Chapter 2 - Connecting Network Components

Archived content. No warranty is made as to technical accuracy. Content may contain URLs that were valid when originally published, but now link to sites or pages that no longer exist.

A note from TechNet: This chapter was taken from the Microsoft Press book titled "Networking Essentials, Second Edition." To order the complete book, see the information in the document titled "How to Order MS Press Training Products" in the Windows NT Server Training directory.

Lesson 1 Network Cabling the Physical Media

Lesson 2 Wireless Network Communications

Lesson 3 Network Adapter Cards

Chapter 2 Review

Welcome to Chapter 2, Connecting Network Components. In this chapter you will see how the hardware presented in Chapter 1the servers, the client computers, and the peripherals are physically connected.

You will learn about the different physical media, which connect computers. Though cable is the most common medium, people on the move who need to be connected to their networks cannot drag cable along with them. Wireless communications is filling this need, and this chapter will present an overview of the current wireless technology which allows mobile computers to remain part of cabled networks.

Ultimately, no matter what type of media a network uses, the data will have to actually leave and enter a computer. It does this through a network adapter card, which connects the computer to either cable or the wireless environment. As with cable, there are many types of cards available, and, as this unit explains, choosing the right one is critical to the success of the network.

On This Page

The Case Study
Lesson 1: Network Cabling the Physical Media
Lesson 2: Wireless Network Communications
Lesson 3: Network Adapter Cards
Chapter 2 Review

The Case Study

In the case study for this unit you will evaluate the recommendations for a cabling scheme for your company's new office building.

The Troubleshooter

You will get a chance to troubleshoot a problem that arises when new client computers are added to an existing network.

The LAN Planner
The LAN Planner contains questions you need to ask when selecting cabling and network adapter cards for your network.

Top Of Page

Lesson 1: Network Cabling the Physical Media

What This Lesson Does

This lesson presents the essential LAN cabling concepts.

You will learn about the major cable types including their construction, features, and operation. This information will help you determine what type of cabling is best for any networking situation.

Objectives

By the end of this lesson, you will be able to:

- Define terms related to cabling including shielding, crosstalk, attenuation, and plenum.
- Identify the primary types of network cabling.
- Distinguish between baseband and broadband transmissions and identify appropriate uses for each.
- Determine which type of cabling and connection hardware would be appropriate for a particular network environment.

Estimated lesson time 50 minutes

Primary Cable Types

The vast majority of networks today are connected by some sort of wire or cabling, which act as the network transmission medium carrying signals between computers. There is a variety of cable that can meet the varying needs and sizes of networks, from small to large.

Cabling can be confusing. Belden, a leading cable manufacturer, publishes a catalog that lists more than 2,200 types of cabling. Fortunately, only three major groups of cabling connect the majority of networks:

- Coaxial
  - Twisted-pair
    - Unshielded twisted-pair
    - Shielded twisted-pair
- Fiber-optic

The next part of this lesson will describe the features and components of these three major cable types. Understanding their differences will help you determine when to use each type of cabling.

Coaxial

At one time, coaxial cable was the most widely used network cabling. There were a couple of reasons for coaxial's wide usage. Coaxial was relatively inexpensive, and it was light, flexible, and easy to work with. It was so popular that it became a safe, easily supported installation.
In its simplest form, coaxial consists of a core made of solid copper surrounded by insulation, a braided metal shielding, and an outer cover. One layer of foil insulation and one layer of braided metal shielding is referred to as dual shielded. However, quad shielding is available for environments that are subject to higher interference. Quad shielding consists of two layers of foil insulation and two layers of braided metal shielding.

![Coaxial cable showing various layers](image)

**Figure 2.1: Coaxial cable showing various layers**

Shielding refers to the woven or stranded metal mesh (or other material) that surrounds some types of cabling. Shielding protects transmitted data by absorbing stray electronic signals, called noise, so that they do not get onto the cable and distort the data.

The core of a coaxial cable carries the electronic signals which make up the data. This core wire can be either solid or stranded. If the core is solid, it is usually copper.

The core is surrounded by a dielectric insulating layer which separates it from the wire mesh. The braided wire mesh acts as a ground and protects the core from electrical noise and crosstalk. Crosstalk is signal overflow from an adjacent wire.

The conducting core and the wire mesh must always be separated from each other. If they touch, the cable will experience a short, and noise or stray signals on the mesh will flow onto the copper wire. This will destroy the data.

The entire cable is surrounded by a non-conducting outer shield, usually made of rubber, Teflon, or plastic.

Coaxial cable is more resistant to interference and attenuation than twisted-pair cabling. Attenuation is the loss of signal strength which begins to occur as the signal travels further along a copper cable.

![Attenuation causes signals to deteriorate](image)

**Figure 2.2: Attenuation causes signals to deteriorate**

The stranded, protective sleeve can absorb stray electronic signals so they do not affect data being sent over the inner copper cable. For this reason, coaxial is a good choice for longer distances and for reliably supporting higher data rates with less sophisticated equipment.

**Types of Coaxial Cable**

There are two types of coaxial cable:
- Thin (thinnet)
- Thick (thicknet)

What type you select depends on the needs of your particular network.

**Thinnet**

Thinnet is a flexible coaxial cable about .25 inch thick. Because this type of coaxial is flexible and easy to work with, it can be used in almost any type of network installation. Networks that use thinnet have the cable connected directly to a computer’s network adapter card.

![Thinnet cable](image)

**Figure 2.3: Close-up view of thinnet cable showing where it connects to a computer**

Thinnet coaxial cable can carry a signal up to approximately 185 meters (about 607 feet) before the signal starts to suffer from attenuation.

Cable manufacturers have agreed upon certain designations for different types of cable. Thinnet is included in a group referred to as the RG-58 family and has a 50-ohm impedance. Impedance is the resistance, measured in ohms, to alternating current flowing in a wire. The main difference in the RG-58 family is the center core of copper. It can either be a stranded wire or solid copper core.

![RG-58 coaxial](image)

**Figure 2.4: RG-58 coaxial showing stranded wire and the solid copper cores**

<table>
<thead>
<tr>
<th>Cable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RG-58 /U</td>
<td>Solid copper core</td>
</tr>
<tr>
<td>RG-58 A/U</td>
<td>Stranded wire core</td>
</tr>
<tr>
<td>RG-58 C/U</td>
<td>Military specification of RG-58 A/U</td>
</tr>
<tr>
<td>RG-59</td>
<td>Broadband transmission such as cable television</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>RG-6</td>
<td>Larger in diameter and rated for higher frequencies than RG-59, but used for broadband transmissions as well</td>
</tr>
<tr>
<td>RG-62</td>
<td>ArcNet networks</td>
</tr>
</tbody>
</table>

**Thicknet**

Thicknet is a relatively rigid coaxial cable about 0.5 inch in diameter. It is sometimes referred to as Standard Ethernet because it was the first type of cable used with the popular network architecture Ethernet. The copper core is thicker than a thinnet core.

![Thicknet vs Thinnet](image)

**Figure 2.5: Thicknet cable has a thicker core than thinnet**

The thicker the copper core, the farther the cable can carry signals. This means that thicknet can carry signals farther than thinnet. Thicknet can carry a signal for 500 meters (about 1,640 feet). Therefore, because of thicknet's ability to support data transfer over longer distances, it is sometimes used as a backbone to connect several smaller thinnet-based networks.

A device called a transceiver connects the thinnet coaxial to the larger thicknet coaxial cable.

![Thicknet Transceiver](image)

**Figure 2.6: Thicknet cable transceiver with detail of a vampire tap piercing the core**

A transceiver designed for thicknet Ethernet includes a connector known as a vampire tap or a piercing tap to make the actual physical connection to thicknet core. This connector is pierced through the insulating layer and makes direct contact with the conducting core. Connection from the transceiver to the network adapter card is made using a transceiver cable (drop cable) to connect to the attachment unit interface (AUI) port connector on the card. An AUI port connector for thicknet is also known as a *Digital Intel Xerox* (DIX) connector after the three companies that developed it and its related standards, or as a DB-15 connector.

**Thinnet vs. Thicknet**

As a general rule, the thicker the cable, the more difficult it is to work with. Thin cable is flexible, easy to install, and relatively inexpensive. Thick cable does not bend easily and is, therefore, harder
to install. This is a consideration when an installation calls for pulling cable through tight spaces such as conduits and troughs. Thick cable is more expensive than thin cable, but will carry a signal farther.

**Coaxial Connection Hardware**

Both thinnet and thicknet use connection components, known as a BNC (British Naval Connector), to make the connections between the cable and the computers. There are several important components in the BNC family, including the following:

- The BNC cable connector

  The BNC cable connector is either soldered or crimped to the end of a cable.

  ![BNC cable connector](image)

  **Figure 2.7: BNC cable connector**

- The BNC T connector

  This connector joins the network interface card in the computer to the network cable.

  ![BNC T connector](image)

  **Figure 2.8: BNC T connector**

- The BNC barrel connector

  This connector is used to join two lengths of thinnet cable to make one longer length.

  ![BNC barrel connector](image)

  **Figure 2.9: BNC barrel connector**

- The BNC terminator

  A BNC terminator closes each end of the bus cable to absorb stray signals. Without BNC terminators, a bus network will not function.
Coaxial Cable Grades and Fire Codes

The type of cable grade that you should use depends on where the cables will be in your office. Coaxial cables come in two grades:

- Polyvinyl chloride
- Plenum

Polyvinyl chloride (PVC) is a type of plastic used to construct the insulation and the cable jacket for most types of coaxial cable. PVC coaxial cable is flexible and can be easily routed in the exposed areas of an office. However, when it burns, it gives off poisonous gases.

A plenum is the short space in many buildings between the false ceiling and the floor above; it is used to circulate warm and cold air through the building. Fire codes are very specific on the type of wiring that can be routed through this area, because any smoke or gas in the plenum will eventually become part of the air breathed by everyone in the building.

Plenum cabling refers to coaxial cabling that contains special materials in its insulation and cable jacket. These materials are certified to be fire resistant and produce a minimum amount of smoke. This reduces poisonous chemical fumes. Plenum cable can be used in the plenum area and in vertical runs (for example, in a wall) without conduit. However, plenum cabling is more expensive and less flexible than PVC cable.

Note: Please consult your local fire and electrical codes for specific regulations about running networking cable in your office.
Coaxial Considerations

Consider these coaxial capabilities when making a decision on the type of cabling to use.

Use coaxial cable if you need:

- A medium that will transmit voice, video, and data.
- To transmit data longer distances than less expensive cabling can transmit.
- A familiar technology that offers reasonable data security.

Q & A

This is a two-part exercise. In the first part, supply the missing word(s) to complete the sentence. In the second part, identify the types of cable shown.

1. Coaxial consists of a core made of solid or stranded ___________ ___________.
2. If the coaxial conducting core and wire mesh touch, the cable will experience a ___________.
3. The core of coaxial cable is surrounded by an ___________ ___________ which separates it from the wire mesh.
4. Thicknet is sometimes used as a _____________ to connect thinnet segments.
5. Thinnet can carry a signal about 185 meters before the signal starts to suffer from _________________.
6. The electronic signals which make up the data are actually carried by the ________ in a coaxial cable.
7. A flexible coaxial cable that is easily routed but should not go into crawl spaces is ________.
8. Coaxial that contains special materials in its insulation and cable jacket is called _____________ cabling.

Answers

1. copper conductor
2. short
3. insulating layer
4. backbone
5. attenuation
6. core
7. PVC
8. plenum

Identify the following components.
1. __________

2. ________________

**Answers**

1. terminator
2. BNC T connector

**Twisted-Pair Cable**

In its simplest form, twisted-pair cable consists of two insulated strands of copper wire twisted around each other. There are two types of twisted-pair cable: unshielded twisted-pair (UTP) and shielded twisted-pair (STP).

![UTP and STP cables](image)

**Figure 2.12: Unshielded twisted-pair and shielded twisted-pair cables**

A number of twisted-pair wires are often grouped together and enclosed in a protective sheath to form a cable. The actual number of pairs in a cable varies. The twisting cancels out electrical noise from adjacent pairs and from other sources such as motors, relays, and transformers.

**Unshielded Twisted-Pair (UTP)**

UTP using the 10BaseT specification is the most popular type of twisted-pair cable and is fast becoming the most popular LAN cabling. The maximum cable length segment is 100 meters or about 328 feet.
UTP consists of two insulated copper wires. Depending on the particular purpose, there are UTP specifications which govern how many twists are permitted per foot of cable. In the North American continent, UTP cable is the most commonly used cable for existing telephone systems and is already installed in many office buildings.

**Figure 2.13: UTP cable**

UTP is specified in the Electronic Industries Association and the Telecommunications Industries Association (EIA/TIA) 568 Commercial Building Wiring Standard. EIA/TIA 568 used UTP in creating standards that apply to a variety of building and wiring situations and ensure consistency of products for customers. These standards include five categories of UTP:

- Category 1
  This refers to traditional UTP telephone cable which can carry voice but not data. Most telephone cable prior to 1983 was Category 1 cable.

- Category 2
  This category certifies UTP cable for data transmissions up to 4 Mbps (megabits per second). It consists of four twisted-pairs.

- Category 3
  This category certifies UTP cable for data transmissions up to 10 Mbps. It consists of four twisted-pairs with three twists per foot.

- Category 4
  This category certifies UTP cable for data transmissions up to 16 Mbps. It consists of four twisted-pairs.

- Category 5
  This category certifies UTP cable for data transmissions up to 100 Mbps. It consists of four twisted-pair of copper wire.

Most telephone systems use a type of UTP. In fact, one reason why UTP is so popular is because many buildings are prewired for twisted-pair telephone systems. As part of this prewiring, extra UTP is often installed to meet future cabling needs. If preinstalled twisted-pair cable is of sufficient grade to support data transmission, it can be used in a computer network. Caution is required, however, because common telephone wire may not have the twisting and other electrical characteristics required for clean, secure, computer data transmission.

One potential problem with all types of cabling is crosstalk. You may remember that crosstalk is defined as signals from one line getting mixed with signals from another line. UTP is particularly susceptible to crosstalk. Shielding is used to reduce crosstalk.

**Figure 2.14: Crosstalk occurs when signals from one line mix into another line**


**Shielded Twisted-Pair (STP)**

STP uses a woven copper braid jacket which is a higher-quality, more protective jacket than UTP has. STP also uses a foil wrap between and around the wire pairs, and internal twisting of the pairs. This gives STP excellent shielding to protect the transmitted data from outside interference.

What this means is that STP is less susceptible to electrical interference and supports higher transmission rates over longer distances than UTP.

![STP cable](image)

**Figure 2.15: STP cable**

**Twisted-Pair Cabling Components**

- Connection hardware

  Twisted-pair uses RJ-45 telephone connectors to connect to a computer. This is similar to the RJ-11 telephone connector. Although they look alike at first glance, there are crucial differences between them.

  The RJ-45 is slightly larger, and will not fit into the RJ-11 telephone jack. The RJ-45 houses eight cable connections, while the RJ-11 only houses four.

![RJ-45 connector and jack](image)

**Figure 2.16: RJ-45 connector and jack**

Several components are available to help organize large UTP installations and make them easier to work with. These include:

- Distribution racks and rack shelves

  Distribution racks and rack shelves can create more room for cables where there isn't much floor space. They are a good way to centralized and organize a network that has a lot of connections.

- Expandable patch panels

  These come in various versions that support up to 96 ports and transmission speeds of 100 Mbps.

- Jack couplers

  These single or double RJ-45 jacks snap into patch panels and wall plates and support data rates to 100 Mbps.

- Wall plates
These support two or more couplers.

**Figure 2.17: Various twisted-pair cabling components**

**Twisted-Pair Considerations**

Use twisted-pair cable if:

- Your LAN is under budget constraints.
- You want a relatively easy installation where computer connections are simple.

Do not use twisted-pair cable if:

- You must be absolutely sure of data integrity transmitted over great distances at high speeds.

**Q & A**

Fill in the blanks in the following sentences.

1. The most popular type of twisted-pair cable is ______ (10BaseT).
2. UTP cable for data transmissions up to 10 Mbps is category ______.
3. UTP cable for data transmissions up to 100 Mbps is category ______.
4. STP uses a foil wrap for ________________.
5. STP is less susceptible to electrical ________________ and supports higher transmission rates over longer distances than UTP.
6. Twisted-pair uses ______ telephone connectors to connect to a computer.
7. The RJ-45 connection houses _____ cable connections while the RJ-11 only houses ____.

**Answers**

1. UTP
2. 3
3. 5
4. shielding
5. interference
6. RJ-45
7. 8, 4

**Fiber-Optic Cable**

In fiber-optic cable, optical fibers carry digital data signals in the form of modulated pulses of light. This is a relatively safe way to send data because no electrical impulses are carried over the fiber-optic cable. This means that fiber-optic cable cannot be tapped and the data stolen, which is possible with any copper-based cable carrying data in the form of electronic signals.

Fiber-optic cable is good for very high-speed, high-capacity data transmission because of the lack of attenuation and the purity of the signal.

**Fiber-Optic Composition**

Optical fibers consists of an extremely thin cylinder of glass, called the core, surrounded by a concentric layer of glass, known as the cladding. The fibers are sometimes made of plastic. Plastic is easier to install, but cannot carry the light pulses as far as glass.

Each glass strand passes signals in only one direction, so a cable consists of two strands in separate jackets. One strand transmits and one receives. A reinforcing layer of plastic surrounds each glass strand while kevlar fibers provide strength. See Figure 2.18 for an example of kevlar fibers. The kevlar fibers in the fiber-optic connector are placed between the two cables, which are encased in plastic.

![Fiber optic cable diagram](image)

**Figure 2.18: Fiber-optic cable**

Fiber-optic cable transmissions are not subject to electrical interference and are extremely fast (currently transmitting about 100 Mbps with demonstrated rates of up to > 1Gbps). They can carry a signal the light pulse for many miles.

**Fiber-Optic Considerations**

Use fiber-optic cable if you:

- Need to transmit data at very high speeds over long distances in a very secure media.

Do not use fiber-optic cable if you:
• Are under a tight budget. (*Note: Pricing for fiber optic cable is competitive to hi-end copper cabling.)

• Do not have the expertise available to properly install it and connect devices to it. (*Note: Fiber optic cable is increasingly easier to work with. Polishing and terminating techniques require fewer parts and less expertise.)

Q & A

Fill in the blanks in the following sentences.

1. Optical fibers carry ______________ data signals in the form of light pulses.

2. Fiber-optic cable cannot be ______________ and the data stolen.

3. Fiber-optic cable is better for very high speed, high-capacity data transmission than ______________ cable because of the lack of attenuation and the purity of the signal.

4. Fiber-optic cable transmissions are not subject to electrical ______________.

Answers

1. digital
2. tapped
3. copper
4. interference

Signal Transmission

Two techniques can be used to transmit the encoded signals over cablebaseband and broadband transmission.

Baseband Transmission

Baseband systems use digital signaling over a single frequency. Signals flow in the form of discrete pulses of electricity or light. With baseband transmission, the entire communication channel capacity is used to transmit a single data signal. The digital signal uses the complete bandwidth of the cable, which constitutes a single channel. A cable’s total bandwidth is the difference between the highest and lowest frequencies that are carried over that cable.

Each device on a baseband network transmits bidirectionally, and some can transmit and receive at the same time.

![Figure 2.19: Baseband transmission showing bidirectional digital wave](http://technet.microsoft.com/en-us/library/cc723461(d=printer).aspx)

As the signal travels along the network cable, it gradually decreases in strength and can become distorted. If the cable length is too long, the result is a signal that is weak or distorted. The received signal may be unrecognizable or misinterpreted.

As a safeguard, baseband systems sometimes use repeaters to receive an incoming signal and retransmit it at its original strength and definition to increase the practical length of a cable.
Broadband Transmission

Broadband systems use analog signaling and a range of frequencies. With analog transmission, the signals are continuous and nondiscrete. Signals flow across the physical medium in the form of electromagnetic or optical waves. With broadband transmission, signal flow is unidirectional.

Figure 2.20: Broadband transmission showing unidirectional analog wave

If sufficient total bandwidth is available, multiple analog transmission systems such as cable television and network transmissions can be supported simultaneously on the same cable.

Each transmission system is allocated a part of the total bandwidth. All devices associated with a given transmission system, such as all computers using a LAN cable, must then be tuned so that they use only the frequencies that are within the allocated range.

While baseband systems use repeaters, broadband systems use amplifiers to regenerate analog signals at their original strength.

Because broadband transmission signal flow is unidirectional, there must be two paths for data flow in order for a signal to reach all devices. There are two common ways to do this:

- Mid-split broadband configuration divides the bandwidth into two channels, each using a different frequency or range of frequencies. One channel is used to transmit signals, the other to receive signals.

- In dual-cable broadband configuration, each device is attached to two cables. One cable is used to send and the other is used to receive.

Q & A

Fill in the blanks in the following sentences.

1. Baseband systems use ____________ signaling over a single frequency.
2. Each device on a ____________ network can transmit and receive at the same time.
3. Broadband systems use ____________ signaling and a range of frequencies.
4. With ____________ transmission, the signal flow is unidirectional.

Answers

1. digital
2. baseband
3. analog
4. broadband

The IBM Cabling System
IBM developed its own cabling system, complete with its own numbers, standards, specifications, and designations. Many of these parameters, however, are similar to non-IBM specifications.

The IBM cabling system was introduced in 1984 in order to define these components:

- Cable connectors
- Face plates
- Distribution panels
- Cable types

The IBM cabling component that is unique is the IBM connector. The IBM connector is different from standard BNC or other connectors because it is neither male nor female but hermaphroditic in that two of them can be connected to each other. These IBM connectors required special face plates and distribution panels to accommodate their unique shape.

The IBM cabling system classifies cable as types. For example, Category 3 cable (voice grade UTP) is referred to by the IBM system as Type 3.

The cable definitions specify which cable would be appropriate for a given application or environment. The wire indicated in the system conforms to American Wire Gauge (AWG) standards.

**AWG: the Standard Cable Measurement**

In cable measurements you will often see the word gauge followed by the initials AWG. AWG is a measurement system for wire that specifies its thickness. As the thickness of the wire increases, the AWG number decreases. Telephone wire is often used as a reference point. It has a thickness of 22 AWG. A wire of 14 AWG would be thicker than telephone wire, and 26 AWG would be thinner than telephone wire.

**IBM Cabling System**

<table>
<thead>
<tr>
<th>IBM type</th>
<th>Standard label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1</td>
<td>Shielded twisted-pair (STP)</td>
<td>Two pair of 22 AWG wires surrounded by an outer braided shield. Used for computers and MAUs.</td>
</tr>
<tr>
<td>Type 2</td>
<td>Voice and data cable</td>
<td>A voice and data shielded cable with two twisted-pairs of 22 AWG wires for data, an outer braided shield, and then four twisted-pairs of 26 AWG for voice.</td>
</tr>
<tr>
<td>Type 3</td>
<td>Voice grade cable</td>
<td>Consists of four solid, unshielded twisted-pair 22 or 24 AWG cables.</td>
</tr>
<tr>
<td>Type 4</td>
<td>Not yet defined</td>
<td></td>
</tr>
<tr>
<td>Type 5</td>
<td>Fiber-optic cable</td>
<td>Two 62.5/125-micron multimode optical fiberthe industry standard.</td>
</tr>
<tr>
<td>Type 6</td>
<td>Data patch cable</td>
<td>Two 26 AWG twisted-pair stranded cables with a dual foil and braided shield.</td>
</tr>
</tbody>
</table>
Type 7 | Not yet defined
---|---
Type 8 | Carpet cable  
Housed in a flat jacket for use under carpets. Two shielded twisted-pair 26 AWG cables. Limited to one-half the distance of Type 1 cable.
Type 9 | Plenum  
Fire safe. Two shielded twisted-pair cables.

Selecting Cabling

To determine which cabling is the best for a particular site you need to answer the following questions:

- How heavy will the network traffic be?
- What are the security needs of the network?
- What are the distances the cable must cover?
- What are the cable options?
- What is the budget for cabling?

The more the cable protects against internal and external electrical noise, the farther and faster the cable will carry a clear signal. However, the better the speed, clarity, and security, the higher the cabling cost.

Cabling Considerations

As with most network components, there are trade-offs with the type of cable you purchase. If you work for a large organization and choose the least expensive cable, the accountants may initially be pleased, but you may soon notice that the LAN is inadequate in both transmission speed and data security.

Cabling depends on the needs of a particular site. The cabling you purchase to set up a LAN for a small business has different requirements than those of a larger organization, such as a major banking institution.

Some of the considerations which affect cabling price and performance include:

- Installation logistics
  
  How easy is the cable to install and work with? In a small installation where distances are short and security isn’t a major issue, it does not make sense to choose thick, cumbersome, and expensive cable.

- Shielding
  
  The level of shielding required will be an added cost. Almost every network will be using some form of shielded cable. The noisier the area in which the cable is run, the more shielding will be required. Plenum grade cable is more expensive as well.

- Crosstalk
  
  Crosstalk and noise can cause serious problems in large networks where data security is crucial. Inexpensive cabling has low resistance to outside electrical fields generated by power
lines, motors, relays, and radio transmitters. This makes it susceptible to both noise and crosstalk.

- **Transmission speed (part of bandwidth)**

  Transmission rates are measured in megabits per second (Mbps). A standard reference point for current LAN transmission over copper cable is 10 Mbps, however, recent standards now allow > 100 Mbps transmission speeds.

  Thick cable transmits data over a longer distance than thin cable. But thick cable, such as thicknet, is more difficult to work with than thinner cables such as thinnet.

  Fiber-optic cable transmits at more than 1 Gbps, so it is even faster than copper, but requires expertise to install and is relatively expensive.

- **Cost**

  Better cable, which transmits data securely over long distances, is more expensive than thin cable, which is easy to install and work with.

- **Attenuation**

  Attenuation is the reason for cable specifications that recommend certain length limits on different types of cabling. If a signal suffers too much attenuation, it will not be understood by the receiving computer. Most networks have error checking systems that will generate a retransmission if the signal is too weak to be understood, but retransmission takes time and slows down the network.

**Cable Comparison Summary**

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Thinnet coaxial (10Base2)</th>
<th>Thicknet coaxial (10Base5)</th>
<th>Twisted-pair (10BaseT)</th>
<th>Fiber-optic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable cost</td>
<td>More than twisted-pair</td>
<td>More than thinnet</td>
<td>Least expensive</td>
<td>More expensive</td>
</tr>
<tr>
<td>Usable cable length*</td>
<td>185 meters or about 607 feet</td>
<td>500 meters or about 1640 feet</td>
<td>100 meters or about 328 feet</td>
<td>2 kilometers or 6562 feet</td>
</tr>
<tr>
<td>Transmission rates**</td>
<td>10 Mbps</td>
<td>10 Mbps</td>
<td>10 Mbps 4100 Mbps</td>
<td>100 Mbps or more (&gt; 1Gbps)</td>
</tr>
<tr>
<td>Flexibility</td>
<td>Fairly flexible</td>
<td>Less flexible</td>
<td>Most flexible</td>
<td>Very flexible</td>
</tr>
<tr>
<td>Ease of installation</td>
<td>Easy to install</td>
<td>Easy to install</td>
<td>Very easy; possibly already installed</td>
<td>Easy to install</td>
</tr>
<tr>
<td>Susceptibility to interference</td>
<td>Good resistance to interference</td>
<td>Good resistance to interference</td>
<td>Susceptible to interference</td>
<td>Not susceptible to interference</td>
</tr>
<tr>
<td>Special features</td>
<td>Electronic support components less expensive than twisted-pair</td>
<td>Electronic support components less expensive than twisted-pair</td>
<td>Same as telephone wire; often pre-installed in buildings</td>
<td>Supports voice, data, and video</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>----------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Preferred uses</td>
<td>Medium to large sites with high security needs</td>
<td>UTP smaller sites on budget STP Token Ring in any size</td>
<td>Any size installation requiring speed and high data security and integrity</td>
<td></td>
</tr>
</tbody>
</table>

* Usable cable length can vary with specific network installations. As technology improves, usable cable length also increases.

** Transmission rates for specific cable types are beginning to blur. Again, technological advances are producing copper wire that can carry a signal faster than has ever been considered possible.

**Summary**

Choosing the appropriate network cable depends on several factors including installation logistics, shielding, security requirements, transmission speed (in Mbps), and attenuation. There are three primary types of cable: coaxial, twisted-pair, and fiber-optic.

There are two types of coaxial cable, thinnet and thicknet. Both have a copper core surrounded by wire mesh that absorbs noise and crosstalk. Coaxial cable is a good choice for data transmission of long distances.

Twisted-pair cable is available both unshielded and shielded. Unshielded twisted-pair (UTP) is available in five categories of which Category 5 is the most popular for network installations. Shielded twisted-pair (STP) supports higher transmission rates over longer distances than UTP.

Fiber-optic cable is faster and more secure than copper wire cable, but it is relatively expensive and requires some expertise to install.

Broadband and baseband are two transmission techniques. Broadband uses analog signaling to transmit multiple simultaneous transmissions on the same cable. Baseband sends single channel, digital signals.

IBM has its own cabling system complete with its own types. IBM Type 3 cabling, for example, is a voice grade, shielded twisted-pair cable otherwise known as STP.

**Your Next Step**

Cables are the most commonly used way to transmit data between computers. However, the wireless environment is an emerging collection of topologies that may someday do away with the need for physical connections. You will learn about the basics of wireless communication technology in the next lesson.

**Top Of Page**

Lesson 2: Wireless Network Communications

**What This Lesson Does**
This lesson presents an overview of wireless network technology. In this lesson you will learn the differentiation between the various wireless environments and learn about the major wireless transmission and receiving components.

**Objectives**

By the end of this lesson, you will be able to:

- Identify the three types of wireless networks and the uses of each.
- Describe the four transmission techniques used in local area networking.
- Describe the three types of signal transmission used in mobile computing.

**Estimated lesson time 25 minutes**

**The Wireless Environment**

The wireless environment is emerging as a viable networking option. As the technology matures, vendors will be offering more products at attractive prices which, in turn, will mean increased sales and demand. As demand increases, the wireless environment will grow and improve.

The phrase wireless environment is misleading because it implies a network completely free of cabling. In most cases, this is not true. Most wireless networks actually consist of wireless components communicating with a network that uses cables in a mixed component network called a hybrid.

**Wireless Capabilities**

The idea of wireless networks is attracting attention because wireless components can:

- Provide temporary connections to an existing, cabled network.
- Help provide backup to an existing network.
- Provide a certain degree of portability.
- Extend networks beyond the limits of copper or even fiber-optic cables.

**Uses for Wireless**

Difficulty implementing cable is a factor which will continue to push wireless environments toward greater acceptance. Wireless can be especially useful for networking:

- Busy areas such as lobbies and reception areas.
- People who are constantly on the move such as doctors and nurses in hospitals.
- Isolated areas and buildings.
- Departments where the physical setting changes frequently.
- Structures, such as historical buildings, where cabling would be difficult.

**Types of Wireless Networks**

Wireless networks can be divided into three categories based on their technology:

- Local area networks
- Extended local area networks
- Mobile computing

The primary difference between these categories is the transmission facilities. Wireless LANs and extended LANs use transmitters and receivers owned by the company in which the network operates. Mobile computing uses public carriers such as AT&T, MCI, Sprint and the local telephone companies and their public services, to transmit and receive signals.

**Local Area Networks**

A typical wireless network looks and acts almost like a cabled network except for the media. A wireless network adapter card with a transceiver is installed into each computer, and users communicate with the network just as if they were at cabled computers.

**Access Points**

The transceiver, sometimes called an access point, broadcasts and receives signals to and from the surrounding computers and passes data back and forth between the wireless computers and the cabled network.

These wireless LANs use small wall-mounted transceivers to connect to the wired network. The transceivers establish radio contact with portable networked devices. This is not a true wireless LAN because it uses a wall-mounted transceiver to connect to a standard cabled LAN.

![Network diagram](image)

**Figure 2.21: Wireless portable computer connecting to a cabled network access point**

**Transmission Techniques**

Wireless LANs use four techniques for transmitting data:

1. Infrared
2. Laser
3. Narrow-band (single-frequency) radio
4. Spread-spectrum radio

**Infrared**
All infrared wireless networks operate by using an infrared light beam to carry the data between devices. These systems need to generate very strong signals because weak transmission signals are susceptible to light from sources such as windows.

This method can transmit signals at high rates because of infrared light's high bandwidth. An infrared network can normally broadcast at 10 Mbps.

There are four types of infrared networks:

- **Line-of-sight networks**
  
  As the name implies, this version of infrared transmits only if the transmitter and receiver have a clear line of sight between them.

- **Scatter infrared networks**
  
  This technology broadcasts transmissions so they bounce off walls and ceilings and eventually hit the receiver. This has an effective area limited to about 100 feet and has a slow signal because of all of the signal bouncing.

- **Reflective networks**
  
  In this version of infrared networks, optical transceivers situated near the computers transmit toward a common location which redirects the transmissions to the appropriate computer.

- **Broadband optical telepoint**
  
  This version of infrared wireless LAN provides broadband services. This wireless network is capable of handling high quality multimedia requirements that can match those provided by a cabled network.

![Infrared](image)

**Figure 2.22: Wireless portable computer using an infrared light beam to print**

While the speed of infrared and its conveniences are generating interest, infrared has difficulty transmitting distances greater than 100 feet. It is also subject to interference from the strong ambient light found in most business environments.

**Laser**

Laser technology is similar to infrared technology in that it requires a direct line of sight, and any person or thing that breaks the laser beam will block the transmission.

**Narrow-Band (Single-Frequency) Radio**
This approach is similar to broadcasting from a radio station. The user tunes both the transmitter and the receiver to a certain frequency. This does not require line of sight focusing because the broadcast range is 5000 meters square. However, because the signal is high frequency, it cannot go through steel or load-bearing walls.

Customers subscribe to this method from a service provider such as Motorola. The service provider handles all of the Federal Communications Commission (FCC) licensing requirements. This method is relatively slow; transmission is in the 4.8 Mbps range.

**Spread-Spectrum Radio**

Spread-spectrum radio broadcasts signals over a range of frequencies. This helps it avoid narrow-band communication problems.

The available frequencies are divided into channels or hops. The spread-spectrum adapters tune in to a specific hop for a predetermined length of time and then switch to a different hop. A hopping sequence determines the timing. The computers in the network are all synchronized to the hop timing. This type of signaling provides some "built-in" security in that the frequency hopping algorithm of the network would have to be "known" in order to tap into the data stream.

To further enhance security and to keep unauthorized users from listening in to the broadcast, the sender and the receiver can encrypt (code) the transmission.

The typical speed of 250 Kbps (kilobits per second) makes this method much slower than the others. However, some implementations of spread-spectrum radio can offer transmission speeds of 4 Mbps over distances of two miles outdoors and > 800 feet indoors.

This is one area where the technology actually provides for a truly wireless network. For example, two or more computers equipped with Xircom CreditCard Netwave Adapters and an operating system such as Microsoft Windows 95 or Microsoft Windows NT can act as a peer-to-peer network with no connecting cables. However, if you have an existing Windows NT Server-based network, you can tie the above wireless network into it by adding a Netwave Access Point to one of the computers on the Windows NT Server-based network.

**Point-to-Point Transmission**

This method of data communication does not fall neatly into the present definitions of networking. It uses a point-to-point technology that transfers data from one computer to another as opposed to communicating among several computers and peripherals. However, additional components such as single and host transceivers are available. These can be implemented in either stand-alone computers or computers already on a network to form a wireless data transfer network.

This technology involves wireless serial data transfer that:

- Uses a point-to-point radio link for fast, error-free data transmission.
- Penetrates through walls, ceilings, and floors.
- Supports data rates from 1.2 to 38.4 Kbps up to 200 feet indoors or one-third of a mile with line-of-site transmission.

This type of system will transfer data between computers, and between computers and other devices such as printers or bar code readers.

**Extended Local Area Networks**

Other types of wireless components are able to do jobs in the extended LAN environment similar to their cabled counterparts. A wireless LAN bridge, for example, can connect networks up to three miles apart.
Multipoint Wireless Connectivity

A component called a wireless bridge offers an easy way to link buildings without using cable. As a foot bridge provides a path between two points for people, a wireless bridge provides a data path between two buildings. The AIRLAN/Bridge Plus, for example, uses spread-spectrum radio technology to create a wireless backbone to tie locations together over distances beyond the reach of LANs. Depending on conditions, this can be up to three miles.

The cost of such a component may be justified because it eliminates the expense of leased lines.

![Diagram of two buildings connected by a wireless bridge]

Figure 2.23: Wireless bridge connecting two LANs

The Long-Range Wireless Bridge

If the wireless bridge will not reach far enough, an organization might consider a long-range wireless bridge. These also use spread-spectrum radio technology to provide both Ethernet and Token Ring bridging for up to 25 miles.

As with the original wireless bridge, the cost of the long range bridge may be justified because it eliminates the need for T1 line or microwave connections. T1 is the standard digital line service and provides transmission rates of 1.544 Mbps. It can carry both voice and data.

Q & A

Fill in the blanks in the following sentences.

1. Wall mounted ________________ connected to the wired LAN maintain and manage radio contact between portable devices and the cabled LAN.

2. Broadband optical telepoint transmission is a type of ________________ network capable of handling high-quality multimedia requirements.

3. A component called a wireless ________________ offers an easy way to link buildings without using cable.

4. Spread-spectrum broadcasts signals over a range of ________________.

5. Point-to-point transmission involves wireless ____________ data transfer.

6. In local area networks a transceiver, sometimes called an ________________ ________________, broadcasts and receives signals to and from the surrounding computers.
**Answers**

1. transceivers
2. infrared
3. bridge
4. frequencies
5. serial
6. access point

**Mobile Computing**

Wireless, mobile networks involve telephone carriers and public services to transmit and receive signals using:

- Packet-radio communication
- Cellular networks
- Satellite stations

Traveling employees can use this technology with portable computers or PDAs (Personal Digital Assistants) to exchange e-mail, files, or other information.

While this form of communication offers conveniences, it is slow. Transmission rates range from 8 Kbps to 19.2 Kbps. The rates get even slower when error correction is included.

Mobile computing incorporates wireless adapters that use cellular telephone technology to connect portable computers with the cabled network. Portable computers use small antennas to communicate with radio towers in the surrounding area. Satellites in near-earth orbit pick up low-powered signals from portable and mobile networked devices.

**Packet-Radio Communication**

This system breaks a transmission into packets, similar to other network packets, that include:

- The source address
- The destination address
- Error-correction information

The packets are uplinked to a satellite which broadcasts them. Only devices with the correct address can receive the broadcast packets.

**Cellular Networks**

Cellular Digital Packet Data (CDPD) uses the same technology and some of the same systems as cellular telephones. It offers computer data transmissions over existing analog voice networks between voice calls when the system is not busy. This is very fast technology that only suffers subsecond delays, which makes it reliable enough for real-time transmission.

As in other wireless networks, there must be a way to tie in to the existing cabled network. Nortel out of Mississauga, Ontario, Canada is one company that makes an Ethernet interface unit (EIU) that can provide this connection.
**Satellite Stations**

Microwave systems are good for interconnecting buildings in small, short-distance systems such as those on a campus or in an industrial park.

Microwave is currently the most widely used long distance transmission method in the United States. It is excellent for communicating between two line of sight points such as:

- Satellite to ground links.
- Between two buildings.
- Across large, flat, open areas such as bodies of water or deserts.

A microwave system consists of:

- Two radio transceivers one to generate (transmitting station) and one to receive (receiving station) the broadcast.
- Two directional antennas pointed at each other to implement communication of the signals broadcast by the transceivers. These antennas are often installed on towers to give them more range and raise them above anything which might block their signals.

**Q & A**

Fill in the blanks in the following sentences.

1. Wireless ____________ LANs involve telephone carriers and public services to transmit and receive signals.

2. CDPD uses the same technology and some of the same systems as ____________ telephones.

3. Currently, the most widely used long-distance transmission method in the United States is _________________.

**Answers**

1. mobile
2. cellular
3. microwave

**Summary**

Wireless networking is emerging as a transmission method for local area networks, extended local area networks, and mobile computing. A typical wireless network acts like a cabled network. A wireless network adapter card with a transceiver is installed into each computer, and users communicate with the network just as if they were at cabled computers.

Wireless networks use infrared, laser, narrow-band radio, and spread-spectrum radio transmission techniques. An additional type of technology is point-to-point. It transfers data from one computer to another as opposed to communicating among several computers and peripherals.

LANs can be extended using a component called a wireless bridge. It provides a way to link buildings separated by 25 miles or less without using cable.

Mobile computing involves telephone carriers and public services to transmit and receive signals using packet-radio communication, cellular networks, and satellite stations.
Your Next Step

Now that you have been introduced to the technology and the components that connect computers to each other, you are ready to learn about the component that acts as the point-of-data entry and exit between the computer and the network the network adapter card. Knowing the key features of network adapter cards will help you select the appropriate one for your site.

Top Of Page

Lesson 3: Network Adapter Cards

What This Lesson Does

This lesson introduces the basic features and functions of network adapter cards and how they can affect network performance. It describes the different cable media connector types as well as the configuration options for a network adapter card.

This lesson provides you with all of the information you need to select the right network adapter cards for your network.

Objectives

By the end of this lesson, you will be able to:

- Describe the role of the network adapter card in a network including preparing, sending, and controlling data.
- Describe the configurable options for network adapter cards.
- List the primary considerations for selecting a network adapter card.
- Describe at least two enhancements to network adapter cards that will improve network performance.

Estimated lesson time 85 minutes

The Role of the Network Adapter Card

Network adapter cards act as the physical interface or connection between the computer and the network cable. The cards are installed in an expansion slot in each computer and server on the network.

After the card has been installed, the network cable is attached to the card's port to make the actual physical connection between the computer and the rest of the network.
Figure 2.24: Sample network adapter card

The role of the network adapter card is to:

- Prepare data from the computer for the network cable.
- Send the data to another computer.
- Control the flow of data between the computer and the cabling system.

The network adapter card also receives incoming data from the cable and translates it into bytes the computer's CPU can understand.

Stated at a more technical level, the network adapter card contains the hardware and firmware (software routines stored in read-only memory) programming that implements the Logical Link Control and Media Access Control functions (in the Data Link layer function of the OSI model).

Preparing the Data

Before data can be sent over the network, the network adapter card must change it from a form the computer can understand to another form which can travel over a network cable.

Data moves through a computer along paths called busses. These are actually several data paths placed side by side. Because several paths are side by side (parallel), data can move along them in groups instead of a single (serial) data stream.

Older busses, such as those used in the original IBM personal computer, were known as 8-bit busses because they could move data 8 bits at a time. The IBM PC/AT used a 16-bit bus, which means it could move data 16 bits at a time. Many computers use 32-bit buses. When data travels on a computer's bus, it is said to be traveling in parallel because the 16 or 32 bits are moving along side by side. Think of a 16-bit bus as being a 16-lane highway with 16 cars moving side by side (moving in parallel), each carrying one bit of data.

On the network cable, data must travel in a single bit stream. When data travels on a network cable it is said to be traveling as a serial transmission because one bit follows another. In other words, the cable is a one-lane highway. The data on these highways always travel in one direction. The computer is either sending or receiving data.

The network adapter card takes data traveling in parallel as a group and restructures it so that it will flow through the 1-bit wide serial path of the network cable. This is accomplished through the translation of the computer's digital signals into electrical and optical signals that can travel on the network's cables. The component responsible for this is the transceiver (transmitter/receiver).
Figure 2.25: Parallel data stream converted to a serial data stream

Network Address

In addition to transforming data, the network adapter card also has to indicate its location, or address, to the rest of the network to distinguish it from all of the other cards on the network.

Network addresses are determined by the IEEE (Institute of Electrical and Electronics Engineers, Inc.) committee. The committee assigns blocks of addresses to each network adapter card manufacturer. The manufacturers hardwire these addresses into chips on the card by a process known as burning the address into the card. With this process each card, and therefore each computer, has a unique address on a network.

The network adapter card also participates in several other functions in taking data from the computer and getting it ready for the network cable.

1. The computer and network adapter card must communicate in order to move data from the computer to the card. On cards that can utilize direct memory access (DMA), the computer assigns some of its memory space to the network adapter card.

2. The network adapter card signals the computer requesting the computer's data.

3. The computer's bus moves the data from the computer's memory to the network adapter card.

Data can often move faster than the network adapter card can handle it, so the data is sent to the card's buffer (RAM) where it is held temporarily during both the transmission and reception of data.

Sending and Controlling Data

Before the sending network adapter card actually sends data over the network, it carries on an electronic dialog with the receiving card so that both cards agree on the following:

- Maximum size of the groups of data to be sent
- The amount of data to be sent before confirmation
- The time intervals between sending data chunks
- The amount of time to wait before confirmation is sent
- How much data each card can hold before it overflows
- The speed of the data transmission

If a newer, faster, more sophisticated card needs to communicate with an older, slower model, both cards need to find a common transmission speed each can accommodate. Some newer network adapter cards incorporate circuitry that allows the card to adjust to the rate of the slower card.
Each card signals to the other indicating its parameters and accepting or adjusting to the other card's parameters. When all of the communication details have been determined, the two cards begin sending and receiving data.

**Q & A**

For the following sentences, circle True if the statement is true or False if the statement is false.

1. The network adapter card converts serial data from the computer into parallel data for transmission over the network cable. True False

2. 16-bit and 32-bit are currently the two most popular bus widths. True False

3. To help move data onto the network cable, the computer assigns all of its memory to the network adapter card. True False

4. Data is temporarily held in the network adapter card's transceiver which acts as a buffer. True False

5. Both sending and receiving network adapter cards must agree on transmission speeds. True False

**Answers**

1. False. The reverse is true. The card converts parallel data to serial data.

2. True.

3. False. The computer can assign some of its memory to the card, but not all of it.

4. False. Only RAM acts as a buffer. The transceiver transmits and receives data.

5. True.

**Configuration Options and Settings**

Network adapter cards often have configurable options that must be set for the network adapter card to function properly. Examples include:

- Interrupt (IRQ)
- Base I/O port address
- Base memory address
- Transceiver

**Note:** Sometimes it is possible to specify network adapter card settings in software, but these settings commonly must match jumper or dual inline package (DIP) switch settings configured on the network adapter card. See the network card product documentation for DIP switch settings.

(*Note: Many newer network adapter cards use the Plug-and-Play (PnP) technology, which makes manually setting the network adapter card options obsolete).
Figure 2.26: Older network adapter card with DIP switches

Interrupt (IRQ)

Interrupt request lines are hardware lines over which devices such as input/output ports, the keyboard, disk drives, and network adapter cards can send interrupts or requests for service to the computer's microprocessor.

Interrupt request lines are built into the computer's internal hardware and are assigned different levels of priority so that the microprocessor can determine the relative importance of incoming service requests.

When the network adapter card sends a request to the computer, it uses an interruptan electronic signal sent to the computer's CPU. Each device in the computer must use a different interrupt request line or interrupt (IRQ). The interrupt line is specified when the device is configured. See the examples in the following table.

In most cases, IRQ3 or IRQ5 can be used for the network adapter card. IRQ5 is the recommended setting if it is available, and it is the default for most systems. Use a system diagnostic tool such as Microsoft Diagnostic (MSD) to determine which IRQs are already being used.

If neither IRQ3 nor IRQ5 is available, you can refer to the following table for alternative values to use. The IRQs listed as available usually can be used for a network adapter card. If the computer does not have the hardware device listed for a specific IRQ, that IRQ should be available.

<table>
<thead>
<tr>
<th>IRQ</th>
<th>Computer with an 80286 processor (or higher)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 (9)</td>
<td>EGA/VGA (enhanced graphics adapter/video graphics adapter)</td>
</tr>
<tr>
<td>3</td>
<td>Available (unless used for second serial port [COM2, COM4] or bus mouse)</td>
</tr>
<tr>
<td>4</td>
<td>COM1, COM3</td>
</tr>
<tr>
<td>5</td>
<td>Available (unless used for second parallel port [LPT2] or sound card)</td>
</tr>
<tr>
<td>6</td>
<td>Floppy-disk controller</td>
</tr>
<tr>
<td>Port</td>
<td>Device</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>7</td>
<td>Parallel port (LPT1)</td>
</tr>
<tr>
<td>8</td>
<td>Real-time clock</td>
</tr>
<tr>
<td>10</td>
<td>Available</td>
</tr>
<tr>
<td>11</td>
<td>Available</td>
</tr>
<tr>
<td>12</td>
<td>Mouse (PS/2)</td>
</tr>
<tr>
<td>13</td>
<td>Math coprocessor</td>
</tr>
<tr>
<td>14</td>
<td>Hard-disk controller</td>
</tr>
<tr>
<td>15</td>
<td>Available</td>
</tr>
</tbody>
</table>

**Base I/O Port**

The base input/output (I/O) port specifies a channel through which information flows between the computer's hardware (such as the network adapter card) and its CPU. The port appears to the CPU as an address.

Each hardware device in a system must have a different base I/O port number. The port numbers (in hexadecimal format) in the following table are usually available to assign to a network adapter card unless they are already in use. Those with a device listed next to them are addresses commonly used for the devices. Check the computer documentation to determine which addresses are already in use.

**Base I/O Port Settings**

<table>
<thead>
<tr>
<th>Port</th>
<th>Device</th>
<th>Port</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 to 20F</td>
<td>Game port</td>
<td>300 to 30F</td>
<td>Network adapter card</td>
</tr>
<tr>
<td>210 to 21F</td>
<td></td>
<td>310 to 31F</td>
<td>Network adapter card</td>
</tr>
<tr>
<td>220 to 22F</td>
<td></td>
<td>320 to 32F</td>
<td>Hard-disk controller (for PS/2 Model 30)</td>
</tr>
<tr>
<td>230 to 23F</td>
<td>Bus mouse</td>
<td>330 to 33F</td>
<td></td>
</tr>
<tr>
<td>240 to 24F</td>
<td></td>
<td>340 to 34F</td>
<td></td>
</tr>
<tr>
<td>250 to 25F</td>
<td></td>
<td>350 to 35F</td>
<td></td>
</tr>
<tr>
<td>Address Ranges</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>260 to 26F</td>
<td>360 to 36F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>270 to 27F LPT3</td>
<td>370 to 37F LPT2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>280 to 28F</td>
<td>380 to 38F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>290 to 29F</td>
<td>390 to 39F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2A0 to 2AF</td>
<td>3A0 to 3AF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2B0 to 2BF</td>
<td>3B0 to 3BF LPT1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2C0 to 2CF</td>
<td>3C0 to 3CF EGA/VGA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2D0 to 2DF</td>
<td>3D0 to 3DF CGA/MCGA (also EGA/VGA, in color video modes)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2E0 to 2EF</td>
<td>3E0 to 3EF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2F0 to 2FF COM2</td>
<td>3F0 to 3FF Floppy-disk controller; COM1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Base Memory Address**

The base memory address identifies a location in a computer's memory (RAM). This location is used by the network adapter card as a buffer area to store the incoming and outgoing data frames. This setting is sometimes called the RAM start address.

Often, the base memory address for a network adapter card is D8000. (For some network adapter cards, the final "0" is dropped from the base memory address for example, D8000 would become D800.) It is necessary to select a base memory address that is not already being used by another device.

**Note:** Some network adapter cards do not have a setting for the base memory address because they do not use any system RAM addresses.

Some network adapter cards contain a setting that allows you to specify the amount of memory to be set aside for storing data frames. For example, for some cards you can specify either 16K or 32K of memory. Specifying more memory provides better network performance but leaves less memory available for other uses.

**Selecting the Transceiver**

The network adapter card may have other settings that need to be defined during configuration. For example, some cards come with an external and an on-board transceiver. In this case, you would have to determine which transceiver you want to use and then make the appropriate choice on your card.

The choice on the card is usually done with jumpers. Jumpers are small connectors that tie two pins together to determine which circuits the card will use.
Figure 2.27: Network adapter card showing external and on-board transceivers

**Q & A**

Fill in the blanks in the following sentences.

1. In an 80386 computer, COM1 typically uses IRQ _____ and LPT1 typically uses IRQ _____.
2. IRQ lines are assigned different levels of ______________ so that the CPU can determine how important the request is.
3. The recommended setting for a network adapter card is IRQ _____.
4. Every device on the computer must use a _______________ IRQ line.
5. Each hardware device needs a default _________ __/_ ___ ______ number.
6. Choosing the appropriate transceiver on an adapter card that can use either an external or an on-board transceiver is usually done with ______________.

**Answers**

1. 4, 7
2. priority
3. 5
4. different or separate
5. base I/O port
6. jumpers

**Network Adapter Card Compatibility**

To ensure compatibility between the computer and the network, the network adapter card must:

- Fit with the computer's internal structure (data bus architecture).
- Have the right type of cable connector for the cabling.
A card that would work in an Apple computer communicating in a bus network, for example, would not work in an IBM computer in a ring environment. The ring requires cards that are physically different from those used in a bus, and Apple uses a different type of network communication method.

**Data Bus Architecture**

In the personal computer environment, there are four types of computer bus architectures: ISA, EISA, Micro Channel, and PCI. Each type of bus is physically different from the others. It is essential that the network adapter card and the bus match.

- **ISA (Industry Standard Architecture)**
  
  ISA is the architecture used in the IBM PC, XT and AT computers and all of their clones. It allows various adapters to be added to the system by means of inserting plug-in cards in expansion slots. ISA was expanded from an 8-bit path to a 16-bit path in 1984 when IBM introduced the IBM PC/AT. ISA refers to the expansion slot itself (an 8-bit slot or a 16-bit slot). The 8-bit slots are shorter than the 16-bit slots which actually consist of two slots, one behind the other. An 8-bit card could fit into a 16-bit slot, but a 16-bit card could not fit into an 8-bit slot.

  ISA was the standard personal computer architecture until Compaq and several other companies developed the EISA bus.

- **EISA (Extended Industry Standard Architecture)**

  This is the bus standard introduced in 1988 by a consortium of nine computer-industry companies: AST Research, Inc., Compaq, Epson, Hewlett-Packard, NEC, Olivetti, Tandy, Wyse Technology, and Zenith.

  EISA offers a 32-bit data path and maintains compatibility with ISA while providing for additional features introduced by IBM in its Micro Channel Architecture bus.

- **Micro Channel Architecture**

  IBM introduced this standard in 1988 as part of its PS/2 roll out. Micro Channel Architecture is electrically and physically incompatible with the ISA bus. Unlike the ISA bus, the Micro Channel functions as either a 16-bit or a 32-bit bus and can be driven independently by multiple bus master processors.

- **PCI (peripheral component interconnect)**

  This is a 32-bit local-bus used in most Pentium computers and in the Apple Power Macintosh. The current PCI bus architecture meets most of the requirements for providing Plug and Play functionality. Plug and Play is both a design philosophy and a set of personal computer architecture specifications. The goal of Plug and Play is to enable changes to a personal computer configuration with no intervention by the user. The installation of any device should be a simple, fail-safe operation. Microsoft Windows 95 is a Plug and Play-compliant operating system.
**Figure 2.28: ISA, EISA, Micro Channel, and PCI network adapter cards**

**Network Cabling and Connectors**

The network adapter card performs three important functions in coordinating activities between the computer and the cabling:

- Making the physical connection to the cable.
- Generating the electrical signals that travel over the cable.
- Following specific rules controlling access to the cable.

To select the appropriate card for your network, you need to determine the type of cabling and cabling connectors it will have.

Each type of cable has different physical characteristics which the network adapter card must accommodate. Therefore, each card is built to accept a particular type of cable such as coaxial, twisted-pair, or fiber-optic.

Some network adapter cards have more than one interface connector. For example, it is not uncommon for a network adapter card to have both a thinnet and thicknet connector, or a twisted-pair and a thicknet connector.

If a card has more than one interface connector, make a selection either by setting jumpers or DIP switches on the card itself, or by using a software-selectable option. Consult the network adapter card documentation for information on how to properly configure the card. Three examples of typical connectors found on network adapter cards follow.

A thinnet network connection uses a coaxial BNC connector as shown in Figure 2.29.
Figure 2.29: Thinnet network connection for a coaxial BNC connector

A thicknet network connection uses a 15-pin attachment unit interface (AUI) cable to connect the 15-pin (DB-15) connector on the back of the network adapter card to an external transceiver. As you may recall from Lesson 1, "Network Cablingthe Physical Media," the external transceiver uses a vampire tap to connect into the thicknet cable.

![Thinnet network connection for a coaxial BNC connector](image)

Figure 2.30: Thicknet network connection for a 15-pin AUI

**Caution**: Be careful not to confuse a joystick port with an AUI network adapter port. They both look alike. You will need to be familiar with the specific hardware configuration in order to know whether the connector is for a network adapter card or a joystick.

An unshielded twisted-pair connection uses an RJ-45 connector, as shown in Figure 2.31. The RJ-45 connector is similar to an RJ-11 telephone connector but is larger in size because it has eight conductors; an RJ-11 only has 4 conductors.

![RJ-45 connector](image)

Figure 2.31: RJ-45 connector

Some proprietary twisted-pair networking topologies use the RJ-11 connector. These topologies are sometimes referred to as pre-10BaseT. The RJ-11 connector is the same connector that is used on a telephone wire.

**Q & A**

Fill in the blanks for questions 1 through 4, and then identify the connectors illustrated for letters A through C.

1. ISA was the standard bus until Compaq and others developed the ______ bus.

2. The __________________________ bus functions as either a 16-bit or a 32-bit bus and can be driven independently by multiple bus master processors.

3. Telephone wire uses an _________ connector.
4. Plug and Play is both a design philosophy and a set of personal computer specifications.

**Answers**

1. EISA
2. Micro Channel
3. RJ-11
4. architecture

Identify the Ethernet media connector types:

1. Connector: ________________

2. Connector: ________________

3. Connector: ________________
Answers

1. BNC
2. AUI or DIX
3. RJ-45

Network Performance

Because of the effect it has on data transmission, the network adapter card has a great affect on the performance of the entire network. If the card is slow, data will not pass to and from the network quickly. On a bus network, where no one can use the network until the cable is clear, a slow card can increase wait times for all users.

After identifying the physical requirements of the card the type of connector it needs and the type of network in which it will be used it will be necessary to consider several other factors which affect the capabilities of the card.

Although all network adapter cards conform to certain minimum standards and specifications, some cards feature enhancements which greatly improve server, client, and network performance.

You can speed up the movement of data through the card with the following:

- Direct memory access (DMA)

  With this method, the computer moves data directly from the network adapter card's buffer to the computer's memory, without using the computer's microprocessor.

- Shared adapter memory

  In this method, the network adapter card contains RAM which it shares with the computer. The computer identifies this RAM as if it is actually installed in the computer.

- Shared system memory

  In this system, the network adapter card's processor selects a section of the computer's memory and uses it to process data.

- Bus mastering

  With bus mastering, the network adapter card takes temporary control of the computer's bus, by-passes the computer's CPU, and moves data directly to the computer's system memory. This speeds up computer operations by freeing the computer's processor to concentrate on other tasks. These cards are expensive, but they can improve network performance by 20 to 70 percent.

  Both EISA and Micro Channel Architecture network adapter cards offer bus mastering.

- RAM buffering

  Current network traffic travels at a speed which is often too fast for most network adapter cards. RAM chips on the network adapter card form a buffer. When the card receives more data than it can process immediately, the RAM buffer holds some of the data until the adapter card can process it.

  This speeds up the card's performance and keeps the card from becoming a bottleneck.
• Onboard microprocessor

With a microprocessor, the network adapter card does not need the computer to help process data. Most cards feature their own processors which speed network operations.

Servers

Because they handle such high volumes of network traffic, servers should be equipped with the highest-performance cards possible.

Workstations

Workstations can use less expensive cards if their main network activities are limited to applications that do not generate great volumes of network traffic, such as word processing. Other applications, such as databases or engineering applications, will quickly overwhelm inadequate network adapter cards.

Specialized Network Adapter Cards

Wireless Network Adapter Cards

There are wireless network adapter cards available that support the major network operating systems.

These cards often come with:

• Indoor omnidirectional antenna and antenna cable.
• Network software to make the adapter card work with a particular network.
• Diagnostic software for troubleshooting.
• Installation software.

These network adapter cards can be used to:

• Create an all wireless LAN.
• Add wireless stations to a cabled LAN.

Usually, these cards are used with a component called a wireless concentrator, which acts as a transceiver to send and receive signals.

Fiber Optic Network Adapter Cards

"Fiber to the desktop" has become a watch phrase for the computing industry. As transmission speeds increase to accommodate the "bandwidth" hungry applications and multi-media data streams, that are common on today's intranets, fiber optic network cards allow direct connections to the high speed fiber optic networks. These cards should be used in special cases only due to the high cost of these devices.

Remote-Boot PROMs

In some environments, security is such an important consideration that workstations do not have disk drives. Without disk drives, users are not able to copy information to either floppy or hard disks and, therefore, cannot take any data from the work site.

However, because computers normally start from either a floppy or hard disk, there has to be some other source for the software that initially starts the computer and connects it to a network. In
these environments, the network adapter card can be equipped with a special chip called a remote-boot PROM (programmable read-only memory) which contains the hardwired code that starts the computer and connects the user to the network.

With remote-boot PROMs diskless workstations can join the network when they start.

**Summary**

Network adapter cards are the interface between the computer and the network cable. The function of the network adapter card is to prepare, send, and control data on the network. To prepare data for the network, the card uses a transceiver to reformat data from parallel to serial transmission. Each card has its own unique address which allows it to be distinguished from all of the other cards on the network.

Network adapter cards have configurable options that must be set. These options include the interrupt (IRQ), the base I/O port address, and the base memory address.

To ensure compatibility between the computer and network, the network adapter card must fit the computer's data bus architecture and have the right type of cable connector for the cabling.

The network adapter card has a great affect on the performance of the entire network. There are several ways to enhance network performance with the network adapter card. Some cards have enhancements designed into them. These include direct memory access, shared adapter memory, shared system memory, and bus mastering. Performance can also be enhanced through RAM buffering and with the use of an on-board microprocessor.

There are also network adapter cards for specialized environments, such as wireless and fiber optic networks, and workstations without disk drives in high-security environments.

A check list for buying a network adapter card includes:

- Bus width (32-bit is faster than 16-bit)
- Bus type (PCI, EISA and Micro Channel are faster than ISA)
- Memory transfer (shared memory is faster than I/O or DMA)
- Bus mastering
- Vendor considerations (stability, reliability, experience, and so on)

**Activity**

Run Demo 6.

**Your Next Step**

With the completion of this lesson, you now know the fundamentals of network adapter cards. So far in the kit, you have been introduced to the basic network components and design concepts common to most LANs.

You are now ready to go on to the Chapter 2 Review and apply what you have learned.

**Chapter 2 Review**
In Chapter 2 you learned how computers are connected to form networks. You started with cabling and related components, then moved to wireless communications, and finally learned about network adapter cards.

In today's environment, cable connects most networks. Coaxial has traditionally been the cable of choice. However, UTP and fiber-optic cable are currently replacing coaxial in many installations.

Wireless networks are also gaining popularity as prices fall and the technology matures. Today, most wireless installations actually connect to a cabled LAN. Three popular wireless technologies are:

- Infrared
- Narrow-band radio
- Spread-spectrum radio

Network adapter cards act as the interface between the computer and both cable and wireless connections. There are options that must be set correctly if network adapter cards are to function properly. These options include the following:

- Interrupt (IRQ)
- Base I/O port address
- Base memory address
- Transceiver selection

Some network adapter cards have features designed into them that can enhance network performance, such as direct memory access and shared system memory.

Checkup

Follow the instructions for each exercise as indicated. The answers for all of the exercises are after the last exercise.

Note: To get the most out of the Checkup exercises, you may want to cover the answers with a piece of paper until you have answered the questions. If your answer differs from the one in the book, you should review the appropriate text.

Exercise 1: Matching

Match each item in the Column A with the best choice from Column B. One item in Column B will not be used, and items will be used no more than once.

<table>
<thead>
<tr>
<th>Column A</th>
<th>Column B</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Fiber-optic ____</td>
<td>A. Requires direct line-of-sight.</td>
</tr>
<tr>
<td>2. STP ____</td>
<td>B. The short space in buildings between the false ceiling and the floor above it.</td>
</tr>
<tr>
<td>3. Thinnet ____</td>
<td>C. Supports voice, data, and video.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4. Scatter infrared</td>
<td>D. Typically used as the backbone in a large Ethernet network.</td>
</tr>
<tr>
<td>5. Laser</td>
<td>E. Typically uses RJ-45 connectors.</td>
</tr>
<tr>
<td>6. Plenum</td>
<td>F. Signals bounce off walls and ceilings.</td>
</tr>
<tr>
<td>7. Thicknet</td>
<td>G. RG-58 family of cables that carries signal up to 185 meters.</td>
</tr>
<tr>
<td>9. COM1</td>
<td>I. Typically uses IRQ 4.</td>
</tr>
<tr>
<td></td>
<td>J. Typically uses IRQ 5.</td>
</tr>
<tr>
<td></td>
<td>K. Typically uses IRQ 7.</td>
</tr>
</tbody>
</table>

**Exercise 2: True or False**

For the following sentences, circle True if the statement is true or False if the statement is false.

1. Because thinnet is lighter and more flexible than thicknet, it can carry data farther, faster.  
   True False

2. The maximum distance for UTP (10BaseT) is about 100 meters (328 feet). True False

3. Data often moves faster in a network adapter card than it does in the computer. True False

4. Devices use the IRQ lines to send interrupts or requests for service to the computer's microprocessor. True False

5. A Micro Channel adapter can be used in an EISA slot. True False

6. Thicknet networks require an 8-pin RJ-11 plug to connect to a network adapter card. True False

**Exercise 3: Open-Ended**

Supply the items for the lists below.

1. List three of the configuration options for a network adapter card.
   a. ____________________________
   b. ____________________________
   c. ____________________________

2. List three types of enhancements to network adapter cards that can improve network performance.
a. ________________________________
b. ________________________________
c. ________________________________

Checkup Answers

Exercise 1: Matching

1. C
2. E
3. G
4. F
5. A
6. B
7. D
8. K
9. I

Exercise 2: True or False

1. False. Thick copper wire, with less resistance because of its diameter, carries more data farther, faster than thin wire.
2. True.
3. False. The opposite is true. Data moves from the computer to the adapter card faster than the card can handle it. This is why better cards are sold with on-board RAM, to act as a buffer for the incoming data until the card can take care of it.
4. True.
5. False. They are physically different and cannot be compatible. Network adapter cards are made specifically for one bus or the other.

Exercise 3: Open-Ended

1. List three of the configuration options for a network adapter card. (Four were discussed; any three of the following would be fine.)
   a. IRQ (Interrupt)
   b. Base I/O port address
   c. Base memory address
   d. Transceiver setting

2. List three types of enhancements to network adapter cards that can improve network performance.
a. Direct memory address (DMA)
b. Shared adapter memory
c. Shared system memory
d. Bus mastering
e. RAM buffering

Case Study Problem

The Setting

You have been asked to review the proposals submitted by a consulting firm for the cabling scheme for your company's new office building.

<table>
<thead>
<tr>
<th>Location</th>
<th>Distance</th>
<th>Location</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A to B</td>
<td>50 feet</td>
<td>Hub to A</td>
<td>500 feet</td>
</tr>
<tr>
<td>B to C</td>
<td>50 feet</td>
<td>Hub to B</td>
<td>525 feet</td>
</tr>
<tr>
<td>C to D</td>
<td>50 feet</td>
<td>Hub to C</td>
<td>550 feet</td>
</tr>
<tr>
<td>D to E</td>
<td>200 feet</td>
<td>Hub to D</td>
<td>575 feet</td>
</tr>
<tr>
<td>E to F</td>
<td>75 feet</td>
<td>Hub to E</td>
<td>500 feet</td>
</tr>
<tr>
<td>F to G</td>
<td>75 feet</td>
<td>Hub to F</td>
<td>425 feet</td>
</tr>
<tr>
<td>G to H</td>
<td>75 feet</td>
<td>Hub to G</td>
<td>350 feet</td>
</tr>
<tr>
<td>H to I</td>
<td>75 feet</td>
<td>Hub to H</td>
<td>300 feet</td>
</tr>
<tr>
<td>I to J</td>
<td>200 feet</td>
<td>Hub to I</td>
<td>275 feet</td>
</tr>
<tr>
<td>J to K</td>
<td>50 feet</td>
<td>Hub to J</td>
<td>350 feet</td>
</tr>
<tr>
<td>K to L</td>
<td>50 feet</td>
<td>Hub to K</td>
<td>325 feet</td>
</tr>
<tr>
<td>L to M</td>
<td>50 feet</td>
<td>Hub to L</td>
<td>275 feet</td>
</tr>
<tr>
<td>A to M</td>
<td>725 feet</td>
<td>Hub to M</td>
<td>225 feet</td>
</tr>
</tbody>
</table>
The Problem

The consulting firm has recommended that you implement 10BaseT Category 5 UTP wire for your company’s network.

Your Solution

1. Where does this recommendation violate the UTP and 10BaseT specifications?

2. What type of cabling might you recommend instead?

Suggested Solution

1. The distances for A, B, C, D, E, F, and G to the hub all exceed the maximum cable length of 328 feet specified by 10BaseT. Therefore this solution would not work.

2. You could use thinnet with a multiport repeater where the hub is in the picture. All of the cable lengths from the hub to individual computers are less than 185 meters, or 607 feet.

You could also use a star wired fiber-optic network for this situation, but it would cost significantly more than the coaxial solution.

The Troubleshooter

Listed below are questions you need to ask regarding cabling and network adapter cards when troubleshooting a variety of network problems. Use them to help you troubleshoot the problem which follows.
**Two Important Troubleshooting Questions**

The first troubleshooting question should always be: "Did the thing ever work correctly?"

Yes ____
No ____

The next question should be, "What has changed since then?"

---

**Cabling**

Most network engineers have learned to check cabling first because experience has taught them that the majority of network problems can be found in the cabling.

Is the cabling connected properly?

Yes ____
No ____

Is the cable broken or frayed?

Yes ____
No ____

Is the cable too long?

Yes ____
No ____

Does the cable conform to the specifications of the network adapters?

Yes ____
No ____

Is the cable crimped or bent too sharply?

Yes ____
No ____

Does the network cable run near a source of interference such as an air conditioner, transformer, or large electric motor?

Yes ____
No ____

Is the cabling terminated properly?

Yes ____
No ____
**Adapter Cards**

The most common network adapter problems are interrupt conflicts and transceiver settings. The following questions will help you determine if the network adapter card is the source of your problem.

Do the settings on the card match the settings in the network software you are using?

Yes ____  
No ____  

Is there an I/O address conflict between the network adapter card and another card installed in the computer?

Yes ____  
No ____  

Is there an interrupt conflict between the network adapter card and another card installed in the computer?

Yes ____  
No ____  

Is there a memory conflict between the network adapter card and another card installed in the computer?

Yes ____  
No ____  

Is the cable plugged into the correct interface (AUI, BNC, or RJ-45)?

Yes ____  
No ____  

Is the network adapter card set to the speed setting that your network is using?

Yes ____  
No ____  

Are you using the correct type of network card for your network? (That is, are you trying to use a Token Ring card in an Ethernet network?)

Yes ____  
No ____  

If you are using more than one network adapter card in the computer, do their settings conflict?

Yes ____  
No ____  

**Can You Solve This Problem?**
Refer back to the questions to arrive at possible causes of the problem situation described below. Remember, there could be several causes and solutions.

The Situation

You have a 20-user, thinnet, coaxial bus network which has been in use for about a year. Three new client computers are going to be added to the network.

The Available Facts

Your vendor was in over the weekend adding the new computers, and when you came in Monday morning, nobody could access the server.

Your Solution

Cause of the Problem

List two things which could cause the network not to function.

1. __________________________

2. __________________________

Possible Solution

What could you do to resolve each of the two possible causes you listed above?

________________________________________________________

________________________________________________________

________________________________________________________

Impact of Your Solution on Network Users

What will be the impact of each of your solutions on network users (assuming that they repair the problem)?

________________________________________________________

________________________________________________________

________________________________________________________

Suggested Solution

Cause of the Problem

The answers you have written down might not be listed, but they could still be correct. This list is not exhaustive, it just lists some of the causes of the problem.

1. The network cable might not be correctly connected, that is, it might have a break in it caused by adding the new computers.

2. The new cable added to service the new computers might not be the correct type for your network.
3. The new cable added to your network might have a short in it.

4. The existing network cabling might have been damaged by rough handling during the installation of the new computers.

5. The addition of the new cable needed for the new computers might have made your total network cable length exceed the maximums specified for the type of network you have.

6. The bus network might be missing a terminator. It might have been removed or fallen off by accident during the installation of the new computers.

Possible Solution

What could you do to resolve the each of the two possible causes you listed above?

1. Find and repair the break or disconnection in the cable.

2. Check the cable type of the existing cable and make sure the new cables are of the same type. If they are different replace the new cables with cables of the correct type. For example, the original cable might be RG-58A/U and the new cables might be RG-62 /U. These two cable types are not compatible.

3. Test the new cables with an ohmmeter to see if they are shorted.

4. Check all of the cables in the new installation for shorts, frayed cables, breaks, and so on.

5. If the maximum coaxial cable length (185 meters) has been exceeded, you might have to add a repeater to your network so that you will have two network cable segments which are within specifications.

Impact of Your Solution on Network Users

What will be the impact of each of your solutions on network users (assuming that they repair the problem)?

The impact for each of the solutions listed above is very positive. Before the repair, the network did not function, and afterwards, it works.

With new users on the network, monitor the network's performance to ensure that it is not suffering from degradation.

The LAN Planner

Note: This LAN Planner is only concerned with networking subjects presented in this unit. Appendix B, "Network Planning and Implementation," summarizes information from all of the LAN Planners in the kit to take you step-by-step through the complete LAN planning process. Therefore, the information you contribute here will be used in the last lesson as part of a complete LAN plan specifically for your site.

Choosing Your Networking Media

Research has shown that about 90 percent of all new network installations are using UTP cable in a star bus topology. Because most of the cost of cable installation is labor, there is often little cost difference between using Category 3 UTP cable and Category 5 UTP cable. Most new installations use Category 5 because it supports transmission speeds of up to 100 Mbps. Category 5 allows you to install a 10 Mbps solution now, and upgrade it later to a 100 Mbps solution.

However, UTP cable may not be suitable for all networking situations.
Each of the following sections will ask you several questions about your network cable needs. If you answer yes to most of the questions in a section, then that type of cable is probably the correct cable type to choose for your network.

**Note:** UTP is currently the most popular cabling. Unless there is a compelling reason to use another type, UTP should be your first consideration.

Put a check mark on the line next to the choice which applies to your site. To determine which type of cabling would be most appropriate for your site, simply total the number of each type of cable indicator (UTP, coaxial, STP, fiber-optic). The indicator with the highest score is the candidate unless there is a specific requirement for particular type of cable such as fiber-optic (distance and security). In cases where more than one type of cable is indicated, choose UTP where possible.

**Unshielded Twisted-Pair**

Is ease of troubleshooting and long-term maintenance costs important?

Yes ___ UTP cable  
No ___ Any of the discussed cable types

Are most of your computers within 100 meters of your wiring closet?

Yes ___ UTP cable  
No ___ Coaxial or fiber-optic cable

Is ease of reconfiguration important?

Yes ___ UTP cable  
No ___ Any of the discussed cable types

Does any of your staff have experience with UTP cable?

Yes ___ UTP cable  
No ___ UTP, depends on other factors

**Note:** Even if no one has experience with UTP, someone may have transferable experience with another type of cable such as coaxial, STP, or even fiber-optic.

**Shielded Twisted-Pair**

Does your network have any existing STP cabling?

Yes ___ STP cable  
No ___ Any of the discussed cable types

Does the topology or network card you want to use require the use of STP cable?

Yes ___ STP  
No ___ Depends on other factors

Do you have a need for cable which is more resistant to EMI (interference) than UTP?

Yes ___ STP, coaxial, or fiber-optic cable  
No ___ Depends on other factors, UTP cable
Coaxial

Do you have existing coaxial cabling in your network?
Yes ____ Coaxial cable
No ____ Any of the discussed cable types

Is your network very small (less than ten computers)?
Yes ____ Coaxial cable (bus), UTP cable
No ____ Any of the discussed cable types, depends on other factors

Is your network going to be installed in an open area using cubicles to separate work areas?
Yes ____ Coaxial, or UTP cable
No ____ Depends on other factors

Do you have a need for cable which is more resistant to EMI than UTP?
Yes ____ Coaxial, fiber-optic, or STP cable
No ____ Depends on other factors, UTP cable

Fiber-Optic

Note: Some situations require fiber-optic cable. This is especially true where other types of cable will not meet specific distance or security requirements. In such cases, fiber is the only type of cable that can be considered regardless of what the questions in the other areas indicate. In the questions below, "Any" means that UTP can be considered, depending on your other site considerations.

Do you have a need for network cabling which is immune to electromagnetic interference (EMI)?
Yes ____ Fiber-optic cable
No ____ Any of the discussed cable types, depends on other factors

Do you have a need for network cabling which is relatively secure from most eavesdropping or corporate intelligence gathering equipment?
Yes ____ Fiber-optic cable
No ____ Any of the discussed cable types, depends on other factors

Do you have a need for network transmission speeds which are higher than those supported by copper media?
Yes ____ Fiber-optic cable
No ____ Any of the discussed cable types, depends on other factors

Do you have a need for longer cabling distances than those supported by copper media?
Yes ____ Fiber-optic cable
No ____ Any of the discussed cable types, depends on other factors
Do you have a budget that can absorb the costs of implementing fiber?
Yes ____ Fiber-optic or any of the discussed cable types, depends on other factors
No ____ Any of the discussed cable types, depends on other factors

**Wireless Network Communications**

**Note:** In the questions below, wireless, like fiber-optic, may be the only option in some cases regardless of what the questions in the other areas indicate. Keep in mind that wireless can also be used in combination with a cabled network.

Do users on your network need to physically move their computers in the course of their work day?
Yes ____ Wireless, depends on other factors
No ____ Any of the discussed cable types, depends on other factors

Are there limitations which make it very difficult or impossible to cable computers to the network?
Yes ____ Wireless
No ____ Any of the discussed cable types, depends on other factors

Does your network have unique needs which are best fulfilled by one or more of the features of current wireless technology, such as computer mobility, or the ability to have a network in a building in which it is very difficult or impossible to install cable?
Yes ____ Wireless
No ____ Any of the discussed cable types, depends on other factors

**Choosing Your Network Adapter Card**

There are dozens of manufacturers making each type of network adapter card, and each card has slightly different features, such as setup (using jumpers and switches, or on newer cards using a software setup program or Plug-and-Play, PnP), bus type, and so on. You should do some research to determine which card is best for you because the industry is constantly changing and updating. The best card this month might be superseded by another manufacturer's card next month.

If you can answer yes to each of the following questions, then the card you have chosen will probably work in your environment.

**Note:** These questions are not designed to promote a particular card, but, rather, to ensure that the card you choose is compatible with the rest of your network.

Are there drivers available for the card that will work with the operating system you are using?
Yes ____
No ____

Is the card compatible with the cable type and topology you have chosen?
Yes ____
No ____

Is the card compatible with the bus type of the computer into which it will be installed?
Yes ____

No ____

The LAN Planner Summary

**Note:** This information will be taken into account in the final lesson.

Based on the information generated in the LAN Planner, your network components should be:

Cable: __________________________________________

Top Of Page

**Links Table**

Community Content

© 2012 Microsoft. All rights reserved.