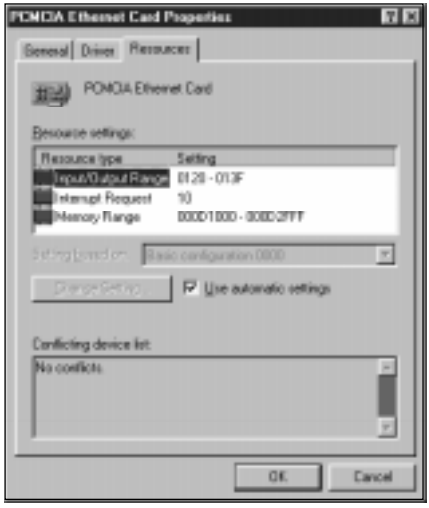


Figure 5.1 Windows 95 Device Manager PCMCIA Ethernet Card Properties dialog box.

Configuration Scenario

Suppose you want to install a network adapter in your computer, which is already using COM 1, COM 2, LPT 1, and LPT 2 (all using their common default settings). You have a network card that is configured for IRQ 7 and I/O port 0x300. Which device will be in conflict with the network adapter? If you take a look at the interrupt lines listed in Table 5.1, you will see that LPT 1 uses interrupt 7 for its communications. This means that either LPT 1 or the network card will have to use a different interrupt to resolve the conflict. If you decide to reset the interrupt on the network card, what interrupts can you use based on the information given? Again, from Table 5.1, you should see that IRQ 5 is taken by LPT 2, and IRQs 4 and 3 are being used by COM 1 and 2, respectively. This means that the normally available interrupts 9, 10, 11, and 15 would most likely be open.

If you are using Windows 95, you can view a list of interrupts in use by selecting the Computer Properties dialog box in the Device Manager, shown in Figure 5.2. This would give you a quick view of the resources in use on your computer. To see the resources in use on a Windows NT system, you would use the Windows NT Diagnostics program.

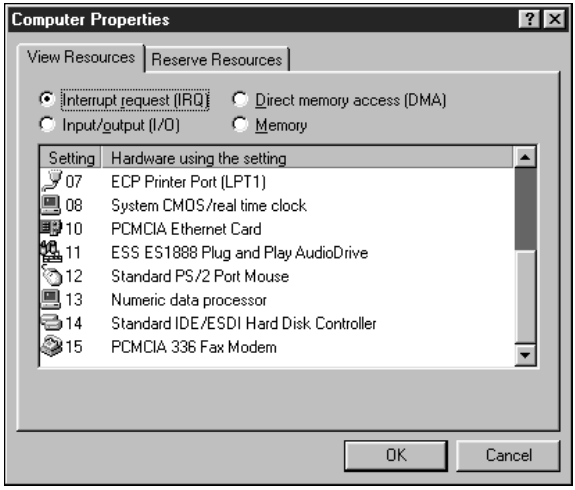


Figure 5.2 Windows 95 Device Manager Computer Properties dialog box.

Repeaters And Amplifiers

As mentioned in Chapter 4, signal strength degrades, or attenuates, over distance. To counteract signal degradation, you can use repeaters and/or amplifiers, which boost the signals that pass through them on the network.

Repeaters are used in networks with digital signaling schemes to combat attenuation. Also known as baseband transmission, digital signals consist of data bits that are either on or off, represented by a series of ones and zeros. Repeaters allow for reliable transmission at greater distances than the media type would normally allow. When a repeater receives an attenuated incoming baseband transmission, it cleans up the signal, increases its strength, and passes it on to the next segment.

Amplifiers, although similar in purpose, are used to increase transmission distances on networks that use analog signaling, referred to as broadband transmission. Analog signals can transfer both voice and data simultaneously—the wire is divided into multiple channels so different frequencies can be transferred at the same time.

Repeaters (and amplifiers) operate at the Physical layer of the OSI model. They can be used to connect cable segments—even those using different media types—as long as both segments to be joined use the same media-access method. In fact, most hubs (excluding passive hubs) function as repeaters.

Usually, network architectures specify the maximum number of repeaters allowed on a single network. The reason for this is a phenomenon called *propagation delay*. In cases where there are multiple repeaters on the same network, the brief period of time each repeater takes to clean up and amplify the signal, multiplied by the number of repeaters/amplifiers, can cause a noticeable delay of transmissions on the network. When deciding whether to choose repeaters as a connection option, you must also consider that they have no addressing or translation capability, and thus, cannot be used to ease network congestion.

Hubs

A hub is a hardware device, operating at the OSI Physical layer, that acts as a central connecting point and joins lines in a star network configuration (star configuration is covered in the next section). There are three main types of hubs: passive, active, and intelligent. Passive hubs, which don't require power, act merely as a physical connection point, adding nothing to the signals that pass through. Active hubs, on the other hand, require power,

which they use to regenerate and strengthen signals passing through them. Intelligent hubs can provide services such as packet switching and traffic routing.

Bridges

The bridge is another device used to connect network segments. Bridges can be an improvement over repeaters because bridges ease congestion on busy networks. Bridges read the target destination's MAC address from each incoming data packet, then examine the "bridging" tables to determine what to do with the packet.

Bridges operate at the Data Link layer of the OSI model.

Because it functions basically as a repeater, a bridge can receive transmissions from any segment; however, it is more discriminating than a repeater in retransmitting these signals. If the packet's destination address is on the same segment the packet was received on, the bridge will not forward the packet. But, if the packet's destination lies on a different segment, the bridge knows to pass it along. By only fowarding packets destined for other network segments, the bridge reduces network congestion. However, bridges do forward all broadcast transmissions they receive, and therefore, are unable to reduce broadcast traffic.

Bridges can connect segments that use different media types; for example, a connection of 10BaseT media to 10Base2. Bridges can also connect networks using different media-accessing schemes, such as an Ethernet network and a Token Ring network. An example of such a device is a translation bridge, which is a bridge that translates between different media-access methods, allowing the translation bridge to link various network types. Another special type of bridge, a transparent bridge (or learning bridge), "learns" over time where to direct packets it receives. It does this by continually building bridging tables, adding new entries when they become necessary.

Possible disadvantages of bridges are the fact that they take longer than repeaters to pass data through because they examine the MAC address of each packet. They are also more expensive and difficult to operate.

Routers

A router is a networking connectivity device that works at the OSI Network layer and can link two or more network segments (or subnets). It functions in a similar manner to a bridge; but, instead of using the machine's MAC address to filter traffic, it uses the network address information found in the Network layer area of the data packet. After obtaining this address information, the router uses a routing table of network addresses to determine where to forward the packet. It does this by comparing the packet's network address to the entries in the routing table. If a match is found, the packet is sent to the determined route. If a match is not found, however, the data packet is usually discarded.

Routers work at the Network layer of the OSI model.

There are two types of routing devices: static and dynamic. Static routers use routing tables that a network administrator must create and update manually. In contrast, dynamic routers build and update their own routing tables. They use information found on both their own segments and data obtained from other dynamic routers. Dynamic routers contain constantly updated information on possible routes through the network, as well as information on bottlenecks and link outages. This information lets them determine the most efficient path available at a given moment to forward a data packet to its destination.

As routers can make intelligent path choices—and filter out packets they do not need to receive—they help lessen network congestion, conserve resources, and boost data throughput. Additionally, they make data delivery more reliable because routers can select an alternate path for the packet if the default route is down.

The term "router" can refer to a piece of electronic hardware designed specifically for routing. Router can also mean a computer (equipped with a routing table) that is attached to different network segments through multiple NICs, and hence, can fulfill a routing function between the linked segments.

Routers are superior to bridges in their ability to filter and direct data packets across the network. In addition, unlike bridges, they can be set to not forward broadcast packets, which reduces network broadcast traffic. Another major advantage of the router as a connectivity device is that, because it works at the Network layer, it can connect networks that use different

network architectures and media-access methods. Routers cannot translate across protocols. A router can, for example, connect an Ethernet subnet to a Token Ring segment.

Routable protocols, like TCP/IP and IPX/SPX, are those that have Network layer addressing information. A non-routable protocol, such as NetBEUI, does not contain network address information. Because the router operates at this layer, it is only able to process protocols that include network address information.

There are several factors you need to consider when deciding on a router as a connectivity device. Routers are more expensive and difficult to operate than repeaters. They have slower throughput than bridges because they must perform additional processing on the data packet. Also, dynamic routers can add excessive traffic to the network because of the constant messages they send to each other when updating their routing tables.

Brouters

The term *brouter* is a combination of the words "bridge" and "router." As its name would suggest, a brouter combines the functions of a bridge and a router. When a brouter receives a data packet, it checks to see if the packet was sent in either a routable or non-routable protocol. If it is a routable protocol packet, the brouter will perform a routing function, sending the packet to its destination outside the local segment, if necessary.

In contrast, if the packet contains a non-routable protocol, the brouter performs a bridging function, using the MAC address to find the proper recipient on the local segment. Brouters must maintain both bridging and routing tables to perform these two functions; therefore, they operate at both the Data Link and Network layers of the OSI model.

Gateways

A gateway is a method of enabling communications between two or more network segments. A gateway is usually a dedicated computer that runs gateway software and provides a translation service, which allows for communications between dissimilar systems on the network. For example, using a gateway, an Intel-based PC on one segment can both communicate and share resources with a Macintosh computer or a mainframe.

Another function of gateways is to translate protocols. A gateway can receive an IPX/SPX message that is bound for a client running another protocol, such as TCP/IP, on a remote network segment. After it determines

that the message packet's destination is a TCP/IP station, the gateway will actually convert the message data to the TCP/IP protocol. (This is in contrast with a bridge, which merely "tunnels" a message using one protocol inside the data format of another protocol—if translation is to occur, the receiving end does it.) Mail gateways perform similar translation operations. They convert emails and other mail transmissions from your native mail application's format to a more universal mail protocol, such as SMTP, which can then be used to route the message across the Internet.

Gateways primarily operate at the Application layer of the OSI model, although they often fulfill certain functions at the Session layer and occasionally as low as the Network layer. However, for most purposes, consider the gateway to operate only at or above the Transport layer.

Although gateways have many advantages, you need to consider a few things when deciding whether to use them on your network. Gateways are difficult to install and configure. They are also more expensive than other connectivity devices. One other issue: Due to the extra processing cycle that the translation process requires, gateways can be slower than routers and related devices.

Network Topologies

A network's topology is a description of its physical layout. How computers are connected to each other on the network and the devices that connect them are included in the physical topology. There are four basic topologies: bus, ring, star, and mesh. Other topologies are usually hybrids of two or more of the main types. Choosing the physical topology type for your network is one of the first steps in planning. The choice of a topology will depend on a variety of factors, such as cost, distances, security needs, which network operating system you intend to run, and whether the new network will use existing hardware, conduits, and so on.

Bus

A physical bus topology, also called a linear bus, consists of a single cable to which all the computers in the segment are attached (see Figure 5.3). Messages are sent down the line to all attached stations, regardless of which one is the recipient. Each computer examines every packet on the wire to determine whom the packet is for; if it is for another station, the computer discards it. Likewise, a computer will receive and process any packets on the bus that are addressed to it.

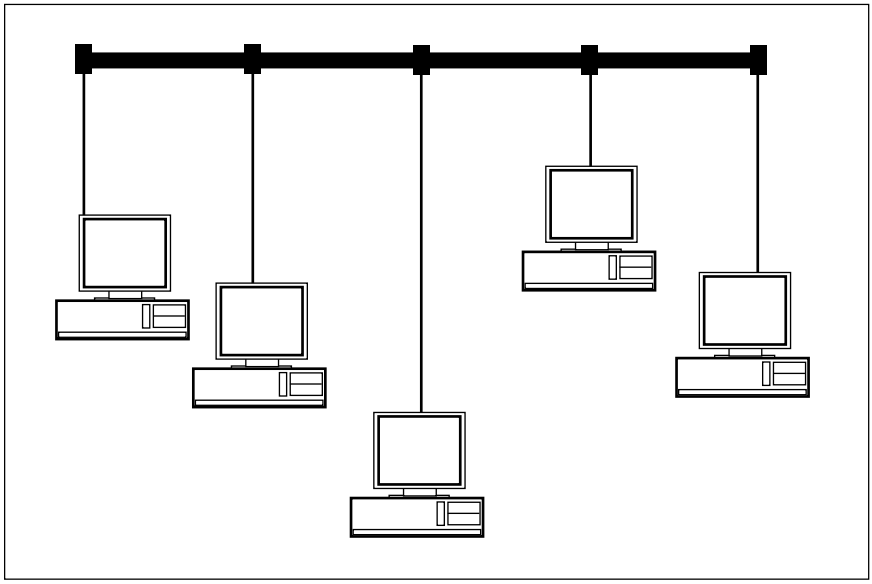


Figure 5.3 The bus topology connects computers to a linear segment.

The bus' main cable, known as the backbone, is terminated at each end to prevent message transmissions from bouncing back and forth between the two ends of the bus. Two media types commonly used in bus networks, Thicknet and Thinnet (refer back to Chapter 4 for discussion of these terms), require 50-ohm terminators. Without proper termination, communications on the bus will be unreliable, or will fail altogether.

The bus topology is the fastest and simplest way to set up a network. It requires less hardware and cabling than other topologies, and it is easier to configure. It is good way to quickly set up a temporary network. It is also usually the best choice for small networks (that is, those with 10 computers or less).

There are a couple of drawbacks you should be aware of when considering whether to implement a bus topology for your network. A malfunction of a station or other component on the network can be difficult to isolate. Furthermore, a malfunction in the bus backbone can bring down the entire network.

All things considered, if your goal is to set up a small or temporary network, a linear bus topology is the best way to go.

Ring

Ring topologies are commonly seen in Token Ring and FDDI (fiber optic) networks. In a physical ring topology, the data line actually forms a logical ring to which all computers on the network are attached (see Figure 5.4). Unlike a bus topology, which uses a contention scheme to allow the stations to access the network media, media access on the ring is granted by means of a logical "token" that is passed around the circle to each station, giving it an opportunity to transmit a packet if it needs to. This configuration allows each networked computer a more equitable opportunity to access the media, and hence, to transmit its data. A computer can only send data when it has possession of the token.

Because each computer on the ring is part of the circle, it is capable of retransmitting any data packets it has received that are addressed to other stations on the ring. This regeneration keeps the signal strong, eliminating the need for repeaters. Because the ring forms a continuous loop, termination is not required. A ring network topology is relatively easy to install and configure, requiring minimal hardware.

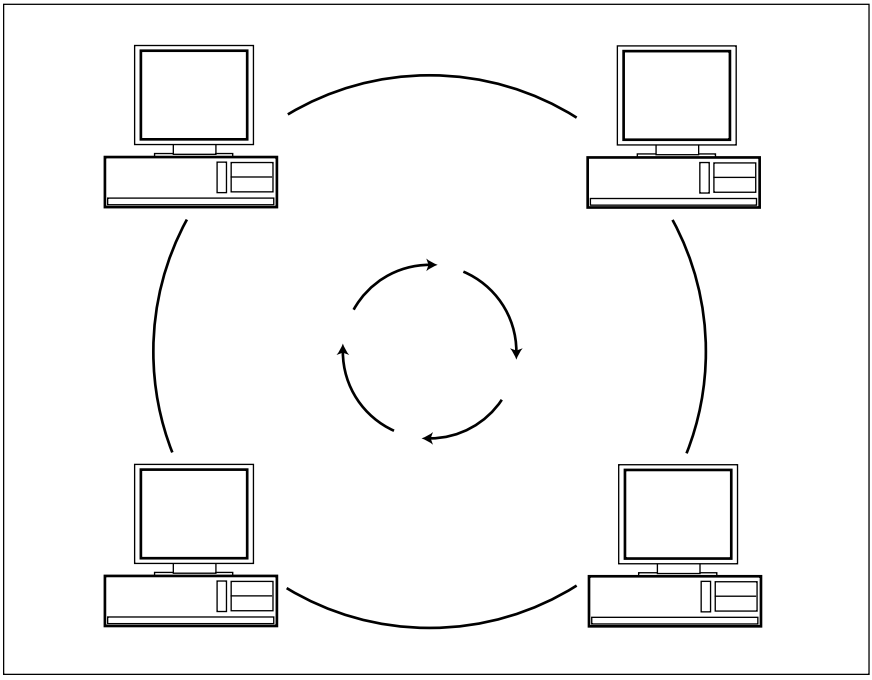


Figure 5.4 The ring topology creates a physical and logical loop.

A physical ring topology has several disadvantages. As with a linear bus, a malfunction on one station can bring down the entire network. It is also difficult, especially in larger networks, to maintain a logical ring. Finally, if adjustments or reconfigurations are necessary on any part of the network, you must temporarily bring down the entire network.

The ring topology provides equal access to the network media for all computers.

Star

In a star topology, all computers on the network are connected to one another using a central hub (see Figure 5.5). Each data transmission that the station sends goes directly to the hub, which then sends the packet on toward its destination. Like in the bus topology, a computer on a star network can attempt to send data at any time; however, only one may actually transmit at a time. If two stations send signals out to the hub at exactly the same time, neither transmission will be successful, and each computer will

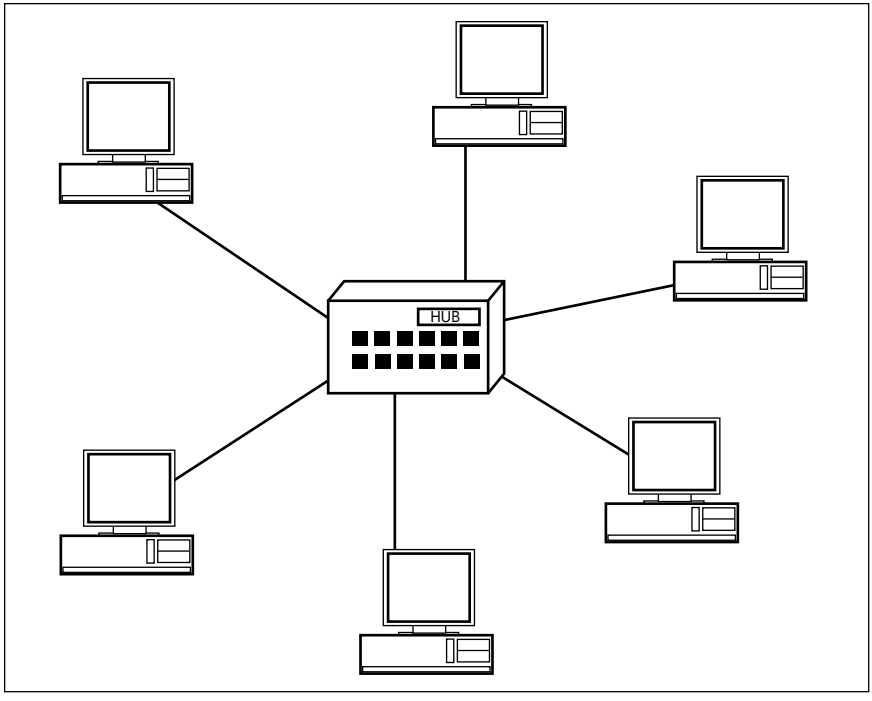


Figure 5.5 In the star topology, computers are connected to one another via a central hub.

have to wait a random period of time before reattempting to access the media. Star topologies are generally more scalable than other types.

A major advantage of implementing a star topology is that, unlike on a linear bus, a malfunction of one station will not disable the entire network. It is easier to locate cable breaks and other malfunctions in a star topology. This capability facilitates the location of cable breaks and other malfunctions. Additionally, the star topology's centralized hub makes it is easier to add new computers or reconfigure the network.

There are a couple of drawbacks inherent in the implementation of a star topology. For one, this type of configuration uses more cabling than most other networks because of the separate lines required to attach each computer to the hub. Also, the central hub handles most functions, so failure of this one piece of hardware will shut down the entire network.

The star topology is the easiest topology to reconfigure.

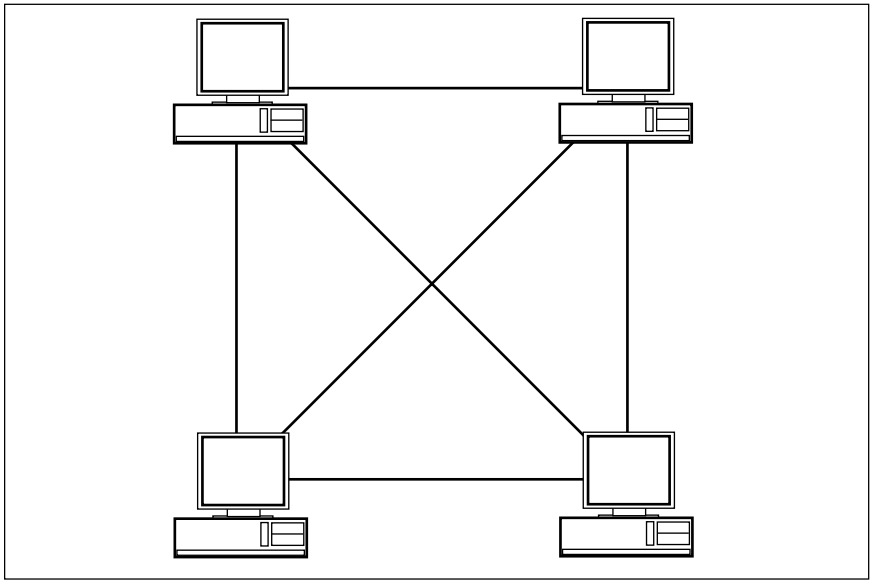


Figure 5.6 The mesh topology connects each and every computer to one another.

Mesh

The mesh topology connects each computer on the network to the others (see Figure 5.6). Meshes use a significantly larger amount of network cabling than do the other network topologies, which makes it more expensive. Additionally, these networks are much more difficult to install than the other topologies. So why would someone use a mesh? The answer is fault tolerance. Fault tolerance is the ability of a system to work around a failure. On a network with a broken segment, that means going around it. Every computer has multiple possible connection paths to the other computers on the network, so a single cable break will not stop network communications between any two computers.

The mesh topology is highly fault tolerant.

Hybrids

Many organizations choose to use a combination of the main network topologies. We will discuss three such hybrids: star bus, star ring, and hybrid mesh.

Star Bus

As its name implies, the star bus hybrid topology brings together the star and bus topologies (see Figure 5.7). The advantages of using a star bus are that no single computer or segment failure can bring down the entire network. Also, if a single hub fails, only the computers connected to that hub cannot communicate on the network, whereas the other computers are not affected and can continue normal communications.

Star Ring

The star ring topology is also known as a star-wired ring because the hub itself is wired as a ring. As you can see in Figure 5.8, the star ring looks identical to the star topology on the surface, but the hub is actually wired as a logical ring. This topology is popular for Token Ring networks because it is easier to implement than a physical ring, but it still provides the token-passing capabilities of a physical ring inside the hub. Just like in the ring topology, computers are given equal access to the network media through the passing of the token. A single computer failure cannot stop the entire network, but if the hub fails, the ring that the hub controls also fails.

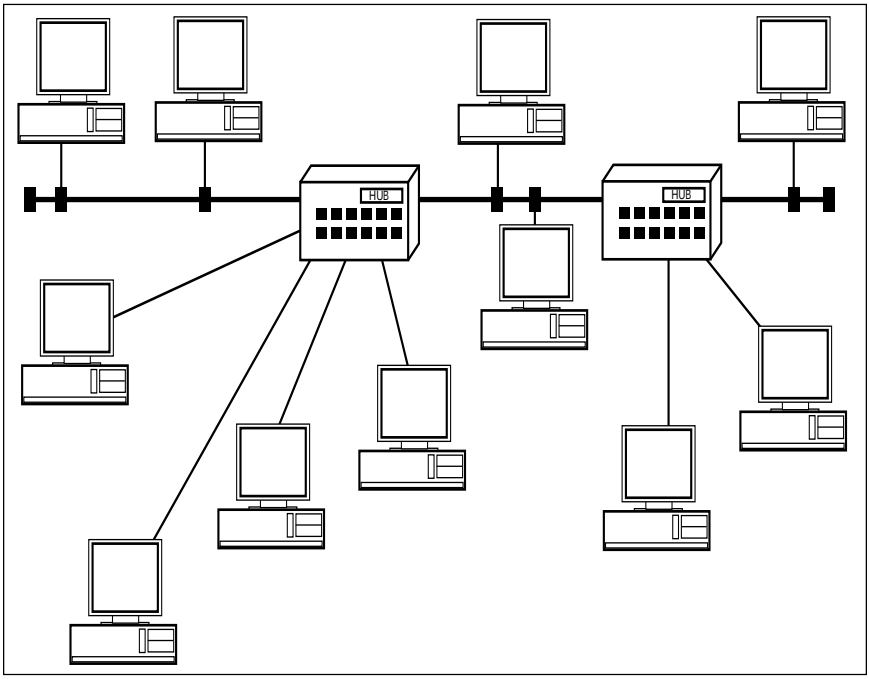


Figure 5.7 A star bus topology.

Hybrid Mesh

Implementing a true mesh on a large network would be expensive, time consuming, and difficult. A hybrid mesh network can provide some of the essential benefits of a true mesh network without using as much cable. Most large organizations do not have mission-critical data stored on all the computers in the network; rather, they store it on the network's servers. Companies that would like to provide their networks with fault tolerance at the network-cabling level may want to limit their mesh to only the mission-critical computers on the network. This means that the mesh exists on only part of the network (see Figure 5.9). This type of mesh still provides fault tolerance among the mission-critical servers, but does not add extra protection for individual network clients. A hybrid mesh would cost less than a complete mesh network, but it would not be as fault tolerant.

Networking Standards And Technologies

In an effort to standardize networking technologies, two groups defined networking standards: the International Standards Organization (ISO) and

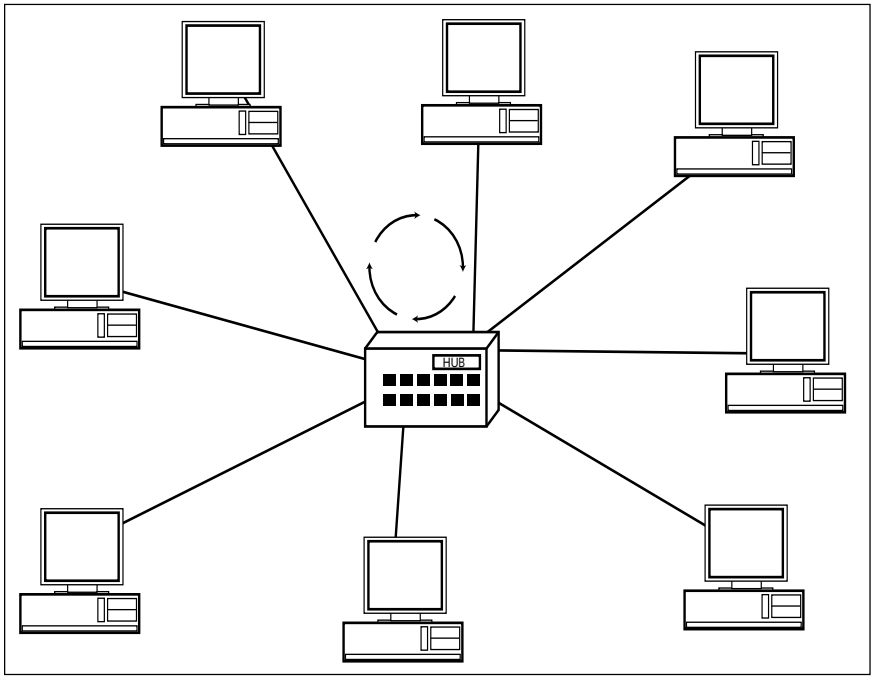


Figure 5.8 The star ring looks identical to the star topology on the surface, but the hub is actually wired as a logical ring.

the Institute of Electrical and Electronic Engineers (IEEE). The ISO created the OSI Reference Model and the IEEE further defined the lower layers of the OSI model.

IEEE 802

The IEEE started its project to further define the Physical and Data Link layers of networking in February of 1980. It named the project 802 after the year and month of the project's beginning. The 802 Project resulted in 12 different specifications that defined network topologies, interface cards, and connections. The specifications that you should be concerned with for the Networking Essentials exam are:

- 802.2 Divided the OSI model's Data Link layer into the Logical Link Control (LLC) and Media Access Control (MAC) sublayers (see Figure 5.10)
- 802.3 Defined Ethernet Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
- 802.5 Defined standards for Token Ring networks

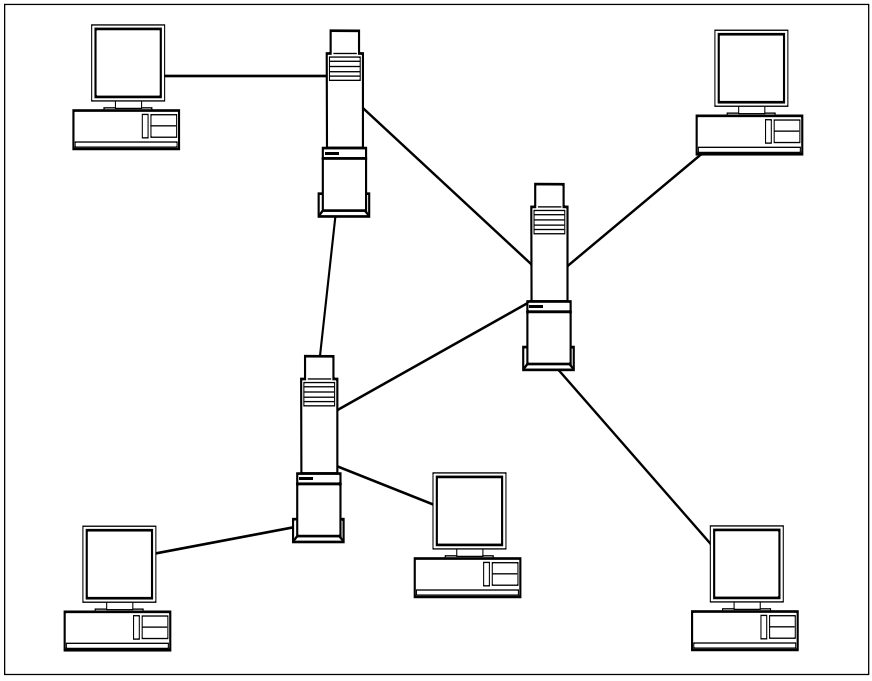


Figure 5.9 The hybrid mesh provides partial fault tolerance at a lower cost than a true mesh.

802.2—Division Of The Data Link Layer

The IEEE decided to further divide the OSI Reference Model's Data Link layer to separate its responsibilities into a Logical Link Control (LLC) sublayer and a Media Access Control (MAC) sublayer (see Figure 5.10). The LLC sublayer is responsible for maintaining a link when two computers are sending data across the network. The LLC exposes Service Access Points (SAPs), which allow computers to communicate with the upper layers of network stack.

802.3—Ethernet CSMA/CD

The 802.3 standard essentially describes how computers communicate on an Ethernet network using CSMA/CD. There are three basic parts to this description:

- Carrier Sense A computer checks to see if the network is being used before it attempts to transmit. This is called carrier sense because the computer actually listens to the network to see if a carrier signal is present. If there is no carrier signal, the computer sends its data

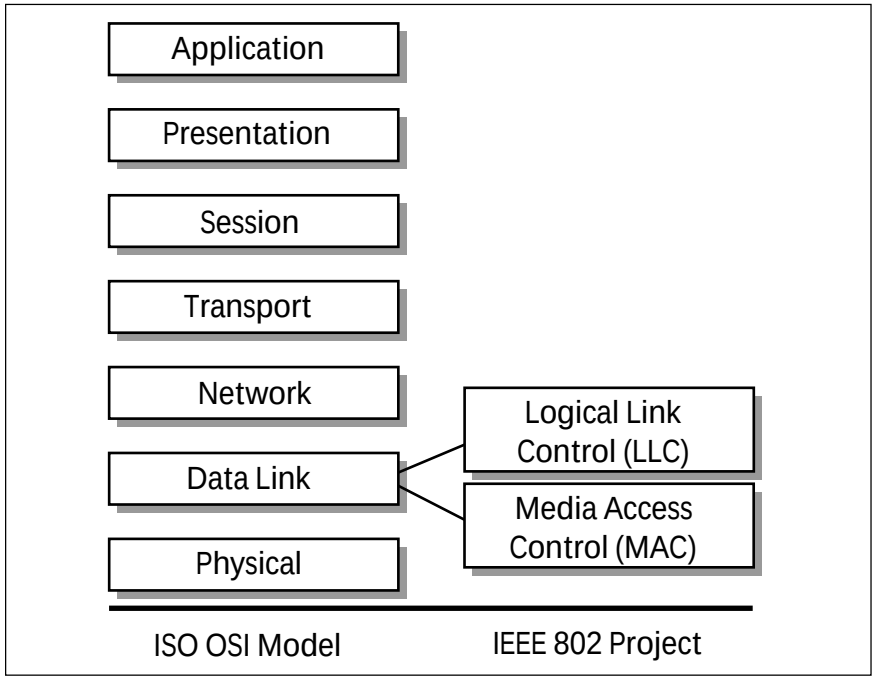


Figure 5.10 The IEEE 802.2 specification subdivided the OSI Reference Model's Data Link layer.

transmission. If there is a carrier signal (meaning another computer is transmitting), the computer does not transmit data until the carrier wave has terminated.

- Multiple Access All computers connected to the wire can transmit when they have data to send. They do not have to take turns transmitting data, meaning multiple computers can access the wire at a given time.
- Collision Detection If two computers do transmit data at the same time, their transmission signals can collide; the computers that sent the data have the ability to detect the collision. If the computers detect a collision or multiple carrier signals, they will resend their data. Each computer waits a random interval before transmitting again. Because each computer resends the data after separate random wait periods, the chance of both computers retransmitting at the same time is minimal.

A large number of collisions can seriously slow down network performance because each computer must retransmit its data. If collisions are affecting your network performance, you should consider segmenting your network with a router.

802.5—Token Ring

Token Ring networks use a token-passing method to provide equal access to the network for all computers. Computers cannot transmit data unless they have the token (a small data frame). Token passing keeps two computers from transmitting on the network wire at the same time, which eliminates collisions. The token is passed from one computer's nearest active upstream neighbor (NAUN). Once the computer finishes transmitting, the token is passed to the nearest active downstream neighbor (NADN).

Token Ring networks use a larger data frame than Ethernet networks. This allows Token Ring networks to transfer large data blocks more efficiently than Ethernet networks.

Errors in a Token Ring network can be detected by a process called "beaconing." The first computer that is powered on in a Token Ring network becomes the Active Monitor (the other computers on the network are Standby Monitors). The Active Monitor is responsible for ensuring that the data successfully travels around the ring. The Active Monitor does this by sending out a data packet to its NADN every seven seconds. The data packet travels around the ring and is eventually returned to the Active Monitor. If a computer does not receive a packet from its NAUN every seven seconds, it creates a packet that announces its address, its NAUN's address, and its beacon type (Active or Standby). The packet travels the network to its farthest point, which indicates where the break or error is located. The computers on the ring can use that information to automatically reconfigure the ring to avoid the cable break. Token Ring's ability to function in spite of a single failure means that it is fault tolerant.

A physical ring structure is different from the logical Token Ring network. Token Ring and CSMA/CD describe how computers communicate on the network. The physical topology looks different than the logical method the computers use to communicate on the network.

In a Token Ring network, computers are typically connected to a multistation access unit (usually referred to as an MAU or MSAU) and a smart multistation access unit (SMAU). These devices are essentially Token Ring hubs

that are wired as logical rings. Each hub has connections for computers and a ring in (RI) and ring out (RO) connection so that multiple MAUs can be connected. An IBM MSAU has 10 connection ports that can host up to 8 computers. There can be up to 33 MSAUs on a Token Ring network.

AppleTalk

AppleTalk is the name of the networking method used by Apple Macintosh computers. The cabling system for an AppleTalk network is called LocalTalk. LocalTalk uses a network media-access method called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which is similar to the Ethernet CSMA/CD method. The major difference between the two methods is that in CSMA/CA, the computer actually broadcasts a warning packet before it begins transmitting on the wire. This packet eliminates almost all collisions on the network because each computer on the network does not attempt to broadcast when another computer sends the warning packet. The major drawback of trying to avoid network collisions is that broadcasting the intent to send a message increases network traffic.

AppleTalk also differs from other networking implementations in that it has a dynamic network addressing scheme. During bootup, the AppleTalk card broadcasts a random number on the network as its card address. If no other computer has claimed that address, the broadcasting computer configures the address as its own. If there is a conflict with another computer, the computer will try to use different combinations until it finds a working configuration.

ARCNet

The Attached Resource Computer Network (ARCNet) was created in 1977 by Datapoint Corporation. ARCNet uses a token-passing method in a logical ring similar to Token Ring networks. However, the computers in an ARCNet network do not have to be connected in any particular fashion. ARCNet can utilize a star, bus, or star bus topology. Data transmissions are broadcast throughout the entire network, which is similar to Ethernet. However, a token is used to allow computers to speak in turn. The token is not passed in a logical ring order because ARCNet does not use the ring topology; instead, the token is passed to the next-highest numerical station number. Station numbers are set on the ARCNet network adapters via dual in-line package (DIP) switches on the card. You can set the station identifier on the card yourself. When setting this identifier, it is best to

make the numbers increase based on proximity of one adapter to another. For instance, you wouldn't want stations five and six to be on the opposite ends of the network because the token would have to cross the entire network to go from station five to six.

ARCNet is no longer a popular networking method because you must manually configure ARCNet cards, and ARCNet speeds are a mere 2.5 Mbps. However, you should know that ARCNet uses RG-62 (93 ohms) cabling; it can be wired as a star, bus, or star bus; and it uses a logical-ring media-access method.

FDDI

The Fiber Distributed Data Interface (FDDI) is another networking standard to consider. FDDI uses fiber cable and a token-passing media-access mechanism to create a fast and reliable network. Speeds of FDDI rings can be up to 100 Mbps and include 500 nodes over a distance of 100 kilometers (62 miles).

FDDI rings have the ability to implement priority levels in token passing. For instance, a mission-critical server may be given a higher priority than other computers on the network, which would allow it to pass more data frames on the network than the other machines.

FDDI rings can be implemented with two rings: a primary and a secondary ring. All data is transmitted on the primary ring, while the secondary ring provides fault tolerance. If there is a break in the primary ring, the secondary ring can be used to compensate for the cable break. Data is actually passed in the opposite direction on the secondary ring so that the cable break does not stop the ring's communications (see Figure 5.11).

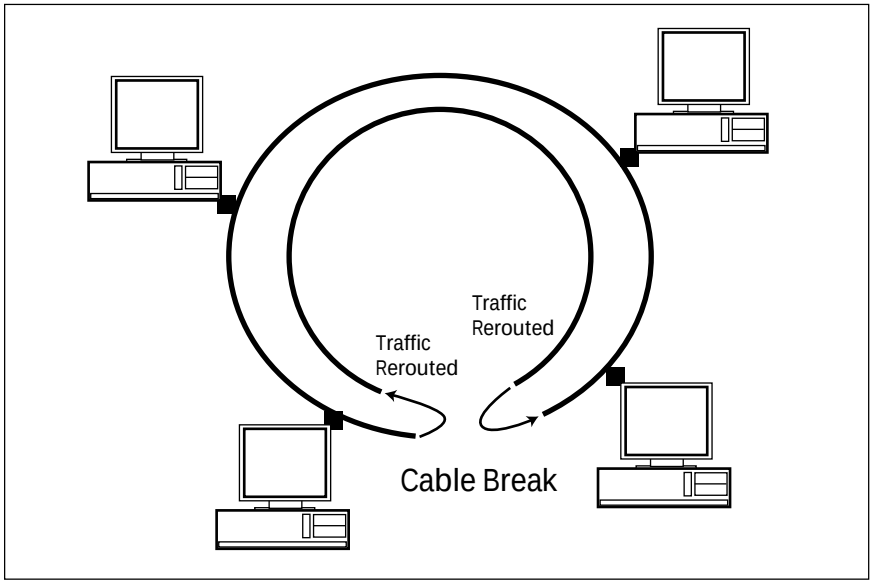


Figure 5.11 The FDDI network can recover from cable breaks using its secondary ring.

Practice Questions

Question 1

You are considering starting a training company that provides on-site classroom instruction to various businesses. Your service will include a temporary networked classroom environment. Assuming that the facilities do not have pre-installed wiring and that the classroom will use 10 or less computers, which topology would require the least equipment and be the easiest to set up and tear down? [Choose the best answer]

- ❍ a. Star
- ❍ b. Bus
- ❍ c. Ring
- ❍ d. Mesh

The best answer to this question is b. The bus is the easiest topology to use for temporary networks. The bus topology does not require hubs and minimizes the amount of cable that you will need. The ring topology would be slightly more difficult than a bus because you would have to hook up a physical ring or use a hub that was wired as a ring. Star would be easy to set up, but would require at least one hub. Additionally, the star topology would probably require more wire because every computer would have to be connected to the hub. Mesh would require the most cabling and would be difficult to configure.

Question 2

If you must configure a network for three mission-critical servers and want to provide a highly fault-tolerant cabling scheme, which topology would you implement? [Choose the best answer]

- ❍ a. Star
- ❍ b. Bus
- ❍ c. Ring
- ❍ d. Mesh

The best answer is d. The mesh is a highly fault-tolerant architecture that gives computers multiple access routes to one another. The other topologies provide only one connection path between each computer. Warning: Do not read FDDI ring into the question set. If the question wanted you to consider an FDDI ring topology, it would have specifically stated "FDDI ring."

Question 3

Which of the following network access methods sends a signal indicating its intent to transmit data on the wire? [Choose the best answer]

- ❍ a. CSMA/CD
- ❍ b. Token passing
- ❍ c. CSMA/CA
- ❍ d. Beaconing

The correct answer is c. Only Carrier Sense Multiple Access with Collision Avoidance broadcasts its intent to send data on the wire. Token passing uses a token to avoid collisions and Carrier Sense Multiple Access with Collision Detection causes the computer to retransmit frames if a collision is detected. Beaconing is the method that Token Ring networks use to identify and route network communications around a network error.

Question 4

Which type of network media-access method do IBM LANs with multistation access units employ?

- ❍ a. Beaconing
- ❍ b. Token passing
- ❍ c. CSMA/CD
- ❍ d. CSMA/CA

The answer here is b. IBM networks that employ MAUs are Token Ring networks. Token Ring networks use token passing to allow a single station to transmit on the network at a time.

Question 5

Your network is experiencing heavy traffic and signal attenuation due to long cable distances between computers.

Required Result:

- Correct the signal attenuation problem.

Optional Desired Results:

- Reduce the broadcast traffic that is present on your network.
- Filter the network traffic to reduce the number of frames transferred across the network.

Proposed Solution:

- Install repeaters between distant segments.

Which results does the proposed solution produce?

❍ a. The proposed solution produces the required result and produces both of the optional desired results.

❍ b. The proposed solution produces the required result and produces only one of the optional desired results.

❍ c. The proposed solution produces the required result but does not produce any of the optional desired results.

❍ d. The proposed solution does not produce the required result.

The answer to this question is c. The repeaters will stop the signal attenuation by regenerating the signal, but they do not have the ability to reduce traffic in any way.

Question 6

Your network is experiencing heavy traffic and signal attenuation due to long cable distances between computers.

Required Result:

- Correct the signal attenuation problem.

Optional Desired Results:

- Reduce the broadcast traffic that is present on your network.
- Filter the network traffic to reduce the number of frames transferred across the network.

Proposed Solution:

- Install repeaters between distant segments. Install routers and configure them to filter broadcast traffic.

Which results does the proposed solution produce?

❍ a. The proposed solution produces the required result and produces both of the optional desired results.

❍ b. The proposed solution produces the required result and produces only one of the optional desired results.

❍ c. The proposed solution produces the required result but does not produce any of the optional desired results.

❍ d. The proposed solution does not produce the required result.

The correct answer to this question is a. The routers have the ability to filter the broadcast traffic and route packets to the correct computers. Routers are usually used to segment the network and reduce the traffic on the wire. The repeaters will correct the signal attenuation problem.

Question 7

Which of the following network devices functions at the Network layer of the OSI model?

- ❍ a. Bridge
- ❍ b. Repeater
- ❍ c. Router
- ❍ d. Gateway

The answer here is c. Routers function at the Network layer; bridges function at the Data Link layer; and gateways function at the Transport layer of the OSI model and higher.

Question 8

You are installing a network card in a computer that has several devices configured. There is a printer on LPT 1, a mouse on COM 1, a modem on COM 2, and a SCSI host adapter occupying IRQ 10. The computer also has a sound card using IRQ 5. If your network card supports IRQs 3 through 5 and 9 through 11, which of the following IRQs could you set it for in this computer? [Check all correct answers]

- ❑ a. IRQ 3
- ❑ b. IRQ 4
- ❑ c. IRQ 10
- ❑ d. IRQ 11

The correct answer is d, IRQ 11. COM 1 is using IRQ 4, COM 2 is using IRQ 3, and LPT1 is using IRQ5, so the only remaining open IRQ is 11.

Question 9

Which of the following is most likely the problem if the operating system is unable to detect the network card? [Choose the best answer]

- ❍ a. Wrong frame type is set on the network card
- ❍ b. Wrong IRQ is set on the network card
- ❍ c. Wrong IRQ is set on the IDE controller card
- ❍ d. Wrong protocol is bound to the network adapter

Only answer b is correct. The only situation that would cause the operating system to miss the network card is an incorrect IRQ setting. The wrong protocol and/or frame type would only disable the network communications. An incorrect setting on an IDE controller would probably keep the computer from booting. To answer this type of question, it is best that you memorize the common IRQs and their related devices (see Table 5.1 earlier in this chapter).

Question 10

Your network uses only the NetBEUI protocol. You would like to segment the network to reduce traffic. Which of the following devices could you use for this network?

- ❍ a. Router
- ❍ b. Bridge
- ❍ c. Gateway
- ❍ d. Multiplexer

The correct answer is b. Routers have the ability to segment the network, but NetBEUI is a non-routable protocol, so you cannot use a router on this particular network (unless you decide to choose a different protocol). Bridges can work with any protocol because they only look at the MAC address of the packet.

Question 11

Your company has two LANs that use different protocols. You need to connect the two LANs, but you do not want to configure additional protocols on either network. Which device could you use to perform this task?

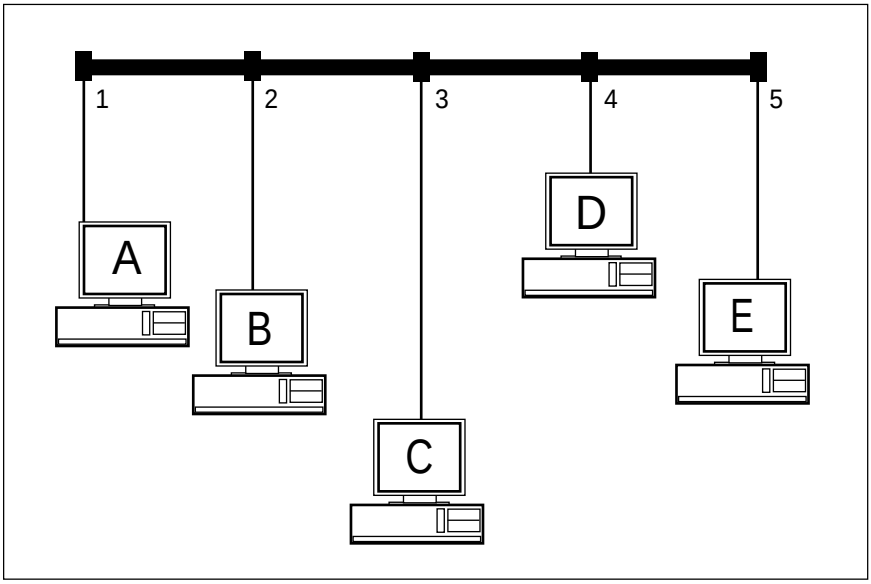
- ❍ a. Bridge
- ❍ b. Router
- ❍ c. Brouter
- ❍ d. Gateway

The correct answer is d. Only the gateway has the ability to translate from one protocol to another. The simple answer of "router" for b does not include a multiprotocol router.

Question 12

At which location(s) should there be terminators on the pictured Thinnet (bus topology) network (see graphic)? [Check all correct answers]

- ❑ a. Location 1
- ❑ b. Location 2
- ❑ c. Location 3
- ❑ d. Location 4
- ❑ e. Location 5



The answers to this question are a and e, locations 1 and 5, respectively. Remember that the bus topology requires a terminator at each end of the network.

Need To Know More?

Chellis, James, Charles Perkins, and Matthew Strebe: *MCSE: Networking Essentials Study Guide, 2nd Edition*. Sybex Network Press, San Francisco, CA, 1998. ISBN 0-7821-2220-5. Chapter 1, "An Introduction to Networks," contains excellent coverage of the various topics contained within this chapter.

Microsoft Press: *Networking Essentials, 2nd Edition*. Redmond, WA, 1997. ISBN 1-57231-527-X. Unit 1, Lesson 3, "Network Design," discusses all of the topics in this chapter in great detail.

Search the TechNet CD (or its online version through www.microsoft.com) using the keywords "topology," "Ethernet," "hubs," "bridges," "routers," and "brouters."