Cabling And Interfaces

Terms you'll need to understand:

- √ Network media
- √ Unshielded twisted-pair
- √ Shielded twisted-pair
- √ Coaxial cable
- √ Thinnet cable
- √ Thicknet cable
- √ Wireless media
- √ Broadband
- √ ARCNet
- √ Plenum
- √ Fiber optic cable
- √ Network Device Interface Specification (NDIS)
- √ Open Data-link Interface (ODI)
- √ Media Access Control (MAC)

Techniques you'll need to master:

- √ Understanding cable types, their advantages, and their disadvantages
- √ Knowing which cable type to use with network technologies
- √ Understanding NDIS and ODI

At the most basic level of any network communications lies the medium by which data is transmitted. For the purposes of data transmission, the term "media" can include both cabling and wireless technologies. Although physical cables are the most commonly used media for network connectivity, wireless technologies are becoming increasingly popular for their ability to link wide area networks (WANs). The type of media you use in your network is a key consideration. Media vary in several ways, including data transmission speed, ease of installation, and expense. When planning your network, you should consider these and other factors carefully.

Cable Types

There are several different cable types that are used in modern networks. Size, cost, data transfer rates, minimum/maximum lengths, and ease of installation vary for all of them. Various networking situations and requirements may require distinctly different cable types. This section describes the uses and limitations of each type of cable.

Twisted-Pair Cable

Twisted-pair cable is a media type used in many network topologies, including Ethernet, ARCNet, and IBM Token Ring. Twisted-pair cabling comes in two types: shielded and unshielded.

Probably the most commonly used type of networking cable in America, twisted-pair cabling was originally developed for use in telephone lines. A familiar example would be the cabling used to connect the telephone to the wall jack—CAT1, two-pair, unshielded twisted-pair (UTP) cabling, also known as "silver satin" cable. This is one type of twisted-pair cabling that typically consists of two pairs of insulated copper wires, twisted around each other, then enclosed within a plastic sheath. The twisting of the wires around each other provides a degree of protection from crosstalk (we'll cover this shortly) and other types of outside interference.

Unshielded Twisted-Pair Cabling

The Electronics Industries Association and the Telecommunications Industries Association (EIA/TIA) have created standards (EIA/TIA 568 Commercial Building Wiring Standard) that define UTP cable categories. Five types of UTP are available. They are referred to, in ascending quality order, as CAT1 through CAT5. The higher category cables usually contain more wire pairs, and these wires contain a higher number of twists per foot.

The CAT1 telephone cabling that we have already mentioned, although adequate for voice communications, does not support digital data transfer, and, therefore, should not be used in this capacity. CAT2 cabling is an older type of UTP that is rarely used. It supports data transfer rates of up to 4 Mbps. CAT3 cable, with a data transfer rate of up to 10 Mbps, is the realistic minimum grade of UTP required for today's data networks. In fact, CAT3 cable is the lowest category of UTP that meets the IEEE 802.3 (explained in the next chapter) standards for a 10BaseT Ethernet network.

CAT4 cable is an intermediate UTP cable specification that supports data transfer rates of up to 16 Mbps. For new network installations, UTP CAT2 through 4 have been largely abandoned in favor of the newer CAT5 UTP, which can handle data transfer rates up to 100 Mbps.

Unshielded twisted-pair cabling is connected from each host computer's NIC to the network patch panel, which is then connected to a network hub, using RJ-45 connectors at each connection point. An RJ-45 connector is an eight-wire (four-pair) media connector. It is slightly larger than (but similar in appearance to) the RJ-11 connector used to attach a phone line from a wall jack to your telephone or modem.

> ***Note:*** *It is possible, though unusual, to use an RJ-11 connector for data networking because RJ-11 is usually used to attach lower grades of cable.*

A good example of this configuration is the Ethernet 10BaseT standard network, which is characterized by UTP (CAT3 through 5) cable that uses RJ-45 connectors. Shielded twisted-pair (STP) cable can also be used, but it is less common. This cable type supports a data transmission rate of 10 through 100 Mbps and can transmit data up to 100 meters without a repeater. 10BaseT networks are a popular all-around choice because they are supported on most platforms, use inexpensive media, and are easier to troubleshoot than other network types. It is also possible in many cases to run UTP through already-existing telephone line conduits, thus adding to its ease of installation.

Although it is inexpensive and easier to install, UTP cabling is not without its drawbacks: namely, interference from outside electromagnetic sources, and signal crossing between adjacent wires, called *crosstalk*. To some degree, the wire's design—the twisting of one wire around the other—cancels out much of the natural signal overflow and interference that exist from one wire to the other. Although electromagnetic interference and crosstalk can

occur on other media types, UTP is particularly susceptible because it lacks the shielding present in other cable types. This lack of shielding also makes UTP particularly vulnerable to wiretapping—a point you should examine carefully if data security is a priority.

UTP is also subject to a greater degree of attenuation, or lessening of signal strength over distance, than other cable types. This means that cable segments using UTP have the most stringent distance limitations—no segment may exceed 100 meters in length. Cable length maximums exist because signals weaken over distance, as they are partly absorbed by the media on which they travel. This attenuation causes the signals to become unreadable after the specified distances, unless a repeater (a device that cleans up and retransmits the signal) is used.

Shielded Twisted-Pair Cabling

Shielded twisted-pair (STP) cabling has traditionally been used in several network types, including AppleTalk and Token Ring. STP, which is of similar internal construction, is subject to the same 100-meter restriction as UTP. In addition, shielded twisted-pair cable usually contains, at its core, four or more pairs of twisted copper wires. STP differs from UTP in that it contains shielding—an electrically grounded woven copper mesh or aluminum foil that surrounds the cable's internal wires. This shielding separates them from the cable's outer sheath and provides resistance to external electromagnetic interference (EMI). Some types of STP also use shielding internally around each wire pair to keep the pair separated from the others, which further reduces crosstalk. Additionally, STP is considered to be more secure than UTP, because its shielding makes it somewhat less vulnerable to wiretapping.

STP cabling data transmission rates and distance restrictions are identical to those of UTP. Although STP provides more protection from EMI than UTP, it is not often used in newer network installations because it is more difficult to install and maintain. One reason for this is that the shielding makes the cable less flexible; another consideration is that STP usually requires electrical grounding.

Coaxial Cable

Coaxial cable was the first cable type used to connect computers to a network, and it helped form the basis of the original Ethernet standard. This cable type consists of a copper conductive center wire that is thicker than the wires found in twisted-pair cable, thus enabling higher data transmission rates over longer distances. The center conductor is covered by a layer of

plastic foam insulating material, which, in turn, is surrounded by a second conductor, usually woven copper mesh or aluminum foil. This outer conductor is not used to transfer data, but it provides an electrical ground and shields the center conductor from internal and external interference.

Although not used as much as UTP in newer network installations, coaxial cabling is still common in much of the already-installed computer network base. It is also the type of cabling used for cable television hookups. Coaxial cabling can transmit data at 10 Mbps, for maximum distances of 185 to 500 meters. Coaxial cable manufacturers have created specifications that separate coaxial cables into categories (see Table 4.1) depending on characteristics such as impedance (current resistance, measured in ohms) and cable thickness. Coaxial cabling schemes usually require terminators, the impedance of which must be properly matched to the cable type. The two main coaxial cable types used in local area networks are Thin Ethernet (also known as "Thinnet") and Thick Ethernet (also known as "Thicknet"). In coaxial configurations, Thinnet and Thicknet are often combined within the same network, with Thicknet cabling used for the backbones and Thinnet used for the branch segments.

Thinnet

Thinnet cable, also referred to as RG-58 cable, is the most commonly used coaxial media in computer networks. Second in popularity only to UTP, it is the most flexible of the coaxial cable types, about one-quarter inch in diameter. Thinnet cable can be used to connect each computer

Table 4.1 Coaxial cable types.

Type	Name
RG-8 and RG-11	Thicknet (50 ohms)
RG-58 Family:	Thinnet (50 ohms)
RG-58/U	Thinnet, solid copper center conductor
RG-58 A/U	Thinnet, wire-strand center conductor
RG-58 C/U	Thinnet, military grade
RG-59	Broadband/Cable television (75 ohms)
RG-59 /U	Broadband/Cable television (50 ohms)
RG-62	ARCNet (93 ohms)

directly to the others on the LAN, using British Naval Connector (BNC) T-connectors and 50-ohms terminators. Because Thinnet configurations require no special equipment or external transceivers and can be used without hubs, Thinnet cabling schemes are an easy and relatively inexpensive way to set up a small network quickly.

According to the IEEE specification for 10Base2 Ethernet networks, the BNC T-connectors (shown in Figure 4.1) and BNC barrel connectors are used to attach RG-58 A/U or RG-58 C/U cable segments to each other. They also link the network cable to the transceiver on each computer's NIC. The BNC barrel connector is similar to the T-connector except that the barrel does not have the bottom part of the "T." Terminators (shown in Figure 4.2), which are resistors that prevent signal echo, are required at both ends of each segment. This configuration supports data transmission speeds of up to 10 Mbps, with maximum cable lengths of 185 meters between repeaters.

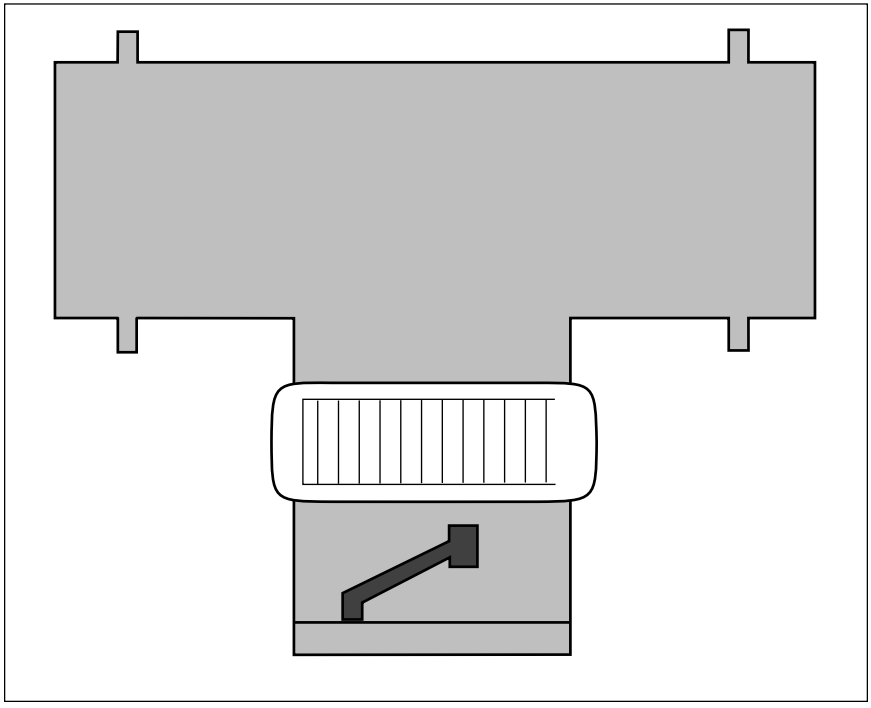


Figure 4.1 An illustration of a BNC T-connector.

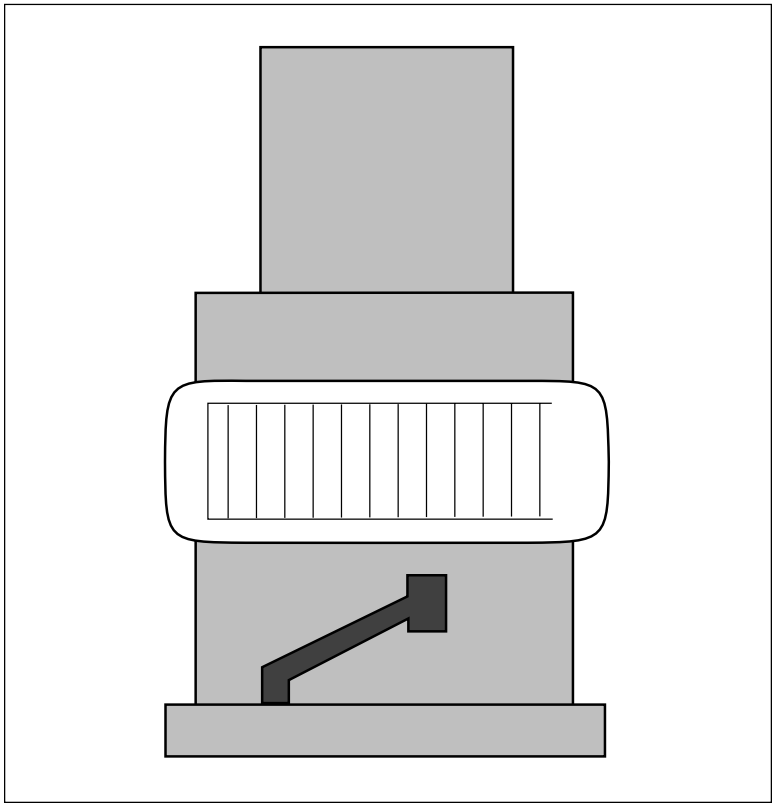


Figure 4.2 An example of a BNC terminator.

Thinnet's greater transmission distance and shielding (which provides better security than twisted-pair cabling), make it a good choice in cases where these qualities are critical. However, because it is less flexible, it is somewhat more difficult to work with. It is also not the best choice in a situation where the network cabling must be installed in existing telephone wiring conduits—if this is an issue, UTP is preferable.

Thicknet

Thicknet, which was used for the original Ethernet specification, is a thicker and more expensive cable than Thinnet. It is similar in construction to Thinnet, but is a great deal less flexible. Thicknet cabling is used as the basis for a standard Ethernet (10Base5) network. The IEEE Thick Ethernet specification for 10Base5 networks uses either RG-8 or RG-11 cable (approximately one-half inch in diameter) as a linear bus. The difference is

that it uses attachment unit interface (AUI) external transceivers connected to each NIC by means of a "vampire," or tap that pierces the cable's sheath to access the wire. Each AUI is connected to a compatible AUI (called a DB15) connector on its computer's NIC. Thicknet cabling has a thick center conductor core, which allows it to transmit reliably at a distance of up to 500 meters per cable segment—a significant distance advantage over Thinnet. For this reason, it is often used to create backbones that link Thinnet networks. Thicknet media can transmit data at a rate of up to 10 Mbps.

Although the thickness of Thicknet cabling allows for longer transmission distances, greater security, and resistance to interference, its rigidity and bulkiness make it very difficult to install. It is also quite expensive. For these reasons, Thicknet networks are rare today. Thicknet is not a good choice for a new network installation if you can use another solution.

ARCNet

ARCNet token-passing networks generally use RG-62 A/U coaxial cable. RG-62 cabling is not used for Ethernet networks. ARCNet cable is similar to cable television cable and at one time was popular in networks. Today, support for ARCNet networks is minimal.

Plenum Cabling

The plenum is the crawl space in a building that lies between the ceiling and the roof. The special grades of fire-resistant cables used in this area are called plenum cables. This area is commonly used for telephone and network wiring. Fire codes require that cabling installed in the plenum area be fire resistant and have casing material that will not give off hazardous fumes if it does burn.

Fiber Optic Cable

At the cutting edge of network cabling technology, fiber optic cable provides superior data transmission speed over longer distances. It is also immune to interference and eavesdropping. Fiber optic cable consists of a glass or plastic center conductor, surrounded by another layer of glass or plastic cladding, and a protective outer jacket (see Figure 4.3). Data is transmitted across the cable by a laser or light-emitting diode (LED) transmitter that sends one-way light pulses through the center glass fiber. The glass cladding helps to keep the light focused into the inner core. The signal is received at the other end by a photodiode receiver that converts the light pulses to an electrical signal that the receiving computer can use.

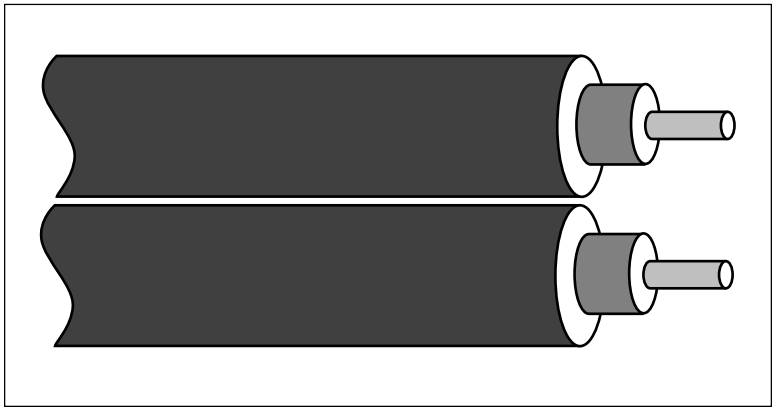


Figure 4.3 A drawing of fiber optic cable.

Be ready to identify drawings of fiber cabling, twisted-pair cabling, T-connectors, and terminators.

Data transmission speeds for fiber optic networks range from 100 Mbps to 2 Gbps (Gigabits per second), and data can be sent reliably up to a distance of 2 kilometers without a repeater. A fiber optic cable can support video and voice, as well as data transmission. Because the light pulses are completely closed within the outer sheath, fiber media are virtually impervious to outside interference or eavesdropping. These qualities make fiber optic cabling an attractive option for networks that must be very secure or require extremely fast transmission over long distances.

Because light pulses can only travel in one direction, fiber optic cabling systems must contain an incoming cable and an outgoing cable for each segment that will be transmitting and receiving data. Fiber cabling is also rigid and difficult to install, making it the most expensive of all network media types. You should probably consider alternate cabling types first, when they are adequate for the situation. Fiber media require special connectors and highly skilled installers, factors that further contribute to the high implementation expense. One way to minimize the expense is to limit use of fiber cabling to network backbones, or in areas where EMI, flammability, or other environmental issues are of concern. You must carefully analyze cost factors versus requirements before deciding on fiber optic cable for a network installation.

Wireless Technologies

In addition to traditional physical media, wireless data transmission methods can provide a convenient, and sometimes necessary, alternative to network cabling connections. Wireless technologies vary in signal type, frequency (higher frequencies mean higher transmission rates), and transmission distance. Interference and cost are significant considerations. Because of the increasing numbers of WANs, and the need for mobile computing solutions, wireless network technologies comprise an ever-growing segment of the network population. The three main types of wireless data transmission technology are radio, microwave, and infrared.

Radio Waves

Radio technologies transmit data via radio frequencies and have practically nonexistent distance limitations. They are used to link LANs over great geographical distances. Radio transmission is generally expensive, subject to government regulation, and is quite susceptible to electronic and atmospheric interference. They are highly susceptible to eavesdropping, and thus, require encryption or other transmission modifications to attain a reasonable level of security.

Microwaves

Microwave transmission uses higher frequencies for both short distance and global transmissions; its main limitation is that the transmitter and receiver must be within the line of sight of each other. Microwave transmission is commonly used to connect LANs in separate buildings, where using physical media is impossible or impractical. A good example of this would be two adjacent skyscrapers, where using cables would be impossible. Microwave is also used in global transmissions, which use geosynchronous satellites and ground-based dishes to adhere to the line-of-sight requirement. Microwave transmission can be extremely expensive, but microwaves are less susceptible to interference and eavesdropping than radio waves and provide higher bandwidth.

Infrared Transmissions

Infrared technologies, which operate at very high frequencies approaching those of visible light, can be used to establish close-range point-to-point or broadcast transmissions. They typically use LEDs to transmit infrared waves to the receiver. Because they can be physically blocked, and can experience

interference from bright light, infrared transmissions are limited to short-distance, line-of-sight applications. Infrared transmission is commonly used within stores or office buildings, or sometimes to link two buildings. Another popular use of infrared is for wireless data transfer in portable computers. Infrared technologies range from inexpensive to very expensive.

Cabling Considerations

When planning a network or adding to an existing network, you must consider several points concerning the cabling: cost, distance, transfer rate, ease of installation, number of nodes supported, and resistance to interference. We have discussed several types of cabling in this chapter, so let's compare the cable types using each of these considerations (see Table 4.2).

When designing or adding to a network, you should take each of the factors in Table 4.2 into consideration. Also, you should know how many computers you will have on the network and on each segment. Table 4.3 illustrates the different types of networking specifications and the number of computers (nodes) that you can have on each.

Table 4.2 Cable type comparisons.

Type	Speed	Distance	Installation	Interference	Cost
10BaseT	10 Mbps	100 M	Easy	Highly susceptible	Least expensive
100BaseT	100 Mbps	100 M	Easy	Highly susceptible	More expensive than 10BaseT
STP	16 Mbps to 155 Mbps	100 M	Moderately easy	Somewhat resistant	More expensive than Thinnet or UTP
10Base2	10 Mbps	185 M	Medium difficulty	Somewhat resistant	Inexpensive
10Base5	10 Mbps	500 M	More difficult than Thinnet	More resistant than most cable	More expensive than most cable
Fiber Optic	100 Mbps to 2 Gbps	2 K	Most difficult	Not susceptible to electronic interference	Most expensive type of cable

Understanding NDIS And ODI

Network software architectures contain several distinct layers. Based loosely on the seven layers of the OSI Reference Model of network protocols, from the bottom layer, which deals with the hardware that makes up the physical connection, to the top layer, which is comprised of the network applications. At one time, the code for all functions of the OSI model was entirely rewritten for each new combination of NIC, protocol, and redirector. This provided for an overly large number of combinations, required a great deal of reworking the code, and was inflexible; each NIC driver could only be bound to a single protocol stack, and vice versa.

To solve this problem, a more modular approach for each layer's function was required. This was addressed by creating device interfaces—blocks of program code that act as a standard communication interface between the functional layers. These device interfaces act as interpreters: One layer does not have to understand the way an adjacent layer performs a certain task for the two layers to communicate and cooperate in getting a task done.

The main benefit of interfaces is that, once written, they provide the same services to, and understand the communications of, drivers and protocols written by any vendor that has adhered to the interface specification. Vendor driver developers do not have to understand the application programming interfaces (APIs) of other vendors in order to develop compatible software. This means that proprietary layers of code can be removed and

Table 4.3 Nodes per network type.

Network Type	Nodes Per Segment	Nodes Per Network
10BaseT	2	1,024
10BaseF*	2	1,024
100BaseT	2	1,024
10Base2 (5 segments, 3 populated)	30	900**
10Base5 (5 segments, 3 populated)	100	1,024

*The 10BaseF specification is similar to 10BaseT except fiber optic cabling is used. The fiber cable can be run at much higher speeds, but if the computers only transfer at 10 Mbps, then the specification is 10BaseF.

** Although the theoretical maximum for a single 10Base2 network is 1,024 nodes, practical limitations on devices per segment result in an effective maximum of 900, or 30 devices for each of 60 segments that may have nodes attached.

replaced to allow for changes and upgrades. The OSI Reference Model also allows for multiple pieces of proprietary software to reside together at the same functional layer, thus enabling the binding of multiple NIC drivers to multiple network protocols, using the same intermediary device interface.

Microsoft, in combination with IBM, developed the Network Device Interface Specification (NDIS) as its implementation of the device interface concept, specifically to reside between the NIC (also called MAC or Media Access Control) driver and the protocol stack in the Data Link layer of the OSI Reference Model. NDIS allows for the binding of multiple NDIS-compliant network cards to one protocol stack or multiple protocols to a single NIC, or binds multiple protocols to multiple NICs.

Novell and Apple developed Open Datalink Interface (ODI), Novell's implementation of NDIS. It is used in Novell's NetWare networks, and provides functionality comparable to NDIS. It allows Novell's IPX/SPX protocol (and Microsoft's IPX implementation, NWLINK) to be bound to multiple NIC drivers. It also provides support for NetBIOS names.

Practice Questions

Question 1

10BaseT topologies have which of the following characteristics? [Check all correct answers]

- ❑ a. Use of 50-ohm BNC terminators and T-connectors
- ❑ b. RJ-11 connectors
- ❑ c. UTP cabling
- ❑ d. STP cabling

The answers for this question are c and d. 10BaseT networks typically use some type of twisted-pair cabling (either STP or UTP). Also, BNC terminators and T-connectors are used with Thinnet (10Base2) networks. Although many hubs support 10Base2 and 10BaseT connectors, you should not assume that 10Base2 components will be used on a 10BaseT network. Therefore, answer a is incorrect. RJ-11 connectors are used with regular phone cable or modems and are not normally associated directly with 10BaseT networking. Therefore, answer b is incorrect.

Question 2

If a 10BaseT network has been installed and one of the segments exceeds 100 meters, which type of device can help to prevent signal attenuation?

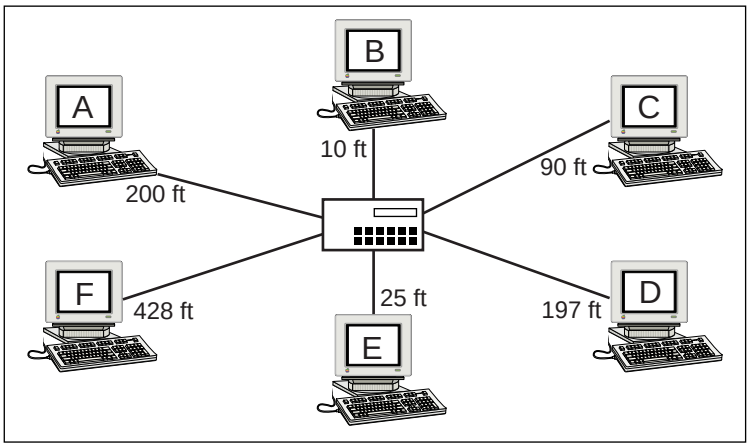
- ❍ a. Tuner
- ❍ b. Receiver
- ❍ c. Amplifier
- ❍ d. Repeater

The correct answer is d. When signal attenuation (the degradation of an electric signal over distance) is a problem, a repeater can be used to duplicate and boost the signal. The trick in this question was the word "amplifier," which acts in a similar manner as a repeater.

Question 3

You have been asked to review XYZ Company's network configuration (see graphic). The network is a 10BaseT network using (CAT5) twisted-pair cabling. Which of the following are problems with this network?

- ❍ a. All of the cables are too long.
- ❍ b. Segments to computers A, D, and F are too long.
- ❍ c. Segments to computers A and F are too long.
- ❍ d. Segment to computer F is too long.



If you know that 10BaseT cable can be 100 meters in length (which is equivalent to about 328 feet), the answer to the question is obviously d. The only segment that is longer than 328 feet is the one going to computer F.

Question 4

Your network consulting firm has been asked to implement a network for a small company. It wants to connect its 25 computers to a small LAN.

Required Result:

- The company needs a network that must be able to support transfer rates up to 10 Mbps.

Optional Desired Results:

- The company would like to minimize costs.
- The company would like to use the existing cabling with RJ-45 connectors currently installed in the building.

Proposed Solution:

- Implement a Thinnet network.

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 results.

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

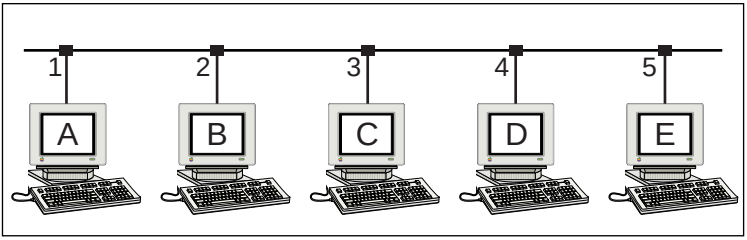
❍ d. The proposed solution does not produce the required result.

Because the proposed solution is 10Base2 or Thinnet, only answer c is correct. 10Base2 allows for a 10 Mbps transfer rate, but it is not the least expensive solution in this case and it cannot utilize the existing cabling with RJ-45 connectors. To successfully answer this question, you should know that cable with RJ-45 connectors is used in 10BaseT networks and that it can handle transmission speeds of up to 10 Mbps. Because cable with RJ-45 connectors is already preinstalled, a 10BaseT network would meet required and optionally desired results.

Question 5

You are assembling a five-host 10Base2 network as shown in the graphic. Which locations on the network cable will require both a T-connector and a terminator? [Check all correct answers]

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



The correct answers are a and e. Thinnet (10Base2) cable must be terminated at both ends. According to the graphic, one end is at location 1 (computer A) and the other end is at location 5 (computer E). The other locations only require a T-connector to attach the two sides of the coaxial cable.

Question 6

You are installing a network between two buildings for a graphics publishing company. The company is going to connect its small network between the two buildings, which are approximately 900 meters apart. Each building already has a small 10BaseT LAN.

Required Result:

- Connect the LANs in each building with the appropriate type of cabling.

Optional Desired Results:

- The segment attaching the two buildings should be immune to electronic interference.
- The cabling should be inexpensive and easy to install.

Proposed Solution:

- Install a 10BaseFL (fiber optic) line connecting the two buildings.

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 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 the question is b. The proposed solution is the only appropriate choice because only a fiber optic cable could traverse the 900 meters between the two buildings. Fiber optic cable is not vulnerable to electronic interference; however, it isn't easy to install. Fiber optic cable is also expensive.

Question 7

Of the following cable types, which is the most susceptible to crosstalk?

- ❍ a. STP
- ❍ b. CAT5 UTP
- ❍ c. Coaxial
- ❍ d. Fiber optic

Answer b is correct. Unshielded twisted-pair is the most susceptible to crosstalk (communication bleed-over from one wire to another). Coaxial and STP are also susceptible to crosstalk, but they have shielding to reduce the chance of it.

Question 8

Which of the following cable types is used for ARCNet (Attached Resource Computer Networks)? [Check the best answer]

- ❍ a. CAT5 UTP
- ❍ b. RG-62
- ❍ c. RJ-45
- ❍ d. RG-58

For ARCNet, always choose RG-62 cabling, which makes answer b correct. The standard cable for ARCNet is RG-62. ARCNet can use fiber optic and twisted-pair cabling; however, this question is asking you to choose a single "best" answer, therefore, it's kind of tricky.

Question 9

Which type of connectors are characteristic of a Thinnet network? [Check all correct answers]

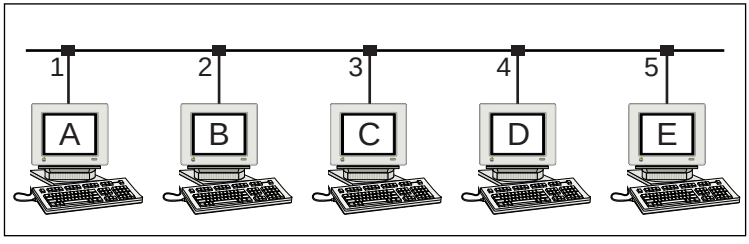
- ❑ a. BNC barrel connectors
- ❑ b. Vampire tap
- ❑ c. T-connector
- ❑ d. AUI connector
- ❑ e. Terminators

Answers a, c, and e are correct. Thicknet (10Base5) uses vampire taps and AUI connectors. Thinnet (10Base2) uses BNC barrel and T-connectors, and terminators should be placed at the end of each segment of the network.

Question 10

On a 10Base2 network (as depicted in the graphic), client B cannot connect to any other computers. All other machines are communicating correctly on the network. Which of the following is the most likely cause of the network problem?

- ❍ a. Faulty terminator
- ❍ b. High rate of collisions
- ❍ c. Faulty cabling between clients A and B
- ❍ d. Faulty cabling between clients B and C
- ❍ e. Faulty network card on client B



Answer e is correct. The most likely cause of networking problems that affects only client B is a faulty network card. The other situations listed would most likely cause network connectivity problems for all computers on the network.

Question 11

What do the NDIS and ODI interfaces allow you to do?

- ❍ a. Bind multiple protocols to a single network adapter
- ❍ b. Bind multiple network cards to a single computer
- ❍ c. Resolve IP addresses to NetBIOS computer names
- ❍ d. Separate the Application layer from the Session layer of the OSI Reference Model

The only correct answer is a. NDIS and ODI are interfaces that were designed to allow you to bind multiple protocols to a single network adapter. They do not perform any of the other functions listed above.

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 2, "Network Components," discusses all cable types at length.

Microsoft Press: *Networking Essentials, 2nd Edition*. Redmond, WA, 1997. ISBN 1-57231-527-X. Unit 2, Lesson 4, "Network Cabling—the Physical Media," 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 "cabling," "NDIS," "Thicknet," and related cable, connector, and interface names.