

1

CHAPTER

INTRODUCTION TO COMPUTER NETWORKS

Chapter Outline

1-1 Introduction
1-2 Network Topologies
1-3 The OSI Model
1-4 The Ethernet LAN
1-5 Home Networking

1-6 Assembling an Office LAN
1-7 Testing and Troubleshooting a LAN
Summary
Questions and Problems

Objectives

- Explain the various LAN topologies
- Define the function of a networking protocol
- Describe CSMA/CD for the Ethernet protocol
- Describe the structure of the Ethernet frame
- Define the function of the network interface card
- Describe the purpose of the MAC address on a networking device
- Discuss how to determine the MAC address for a computer
- Discuss the fundamentals of IP addressing
- Discuss the issues of configuring a home network
- Discuss the issue of assembling an office LAN

Key Terms

local area network (LAN)
protocol
topology
Token Ring topology
token passing
IEEE
deterministic
Token Ring hub
bus topology
ThinNet
star topology
hub
multiport repeater
broadcast
switch
ports
mesh topology
OSI
OSI model
physical layer
data link layer

network layer
transport layer
session layer
presentation layer
application layer
CSMA/CD
frame
network interface card (NIC)
MAC address
organizationally unique identifier (OUI)
Ethernet, physical, hardware, or adapter address
ipconfig /all
IANA
IP address
network number
host number
host address
ISP

private addresses
intranet
IP internetwork
TCP/IP
wired network
wireless network
Wi-Fi
wireless router
range extender
hotspots
Service Set Identifier (SSID)
firewall protection
Stateful Packet Inspection (SPI)
virtual private network (VPN)
Network Address Translation (NAT)
overloading

Port Address Translation
(PAT)
CAT6 (category 6)
RJ-45
Mbps
numerics

ports
crossover
straight-through
uplink port
link light
link integrity test

link pulses
ping
Internet Control Message
Protocol (ICMP)
ipconfig

1-1 INTRODUCTION

Each day, computer users use their computers for browsing the Internet, sending and retrieving email, scheduling meetings, sharing files, preparing reports, exchanging images, downloading music, and maybe checking the current price of an auction item on the Internet. All this requires computers to access multiple networks and share their resources. The multiple networks required to accomplish this are the local area network (LAN), the enterprise network, the campus area network (CAN), the metropolitan area network (MAN), Metro Ethernet, the personal area network (PAN), and the wide area network (WAN).

This text introduces the essentials for implementing modern computer networks. Each chapter steps you through the various modern networking technologies. The accompanying CD-ROM comes with the Net-Challenge simulator software developed specifically for this text. This software provides the reader with invaluable insight into the inner workings of computer networking and with the experience of configuring the router and switch for use in the computer networks.

The ease of connecting to the Internet and the dramatic decrease in computer systems' cost has led to an explosion in their usage. Organizations such as corporations, colleges, and government agencies have acquired large numbers of single-user computer systems. These systems might be dedicated to word processing, scientific computation, process control, or might be general-purpose computers that perform many tasks. This has generated a need to interconnect these locally distributed computer networks. Interconnection allows users to exchange information (data) with other network members. It also allows resource sharing of expensive equipment such as file servers and high-quality graphics printers or access to more powerful computers for tasks too complicated for the local computer to process. The network commonly used to accomplish this interconnection is called a **local area network (LAN)**, which is a network of users that share computer resources in a limited area.

Table 1-1 outlines the CompTIA Network+ objectives and identifies the chapter section that covers each objective. At the end of each chapter section you will find a review with comments of the Network+ objectives presented in that section. These comments are provided to help reinforce the reader's understanding of a particular Network+ objective. The chapter review also includes "Test Your Knowledge" questions to aid in the understanding of key concepts before the reader advances to the next section of the chapter. The end of the chapter includes a complete set of questions as well as sample certification type questions.

Local Area Network (LAN)

Network of users that share computer resources in a limited area

TABLE 1-1 Chapter 1 CompTIA Network+ Objectives

Domain/ Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	<i>Networking Architecture</i>	
1.1	Explain the functions and applications of various network devices	1-5
1.2	Compare and contrast the use of networking services and applications	1-5
1.3	Install and configure the following networking services/applications	1-5
1.4	Explain the characteristics and benefits of various WAN technologies	1-1
1.5	Install and properly terminate various cable types and connectors using appropriate tools	1-6
1.6	Differentiate between common network topologies	1-2
1.7	Differentiate between network infrastructure implementations	1-1, 1-5, 1-6
1.8	Given a scenario, implement and configure the appropriate networking addressing schema	1-4, 1-5
1.12	Given a set of requirements, implement a basic network	1-1, 1-2
2.0	<i>Network Operations</i>	
2.4	Explain the importance of implementing network segmentation	1-5
2.6	Given a scenario, configure a switch using proper features	1-4, 1-5
2.7	Install and configure a wireless LAN infrastructure and implement the appropriate technologies in support of wireless-capable devices	1-5
3.0	<i>Network Media and Topologies</i>	
3.2	Compare and contrast network vulnerabilities and threats	1-5
3.3	Given a scenario, implement network-hardening techniques	1,4 1-5
4.0	<i>Troubleshooting</i>	
4.1	Given a scenario, implement the following network troubleshooting methodology	1-3, 1-5, 1-7
4.2	Given a scenario, analyze and interpret the output of troubleshooting tools	1-4, 1-7

Domain/ Objective Number	Domain/Objective Description	Section Where Objective Is Covered
5.0	<i>Industry Standards, Practices, and Network Theory</i>	
5.1	Analyze a scenario and determine the corresponding OSI layers	1-3
5.2	Explain the basics of network theory and concepts	1-4
5.3	Given a scenario, deploy the appropriate wireless standard	1-5
5.4	Given a scenario, deploy the appropriate wired connectivity standard	1-5, 1-6
5.8	Explain the basics of change management procedures	1-6
5.9	Compare and contrast the following ports and protocols	1-3

1-2 NETWORK TOPOLOGIES

The networking topologies commonly used in computer networks are presented in this chapter. It is important that the student understand the structure of the star topology. The students should also have an understanding of Token Ring and bus topologies even though these are seldom used anymore.

Local area networks are defined in terms of the **protocol** and the **topology** used for accessing the network. The networking protocol is the set of rules established for users to exchange information. The topology is the network architecture used to interconnect the networking equipment. The most common architectures for LANs are the ring, bus, and star, as illustrated in Figure 1-1.

Figure 1-2 shows an example of a LAN configured using the **Token Ring topology**. In this topology, a “token” (shown as a T) is placed in the data channel and circulates around the ring, hence the name *Token Ring*. If a user wants to transmit, the computer waits until it has control of the token. This technique is called **token passing** and is based on the **IEEE 802.5** Token-Ring Network standard. A Token Ring network is a **deterministic** network, meaning each station connected to the network is ensured access for transmission of its messages at regular or fixed time intervals.

Protocol

Set of rules established for users to exchange information

Topology

Architecture of a network

Token Ring Topology

A network topology configured in a logical ring that complements the token passing protocol

Token Passing

A technique where an electrical token circulates around a network—control of the token enables the user to gain access to the network

IEEE

Institute of Electrical and Electronics Engineers, one of the major standards-setting bodies for technological development

Deterministic

Access to the network is provided at fixed time intervals

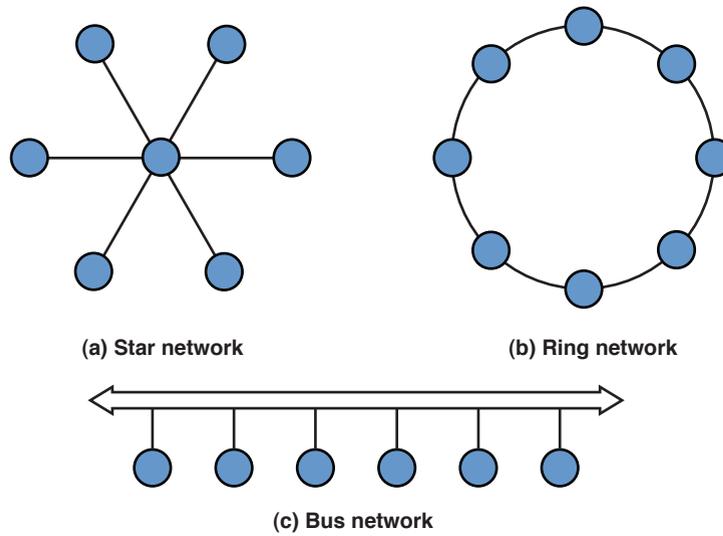


FIGURE 1-1 Network topologies. (From Modern Electronic Communication 9/e, by G. M. Miller & J. S. Beasley, 2008 Copyright © 2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

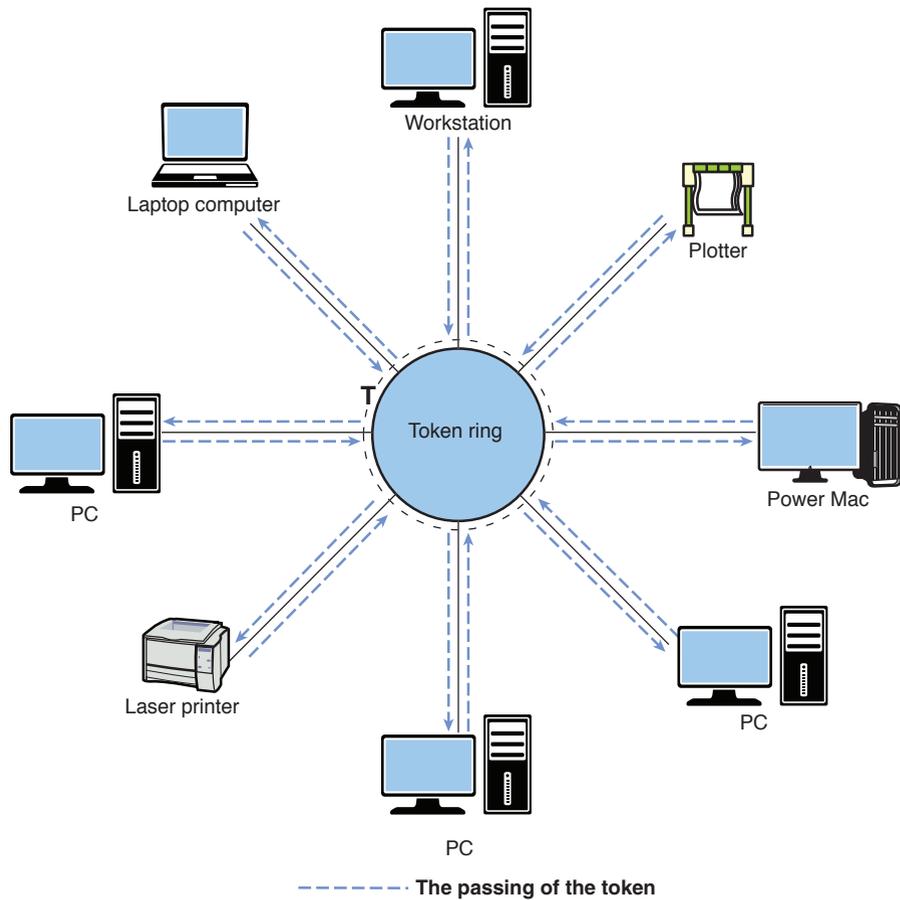


FIGURE 1-2 The Token Ring network topology.

One disadvantage of the Token Ring system is that if an error changes the token pattern, it can cause the token to stop circulating. Additionally, ring networks rely on each system to relay the data to the next user. A failed station can cause data traffic to cease. Another disadvantage of the Token Ring network is from the troubleshooting and maintenance point of view. The Token Ring path must be temporarily broken (path interrupted) if a computer or any device connected to the network is to be removed or added to the network. This results in downtime for the network. A fix to this is to attach all the computers to a central **Token Ring hub**. Such a device manages the passing of the token rather than relying on individual computers to pass it, which improves the reliability of the network. It is important to note that the Token Ring network has become a “legacy” now in computer networking. Ethernet technology has replaced this in almost all modern computer networks.

Token Ring Hub

A hub that manages the passing of the token in a Token Ring network

Figure 1-3 illustrates a **bus topology**. In a bus system, the computers share the media (coaxial cable) for data transmission. In this topology, a coaxial cable (called **ThinNet**) is looped through each networking device to facilitate data transfer.

Bus Topology

The computers share the media (coaxial cable) for data transmission

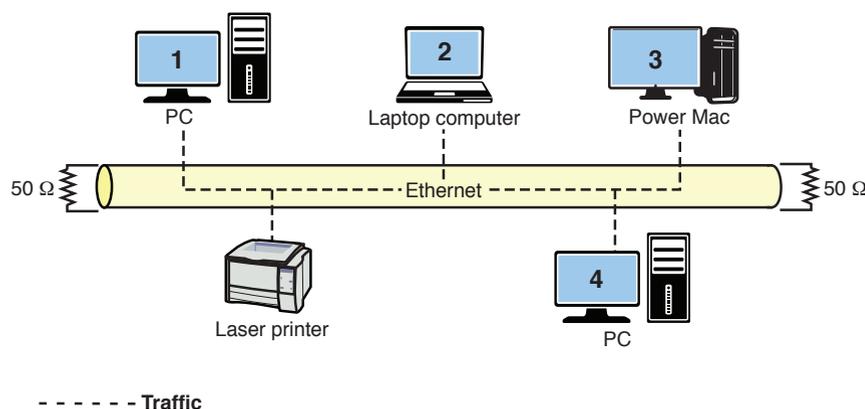


FIGURE 1-3 The bus topology.

In a bus topology, all LAN data traffic is carried over a common coaxial cable link. Referring to Figure 1-3, if computer 1 is printing a large file, the line of communications will be between computer 1 and the printer. However, in a bus system, all networking devices will see computer 1’s data traffic to the printer and the other devices will have to wait for pauses in transmission or until it is complete before they can initiate their own transmission. If more than one computer’s data is placed on the network at the same time, the data will be corrupted and will have to be retransmitted. This means that the use of a shared coaxial cable in a bus topology prevents data transmission from being very bandwidth-efficient. This is one reason, but not the only reason, why bus topologies are seldom used in modern computer networks.

Star Topology

The most common networking topology in today’s LANs where all networking devices connect to a central switch or hub

The **star topology**, shown in Figure 1-4, is the most common networking topology in today’s LANs. Twisted-pair cables (see Chapter 2, “Physical Layer Cabling: Twisted Pair”) with modular plugs are used to connect the computers and other networking devices. At the center of a star network is either a switch or a hub. This connects the network devices and facilitates the transfer of data. For example,

Hub

Broadcasts the data it receives to all devices connected to its ports

Multipoint Repeater

Another name for a hub

Broadcast

Transmission of data by a hub to all devices connected to its ports

if computer 1 wants to send data to the network laser printer, the **hub** or switch provides the network connection. If a hub is used, computer 1's data is sent to the hub, which then forwards it to the printer. However, a hub is a **multipoint repeater**, meaning the data it receives is **broadcast** and seen by all devices connected to its ports. Therefore, the hub will broadcast computer 1's data traffic to all networking devices interconnected in the star network. The data traffic path for this is shown in the solid black arrowed lines going to all networking devices in Figure 1-4. This is similar to the bus topology in that all data traffic on the LAN is being seen by all computers. The fact that the hub broadcasts all data traffic to the devices connected to its network ports makes these devices of limited use in large networks.

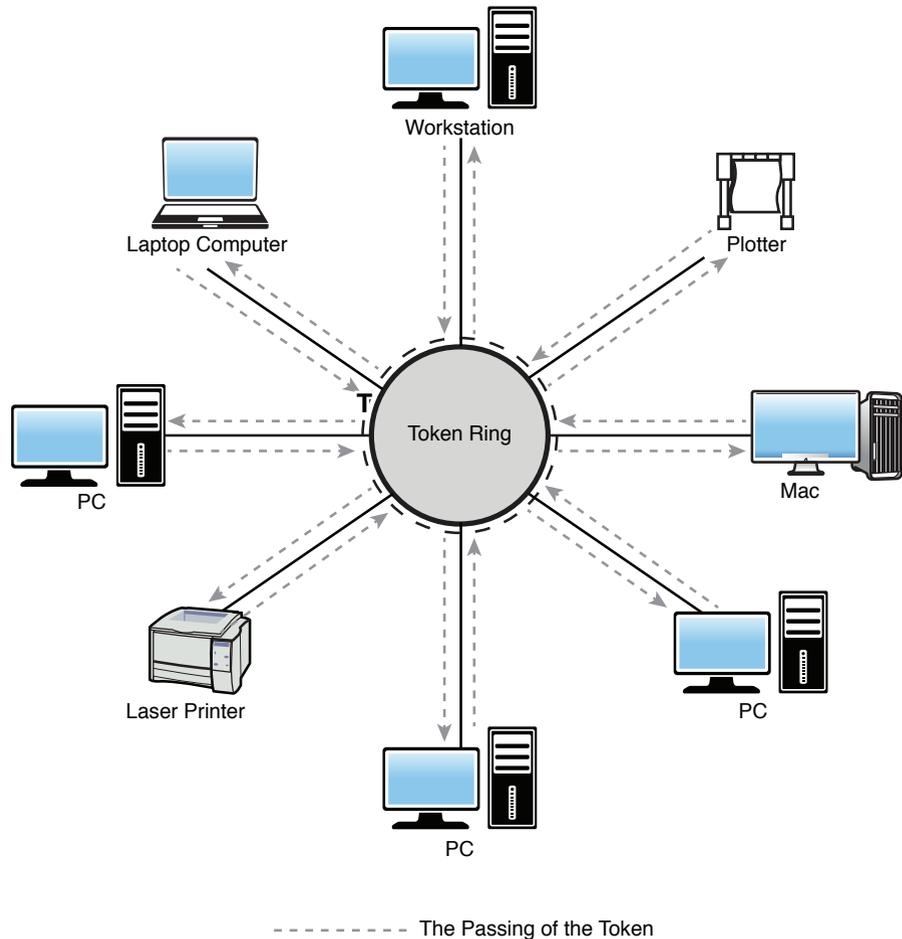


FIGURE 1-4 The star topology.

Switch

Forwards a frame it receives directly out the port associated with its destination address

To minimize unnecessary data traffic and isolate sections of the network, a **switch** can be used at the center of a star network, as shown in Figure 1-4. Networking devices such as computers each has a hardware or physical address. (This concept is fully detailed in section 1-4.) A switch stores the hardware or physical address for each device connected to its ports. The storage of the address enables the switch

to directly connect two communicating devices without broadcasting the data to all devices connected to its **ports**.

For example, if a switch is used instead of a hub, the data from computer 1 is transmitted directly to the printer and the other computers do not see the data traffic. The traffic path for the switched network is shown in the dotted lines in Figure 1-4. The use of a switched connection greatly improves the efficiency of the available bandwidth. It also permits additional devices in the LAN to simultaneously communicate with each other without tying up network resources. For example, while computer 1 is printing a large file, computers 5 and 6 can communicate with each other, as shown in the dashed line in Figure 1-4. For troubleshooting and maintenance, individual computers can be removed without negatively affecting the network in a star or extended star topology. Also the upgrade from a hub to a switched topology can be accomplished without requiring a change in the cable infrastructure and therefore at minimal downtime and expense.

Another topology is the **mesh topology**, shown in Figure 1-5. In this topology, all networking devices are directly connected to each other. This provides for full redundancy in the network data paths but at a cost. The additional data paths increase the cabling costs and the networking hardware cost (for example, expense of multiple network ports for each device connected to the network). Not only that, but the mesh design adds more complexity. This topology can be suitable for high-reliability applications but can be too costly for general networking applications.

Ports

The physical input/output interfaces to the networking hardware

Mesh Topology

All networking devices are directly connected to each other

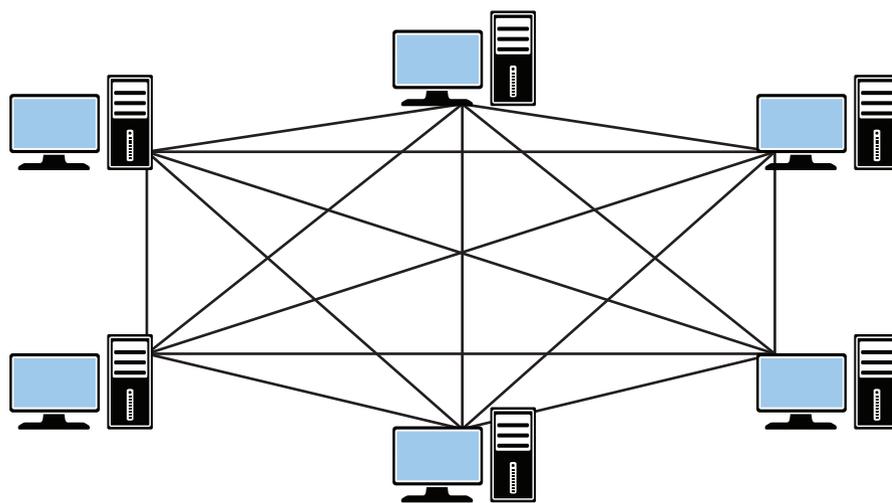


FIGURE 1-5 The mesh topology.

Section 1-2 Review

This section has covered the following **Network+** Exam objectives.

1.6 Differentiate between common network topologies

This section presented the star, ring, bus, and mesh network topologies. You should be able to identify each topology and understand how data travels in each network topology. You should also have a basic understanding of the difference between a topology and protocol.

1.12 Given a set of requirements, implement a basic network

This section also introduced some basic networking hardware, such as the hub and switch. Make sure you have a basic understanding of each device. You should also have developed an understanding that data from a hub is replicated out all ports. This means that the information is seen by all networking devices connected to its ports. You should also know that a switch will filter unicast frames out of the appropriate ports, unlike a hub.

Test Your Knowledge

1. What is the most common network topology today?
 - a. Star
 - b. Hub
 - c. Ring
 - d. Mesh
2. A hub is also called a multiport repeater.
 - a. True
 - b. False
3. The term deterministic means
 - a. Access to the network is provided at random time intervals.
 - b. Access to the network is provided using CSMA/CD.
 - c. Access to the network is provided at fixed time intervals.
 - d. None of these answers is correct.
4. A protocol defines the network architecture used to interconnect the networking equipment.
 - a. True
 - b. False

1-3 THE OSI MODEL

The sections examines the seven layers of the OSI model. The student should memorize all seven layers and know the function of each layer. The student should refer to Table 1-1 for a summary of the OSI layers and a short description of the function.

An open systems interconnect (OSI) reference model was developed by the International Organization for Standardization in 1984 to enable different types of networks to be linked together. The model contains seven layers, as shown in Figure 1-6. These layers describe networking functions from the physical network interface to the software applications interfaces. The intent of the OSI model is to provide a framework for networking that ensures compatibility in the network hardware and software and to accelerate the development of new networking technologies. A discussion of the OSI model follows as well as a summary of the seven layers outlined in Table 1-2.

OSI
Open system interconnect

OSI Model
The seven layers describing network functions

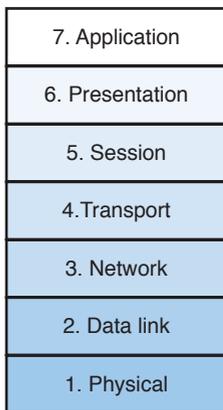


FIGURE 1-6 The seven layers of the OSI reference model.

TABLE 1-2 Summary of the OSI Layers

Layer	Function	Examples
7. Application	Support for applications	HTTP, FTP, SMTP (email)
6. Presentation	Protocol conversion, data translation	ASCII, JPEG
5. Session	Establishes, manages, and terminates sessions	NFS, SQL
4. Transport	Ensures error-free packets	TCP, UDP
3. Network	Provides routing decisions	IP, IPX
2. Data link	Provides for the flow of data	MAC addresses
1. Physical	Signals and media	NICs, twisted-pair cable, fiber

Physical Layer

Provides the electrical and mechanical connection to the network

Data Link Layer

Handles error recovery, flow control (synchronization), and sequencing

Network Layer

Accepts outgoing messages and combines messages or segments into packets, adding a header that includes routing information

Transport Layer

Is concerned with message integrity between source and destination

Session Layer

Provides the control functions necessary to establish, manage, and terminate the connections

Presentation Layer

Accepts and structures the messages for the application

Application Layer

Interacts with application programs that incorporate a communication component such as your Internet browser and email

1. **Physical layer:** Provides the electrical and mechanical connection to the network. Examples of technologies working in this layer are Electronic Industries Alliance/Telecommunications Industry Association (EIA/TIA) related technologies, UTP, fiber, and network interface cards (NICs).
2. **Data link layer:** Handles error recovery, flow control (synchronization), and sequencing (which terminals are sending and which are receiving). It is considered the “media access control layer” and is where Media Access Control (MAC) addressing is defined. The Ethernet 802.3 standard is defined in this area, which is why the MAC address is sometimes called the Ethernet address.
3. **Network layer:** Accepts outgoing messages and combines messages or segments into packets, adding a header that includes routing information. It acts as the network controller. Examples of protocols working in this layer are Internet Protocol (IP) and Internetwork Packet Exchange (IPX).
4. **Transport layer:** Is concerned with message integrity between source and destination. It also segments/reassembles (the packets) and handles flow control. Examples of protocols working in this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
5. **Session layer:** Provides the control functions necessary to establish, manage, and terminate the connections as required to satisfy the user request. Examples of technologies working in this layer are Network File System (NFS) and Structured Query Language (SQL).
6. **Presentation layer:** Accepts and structures the messages for the application. It translates the message from one code to another if necessary. This layer is responsible for data compression and encryption. Examples of technologies working in this layer are American Standard Code for Information Interchange (ASCII) and Joint Photographic Experts Group (JPEG).
7. **Application layer:** Interacts with application programs that incorporate a communication component such as your Internet browser and email. This layer is responsible for logging the message in, interpreting the request, and determining what information is needed to support the request. Examples are Hypertext Transfer Protocol (HTTP) for web browsing, File Transfer Protocol (FTP) for transferring files, and Simple Mail Transfer Protocol (SMTP) for email transmission.

Note

Network administrators often describe networking problems by layer number. For example, a physical link problem is described as a layer 1 problem; a router problem is layer 3; and so on.

The network administrator needs to have a good understanding of all seven layers of the OSI model. Knowledge of the layers can help to isolate the network problem. There are three basic steps in the process of isolating the network problem:

- Is the connection to the machine down? (layer 1)
- Is the network down? (layer 3)
- Is a service on a specific machine down? (layer 7)

The network administrator uses the OSI model to troubleshoot network problems by verifying functionality of each layer. In many cases, troubleshooting the network problem requires the network administrator to isolate at which layer the network problem occurs.

For example, assume that a network is having problems accessing an email server that uses SMTP—a layer 7 application. The first troubleshooting step for the network administrator is to ping the IP address of the email server (layer 3 test). A “ping” to an IP address can be used to check quickly that there is a network connection. (Note: The **ping** command is discussed in detail in section 1-7, “Testing and Troubleshooting a LAN.”) A “reply from” response for the ping indicates the connection to the server is up. A “request timed out” response indicates the network connection is down. This could be due to a cabling problem (layer 1) or a problem with a switch (layer 2) or a router (layer 3), or the email server could be completely down (layer 7). In the case of “request timed out,” the network administrator will have to go directly to the telecommunications closet or the machine to troubleshoot the problem. In this case, the administrator should first check for layer 1 (physical layer) problems. Many times this just requires verifying that a network cable is connected. Cables do get knocked loose or break.

Section 1-3 Review

This section has covered the following **Network+** Exam objectives.

4.1 Given a scenario, implement the following network troubleshooting methodology

The network administrator needs to have a good understanding of all seven layers of the OSI model. Knowledge of the layers can help to isolate the network problem. Remember, there are three basic steps in the process of isolating the network problem:

1. *Is the connection to the machine down? (layer 1)*
2. *Is the network down? (layer 3)*
3. *Is a service on a specific machine down? (layer 7)*

5.1 Analyze a scenario and determine the corresponding OSI layers

The OSI layers have been presented in this section. Develop some method to remember the name, the function, and examples of the seven layers of the OSI model. A good overview of this is presented in Table 1-2. This provides a good start for understanding how the OSI model relates to applications, devices, and protocols.

5.9 Compare and contrast the following ports and protocols

This chapter presented several protocols such as HTTP, TCP, and UDP and how they fit into the OSI model.

Test Your Knowledge

1. TCP functions at which layer of the OSI model?
 - a. Layer 4
 - b. Layer 2
 - c. Layer 3
 - d. Layer 5
 - e. Layer 7
2. HTTP functions at which layer of the OSI model?
 - a. Layer 6
 - b. Layer 5
 - c. Layer 4
 - d. Layer 7
 - e. All of these answers are correct.
3. IP is an example of a protocol that operates in which layer of the OSI model?
 - a. Layer 7
 - b. Layer 6
 - c. Layer 5
 - d. Layer 2
 - e. None of these answers is correct.
4. The NIC operates at which layer of the OSI model?
 - a. Layer 1
 - b. Layer 3
 - c. Layer 5
 - d. Layer 7
 - e. All of these answers are correct.
5. The network address is another name for a layer 4 address.
 - a. True
 - b. False

1-4 THE ETHERNET LAN

The key LAN protocol to understand today is Ethernet (CSMA/CD). It is useful to discuss the Token Ring topology and compare a deterministic network (Token Ring) versus a nondeterministic network (CSMA/CD). The students should be able to use the **ipconfig** command to determine his computer's MAC address. The concept of IP addresses is introduced, and the student should understand the concept of Class A–D networks.

The networking protocol used in most modern computer networks is Ethernet, a carrier sense multiple access with collision detection (CSMA/CD) protocol for local area networks. It originated in 1972, and the full specification for the protocol was provided in 1980 via a joint effort among Xerox, Digital Equipment Corporation, and Intel. Basically, for a computer to “talk” on the Ethernet network, it first “listens” to see whether there is any data traffic (carrier sense). This means that any computer connected to the LAN can be “listening” for data traffic, and any of the computers on the LAN can access the network (multiple access). There is a chance that two or more computers will attempt to broadcast a message at the same time; therefore, Ethernet systems must have the capability to detect data collisions (collision detection).

The information in an Ethernet network is exchanged in a frame format. The frame provides grouping of the information for transmission that includes the header, data, and trailer. The header consists of the preamble, start frame delimiter, destination and source addresses, and length/type field. Next is the actual data being transmitted, followed by the pad used to bring the total number of bytes up to the minimum of 46 if the data field is less than 46 bytes. The last part of the frame is a 4-byte cyclic redundancy check (CRC) value used for error checking. The structure of the Ethernet packet frame is shown in Figure 1-7 and described in Table 1-3.

CSMA/CD

The Ethernet LAN media-access method, carrier sense multiple access with collision detection

Frame

Provides grouping of the information for transmission

Preamble	Start frame delimiter	Destination MAC address	Source MAC address	Length type	Data	Pad	Frame check sequence
----------	-----------------------	-------------------------	--------------------	-------------	------	-----	----------------------

FIGURE 1-7 The data structure for the Ethernet frame. (From Modern Electronic Communication 9/e, by G. M. Miller & J. S. Beasley, 2008. Copyright © 2008 Pearson Education, Inc. Reprinted by permission of Pearson Education, Inc., Upper Saddle River, NJ.)

TABLE 1-3 Components of the Ethernet Packet Frame

Preamble	An alternating pattern of 1s and 0s used for synchronization.
Start frame delimiter	A binary 8-bit sequence of 1 0 1 0 1 0 1 1 that indicates the start of the frame.
Destination MAC address and source MAC address	Each computer has an Ethernet network interface card (NIC) or network adapter that has a unique media access control.
MAC address	MAC address associated with it. The MAC address is 6 bytes (12 hex characters) in length.

Length/type	An indication of the number of bytes in the data field if this value is less than 1500. If this number is greater than 1500, it indicates the type of data format—for example, IP and IPX.
Data	The variable length of data being transferred from the source to the destination.
Pad	A field used to bring the total number of bytes up to the minimum of 46 if the data field is less than 46 bytes.
Frame check sequence	A 4-byte CRC value used for error detection. The CRC is performed on the bits from the destination MAC address through the Pad fields. If an error is detected, the frame is discarded.

The minimum length of the Ethernet frame is 64 bytes from the destination MAC address through the frame check sequence. The maximum Ethernet frame length is 1,518 bytes; 6 bytes for the destination MAC address; 6 bytes for the source MAC address; 2 bytes for length/type; and 1,500 bytes for the data.

Source: Adapted from *Modern Electronic Communication 9/e*, by G. M. Miller & J. S. Beasley, 2008. Copyright © 2008 Pearson Education, Inc. Adapted by permission of Pearson Education, Inc., Upper Saddle River, NJ.

Network Interface Card (NIC)

The electronic hardware used to interface the computer to the network

MAC Address

A unique 6-byte address assigned by the vendor of the network interface card

Organizationally Unique Identifier (OUI)

The first 3 bytes of the MAC address that identifies the manufacturer of the network hardware

How are the destination and source addresses for the data determined within a LAN? Networked devices, such as computers and network printers, each have an electronic hardware interface to the LAN called a **network interface card (NIC)** (see Figure 1-8) or integrated network port. The NIC contains a unique network address called the **MAC address**. MAC stands for “media access control.” The MAC address is 6 bytes, or 48 bits, in length. The address is displayed in 12 hexadecimal digits. The first 6 digits are used to indicate the vendor of the network interface, also called the **organizationally unique identifier (OUI)**, and the last 6 numbers form a unique value for each NIC assigned by the vendor. IEEE is the worldwide source of registered OUIs.



FIGURE 1-8 A 3COM network interface card (courtesy of 3Com Corporation).

The MAC address, also called the **Ethernet, physical, hardware, or adapter address**, can be obtained from computers operating under Microsoft Windows by typing the **ipconfig /all** command while in the command mode or at the MS-DOS prompt. The following is an example of obtaining the MAC address for a computer operating under Windows 7, Windows Vista, or XP.

In Windows XP and Vista, the first step is to enter the command window by selecting **Start** and then **Run**. The Run window, shown in Figure 1-9, displays. Enter **cmd** as shown and click **OK** to open the command prompt. In Windows 7, you can the **cmd** at the search field of the **Start** menu or find it by selecting **Start > Programs > Accessories > cmd**.

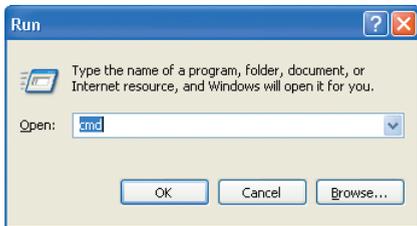


FIGURE 1-9 The Run window used to enter the command prompt in Windows 7.

In the command prompt, enter the **ipconfig /all** command as shown in Figure 1-10. The **/all** switch on the command enables the MAC address information to be displayed—for this example, the information for computer 1. Note that the Host Name for the computer is Computer-1. This information is typically established when the computer’s operating system is installed, but it can be changed as needed. The MAC address is listed under **Ethernet adapter Local Area Connection** as shown in Figure 1-10. The **Media State—Media disconnected** text indicates that no active Ethernet device, such as a hub or switch, is connected to the computer. The **Description** lists the manufacturer and model of the network interface, and the **Physical Address** of **00-10-A4-13-99-2E** is the actual MAC address for the computer.

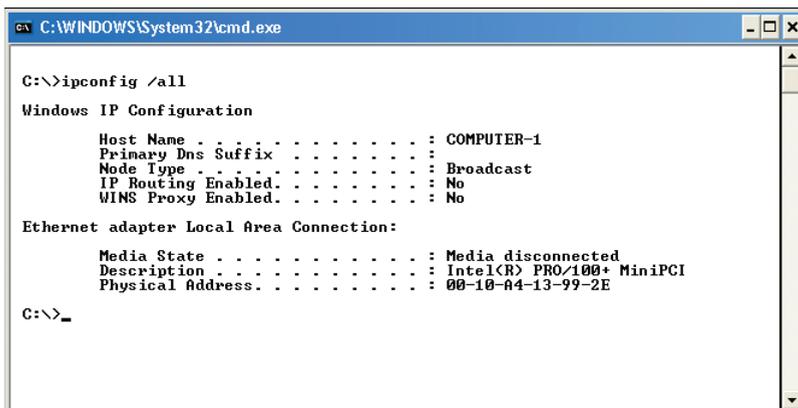


FIGURE 1-10 A typical text screen result when entering the **ipconfig /all** command in the command window.

Ethernet, Physical, Hardware, or Adapter Address
Other names for the MAC address
ipconfig /all
Enables the MAC address information to be displayed from the command prompt

Table 1-4 lists how the MAC address can be obtained for various computer operating systems.

TABLE 1-4 **Commands for Obtaining the MAC Address for Various Operating Systems**

Operating System	Command Sequence	Comments
Windows 98	Click Start > Run , type winipcfg , and press Enter .	The Adapter Address is the MAC address.
Windows NT	Click Start > Run and type winipcfg . In the command prompt, type ipconfig/all and press Enter .	The Physical Address is the MAC address.
Windows 2000	Click Start > Run and type cmd . In the command prompt, type ipconfig/all , and then press Enter .	The Physical Address is the MAC address.
Windows Vista/XP	In Windows XP and Vista, enter the command window by selecting Start and then Run . In the command prompt, type ipconfig/all , and then press Enter .	The Physical Address is the MAC address.
Windows 7, 8, 10	In Windows 7, 8, 10 the text cmd can be entered at the search field of the Start menu. In the command prompt, type ipconfig/all , and then press Enter .	The Physical Address is the MAC address.
Linux	At the command prompt, type ifconfig .	The HWaddr line contains the MAC address.
Mac OS (9.x and older)	Click the Apple , and then select Control Panels > AppleTalk and click the Info button.	The Hardware Address is the MAC address.
Mac OS X	Click Apple > About this MAC > more info > Network > Built-in Ethernet .	The Hardware Address is the MAC address.

In summary, the MAC address provides the information that ultimately enables the data to reach a destination in a LAN. This is also how computer 1 and the printer communicated directly in the star topology example using the switch (refer to Figure 1-4). The switch stored the MAC addresses of all devices connected to its ports and used this information to forward the data from computer 1 directly to the printer. The switch also used the MAC address information to forward the data from computer 5 to computer 6 (refer to Figure 1-4).

MAC addresses are listed in hexadecimal (base-16). The complete MAC address consists of 12 hexadecimal digits. The first 6 digits identify the vendor. The last 6 form a serial number assigned by the manufacturer of the network interface card. A searchable database of IEEE OUI and company ID assignments is available at <http://standards-oui.ieee.org/oui.txt>. Table 1-5 lists a few examples of MAC

addresses. Also large companies may have many OUI numbers assigned to them. For example, the OUI 00-AA-00 is only one of Intel's many OUIs.

TABLE 1-5 A Sample of MAC Addresses

Company ID-Vendor Serial #	Manufacturer (Company ID)
00-AA-00-B6-7A-57	Intel Corporation (00-AA-00)
00-00-86-15-9E-7A	Megahertz Corporation (00-00-86)
00-50-73-6C-32-11	Cisco Systems, Inc. (00-50-73)
00-04-76-B6-9D-06	3COM (00-04-76)
00-0A-27-B7-3E-F8	Apple Computer, Inc. (00-0A-27)

IP Addressing

The MAC address provides the physical address for the network interface card but provides no information as to its network location or even on what LAN or in which building, city, or country the network resides. Internet Protocol (IP) addressing provides a solution to worldwide addressing through incorporating a unique address that identifies the computer's local network. IP network numbers are assigned by **Internet Assigned Numbers Authority (IANA)**, the agency that assigns IP addresses to computer networks and makes sure no two different networks are assigned the same IP network address. The web address for IANA is <http://www.iana.org/>.

IP addresses are classified as either IPv4 or IPv6. IP version 4 (IPv4) is the current TCP/IP addressing technique being used on the Internet. Address space for IPv4 is quickly running out due to the rapid growth of the Internet and the development of new Internet-compatible technologies. However, both IPv4 and IPv6 are being supported by manufacturers of networking equipment and the latest computer operating systems. The details about IPv6 are addressed in Chapter 6, "TCP/IP." IPv4 is currently the most common method for assigning IP addresses. This text refers to IPv4 addressing as "IP addressing." The **IP address** is a 32-bit address that identifies on which network the computer is located and differentiates the computer from all other devices on the same network. The address is divided into four 8-bit parts. The format for the IP address is:

A.B.C.D

where the A.B.C.D values are written as the decimal equivalent of the 8-bit binary value. The range for each of the decimal values is 0–255. IP addresses can be categorized by class. Table 1-6 provides examples of the classes of IP networks, and Table 1-7 provides the address range for each class.

IANA

The agency that assigns IP addresses to computer networks

IP Address

Unique 32-bit address that identifies on which network the computer is located as well as differentiates the computer from all other devices on the same network

TABLE 1-6 The Classes of IPv4 Networks

Class	Description	Example IP Numbers	Maximum Number of Hosts
Class A	Governments, very large networks	44.x.x.x.	$2^{24}=16,777,214$
Class B	Midsize companies, universities, and so on	128.123.x.x	$2^{16}=65,534$
Class C	Small networks	192.168.1.x	$2^8=254$
Class D	Reserved for multicast groups	224.x.x.x	not applicable

TABLE 1-7 The Address Range for Each Class of Network

Class A	0.0.0.0 to 127.255.255.255
Class B	128.0.0.0 to 191.255.255.255
Class C	192.0.0.0 to 223.255.255.255
Class D	224.0.0.0 to 239.255.255.255

Network Number

The portion of the IP address that defines which network the IP packet is originating from or being delivered to

Host Number

The portion of the IP address that defines the location of the networking device connected to the network; also called the host address

Host Address

Same as host number

ISP

Internet service provider

Private Addresses

IP addresses set aside for use in private intranets

Intranet

An internal network that provides file and resource sharing but is not accessed from the Internet

Examples of network addresses also are shown in Table 1-6. The decimal numbers indicate the **network number**, which is the portion of the IP address that defines which network the IP packet is originating from or being delivered to. The x entries for each class represent the **host number**, which is the portion of the IP address that defines the address of the networking device connected to the network. The host number is also called the **host address**. The network number provides sufficient information for routing the data to the appropriate destination network. A device on the destination network then uses the remaining information (the x portion) to direct the packet to the destination computer or host. The x portion of the address is typically assigned by the local network system administrator or is dynamically assigned when users need access outside their local networks. For example, your Internet service provider (**ISP**) dynamically assigns an IP address to your computer when you log on to the Internet. Remember, you can check the IP address assigned to your computer by your ISP using the **ipconfig** command in the command prompt.

For this chapter and the rest of the text, a group of IP addresses called **private addresses** will be used for assigning IP addresses to networks. Private addresses are IP addresses set aside for use in private **intranets**. An intranet is an internal inter-network that provides file and resource sharing. Private addresses are not valid addresses for Internet use because they have been reserved for internal use and are not routable on the Internet. However, these addresses can be used within a private

LAN (intranet) to create an **IP internetwork**. An IP internetwork uses IP addressing for identifying devices connected to the network and is also the addressing scheme used in **TCP/IP** networks. TCP/IP stands for Transmission Control Protocol/Internet Protocol and is the protocol suite used for internetworks such as the Internet. The three address blocks for the private IP addresses are as follows:

10.0.0.0–10.255.255.255
172.16.0.0–172.31.255.255
192.168.0.0–192.168.255.255

The topic of IP addressing will be examined in greater detail throughout the text. For Chapter 1, the objective is to use the IP addresses for configuring the address of the computers for operation in a TCP/IP network.

IP Internetwork

A network that uses IP addressing for identifying devices connected to the network

TCP/IP

Transmission Control Protocol/Internet Protocol, the protocol suite used for internetworks such as the Internet

Section 1-4 Review

This section has covered the following **Network+** Exam objectives:

- 1.8 Given a scenario, implement and configure the appropriate addressing schema

It is important that you understand the structure of the IPv4 address and what bits define the network address and which bits are the host bits. Make sure you understand the structure of both the MAC address and the IPv4 address and know how to get this information from many types of computers.

- 4.2 Given a scenario, analyze and interpret the output of troubleshooting tools

Remember, you can check the IP address assigned to your computer by your ISP using the **ipconfig** command in the command prompt. *Issuing the **ipconfig /all** command enables the network administrator to determine whether the network interface card is connected to a network and to determine the MAC and IP address of a networking device.*

- 5.2 Explain the basics of network theory and concepts

The most common networking protocol, CSMA/CD, has been introduced in this section. Make sure you understand how this protocol manages network access from multiple devices.

Test Your Knowledge

1. How do the IP address and MAC address differ? (Select one.)
 - a. They are the same.
 - b. The MAC address defines the network location.
 - c. The IP address is only used as part of the ARP request.
 - d. The MAC address provides the physical address of the network interface card.

2. The MAC address on a Windows computer can be accessed by typing **ipconfig /all** from the command prompt.
 - a. True
 - b. False
3. The OUI for the MAC address 00-10-A4-13-99-2E is 13992E.
 - a. True
 - b. False
4. Define the acronym NIC.
 - a. Network Interface Card
 - b. National Integrated Communicator
 - c. Network Integration Card
 - d. National Integration Communicator
 - e. None of these answers is correct

1-5 HOME NETWORKING

Wired Network

Uses cables and connectors to establish the network connection

Wireless Network

Uses radio signals to establish the network connection

Setting up a home network is probably one of the first networks that the student sets up. This is an exciting opportunity for the student to demonstrate his/her knowledge of computer networks, but setting up the home network can also be quite a challenge. One of the first questions asked is, “Do I want to set up a wired or wireless home network?” A **wired network** uses cabling and connectors to establish the network connections. A **wireless network** uses radio signals to establish the network connection.

Section 1-6, “Assembling an Office LAN,” introduces setting up wired networks for both office and home networks; however, the home networking technologies are presented in this section.

A wireless home network is probably the most common home network configuration in use today.

Table 1-8 lists the advantages and disadvantages of both wired and wireless networks.

TABLE 1-8 **Wired and Wireless Network Advantages and Disadvantages**

	Advantages	Disadvantages
Wired network	<p>Faster network data transfer speeds (within the LAN).</p> <p>Relatively inexpensive to set up.</p> <p>The network is not susceptible to outside interference.</p>	<p>The cable connections typically require the use of specialized tools.</p> <p>The cable installation can be labor-intensive and expensive.</p>

	Advantages	Disadvantages
Wireless network	User mobility. Simple installations. No cables.	Security issues. The data transfer speed within the LAN can be slower than wired networks.

Wireless networks also go by the name **Wi-Fi**, which is the abbreviated name for the Wi-Fi Alliance (Wi-Fi stands for wireless fidelity). The Wi-Fi Alliance is an organization whose function is to test and certify wireless equipment for compliance with the 802.11x standards, which is the group of wireless standards developed under IEEE 802.11. IEEE is the Institute of Electrical and Electronics Engineers. The most common IEEE wireless standards include

- **802.11a (Wireless-A):** This standard can provide data transfer rates up to 54Mbps and an operating range up to 75 feet. It operates at 5GHz.
- **802.11b (Wireless-B):** This standard can provide data transfer rates up to 11Mbps with ranges of 100–150 feet. It operates at 2.4GHz.
- **802.11g (Wireless-G):** This standard can provide data transfer rates up to 54Mbps up to 150 feet. It operates at 2.4GHz.
- **802.11n (Wireless-N):** This standard provides data transfer rates up to 4 × 802.11g speeds (200+Mbps). It operates either at 2.4GHz or 5GHz.
- **802.11ac (Wireless-AC):** This is the latest wireless standard. It provides single-station data transfer rates of 500Mbps and operates in the 5GHz frequency band.

Figure 1-11 illustrates the placement and type of equipment found in a typical wired or wireless home network. Figure 1-11 (a) shows a wired LAN that is using cabling to interconnect the networking devices. A router is being used to make the connection to the ISP. The router can also contain a switch and a broadband modem. The switch is used to interconnect other networking devices, and the broadband modem is used to make the data connection to the ISP. The most common broadband connections to the ISP are via a cable modem and DSL. In some cases the router, switch, and broadband modem will be separate devices, but most often they will be integrated into one device. One of the computers may also have the configuration settings for managing the router, which can include the settings for connecting to the ISP.

Figure 1-11 (b) shows a wireless LAN that is being used to interconnect the networking devices. A **wireless router** is being used to make the data connection to the ISP, which is typically via a cable or DSL modem. The wireless router also has a wireless access point and will typically have a switch to facilitate wired network connections. Sometimes the broadband modem is integrated into the wireless router. The access point is used to establish the wireless network connection to each of the wireless computers.

Wi-Fi

Wi-Fi Alliance—an organization that tests and certifies wireless equipment for compliance with the 802.11x standards

Wireless Router

Device used to interconnect wireless networking devices and to give access to wired devices and establish the broadband Internet connection to the ISP

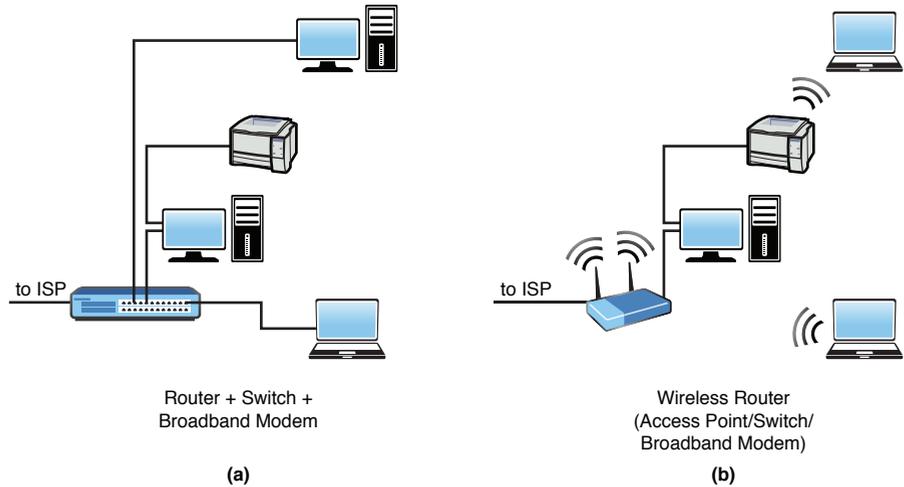


FIGURE 1-11 Examples of (a) wired and (b) wireless Wi-Fi home networks.

The components of a home network can include the following:

- **Hub:** This is used to interconnect networking devices. A drawback to the hub is that it broadcasts the data it receives to all devices connected to its ports. The hub has been replaced by the network switch in most modern networks. Figure 1-12 provides an image of a hub.
- **Switch:** This is the best choice for interconnecting networking devices. It can establish a direct connection from the sender to the destination without passing the data traffic to other networking devices. Figure 1-13 provides an image of a switch.
- **Network adapter:** Wired and wireless network adapters are available. The type of network adapter used in desktop computers is called the network interface card (NIC). Figure 1-14 provides an image of a wired network adapter. This type of NIC is inserted into an expansion slot on the computer’s motherboard and is a wired-only adapter.



FIGURE 1-12 Linksys EtherFast® 8-Port 10/100 Auto-Sensing Hub (courtesy of Linksys).



FIGURE 1-13 Linksys 24-Port 10/100/1000 Gigabit Switch (courtesy of Linksys).



FIGURE 1-14 Linksys Instant Gigabit Network Adapter (courtesy of Linksys).

The PC Card adapter connects to notebook computers and provides an RJ-45 jack for connecting to wired networks. RJ stands for registered jack. This device supports connections to both 10Mbps and 100Mbps networks. Figure 1-15 provides an image of a PC card adapter.



FIGURE 1-15 Linksys EtherFast® 10/100 32-Bit Integrated CardBus PC Card (courtesy of Linksys).

The Wireless-N adapter inserts into a notebook or laptop computer PC Card slot. The Wireless-N technology offers a data transfer speed that is faster than Wireless-G and is also compatible with both Wireless-B and Wireless-G technologies. Figure 1-16 provides an image of a Wireless-N adapter.



FIGURE 1-16 Linksys Wireless-N Notebook Adapter (courtesy of Linksys).

Another option for connecting to networks is to use a network adapter that attaches to a USB port on the computer. This device has the USB type A connector on one end and an RJ-45 jack on the other and will support connections to both 10Mbps, 100Mbps, and 1000Mbps data networks. Figure 1-17 provides an image of a USB network adapter.



FIGURE 1-17 Linksys Compact USB 2.0 10/100 Network Adapter (courtesy of Linksys).

- **Router:** A networking device used to connect two or more networks (for example, your LAN and the Internet) using a single connection to your ISP. A modern home networking router can also contain a switch and a broadband modem. Figure 1-18 provides an image of a router.



FIGURE 1-18 Linksys EtherFast® Cable/DSL Firewall Router with 4-Port Switch (courtesy of Linksys).

- **Access point:** Used to interconnect wireless devices and provide a connection to the wired LAN. The data transfer speeds for access points are dictated by the choice of wireless technology for the clients, but this device will support Wireless-N. Figure 1-19 provides an image of an access point.
- **Wireless router:** This device uses RF to connect to the networking devices. A wireless router typically contains a router, switch, and wireless access point and is probably the most common way to interconnect wireless LANs to the ISP's access device. Note that these devices also have wired network connections available on the system. Figure 1-20 provides an image of a wireless router.



FIGURE 1-19 The Linksys Wireless-N access point.

- **Broadband modem/gateway:** This describes the device used to provide high-speed data access via your cable connection or via a telephone company's DSL connection. A gateway combines a modem and a router into one network box. Figure 1-21 provides an image of a broadband modem/gateway.
- **Cable modem:** This device is used to make a broadband network connection from your home network to the ISP using your cable connection. This setup requires a splitter to separate the cable TV from the home network. Access to the Internet is typically provided by the cable TV service provider. Figure 1-22 provides an image of a cable modem.



FIGURE 1-20 Linksys Wireless-G Broadband Router (courtesy of Linksys).



FIGURE 1-21 Linksys Wireless-G Cable Gateway (courtesy of Linksys).



FIGURE 1-22 Linksys Cable Modem with USB and Ethernet connections (courtesy of Linksys).

- **DSL modem:** This device is used to make a broadband network connection from your home network to the ISP using the telephone line. Broadband access to the Internet is provided via the phone company or a separate ISP. The DSL connection requires the placement of filters on all telephone lines except the one going into the modem to prevent interference. Figure 1-23 provides an image of a DSL modem.



FIGURE 1-23 Linksys ADSL2 Modem (courtesy of Linksys).

Several issues should be considered when planning for a home network, including the following:

- **Data speed:** This will be determined by whether you chose to implement a wired or wireless home network. Wired networks offer the best data transfer rate inside the home network, up to 10Gbps. The best data transfer rates for a wireless home network can be obtained using 802.11n (Wireless-N) technology. This is the next generation of high-speed wireless connectivity providing data transfer rates up to $4 \times 802.11g$ speeds (200+Mbps).
- **Cost:** Implementing a high-speed wired network can be quite expensive. With the networking hardware, cabling, and related hardware, you can incur an unexpected additional cost for implementing the high-speed wired home network. The cost of switching to or implementing an 802.11n Wireless-N network is minimal and is a suitable alternative to a wired network. But remember, the maximum data rate for a Wireless-N network is still much lower than that possible with a wired LAN.
- **Ease of implementation:** A wireless home network is probably the easiest to implement if the cabling and connectors for a wired network are not already installed. The time required to install the wireless home network is usually minimal as long as unexpected problems do not surface.
- **Appearance:** A wireless home network offers the best choice in regards to appearance because there won't be cables and networking hardware scattered around the house. The wireless home network will require a wireless router and an external wired connection to the ISP (refer to Figure 1-11(b)).
- **Home access:** The choice of wired or wireless technology will not affect home access. However, the wired network will offer the best data transfer speed internal to the network, but the wireless network offers the best choice for mobility.
- **Public access:** The choice of wired or wireless technology will not impact public access. The data rate for the connection to/from the ISP will be the limiting factor for the data transfer rate for public access.

It is not uncommon for a wired or wireless home network to stop functioning, although the downtime is usually minimal. The steps for troubleshooting wired and wireless home networks include the following:

- Step 1** Check to ensure that the proper lights for your networking device that connects you to your ISP are properly displayed. Incorrect lights can indicate a connection problem with your cable modem, DSL modem, or telephone connection. Your ISP might also be having a problem, and you might need to call them to verify your connection.
- Step 2** Next, to fix basic connection problems to the ISP, you should reboot the host computer (the computer connected to the router) and reboot the router. This usually will fix the problem, and the correct lights should be displayed. In some cases, you might also have to power down/up your broadband modem. (Note that the broadband modem might be integrated with the router.) Once again, check to see whether the correct lights are being displayed.
- Step 3** You should always verify your hardware cable or phone connection is in place and has not been pulled loose. Make corrections as needed. You should also verify that all wireless units have a network connection. The following

are steps to verify wireless connectivity for Windows 10/8/7, Windows XP, and Mac OS X:

- Windows 10/8/7, Windows Vista: Go to Control Panel > Network and Sharing Center. The wireless connection will show enabled if there is a wireless connection.
 - **Windows XP:** Right-click **My Network Places**. The computer will indicate whether there is a wireless network connection.
 - **Mac OS X:** Click the **Apple icon** > **System Preferences** > **Network**. If you are connected:
 - A green AirPort icon is displayed, and the words “airport is connected to network” appear.
 - A yellow icon indicates that AirPort is turned on but is not connected to a network.
 - A red icon indicates AirPort is turned off.

Also note that if you are connected to a wireless network, a radio wave icon will appear at the top of the screen in the menu bar to indicate you are connected to a wireless network.

Step 4 Sometimes you might need to verify your network settings. This can happen if your computer has lost the data for the settings. In this case, follow the steps provided by the manufacturer of your broadband modem or your ISP.

The following are the basic steps for establishing the wireless connection for a wireless notebook computer running Windows 10/8/7, Windows Vista, XP, or Mac OS X: Windows Vista, XP, or Mac OS X:

- **Windows 10/8:** Go to Control Panel > Network and Sharing Center—Set up a new connection or network. You need to choose the **Connect to the Internet** option and then select **Wireless** to establish a wireless connection.
- **Windows 7:** Click Start > Control Panel > Network and Sharing Center—Set up a new connection or network. You need to choose **Connect to the Internet** option; then select **Wireless** to establish a wireless connection.
- **Windows Vista:** Click Start > Settings > Network Connections and then right-click **Wireless Network Connection**. You might need to click **Enable** and/or **Connect/Disconnect** to establish a wireless connection. A red X indicates a wireless connection is not established.
- **Windows XP:** This can vary depending on your wireless card. Click **Start** > **Programs** and select the setup program for your wireless card. Follow the steps displayed on the screen to establish a wireless network connection. You will need to know the name of the network you want to join as well as the SSID. The SSID is the Service Set Identifier and is used to identify which wireless devices are allowed to connect to the network.
- **Mac OS X:** Click the **Apple icon** > **System Preferences** > **Network**, and then click **Show** > **Network Status** > **Connect** > **Turn AirPort on**. Close the AirPort window and click **Configure** > **By default join a specific network**. Enter the wireless network name (SSID) and password (WEP code); then click **Apply Now**. A radio wave should now appear at the top of the screen in the menu bar, which indicates the network is connected.

There are many choices of wireless technologies for configuring a wireless network. The 802.11b, g, and n (Wireless-B, -G, and -N) technologies are compatible even though they offer different data speeds. If compatible but different wireless technologies are being used, the data transfer speeds will be negotiated at the rate specified by the slowest technology. For example, the 802.11n (Wireless-N) standard offers a faster data rate (comparable to Wireless-G), but when devices of both technologies are present, the data transfer rate will be negotiated at the Wireless-G data rate.

In some cases, the wireless signal might not be reaching all the areas that need coverage. In this case, a device called a **range extender** can be used. This device relays the wireless signals from an access point or wireless router into areas with a weak signal or no signal at all. This improves the wireless remote access from all points in the home. This same technology can also be used to improve connectivity in stores and warehouses and can also be used to provide excellent connectivity in public places such as **hotspots**. Hotspots are defined as a limited geographic area that provides wireless access for the public. Hotspots are typically found in airports, restaurants, libraries, and schools.

Securing the Home Network

Many potential security issues are associated with a wireless network. Securing the home wireless network is extremely important because a wireless signal can be intercepted by the wrong person, and they can possibly connect to your network. The following are some basic steps that can be used to help protect the home network.

- 1. Change the default factory passwords.** Wireless equipment is shipped with default passwords that are set at the factory. These default settings are known by the public, including people who would like to gain access into your network and possibly change your settings. It is best that you select your own password that is a combination of alphanumeric characters.
- 2. Change the default SSID.** The **SSID** is the name used to identify your network and is used by your access point or wireless router to establish an association. Establishing an association means that a wireless client can join the network. The SSID can be up to 32 characters and should be changed often so hackers who have figured out your SSID will no longer have access to your home network.
- 3. Turn encryption on.** Probably the most important thing to do is turn on the security features that include data encryption. These options include Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2. WPA2 is a product certification issued by the Wi-Fi Alliance. It uses a stronger encryption than WPA and is also backward compatible with adapters using WPA. **WPS** is the Wi-Fi Protected setup. WPS simplifies the configuration process, enabling the user to set up WPA PSK without having to enter a long string of symbols, random numbers, or letters. This provides a feature to protect wireless networks, but it is susceptible to brute force attacks.
- 4. Turn off the SSID broadcast.** Wireless systems broadcast the SSID so that the network can be easily identified as an available network. Hackers can use this information to possibly gain access to your network, so you should turn off the SSID broadcast. The exception to this is in hotspots where public access is

Range Extender

Device that relays the wireless signals from an access point or wireless router into areas with a weak signal or no signal at all

Hotspots

A limited geographic area that provides wireless access for the public

Service Set Identifier (SSID)

Name that is used to identify your wireless network and is used by your access point or wireless router to establish an association

available. Please note, hotspots make it easy for the user to gain wireless access but hackers can also be on the same network, so it is important to have encryption turned on.

5. **Enable MAC address filtering.** All computer devices use a unique MAC address for identifying the device. This can be used to select which devices can be allowed access to the network. When MAC address filtering is turned on, only wireless devices that have specific MAC addresses will be allowed access to the network.

Another important security concern is limiting outside access to your home network via your connection to the ISP. The following are some things that can be done to protect the home network from outside threats:

- **Network Address Translation:** The outsider sees only the router IP address because the IP addresses of the internal networking devices are not provided on the Internet. Only the ISP-assigned IP address of the router is provided. The home network typically uses a private address that is not routable on the Internet. (Private IP addresses are blocked by the ISP.)
- **Firewall protection:** A common practice is to turn on the **firewall protection**. The purpose of a firewall is to prevent unauthorized access to your network. Firewall protection is available in both the Windows and MAC operating environments. A type of firewall protection is **Stateful Packet Inspection (SPI)**. This type of firewall inspects incoming data packets to make sure they correspond to an outgoing request. For example, you might be exchanging information with a website. Data packets that are not requested are rejected. The topic of firewalls is covered in more detail in Chapter 12, “Network Security.”
- **Establish a VPN connection when transferring sensitive information:** A **virtual private network (VPN)** establishes a secure network connection and is a way to protect your LAN’s data from being observed by outsiders. The VPN connection capability is available with Windows 10, Windows 8, Windows 7, Windows Vista, Windows XP, and Mac OS X. A VPN connection enables a remote or mobile user to access the network as if they were actually physically at the network. Additionally, the VPN connection is encrypted, providing privacy for the data packets being transmitted.

Firewall Protection

Used to prevent unauthorized access to your network

Stateful Packet Inspection (SPI)

Type of firewall that inspects incoming data packets to make sure they correspond to an outgoing request

Virtual Private Network (VPN)

Establishes a secure network connection and is a way to protect your LAN’s data from being observed by outsiders

IP Addressing in the Home Network

A common question asked about home networks is, “How is IP addressing handled for all the computers connected to the Internet?” The home network typically has only one connection to the ISP, but multiple computers can be connected to the Internet at the same time. The answer is that IP addressing for the home network is managed by the router or wireless router that connects to the ISP. The ISP will issue an IP address to the router from an available pool of IP addresses managed by the ISP. The computers in the home network should be issued private IP addresses

(applicable ranges are 10.0.0.0–10.255.255.255; 172.16.0.0–172.31.255.255; 192.168.0.0–192.168.255.255) using a technique called **Network Address Translation (NAT)**.

Figure 1-24 provides an example. A routable public IP address is issued by the ISP for the wireless router. This public IP address enables all computers in the home network access to the Internet. The wireless router issues private addresses to all computers connected to the network.

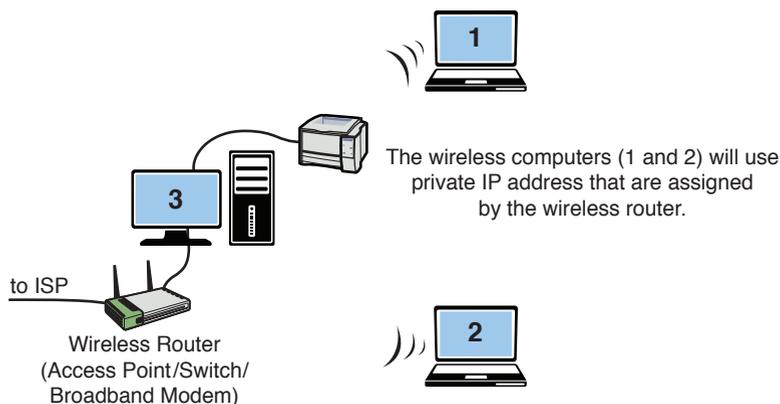


FIGURE 1-24 A home network using a wireless router connected to the ISP.

NAT translates the private IP address to a public address for routing over the Internet. For example, computer 1 in the home network (see Figure 1-24) might establish a connection to an Internet website. The wireless router uses NAT to translate computer 1's private IP address to the public IP address assigned to the router. The router uses a technique called **overloading**, where NAT translates the home network's private IP addresses to the single public IP address assigned by the ISP. In addition, the NAT process tracks a port number for the connection. This technique is called **Port Address Translation (PAT)**. The router stores the home network's IP address and port number in a NAT lookup table. The port number differentiates the computer that is establishing a connection to the Internet because the router uses the same address for all computers. This port number is used when a data packet is returned to the home network. The port number identifies the computer that established the Internet connection, and the router can deliver the data packet to the correct computer.

For example, if computer 1 establishes a connection to a website on the Internet, the data packets from the website are sent back to computer 1 using the home network's routable public IP address. This first step enables the data packet to be routed back to the home network. Next, the router uses the NAT lookup table and port number to translate the destination for the data packet back to the computer 1 private IP address and original port number, which might be different. Figure 1-25 demonstrates an example of the NAT translation process for a home network. The home network has been assigned Class C private IP addresses (192.168.0.x) by the router. The x is a unique number (from 1 to 254) assigned to each computer. The router translates the private IP addresses to the public routable IP address assigned

Network Address Translation (NAT)

Translates the private IP address to a public address for routing over the Internet

Overloading

Where NAT translates the home network's private IP addresses to a single public IP address

Port Address Translation (PAT)

A port number is tracked with the client computer's private address when translating to a public address

by the ISP. Additionally, the router tracks a port number with the public IP address to identify the computer. For example, the computer with the private IP address of 192.168.0.64 is assigned the public IP address 128.123.246.55:1962, where 1962 is the port number tracked by the router.

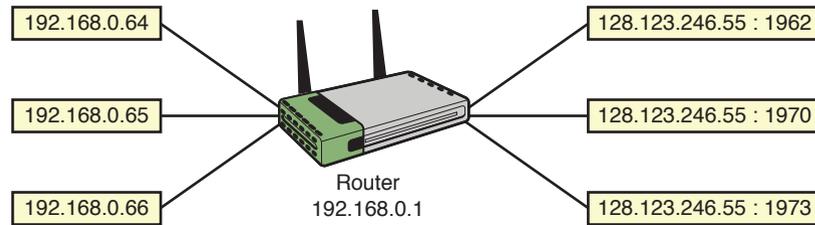


FIGURE 1-25 The NAT translation using PAT.

Section 1-5 Review

This section covered the following **Network+** Exam objectives:

1.1 Explain the functions and applications of various network devices

This section has presented a look at the wireless router, switch, access point, and the firewall. All of these devices are key for providing wireless network access. The purpose of a firewall is to prevent unauthorized access to your network.

1.2 Compare and contrast the use of networking services and applications

The benefit of incorporating a VPN connection for your wireless network is presented. A virtual private network (VPN) establishes a secure network connection and is a way to protect your LAN's data from being observed by outsiders.

1.3 Install and configure the following networking services/applications

This section presents an overview of both NAT (Network Address Translation) and PAT (Port Address Translation).

1.7 Differentiate between network infrastructure implementations

Hotspots are introduced in this section. Hotspots are defined as limited geographic areas that provide wireless access for the public.

1.8 Given a scenario, implement and configure the appropriate networking addressing schema

This section presents an overview of both NAT (Network Address Translation) and PAT (Port Address Translation).

2.4 Explain the importance of implementing network segmentation

This section includes many discussions on the various wireless standards available today. There are many choices of wireless technologies for configuring a wireless network. It is very important that you understand the advantages and limitations of each wireless standard.

2.6 Given a scenario, configure a switch using proper features

This section introduces MAC address filtering. When MAC address filtering is turned on, only wireless devices that have specific MAC addresses will be allowed to access the network.

2.7 Install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless-capable devices

A wireless router typically contains a router, switch, and wireless access point and is probably the most common way to interconnect wireless LANs to the ISP's access device.

3.2 Compare and contrast network vulnerabilities and threats

WPS is the Wi-Fi Protected Setup. WPS simplifies the configuration process enabling the user to set up WPA PSK without having to enter a long string of symbols, random numbers, or letters. This provides a feature to protect wireless networks, but it is susceptible to brute force attacks.

3.3 Given a scenario, implement network-hardening techniques

Probably the most important thing to do is turn on the security features that include data encryption. These options include Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2.

4.1 Given a scenario, implement the following network troubleshooting methodology

The basic steps for troubleshooting the wireless network were discussed in this section. Step 1 is to verify that the proper lights are being displayed on your modem connection.

5.3 Given a scenario, deploy the appropriate wireless standard

This section includes many discussions on the various wireless standards available today. There are many choices of wireless technologies for configuring a wireless network. It is very important that you understand the advantages and limitations of each wireless standard.

5.4 Given a scenario, deploy the appropriate wired connectivity standard

The cable modem is used to make a broadband network connection from your home network to the ISP using your cable connection.

Test Your Knowledge

1. Which of the following issues should be considered when planning for a home network?
 - a. Data speed
 - b. Public access
 - c. Cost
 - d. All of these answers are correct.

2. How does MAC address filtering help to secure a wireless network?
 - a. This is used to help prevent the theft of network interface cards.
 - b. This requires an additional login step requiring the user to enter his MAC address.
 - c. MAC address filtering is seldom used anymore because of NIC restrictions.
 - d. This can be used to select which networking devices can be allowed access to the network.
3. Which of the following are examples of wireless technologies?
 - a. 802.11a
 - b. 802.11g
 - c. 802.11n
 - d. All of these answers are correct.
4. What is NAT?
 - a. Network Asynchronous Transfer
 - b. Network Address Translation
 - c. Network Address Transfer
 - d. None of these answers is correct.

1-6 ASSEMBLING AN OFFICE LAN

This section guides the student through the process of assembling, configuring, and testing the simple office LAN. This gives the student a chance to grasp the basic networking concepts prior to bringing more complex networking hardware and architectures into the picture. The concept of twisted pair cable is introduced in this chapter and is fully explored in Chapter 2. Many networking numerics are used in computer networking, which the student will encounter. The student needs to understand CAT6, RJ-45, and Mbps (megabits per second). The student should understand the purpose of the link light, and if possible, the link light should always be checked. The last part of section 1-6 discusses how to configure the computer's IP address. An example is presented for configuring the computer's IP address.

An example of assembling an office-type LAN is presented in this section. The Ethernet protocol will be used for managing the exchange of data in the network, and the networking devices will be interconnected in a star topology. There are many options for assembling and configuring a LAN, but this example presents a networking approach that is simple and consistent with modern computer networking. It will also provide a good introduction to the networking topics presented in the text.

For this example, three computers and one printer are to be configured in the star topology. Each device in the network will be assigned an IP address from the private address space. The following step-by-step discussion guides you through the process of assembling, configuring, and testing an office LAN:

Step 1 The first step in assembling an office LAN is to document the devices to be connected in the network and prepare a simple sketch of the proposed network. Each device’s MAC and IP addresses should be included in the network drawing documentation.

Figure 1-26 provides an example of a small office LAN. The desired IP addresses and the actual MAC addresses for each computer and printer are listed. Remember, each NIC contains a unique MAC address and the IP addresses are locally assigned by the network administrator. The MAC addresses were obtained by entering the **ipconfig /all** command from the command prompt in Windows 7. Repeat this step for all computing devices connected to the LAN. Table 1-9 provides the results of the MAC address inquiries. Each networking device will be assigned an IP address. Table 1-9 also lists the planned IP addresses of the devices used in this office LAN.

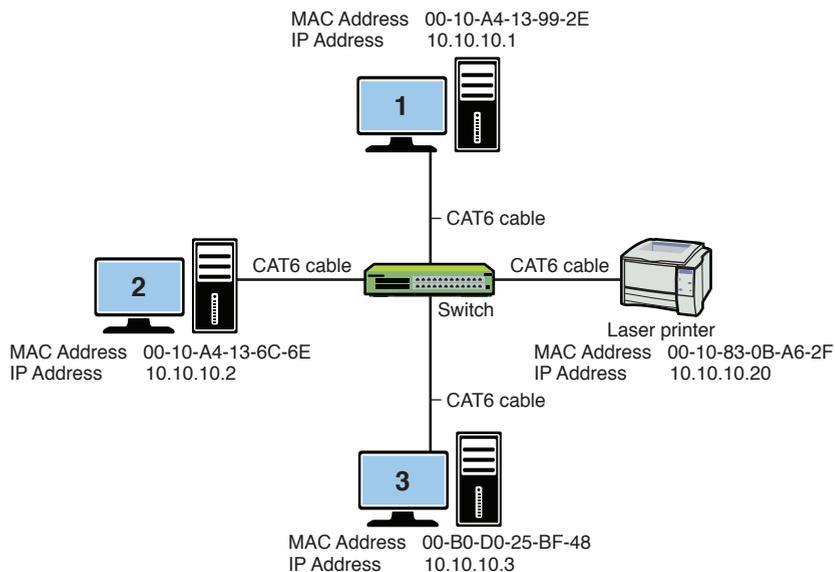


FIGURE 1-26 An example of a small office LAN star topology

TABLE 1-9 The MAC and Assigned IP Address for the Devices in the Office LAN

Device (Hostname)	MAC Address	IP Address
Computer 1	00-10-A4-13-99-2E	10.10.10.1
Computer 2	00-10-A4-13-6C-6E	10.10.10.2
Computer 3	00-B0-D0-25-BF-48	10.10.10.3
Laser Printer	00-10-83-0B-A6-2F	10.10.10.20

Note

In this text, you will function as the network administrator. The network administrator must know how to obtain all IP and MAC address information for devices connected to the network. This requires that the network administrator keep good documentation of the network.

Step 2 Connect all the networking devices using the star topology shown in Figure 1-26.

At the center of this star topology network will be a switch or hub. Recall that either can be used to connect the networking devices. The switch is the best choice because the hub broadcasts data it receives to all devices connected to its ports, and the switch enables the devices to communicate directly. Although hubs are not as sophisticated as switches and are not reflective of modern computer networking, the hub is still suitable for use in small networks.

The connections from the switch to the computers and the printer will be made using premade twisted-pair patch cables. The cable type used here is **CAT6 (category 6)** twisted-pair cable. CAT6 twisted-pair cables have **RJ-45** modular connectors on each end, as shown in Figure 1-27, and are capable of carrying **1000Mbps** (1 gigabit) or more of data up to a length of 100 meters. Chapter 2 covers the twisted-pair media and its various category specifications. If the network hardware and software are properly set up, all computers will be able to access the printer and other computers. Chapter 2 addresses issues associated with the proper cabling including CAT 6/5e.

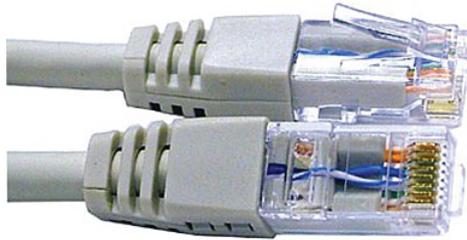


FIGURE 1-27 The RJ-45 twisted-pair patch cables (courtesy of StarTech.com).

CAT6 (category 6)

Twisted-pair cables capable of carrying up to 1000Mbps (1 gigabit) of data up to a length of 100 meters

RJ-45

The 8-pin modular connector used with CAT6/5e/5 cable

Mbps

Megabits per second

Numerics

A numerical representation

The media used for transporting data in a modern computer network are either wireless, twisted-pair, or fiber-optic cables. The principles behind selecting, installing, and testing twisted-pair cabling are presented in Chapter 2. Table 1-10 lists the common **numerics** used to describe the data rates for the twisted-pair media and the older style copper coaxial cable used in a LAN. Common numerics for fiber-optic LANs are also listed. Numerics are an alphanumeric description of a technology. For example, 100BaseT means that this is a 100-Mbps, baseband, twisted-pair technology.

TABLE 1-10 Common Numerics for Ethernet LAN Cabling

Numeric	Description
10Base2	10Mbps over coaxial cable up to 185 m, also called ThinNet (seldom used anymore)
10Base5	10Mbps over coaxial cable up to 500 m, also called ThickNet (seldom used anymore)
10BaseT	10Mbps over twisted-pair
10BaseF	10Mbps over multimode fiber-optic cable
10BaseFL	10Mbps over 850 nm multimode fiber-optic cable
100BaseT	100Mbps over twisted-pair (also called Fast Ethernet)
100BaseFX	100Mbps over fiber
1000BaseT	1000Mbps over twisted-pair
1000BaseFX	1000Mbps over fiber
10GE	10GB Ethernet

The RJ-45 plugs connect to the switch inputs via the RJ-45 jacks. Figure 1-28 shows a simple 8-port switch. The inputs to the switch are also called the input **ports**, which are the interfaces for the networking devices. The switch inputs marked with an “x” or uplink port [Figure 1-28(b)] indicate that these devices are cross-connected, meaning the transmit and receive pairs on the twisted-pair cable are crossed to properly align each for data communication. The term for a cable that has cross-connected TX/RX data lines is **crossover**. Some of the switches might have the port labeled “Uplink,” which indicates the cross-connect capability. Furthermore, some of the newer switches nowadays are equipped with automatic crossover detection, so the users don’t have to worry about whether to use a straight-through cable or a crossover cable. Examples of straight-through and crossover cables are presented in Chapter 2.

Ports

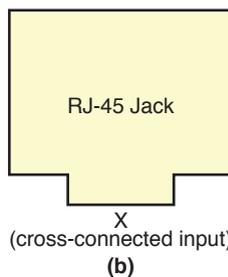
The interface for the networking devices

Crossover

Transmit and receive signal pairs are crossed to properly align the transmit signal on one device with the receive signal on the other device



The switch used to connect the networking devices
(a)



(b)

FIGURE 1-28 (a) The switch used to connect the networking devices; (b) close-up view of “x” input indicating an uplink port (courtesy of Anixter, Inc.).

Straight-through

Transmit and receive signal pairs are aligned end-to-end

Uplink Port

Allows the connection of a switch to another switch without having to use a crossover cable

Figure 1-29(a) provides an example of this cross-connected concept. Switches usually have at least one port that can be switched or selected for use as either a cross-connected or **straight-through** input. A straight-through port is also called an **uplink port**. The uplink port allows for the connection of a switch to a switch or hub without having to use a special cable. Devices requiring the cross-connected input port are computers, printers, and routers. Devices requiring a straight-through connection are uplink connections to other switches or hubs. Figure 1-29(b) provides a block diagram explaining the concept of a straight-through input.

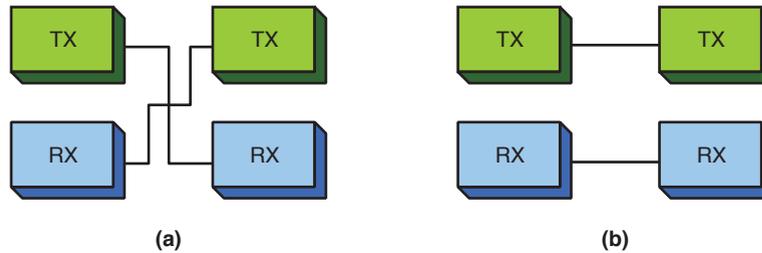


FIGURE 1-29 (a) An example of the wiring on an “x” type input on a hub; (b) an example of straight-through wiring.

Link Light

Indicates that the transmit and receive pairs are properly aligned

Link Integrity Test

Protocol used to verify that a communication link between two Ethernet devices has been established

Link Pulses

Sent by each of the connected devices via the twisted-pair cables when data is not being transmitted to indicate that the link is still up

A networking connection can be verified by examining the **link light** on the switch or hub. The presence of a link light indicates that the transmit and receive pairs are properly aligned and the connected devices are communicating. Absence of the light indicates a possible cabling or hardware problem. The Ethernet protocol uses the **link integrity test** to verify that a communication link between two Ethernet devices has been established. The link light remains lit when communication is established and remains lit as long as there is a periodic exchange of link pulses from the attached devices. **Link pulses** are sent by each of the connected devices via the twisted-pair cables to indicate that the link is up, but the link pulses are not part of the Ethernet packet and are sent at regular intervals when data is not being transmitted.

Step 3 Configure the IP address settings on each computer according to the assigned addresses provided in Table 1-7.

The following describes how the network administrator configures the computers to operate on the LAN. This requires that each computing device be assigned an IP address. The assigned IP addresses for this LAN are provided in Table 1-7. Examples of configuring the computers in the office LAN using Windows 10/8/7, Windows Vista, Windows XP, and Mac OS X follow. A printer is also attached to the network and setup for printers is discussed later in the text.

- **Windows 10/8 Go to Control Panel > Network and Internet—Network and Sharing Center. Click Local Area Connection** and select **Properties**, and then click **Continue**. This opens the Local Area Connection Properties menu. Double-click **Internet Protocol Version 4 (TCP/IPv4)**. This opens the Properties menu. Now select **Use the following IP address**, enter the IP address and subnet mask, and click **OK**.

- **Windows 7:** Click **Start > Control Panel > Network and Internet—Network and Sharing Center**. Click **Local Area Connection** and select **Properties**, and then click **Continue**. This opens the Local Area Connection Properties menu. Double-click **Internet Protocol Version 4 (TCP/IPv4)**. This opens the Properties menu. Now select **Use the following IP address**, enter the IP address and subnet mask, and click **OK**.
- **Windows Vista:** Click **Start > Network Connection** or click **Start > Control Panel > Network and Sharing Center**. Right-click **Local Area Connection** and select **Properties**, and then click **Continue**. This opens the Local Area Connection Properties menu. Double-click **Internet Protocol Version 4 (TCP/IPv4)**. This opens the Properties menu. Now select **Use the following IP address**, enter the IP address and subnet mask, and click **OK**.
- **Windows XP:** To set the IP address in Windows XP, click **Start > Settings > Control Panel** and click **Network Connections**. Right-click **Local Area Connection**, and then click **Properties**. You should see the Local Area Connection Properties menu. Make sure the **TCP/IP** box is checked and the words **Internet Protocol TCP/IP** are highlighted (selected). Click the **Properties** button. You should now see the **Internet Protocol (TCP/IP) Properties** menu. At this point you must specify whether the IP address is to be obtained automatically or if you are to use a specified (static) address. For this example, click **Use the following IP address**. Type the desired IP address and subnet mask and select **OK**.
- **Mac OS X:** Click **Apple > System Preferences > Network**, and then click **Network Status** and select **Built-In Ethernet**. A new screen should appear and with the option **Configure IPv4**; select **Manually**. This option lets you manually set the IP address and subnet mask. Fields should now be displayed for inputting both the IP address and subnet mask. Enter the desired IP address and subnet mask, and select **Apply Now**.

The IP addresses and subnet mask being used in the office LAN example are listed in Table 1-7. The IP address for computer 1 is 10.10.10.1, and in this example, a subnet mask of 255.255.0.0 is being used. Chapter 6 examines subnet masking in detail. For now, leave the remaining fields empty; their purpose will be discussed later in the text. Your network configuration for computer 1 should now be complete. These steps are repeated for computers 2 and 3 in this LAN example.

Section 1-6 Review

This section has covered the following Network+ Exam objectives.

- 1.5 Install and properly terminate various cable types and connectors using appropriate tools

The popular RJ-45 plugs and jacks are introduced in this section. You will find this type of connector on all computer networks. Table 1-10 provides a good description of the common networking cable types.

1.7 Differentiate between network infrastructure implementations

This section introduces the basic steps for implementing a LAN (local area network).

5.3 Given a scenario, deploy the appropriate wired connectivity standard

The common numerics for Ethernet LAN cabling are listed in Table 1-10. This provides a good start for understanding the different types of cable used in Ethernet LANs.

5.4 Given a scenario, deploy the appropriate wired connectivity standard

Table 1-10 provides a good description of the common networking cable types.

5.8 Explain the basics of change management procedures

The first step in assembling an office LAN is to document the devices being connected to the network. It is easy to skip this step, but it is critical that good documentation be a priority.

Test Your Knowledge

1. The “X” on the input to a switch represents a router-only port.
 - a. True
 - b. False
2. A cross-connected input port indicates that
 - a. The transmit and receive pairs are crossed.
 - b. Is only used on connections to routers.
 - c. The cable is wired incorrectly.
 - d. Must be avoided on hub and switch port inputs.
3. A lit link light indicates that (select all that apply)
 - a. The Link Integrity Test is operational.
 - b. Link pulses are being shared by all devices in the LAN.
 - c. A 10Mbps data link has been established.
 - d. A 100Mbps data link has been established.
 - e. All of these answers are correct.

1-7 TESTING AND TROUBLESHOOTING A LAN

The critical next step in computer networking is to verify that the network has connectivity. The students should learn to do the following after the initial setup:

- Check the link lights at each end (if possible).
- Use the **ping** command to verify a link has been established.

The office network is small, and it should be easy for the student to verify connectivity. It is important that the student develop the habit of always confirming a network connection. This becomes critical when the network connections become more complex. The command structure of the **ping** command is presented as well as examples of replies and request timed-out messages.

When the network configurations on the computers are completed and the cable connections are in place, you will need to test and possibly troubleshoot the network. First, verify that the computers are properly connected on the network. Do this by verifying that you have link lights on each switch port that is connected to a computer or other networking device. Link verification will typically appear as a lit link light. An example of a switch with the link light activated is shown in Figure 1-30.

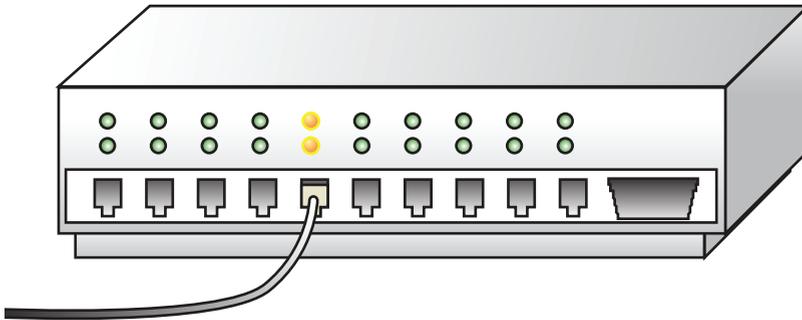


FIGURE 1-30 An example of the link light on a hub.

After you have verified that the networking devices are physically connected, use the **ping** command to verify that the networking devices are communicating. **Ping** uses **Internet Control Message Protocol (ICMP)** echo requests and replies to test that a device on the network is reachable. The ICMP protocol verifies that messages are being delivered. The **ping** command is available in the command window of Windows to verify the networking devices are communicating. The command structure for the **ping** command is as follows:

```
Usage ping[-t][-a][-n count][-l size][-f -i TTL][-v TOS] [-r count][-s
count]
[[-j host-list]:[-k host-list][-w timeout] destination-list
Options
-t                Ping the specified host until stopped
                  To see statistics and continue, type Control-Break
                  To stop, type Control-C
```

Ping

Command used to test that a device on the network is reachable

ICMP

Internet Control Message Protocol

```

-a          Resolve addresses to host-names
-n count   Number of echo requests to send
-l size    Send buffer size
-f         Set Don't Fragment flag in packet
-I
TTL        Time To Live v
TOS        Type Of Service
r count    Record route for count hops
s count    Timestamp for count hops
j host-list Loose source route along host-list
k host-list Strict source route along host-list
w timeout  Timeout in milliseconds to wait for each reply

```

For example, the command **ping 10.10.10.1** is used to ping the IP address for computer 1. The IP address 10.10.10.1 is the destination address. Another example would be the destination IP address for computer 3; in this case **ping 10.10.10.3** would be used. (Refer to Table 1-9 and Figure 1-26 for the IP addresses of the computers in our sample network.)

The following is an example of pinging another computer on the network to verify that the computers are communicating. In this example, computer 1 is used to ping computer 2. Remember, the **ping** command is executed from the command window.

```

ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Reply from 10.10.10.2: bytes 32 time<1ms TTL 128
Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

The text shows that 32 bytes of data are being sent to the computer with the IP address of 10.10.10.2. The “Reply from 10.10.10.2” indicates that computer 2 received the message. If the computer at IP address 10.10.10.2 did not respond, the message “**Request timed out.**” is displayed:

```

ping 10.10.10.2
Pinging 10.10.10.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 0, Lost= 4
(100% loss),

```

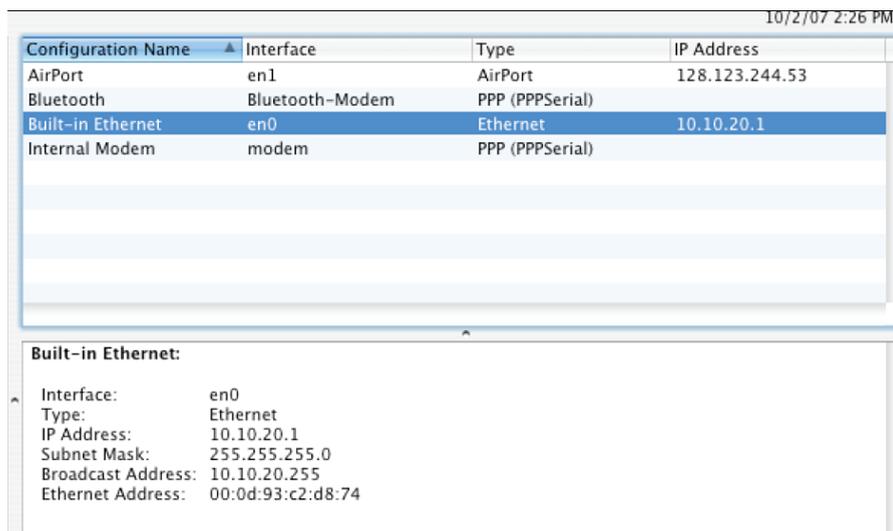
At times you might want to verify the IP address of the computer you are working on. Remember, a method of obtaining the IP address is to enter the command **ipconfig** at the command prompt. You don't need to include the **/all switch** after the **ipconfig** command unless you also want the MAC address information displayed. Figure 1-31 shows an example of displaying the IP address for computer 1.

ipconfig
Command used to display the computer's address

Windows IP Configuration

Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix .:
IP Address.....: 10.10.10.1
Subnet Mask.....: 255.255.0.0
Default Gateway

(a)



10/2/07 2:26 PM

Configuration Name	Interface	Type	IP Address
AirPort	en1	AirPort	128.123.244.53
Bluetooth	Bluetooth-Modem	PPP (PPPSerial)	
Built-in Ethernet	en0	Ethernet	10.10.20.1
Internal Modem	modem	PPP (PPPSerial)	

Built-in Ethernet:

Interface: en0
Type: Ethernet
IP Address: 10.10.20.1
Subnet Mask: 255.255.255.0
Broadcast Address: 10.10.20.255
Ethernet Address: 00:0d:93:c2:d8:74

(b)

FIGURE 1-31 (a) An example of displaying the IP address for computer 1 using the ipconfig command in Windows and (b) an example of the displayed IP address in Mac OS X for the built-in Ethernet connection.

Section 1-7 Review

This section has covered the following **Network+** Exam objectives.

4.1 Given a scenario, implement the following network troubleshooting methodology

*This section introduces the important step for verifying network connectivity using the **ping** command. Several examples of using **ping** to troubleshoot the network are presented.*

4.2 Given a scenario, analyze and interpret the output of troubleshooting tools

An important step in verifying connectivity between two networking devices is to issue the ping command using the destination IP address for the other. The ping command is available from the command window in Windows. Make sure you know how to issue the command and the options available with the command such as implementing continuous pinging and setting the buffer size.

Test Your Knowledge

1. The network administrator needs to verify a network connection. Which of the following steps should be taken? (Select two.)
 - a. Verify the link lights.
 - b. Use the **ping** command to verify network connectivity.
 - c. Perform an ARP request.
 - d. Ping the MAC address.
2. The **ping -t ip address** command (select all that apply)
 - a. Pings the host at the specified IP address until it is stopped.
 - b. Pings the MAC address of the host at the specified IP address.
 - c. Allows the **ping** to pass through routers.
 - d. Allows the **ping** command to be executed from the command prompt.

SUMMARY

This chapter introduced the basic concepts of computer networking. The technologies and techniques for assembling a computer network using the Ethernet protocol have been presented. The student should now understand the following major topics:

- The various LAN topologies
- The concept of CSMA/CD in the Ethernet protocol
- The structure of the Ethernet frame
- The purpose of the network interface card
- The purpose of the MAC address
- How to determine the MAC address for a computer
- The purpose and structure of the IP address
- The concept of private IP addresses
- The OSI Model
- The network topologies and technologies used to implement twisted-pair computer networks
- How to configure and verify a computer's IP address
- How to configure a home network and an office LAN
- The purpose of the link light
- The purpose of using *ping* to test a network connection

QUESTIONS AND PROBLEMS

Section 1-1

1. State whether the following network descriptions are describing a MAN, WAN, or LAN:
 - a. A network of users that share computer resources in a limited area
LAN
 - b. A network of users that share computer resources across a metropolitan area
MAN
 - c. A network that connects local area networks across a large geographic area
WAN

2. Expand the acronym *NIC*.
NIC (Network Interface Card)
3. Expand the acronym *MAC*.
MAC (Media Access Control)
4. Expand the acronym *LAN*.
LAN (Local Area Network)
5. Expand the acronym *WAN*.
WAN (Wide Area Network)

Section 1-2

6. Define the term *protocol*.
Protocol: Set of rules established for users to gain control of the network to exchange information
7. Define the term *topology*.
Topology: The architecture of a network
8. Define the term *deterministic*.
Deterministic: A way of providing access to a network by giving each network device a fixed time interval to access the network
9. A disadvantage of the Token Ring system is that if an error changes the token pattern, it can cause the token to stop circulating. This can be eliminated by adding which of the following?
 - a. Router
 - b. Multiport repeater
 - c. Token passer
 - d. Token Ring hub**
10. State the network topology being used in Figure 1-32 (Bus, Star, Ring, or Mesh).
 - a. Mesh
 - b. Bus
 - c. Ring
 - d. Star

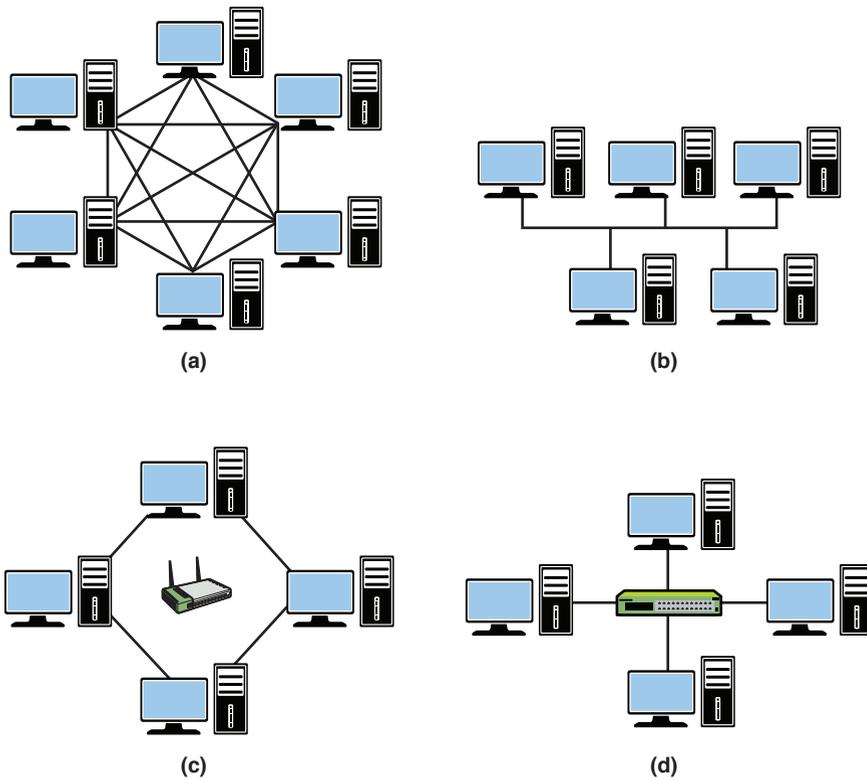


FIGURE 1-32 The networks for question 10.

11. What is the difference between a *hub* and a *switch*?

A hub replicates the data it receives to all devices connected to its ports. A switch forwards the data it receives directly to its destination address when its associated port is known.

Section 1-3

12. What are the seven layers of the OSI model?

1. Physical
2. Data link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

13. Which OSI layer is responsible for adding a header that includes routing information?
Network Layer
14. Which OSI layer is considered the media access control layer?
Data Link Layer
15. Which OSI layer combines messages or segments into packets?
Network Layer
16. What layer does a router work at?
Layer 3
17. Which OSI layer is responsible for the mechanical connection to the network?
Physical
18. The OSI layer responsible for data compression and encryption is which layer?
Presentation
19. TCP functions at what layer of the OSI model?
Layer 4: Transport
20. HTTP functions at what layer of the OSI model?
Layer 7: Application
21. IP and IPX are examples of protocols that operate in what layer of the OSI model?
Layer 3: Network
22. The network interface card operates at what layer of the OSI model?
Layer 1: Physical
23. Why are the layers of the OSI model important to the network administrator?
Knowledge of the OSI layers is used to help isolate a network problem.

Section 1-4

24. Define the acronym *CSMA/CD* and the protocol that uses *CSMA/CD*.
CSMA/CD: Carrier Sense Multiple Access / Collision Detection, Ethernet
25. What information is not included in an Ethernet frame?
 - a. **Frame size**
 - b. Source MAC address
 - c. Pad
 - d. Frame check sequence

26. What is the minimum size of the data payload in an Ethernet frame?

46 bytes

27. What is the minimum and maximum size of an Ethernet frame?

Minimum: 64 bytes

Maximum: 1518 bytes

28. Define the acronym *OUI*. Where is the OUI used?

OUI: Organizationally Unique Identifier. The OUI is found in the first 3 bytes of the MAC address.

29. What does the *OUI* represent?

The OUI identifies the manufacturer of the network device.

30. In Windows Vista or Windows XP, how would you find the Ethernet (MAC) address?

At the command line, type **ipconfig /all**.

31. INTERNET SEARCH: Find the device manufacturer for the following Ethernet devices:

a. 00-C0-4F-49-68-AB

Dell Computer Corporation

b. 00-0A-27-B7-3E-F8

Apple Computer, Inc.

c. 00-04-76-B6-9D-06

3Com Corporation

d. 00-00-36-69-42-27

Atari Corporation

32. State the class of address (A, B, or C) for the following IP addresses:

a. 46.39.42.05 ___A

b. 220.244.38.168 ___C

c. 198.1.0.4 ___C

d. 126.87.12.34 ___A

e. 99.150.200.251 ___A

f. 128.64.32.16 ___B

33. Expand the acronym *TCP/IP*.

TCP/IP: Transmission Control Protocol / Internet Protocol

Section 1-5

34. Cite the three advantages of a wired network.
 1. Faster network data transfer speeds within the LAN
 2. Relatively inexpensive to set up
 3. Network is not susceptible to outside interference
35. Cite three advantages of a wireless network.
 1. User mobility
 2. Simple installations
 3. No cables
36. What does it mean for a wireless networking device to be Wi-Fi compliant?

This means the wireless equipment is compliant with the 802.11x standards.
37. What are the most common types of equipment that are used to establish a broadband connection to the ISP?

Cable and DSL modems
38. Name six issues that should be considered when planning a home network?

Data speed, cost, ease of implementation, appearance, home access, and public access
39. Why is checking the lights of the networking device that connects to the ISP important?

Incorrect lights can indicate a connection problem with your cable modem, DSL modem, or your phone connection, or your ISP could be experiencing technical difficulties.
40. What is the purpose of a range expander?

This device relays the wireless signal from an access point or wireless router into areas with a weak signal or no signal at all.
41. What is a hotspot?

Limited geographic area that provides wireless access for the public
42. List five steps that can be used to protect the home network.
 1. Change the default factory passwords.
 2. Change the default SSID.
 3. Turn on encryption.
 4. Turn off the SSID broadcast.
 5. Enable MAC address filtering.
43. You have the choice of selecting a networking device with WEP and another with WPA. Which offers better security and why?

WPA offers stronger encryption and is supported with most new Wi-Fi systems.

44. What are the potential problems of using the default factory passwords?

Wireless equipment is shipped with default passwords that are set at the factory. These default settings are known by the public, including people who would like to gain access into your network and possibly change your settings.

45. What is the purpose of the SSID, and what can the network administrator do to protect the network from hackers who might have learned the SSID?

The SSID is the name used to identify your network and is used by your access point or wireless router to establish an association. Establishing an association means that a wireless client can join the network. The SSID can be up to 32 characters and should be changed often so hackers who have figured out your SSID will no longer have access to your home network.

46. What is the purpose of MAC filtering on a wireless network?

This can be used to select what devices can be allowed access to the network. When MAC address filtering is turned on, only wireless devices that have allowed MAC addresses will be granted access to the network.

47. How does NAT (Network Address Translation) help protect outsider access to computers in the home network?

The bad guy only sees the router because the IP addresses of the internal networking devices are not provided on the Internet. Only the IP address of the router is provided. The home network typically uses private address space that is not routable on the Internet. (Private IP addresses are blocked by the ISP.)

48. What is Stateful Packet Inspection?

This type of firewall inspects incoming data packets to make sure they correspond to an outgoing request. Data packets that are not requested are rejected.

49. What is a VPN, and how does it protect the data transferred over a wireless network?

VPN is virtual private networking. A VPN connection enables a remote or mobile user to access the network as if they were actually physically at the network. Additionally, the VPN connection is encrypted providing privacy for the data packets being transmitted.

50. How is IP addressing typically handled in a home network?

IP addressing for the home network is managed by the router or wireless router that connects to the ISP. The ISP will issue an IP address to the router from an available pool of IP addresses managed by the ISP. The computers in the home network are issued private IP addresses by the router.

51. What is Port Address Translation (PAT)?

PAT is a form of NAT that allows a single address to represent many inside hosts. A port number is attached to the network connection. This port number identifies the device that is establishing a connection to the Internet. This number is used when a data packet is returned to the home network. The port number identifies the device that established the Internet connection, and the router can deliver the data packet to the correct device.

52. A router on a home network is assigned an IP address of 128.123.45.67. A computer in the home network is assigned a private IP address of 192.168.10.62. This computer is assigned the public IP address 128.123.45.67:1922. Which IP address is used for routing data packets on the Internet? Is overloading being used?

The IP address 128.123.45.67:1922 will be used for routing the data packets on the Internet. Yes, overloading is being used because one routable IP address is being shared by the home network.

Section 1-6

53. Which of the following is not a step in building an office LAN?
- Obtaining proper government permits
 - Configuring the network settings
 - Connecting the devices together
 - Network documentation

54. What does *RJ-45* represent?

- A 45-pin connector for CAT6
- An IEEE standard for data speed
- An 8-pin modular connector for twisted pair Ethernet
- Protocol used to verify a communications link

55. What is an *uplink port*?

An uplink port is a port on a hub or switch that can be used as either a cross-connected or straight-through input. This is used to connect multiple hubs/switches together.

56. What is the maximum speed and length for Category 6 cabling?

CAT6 cable is capable of supporting a data rate of 1000 Mbps (or greater) over a distance of 100 meters.

57. What do the link lights on a hub represent?

The link lights indicate that the transmit and receive pairs of the cable are properly aligned.

58. What does *cross-connected* mean?

When the transmit and receive pairs on the CAT5 cable are crossed to properly align each for data communication, they are said to be cross-connected.

59. Documentation: Draw a network diagram similar to Fig 1-33 consisting of three computers, a switch, and a printer. Use the MAC addresses given in Table 1-9. Assign each network device an IP address from the private address space 192.168.5.x network. You are the network administrator and may choose the host address for each device.

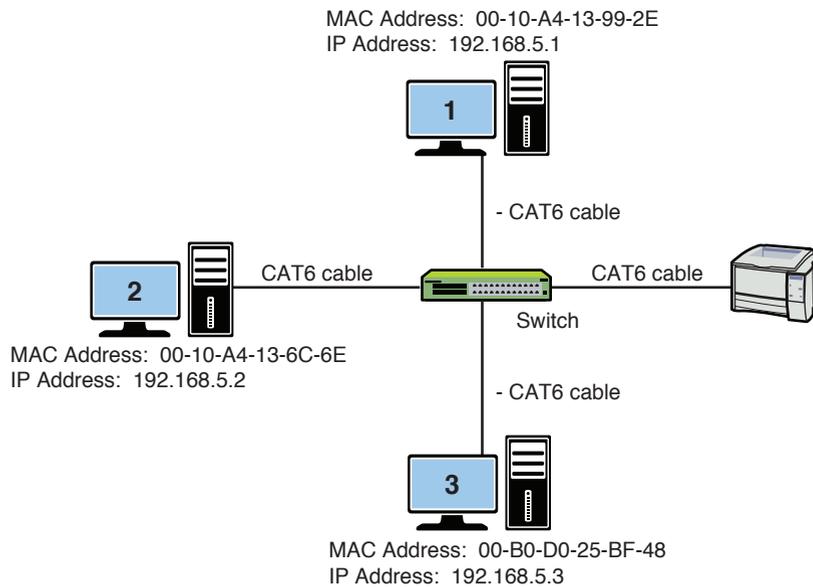


FIGURE 1-33 The sample network diagram for question 59.

Section 1-7

60. What command would you use to ping 10.3.9.42 indefinitely?

ping -t 10.3.9.42

61. What command would you use to ping 192.168.5.36 20 times with 1024 bytes of data?

ping -n 20 -l 1024 192.168.5.36

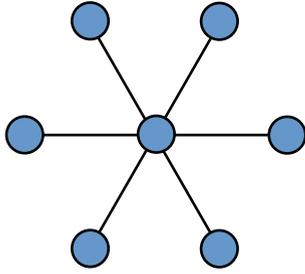
62. Expand the acronym *TTL*.

TTL: Time To Live

CERTIFICATION QUESTIONS

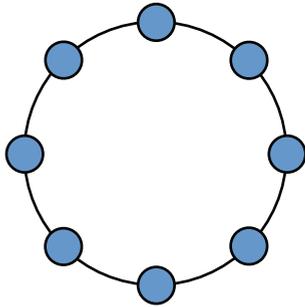
63. In terms of computer security, a switch offers better security than a hub. Why is this?
- a. A hub requires a special pin to activate the connection.
 - b. A hub forwards the data it receives to every device connected to the hub. It is possible for network devices to pick up data intended for a different device. A switch eliminates this by only forwarding data packets to the correct device whenever possible.
 - c. A switch forwards the data it receives to every device connected to the switch. It is possible for network devices to pick up data intended for a different device. A hub eliminates this by only forwarding data packets to the correct device whenever possible.
 - d. The use of the switch guarantees that all devices connected to it will share link integrity pulses. This sharing of the pulses strengthens the security of the connection.
64. What networking protocol does Ethernet use?
- a. Ethernet uses a token ring passing scheme. The computer devices must possess the ring to be able to pass a token.
 - b. Ethernet uses Carrier Access – Multiple Sensing / Collision Detection
 - c. Ethernet uses Carrier Sense – Multiple Access / Collision Detection
 - d. Ethernet uses Collision Sense – Carrier Access / Multiple Pairing
65. Network interface card has a MAC address of 00-00-86-15-7A. From this information, specify the OUI.
- a. There is not sufficient information to specify the OUI.
 - b. The OUI is 86-15-7A.
 - c. The OUI is 86-00-00
 - d. The OUI is 00-00-86
66. An IP address for an internal computer is assigned by
- a. the Internet Assigned Numbers Authority
 - b. the local network administrator
 - c. the user of the computer
 - d. Internet Address Numbers Authority

67. The topology shown is which of the following?



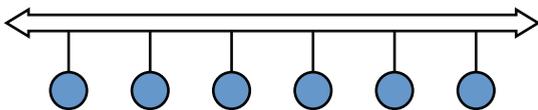
- a. star
- b. token-ring
- c. bus
- d. mesh
- d. None of these answers is correct.

68. The topology shown is which of the following?



- a. star
- b. token-ring
- c. bus
- d. mesh
- d. None of these answers is correct.

69. The topology shown is which of the following?



- a. star
- b. token-ring
- c. bus
- d. mesh
- d. None of these answers is correct.

70. The pad field in an Ethernet packet
- a. is used to bring the total number of bytes up to 46 if the data file is less than 46 bytes.
 - b. is used to bring the total number of bytes up to 64 if the data file is less than 64 bytes.
 - c. is not required with CSMA/CD.
 - d. provides grouping of the information for transmission.
71. The IP address 10.10.20.250 is an example of (select all that apply)
- a. class A address.
 - b. class B address.
 - c. a private IP address.
 - d. a routable IP address.
 - e. a nonroutable Internet IP address.
72. An Intranet is (select all that apply)
- a. uses class E addressing.
 - b. used in high speed (gigabit) Ethernet.
 - c. an internal network that provides file and resource sharing.
 - d. enables Fast Ethernet connections.
 - e. not typically accessed from the Internet



2

CHAPTER

PHYSICAL LAYER CABLING: TWISTED PAIR

CHAPTER OUTLINE

2-1 Introduction
2-2 Structured Cabling
2-3 Unshielded Twisted-Pair Cable
2-4 Terminating CAT6/5e/5 UTP Cables
2-5 Cable Testing and Certification

2-6 10 Gigabit Ethernet over Copper
2-7 Troubleshooting Cabling Systems
Networks
Summary
Questions and Problems

OBJECTIVES

- Describe the six subsystems of a structured cabling system
- Define horizontal cabling
- Define UTP and STP
- Define the categories of UTP cable
- Describe the difference in the T568A and T568B wire color order
- Describe the procedure for placing RJ-45 plugs and jacks on twisted-pair cable
- Describe how to terminate twisted-pair cable for computer networks
- Define the basic concepts for planning a cable installation for an office LAN
- Describe the procedure for certifying a twisted-pair cable for CAT6 and CAT5e
- Describe the issues of running 10 gigabit Ethernet over copper
- Describe the basic steps for troubleshooting cable problems

KEY TERMS

physical layer	MDF (Main Distribution Frame or Main Equipment Room)	full duplex
EIA	CD (Campus Distributor)	gigabit Ethernet
TIA	BD (Building Distributor)	CAT7/7a and CAT6a
campus network	FD (Floor Distributors)	10GBASE-T
EIA/TIA 568-B	workstation or work area outlet (WO)	STP
building entrance	TO (telecommunications outlet)	EMI
entrance facilities (EF)	terminated	T568A
equipment room (ER)	8P8C	T568B
telecommunications closet	patch cable	color map
TR	UTP	TX
backbone cabling	CAT6/6a	continues
horizontal cabling	CAT5/e	RX
TCO	balanced mode	straight-through cable
work area	FastEthernet	wire-map
main cross-connect (MC)	network congestion	crossover cable
intermediate cross-connect (IC)	bottlenecking	link
cross-connect		full channel
horizontal cross-connect (HC)		attenuation (insertion loss)

near-end crosstalk (NEXT)	10GBASE-T
crosstalk	pair data
power sum NEXT (PSNEXT)	Alien Crosstalk (AXT)
equal level FEXT (ELFEXT)	PSANEXT
PSELFEXT	PSAACRF
ACR	F/UTP
PSACR	TCL
return loss	ELTCTL
propagation delay	LCL
nominal velocity of propagation (NVP)	TCTL
delay skew	PSANEXT
IEEE 802.3an-2006	PSAACRF
10GBASE-T	multilevel encoding
	hybrid echo cancellation circuit

This chapter examines the twisted-pair media used to link computers together to form a local area network (LAN). This is called **physical layer** cabling. The term *physical layer* describes the media that interconnects networking devices. The objective of this chapter is for the reader to gain an introductory understanding of the cable media including the category types, the steps for terminating cables, cable testing, certification, and troubleshooting. The main focus is on the use of UTP cable in computer networks, although an overview of shielded twisted-pair (STP) is presented. Fiber-optic cables are playing an important role in modern computer networks and are not overlooked in this text. This media is thoroughly examined in Chapter 3, “Physical Layer Cabling: Fiber Optics.”

Other types of cabling you might encounter in computer networking are RG-6 and possibly RG-59. These types of cables are called *coaxial cables* and are primarily used to connect satellite systems or cable television and modems. Cable terminations for these types of cable include “F-type” and BNC connectors.

2-1 INTRODUCTION

The network physical layer is introduced here in Chapter 2. Unshielded twisted-pair (UTP) cable is examined in detail, and material is included on how to terminate the UTP cable. A critical area for cable installation and testing is certifying that the cable passes CAT5e tests. CAT5e certification based on the Fluke DTX-LT Cable Analyzer tester is discussed. This chapter focuses on CAT5e. The specifications for CAT6 cable is mentioned, but the emphasis is on CAT5e. Feel free to send an email message to Jeff Beasley at jbeasley@nmsu.edu if you need an update for the text that focuses on CAT6 or any other cable standards. I will be preparing this for my computer networking class and will be happy to share this information with you.

This chapter begins with an overview of the concept of structured cabling. This section defines the six subsystems of a structured cabling system and focuses on the basic issues associated with horizontal cabling or wiring a LAN. Next, the basic operational characteristics of UTP cable are examined. The discussion includes an examination of the various categories of UTP cable currently available. Following that is an overview of constructing twisted-pair patch and horizontal link cabling. The tools and techniques for properly terminating UTP cabling for both CAT6 and CAT5e are presented. An introduction to testing and certifying CAT6 and CAT5e cables follows. This section includes several examples of cable test data and how to interpret the test results. The chapter concludes with a section on troubleshooting computer networks, with a focus on cable or physical failures.

Table 2-1 lists and identifies, by chapter section, where each of the CompTIA Network+ objectives is presented in this chapter. At the end of each chapter section is a review with comments of the Network+ objectives presented in that section. These comments are provided to help reinforce the reader’s understanding of a particular Network+ objective. The chapter review also includes “Test Your Knowledge”

Physical Layer

Describes the media that interconnects networking devices

questions to aid in the understanding of key concepts before the reader advances to the next section of the chapter. The end of the chapter includes a complete set of question plus sample certification type questions.

TABLE 2-1 Chapter 2 CompTIA Network+ Objectives

Domain/Objective Number	Domain/Objective Description	Section Where Objective Is Covered
1.0	Network Architecture	
1.5	Install and properly terminate various cable types and connectors using the appropriate tools	2-1, 2-2, 2-3, 2-4, 2-7
2.2	Given a scenario, analyze metrics and reports from monitoring and tracking performance tools	2-3
3.4	Compare and contrast physical security controls	2.2, 2-3
4.2	Given a scenario, analyze and interpret the output of troubleshooting tools	2-5
4.4	Given a scenario, troubleshoot and resolve common copper cable issues	2-4, 2-5, 2-7
5.4	Given a scenario, deploy the appropriate wired connectivity standard	2-2, 2-4

2-2 STRUCTURED CABLING

This section defines the six subsystems of a structured cabling system. The student should be able to identify the purpose of each layer. The focus of the chapter is on the issues associated with horizontal cabling.

The first major standard describing a structured cabling system for computer networks was the TIA/EIA 568-A in 1995. **EIA** is the Electronics Industries Alliance, a trade organization that lobbies for the interests of manufacturers of electronics-related equipment. **TIA** stands for the Telecommunications Industry Association, which is a trade organization that represents the interests of the telecommunications industry. The most important addendum to the EIA/TIA 568-A standard was Addendum 5, published in 1999. This addendum defined the transmission performance specifications for 4-pair 100-ohm category 5e twisted-pair cabling. TIA/EIA adopted new category 6 (CAT6) cable specifications in June 2002. This is the type of cabling recommended for use in today's computer networks, although CAT7 twisted-pair cabling might soon become the recommended standard.

EIA

Electronic Industries Alliance

TIA

Telecommunications Industry Association

The EIA/TIA 568-A standard defined the minimum requirements for the internal telecommunications wiring in buildings and between structures in a **campus network**. A campus network consists of interconnected LANs within a limited geographic area such as a college campus, military base, or group of commercial buildings. The EIA/TIA 568-A was revised and updated many times, and in 2000 a new standard—the **EIA/TIA 568-B**—was published. The three parts of the EIA/TIA 568-B are as follows:

- **EIA/TIA-568-B.1:** Commercial Cabling Standard, Master Document
- **EIA/TIA-568-B.2:** Twisted-pair Media
- **EIA/TIA-568-B.3:** Optical Fiber Cabling Standard

Within the EIA/TIA 569B Commercial Standard for Telecommunication Pathways and Spaces are guidelines defining the six subsystems of a structured cabling system:

1. **Building entrance:** The point where the external cabling and wireless services interconnect with the internal building cabling in the equipment room. This is used by both public and private access (for example, Telco, satellite, cable TV, security, and so on). The building entrance is also called the **entrance facilities (EF)**. Both public and private network cables enter the building at this point, and typically each has separate facilities for the different access providers.
2. **Equipment room (ER):** A room set aside for complex electronic equipment such as the network servers and telephone equipment.
3. **Telecommunications closet:** The location of the cabling termination points that includes the mechanical terminations and the distribution frames. The connection of the horizontal cabling to the backbone wiring is made at this point. This is also called the telecommunications room (**TR**) or telecommunications enclosure (TE). In some older systems, the network administrator might encounter two of the following types of punchdown blocks in the telecommunications closet: a **66** block and a **110** block. These types of terminations use insulation-displacement connectors (IDC) to terminate twisted-pair cables and are commonly used in telephone systems but not computer networks.

Note

One room can serve as the entrance facility, equipment room, and the telecommunications closet.

4. **Backbone cabling:** Cabling that interconnects telecommunication closets, equipment rooms, and cabling entrances in the same building and between buildings.

Campus Network

Interconnected LANs within a limited geographic area

EIA/TIA 568-B

The standard that defines the six subsystems of a structured cabling system

Building Entrance

The point where the external cabling and wireless services interconnect with the internal building cabling

Entrance Facilities (EF)

A room set aside for complex electronic equipment

Equipment Room (ER)/Backbone Cabling

Cabling that interconnects telecommunication closets in the same building and between buildings

Telecommunications Closet

The location of the cabling termination points that includes the mechanical terminations and the distribution frames

TR

Another name for the telecommunications closet

Horizontal Cabling

Cabling that extends out from the telecommunications closet into the LAN work area

TCO

Telecommunications outlet

Work Area

The location of the computers and printers, patch cables, jacks, computer adapter cables, and fiber jumpers

Main Cross-connect (MC)

Usually connects two or more buildings and is typically the central telecommunications connection point for a campus or building. It is also called the main distribution frame (MDF) or main equipment room. The MC connects to Telco, an ISP, and so on. Another term for the MC is the campus distributor (CD).

Intermediate Cross-connect (IC)

Also called the building distributor (BD), this is the building's connection point to the campus backbone. The IC links the MC to the horizontal cross-connect (HC).

5. **Horizontal cabling:** Cabling that extends out from the telecommunications closet into the LAN work area. Typically, the horizontal wiring is structured in a star configuration running to each area telecommunications outlet (TCO). This is the wall plate where the fiber or twisted-pair cable terminates in the room. In some cases, the TCO terminates telephone, fiber, and video in addition to data into the same wall plate.
6. **Work area:** The location of the computers and printers, patch cables, jacks, computer adapter cables, and fiber jumpers.

Figure 2-1 provides a drawing of the structure for a telecommunications–cabling system. In the figure, it shows the connection of the carriers (Telco, ISP, and so on) coming into the ER. The ER is the space set aside for the carrier's equipment contained in the **main cross-connect (MC)** or **intermediate cross—connect (IC)**. The EF consists of the cabling, connector hardware, protection devices that are used as the interface between any external building cabling, and wireless services with the equipment room. This area is used by both public and private access providers (for example, Telco, satellite, cable TV, security, and so on). The ER and EF space is typically combined with the MC equipment room.

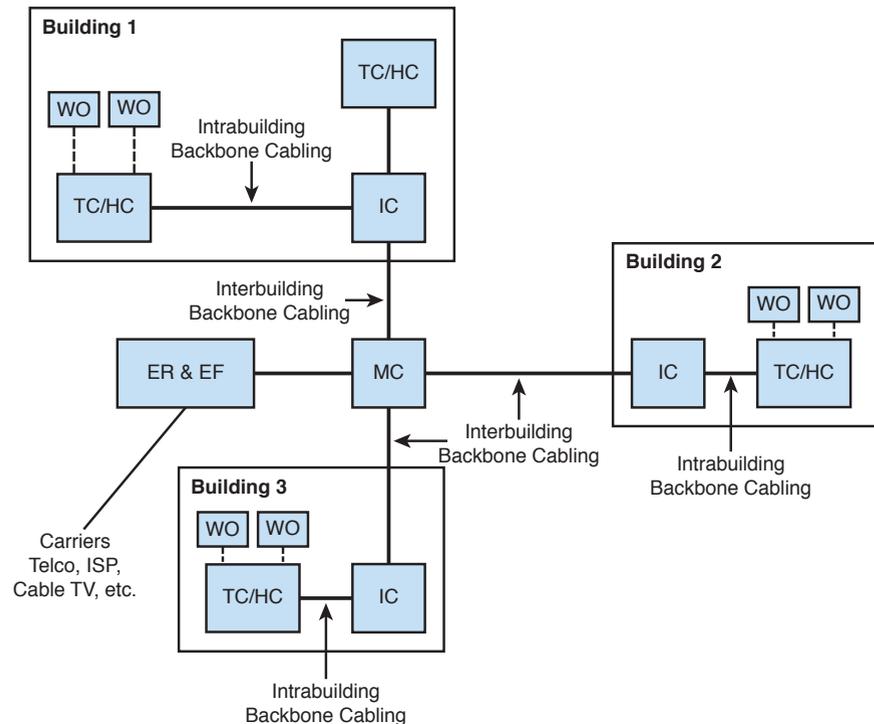


FIGURE 2-1 The telecommunications Cabling System Architecture.

Between the MC and the IC are the campus backbone cabling (listed as the inter-building backbone cabling). This defines the connections between the MC and IC. A definition of a **cross-connect** is a space where you are going to take one or multiple cables and connect them to one or more cables or equipment. For example, you could be bringing in 60 UTP cables, with 50 that are cross-connected to a switch and 10 that are cross-connected to a backbone cable going to another location. Typical connections between the MC and IC are single-mode and multimode fibers and possibly coax for cable TV, although most installations are migrating to fiber. The building backbone cabling (intrabuilding backbone cabling) makes the connection between the IC and the TC/HC. TC is the telecommunications closet, and HC is the **horizontal cross-connect (HC)**. Usually this connection is CAT5 UTP or better, or possibly single- or multimode fiber or some combination. Fiber is the best choice for making these connections, although copper is sometimes used. The horizontal cabling is the cabling between the HC and the work area. It is usually CAT5 UTP or better or fiber. The standard currently specifies CAT6. Fiber is gaining acceptance for connecting to the **work area outlets (WO)**.

Figure 2-2 provides a more detailed view of the cabling from the MC to the IC and the HC. This drawing shows the three layers of the recommended backbone hierarchy cabling for a computer network. The first level of the hierarchy is the MC. The MC connects to the second level of the hierarchy, the IC. The backbone cabling connects the MC to the IC and the IC to the TC/HC. The HC connects the horizontal cabling to the work area and to the WO.

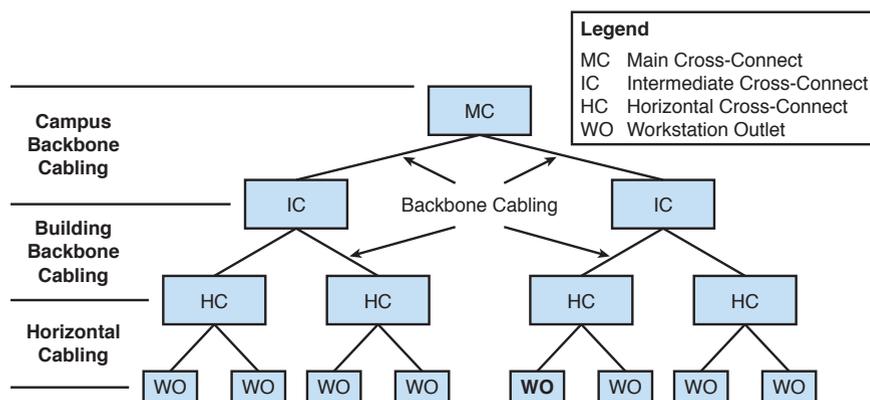


FIGURE 2-2 The Campus Network Hierarchical topology.

The focus of this chapter is on the issues associated with the horizontal cabling and the work area (LAN) subsystems. The text addresses all six subsystems of a structured cabling system, but at the point when the networking concepts and related hardware are introduced. Many of the concepts covered in each structured cabling subsystem require that the reader have a firm grasp of basic networking to gain a full appreciation of how each network piece fits into a structured cabled system.

Cross-connect

A space where you are going to take one or multiple cables and connect them to one or more cables or equipment

Horizontal Cross-connect (HC)

The connection between the building distributors and the horizontal cabling to the work area or workstation outlet—another term used for the HC is the floor distributors (FD)

Workstation or Work Area Outlet (WO)

Also called the TO (telecommunications outlet), it's used to connect devices to the cable plant. The cable type typically used is CAT3, CAT5, CAT5e, CAT6, CAT6A, and various coaxial cables. Devices typically connected to these outlets are PCs, printers, servers, phones, televisions, and wireless access points.

Horizontal Cabling

Permanent network cabling within a building is considered to be *horizontal cabling*, defined as the cabling that extends out from the telecommunications closet into the LAN work area. Take time to plan for your horizontal cabling installation because this is where your network interfaces with the users. There is always a substantial installation cost associated with horizontal cabling, and there is an even greater cost of having to replace or upgrade a cable installation. You don't want to have to re-cable your system very often. Careful attention should be given to planning for the horizontal cabling of a LAN. Make sure you fully understand your current networking needs and that your proposed plan meets the needs. Also make sure your plan addresses the future needs and growth of your network.

Figure 2-3 illustrates the basic blocks of a horizontal cabling system from the telecommunications closet to the computer in the LAN. The following components are typically found in the telecommunications closet:

- A. Backbone cabling interconnecting this closet with other closets
- B. Switch or hub
- C. Patch panels
- D. Patch cables
- E. Cabling to the LAN (horizontal cabling)
- F. Wall plate
- G. Patch cable connecting the computer to the wall plate

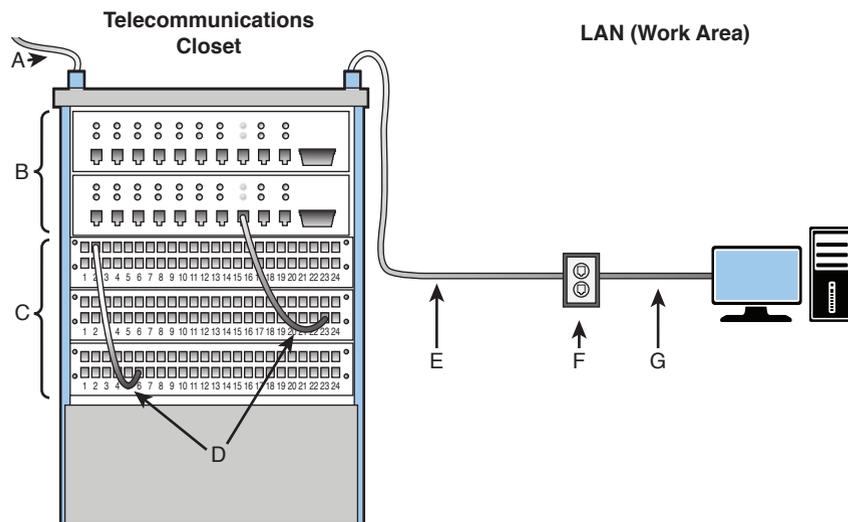


FIGURE 2-3 Block diagram of a horizontal cabling system.

Item E in Figure 2-3 shows the cabling leaving the telecommunications closet. The cable extends to where it is **terminated** at the wall plate (item F) in the LAN or work area. The term *terminated* describes where the cable connects to a jack in a wall plate, a patch panel, or an RJ-45 modular plug. In this case, the cable terminates into an RJ-45 jack in the wall plate. Figure 2-4 provides an example of the RJ-45 wall plate and patch panel.

Note

The proper term for the RJ-45 modular plug used in computer systems is actually **8P8C** for both male and female connectors. 8P8C stands for 8-pin 8-conductors and is defined by ANSI/TIA-968-A and B but is commonly called RJ-45 by both professionals and end users.

An individual cable is used to connect each connector in the outlet to the patch panel in the telecommunications closet (F to E). RJ-45 (8P8C) plugs and jacks are defined in section 2-4. Another 8-pin connector using the 8P8C modular connector is the RJ-48. This type of connector is commonly used in T1 data lines. This type of connector typically uses shielded twisted-pair cabling. Although the RJ-45 and RJ-48 connectors look similar, they do not use the same wiring scheme and are intended for different data-transmission applications.

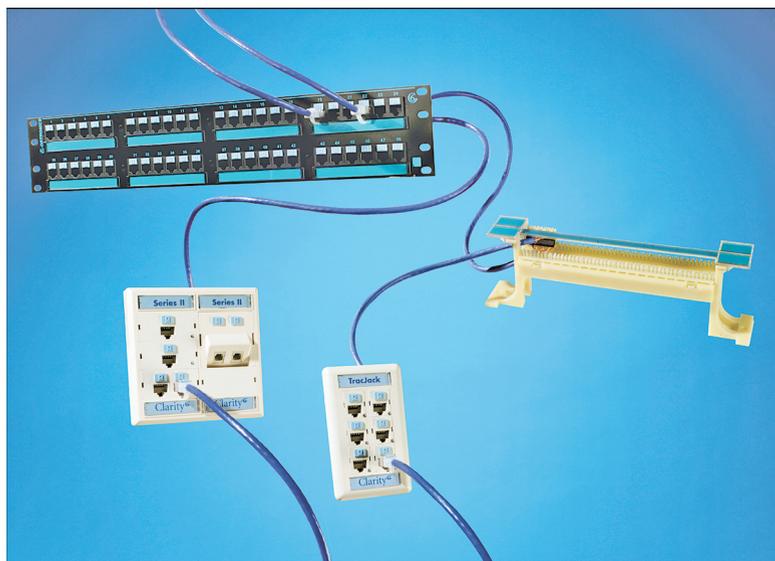


FIGURE 2-4 The Ortronics clarity twisted-pair system (courtesy of Ortronics).

In a star topology, there is an individual cable run for each outlet in the wall plate. This means that you assign one computer to each terminated outlet. A **patch cable** (item G) is used to make the physical connection from the computer to the wall plate, as shown in Figure 2-3. A patch cable is a short cable used to make the physical connection between networking equipment. There is a 100-meter overall length limitation of the cable run from the telecommunications closet to the networking device in the work area. This includes the length of the patch cables at each end (items D and G) plus the cable run (item E). A general rule of thumb is to allow

90 meters for the cable run from the telecommunications closet to the work area (item E). This allows 5 meters of cable length for the work area and 5 meters for the patch cables in the telecommunications closet (item D) and the work area (item G). Figure 2-5 shows an example of the insides of a telecommunications closet.



FIGURE 2-5 Inside a telecommunications closet.

Section 2-2 Review

This section has covered the following **Network+** Exam objectives:

1.5 Install and properly terminate various cable types and connectors using the appropriate tools

The termination of computer cabling associated with a horizontal cabling systems has been presented.

3.4 Compare and contrast physical security controls

This section has provided a through overview of the purpose and function of the telecommunications closet. Figure 2-5 shows an example of the interior of a telecommunications closet.

5.4 Given a scenario, deploy the appropriate wired connectivity standard

The standard that defines structure cabling, the EIA/TIA 568 standard, has been introduced. This is an important standard defining cabling for computer networks.

Test Your Knowledge

1. What is the overall length limitation of a UTP cable run from the telecommunications closet to a networking device in the work area?
 - a. 10 meters
 - b. 100 meters
 - c. 10K meters
 - d. 100K meters
2. The six subsystems of a structured cabling system are the following:
 - Building Entrance
 - Equipment Room
 - Backbone Cabling
 - Telecommunications Closet
 - Vertical Cabling
 - Work AreaTrue or False?
3. Horizontal cabling consists of which of the following basic blocks? (Select two.)
 - a. Switch or hub
 - b. Routers
 - c. Backbone cabling
 - d. Patch panel

2-3 UNSHIELDED TWISTED-PAIR CABLE

UTP (unshielded twisted-pair) cable is an important physical layer component in modern computer networks. The chapter focuses on CAT 5e cable. Many networks are incorporating the use of CAT6 in their installations. The chapter lists the CAT6 specifications, but the fundamental issues are still the same as CAT5e. Many networks are already wired with CAT5/5e, and some new network connections are installing CAT6 just in case. CAT6 provides improved network performance, and the student should be made aware of this.

The main difference between CAT5e and CAT6 is with the transmission performance. The bandwidth increases from 100MHz to 200MHz, and the specifications provide for better noise performance that will enable increased data rates. Most new installations are specifying CAT6 cable. This is a good recommendation because it is always important to use the best cable available for an installation as long as the additional cost is justified. CAT6 specifications require that patch cables be precisely manufactured to maintain CAT6 performance. Also, CAT6 connectors look the same as CAT5e, but they do have significantly different performance specifications. The installation steps presented here are presented for terminating both CAT6 and CAT5e.

A good task would be for the students to prepare a report on CAT6/6a/7 cable, connectors, hardware, and testing. This would be a way for the students to become aware of the latest development with twisted-pair cable.

Unshielded twisted-pair (**UTP**) cable plays an important role in computer networking. The most common twisted-pair standards used for computer networking today are category 6 (**CAT6**), category 6a (**CAT6a**), and category 5e (**CAT5e**). CAT6 cable is tested to provide the transmission of data rates up to 1000Mbps for a maximum length of 100 meters. CAT6a is an improved version of CAT6 and will support 10GB Ethernet.

CAT5e cable is an enhanced version of CAT5 and provides improved performance requirements of the cable. CAT6 provides improved performance and a bandwidth of 250MHz. CAT5/5e twisted-pair cable contains four color-coded pairs of 24-gauge wires terminated with an RJ-45 (8P8C) connector. Figure 2-6 provides an example of a CAT5e cable terminated with an RJ-45 (8P8C) modular plug. CAT6 twisted-pair cable also contains four color-coded wires, but the wire gauge is 23AWG. CAT6 cable has a stiffer feel compared to CAT5e.

The precise manner in which the twist of CAT6/5e/5 cable is maintained, even at the terminations, provides a significant increase in signal transmission performance. CAT5/5e standards allow 0.5 inches of untwisted cable pair at the termination. CAT6 has an even tighter requirement that allows for only 3/8-inch of untwisted cable at the termination. The termination is the point where the cable is connected to terminals in a modular plug, jack, or patch panel.

CAT6/5e/5 twisted-pair cable contains four twisted wire pairs for a total of eight wires. In twisted-pair cable, none of the wires in the wire pairs are connected to ground. The signals on the wires are set up for a high (+) and low (-) signal line. The (+) indicates that the phase relationship of the signal on the wire is positive, and the (-) indicates that the phase of the signal on the wire is negative; both signals are relative to a virtual ground. This is called a **balanced mode** of operation—the balance of the two wire pairs helps maintain the required level of performance in terms of crosstalk and noise rejection.

Balanced Mode

Neither wire in the wire pairs connects to ground



FIGURE 2-6 An example of an RJ-45 modular plug (courtesy of Cyberguys.com).

Table 2-2 lists the various categories of twisted-pair cable defined by the EIA/TIA 568B standard. The table includes an application description and minimum bandwidth for each category. Notice that there is not a listing for CAT1 and CAT2.

TABLE 2-2 Different Categories for Twisted-pair Cable, Based on TIA568B

Category	Description	Bandwidth/Data Rate
Category 3 (CAT3)	Telephone installations Class C	Up to 16Mbps
Category 5 (CAT5)	Computer networks Class D	Up to 100MHz/100Mbps 100-m length
Enhanced CAT5 (CAT5e)	Computer networks	100MHz/1000Mbps applications with improved noise performance in a full duplex mode
Category 6 (CAT6)	Higher-speed computer	Up to 250MHz networks Class E/1000Mbps CAT6 supports 10Gbps but at distances fewer than 100 meters
Category 6a (CAT6a)	Increased bandwidth	Up to 500MHz networks Class Ea/10Gbps
Category 7 (CAT7)	International Organization for Standardization (ISO) standard, not an EIA/TIA standard	Up to 600MHz speed computer networks Class F/10Gbps
Category 7a (CAT7a)	ISO standard, not an EIA/TIA standard	Up to 1000MHz speed computer networks Class FA/10Gbps

FastEthernet

An Ethernet system operating at 100Mbps

Network Congestion

A slowdown on network data traffic movement

Bottlenecking

Another term for network congestion

Full Duplex

Computer system can transmit and receive at the same time

Gigabit Ethernet

1000Mbps Ethernet

CAT7/7a and CAT6a

UTP cable standards that support 10GB data rates for a length of 100 meters

10GBASE-T

10GB over twisted-pair copper

STP

Shielded twisted pair

EMI

Electromagnetic interference

CAT1 and CAT2 cable specifications are not defined in the EIA/TIA 568B standard. The first CAT or category specification is for CAT3. CAT3 is being replaced with CAT5e or better. CAT4 is not listed in the table because the category was removed from the TIA568B standard as its data capacity specification was outdated. The category 5 cable standard was established in 1991, and many computer networks are still using the older CAT5 cables. Certified CAT5 cabling works well in both Ethernet and FastEthernet networking environments that run 10Mbps Ethernet and 100Mbps FastEthernet data rates. Note that the term **FastEthernet** is used to describe the 100Mbps data rate for FastEthernet networks.

In some cases, users on networks are experiencing **network congestion** or **bottlenecking** of the data due to the increased file transfer sizes and the limited bandwidth of their network. These terms describe excessive data traffic that is slowing down computer communications even in FastEthernet networks. Basically, the demands on the network exceeded the performance capabilities of the CAT5 cable. The slowdown of the data is of major concern in computer networks. File access time is delayed, productivity is affected, and the time required to complete a task is increased. A slowdown in your network could be costing your company money. Can you imagine the consequences if a slowdown in your network causes a delay in the company's billing?

TIA/EIA ratified the CAT5e cabling specification in 1999 to address this continuing need for greater data handling capacity in the computer networks. The enhanced CAT5 cable (CAT5e) provides an improvement in cable performance, and if all components of the cable installation are done according to specification, then CAT5e will support **full duplex gigabit Ethernet** (1000Mbps Ethernet) using all four wire pairs. Full duplex means that the computer system can transmit and receive at the same time. TIA/EIA ratified the CAT6 cabling specification in June 2002. This cable provides an even better performance specification and 250MHz of bandwidth, and maintains backward compatibility with CAT5/5e. CAT6 can support 10Gbps data rates but over a distance less than 100 meters. The **CAT6a** standard supports 10GBGB data rates up to 100 meters, and **CAT7** will also support 10Gbps up to 100 meters with improved bandwidth. The 10GBGB standard over copper is called **10GBASE-T**.

Shielded Twisted-Pair Cable

In some applications, a wire screen or metal foil shield is placed around the twisted-pair cable. Cable with the addition of a shield is called **STP** cable. The addition of this shield reduces the potential for electromagnetic interference (**EMI**) as long as the shield is grounded. EMI originates from devices such as motors and power lines and from some lighting devices such as fluorescent lights.

The shield on the twisted-pair cable does not reject all potentially interfering noise (EMI), but it does greatly reduce noise interference. There is an active debate in the networking community as to which product is superior, UTP or STP. It is important to note that the objective of both cables is to successfully transport data from the telecommunications closet to the work area. Industry testing on STP cable has shown that the addition of a shield does increase the usable bandwidth of the cable by increasing the noise rejection between each of the wire pairs. However, the tests have shown that there is not a significant advantage of placing a shield over a properly installed 4-pair 100-ohm UTP cable. Additionally, STP is more expensive and the increased costs may not justify the benefits. For now, most manufacturers are recommending the use of UTP cable for cabling computer networks except for very noisy environments.

Section 2-3 Review

This section has covered the following **Network+** Exam objectives:

- 1.5 Install and properly terminate various cable types and connectors using the appropriate tools

The RJ-45 modular plug used in most computer networks has been presented. The RJ-45 plug is also called 8P8C. Table 2-2 lists the different categories for twisted-pair cable, based on TIA568B. Make sure you know the different category types. You should also understand that the precise manner in which the twist of the wire pairs is managed provides for a significant increase in signal transmission performance.

- 2.2 Given a scenario, analyze metrics and supports from monitoring and tracking performance tools

This section introduced the concept of network congestion or bottlenecking of the data due to the increased file transfer sizes and the limited bandwidth of the network. Selecting the proper UTP cable can help minimized this problem.

Test Your Knowledge

1. What is the data rate for FastEthernet?
 - a. 10Mbps
 - b. 100Mbps
 - c. 1000Mbps
 - d. 10Kbps
 - e. None of these answers is correct.
2. What type of cable is currently recommended for LAN work areas?
 - a. Shielded twisted-pair
 - b. CAT6 shielded twisted-pair
 - c. CAT 5e UTP
 - d. CAT6 UTP
 - e. CAT7 UTP
3. What is the benefit of shielded twisted-pair cable?
 - a. Ease of installation
 - b. Excellent EMI protection
 - c. Less expensive
 - d. Preferred by industry for all installations
 - e. None of these answers is correct.

2-4 TERMINATING CAT6/5E/5 UTP CABLES

This section introduces the techniques for terminating high-performance UTP cables. Important concepts, such as the wiring schemes for T568A and T568B, are presented. The topic of straight-through and crossover cables is presented. The student should understand the relationship of properly aligning the TX and RX pairs and the link light. The section concludes with the steps for terminating twisted-pair cable with RJ-45 (8P8C) connectors.

This section introduces the techniques for terminating high-performance UTP cables. Terminating the RJ-45 (8P8C) connector for CAT6/5e/5 cable is defined by the EIA/TIA standard EIA/TIA568-B.2 and B.2-1. This portion of the standard defines the specifications of the copper cabling hardware. The standard specifies cabling components, transmission, system models, and the measurement procedures needed for verification of the balanced twisted-pair cabling.

Within the EIA/TIA568B standard are the wiring guidelines **T568A** and **T568B**. These wiring guidelines specify the color of wire that connects to which pin on the connector. The specification of the wire color that connects to which pin is called a **color map**. Table 2-3 provides the color maps specified by the T568A and T568B wiring guidelines.

T568A

Wire color guidelines specified under the EIA/TIA568B standard

T568B

Wire color guidelines specified under the EIA/TIA568B standard

Color Map

The specification of which wire color connects to which pin on the connector

TABLE 2-3 The Wiring Color Schemes for T568A and T568B

Pin #	568A Wire Color	568B Wire Color
1	White-Green	White-Orange
2	Green	Orange
3	White-Orange	White-Green
4	Blue	Blue
5	White-Blue	White-Blue
6	Orange	Green
7	White-Brown	White-Brown
8	Brown	Brown

Figure 2-7(a) shows the placement of the wire pairs in the RJ-45 (8P8C) modular plug for the T568A standard; Figure 2-7(b) shows the placement of the wire pairs in the RJ-45 (8P8C) modular plug for the T568B standard. The pin numbers for the RJ-45 (8P8C) modular plug are shown at the top of the figure, and a wire color table is provided for reference. In the T568A wire color scheme (Figure 2-7[a]), a white-green wire connects to pin 1, the wire color green connects to pin 2, the wire color connected to pin 3 is white-orange, and so on. Similar information is provided in Figure 2-7(b) for the T568B wiring standard. The color of the wire connected to pin 1 is white-orange, pin 2 is orange, pin 3 is white-green, and so on. This information also agrees with Table 2-2.

A common question is, “What is the difference between T568A and T568B?” Basically, these are just two different manufacturer standards used to wire the modular connector hardware. There is not a performance improvement with either, just a color order choice. Industry tends to favor the T568A wiring order; however, either order can be used as long as the order is maintained throughout the network.

This material has defined the wire color order for terminating the RJ-45 (8P8C) plugs and jacks onto the CAT6/5e twisted-pair cables. Be able to describe the difference between the T568A and T568B wire color order. Also make sure you know what wire color configuration you are using in a network, T568A or T568B, and that you specify hardware that is compatible with your selected color scheme.

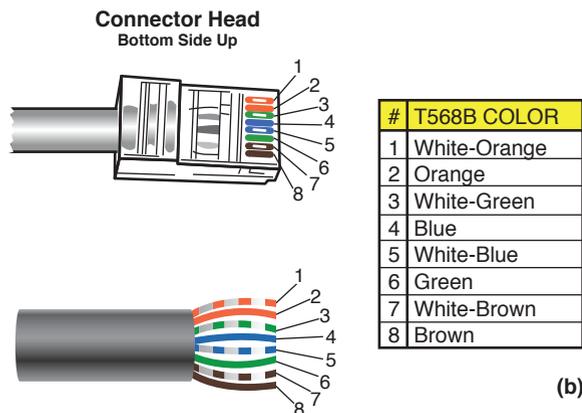
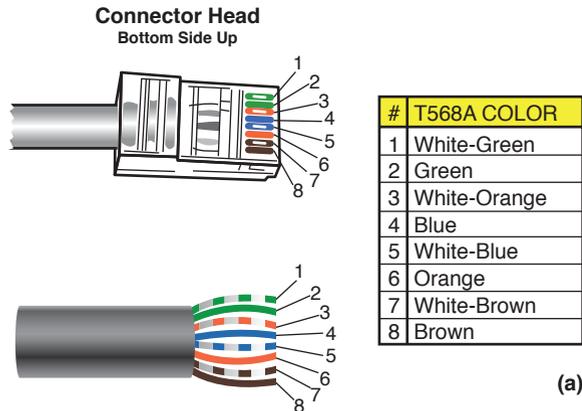


FIGURE 2-7 (a) The wiring of the RJ-45 (8P8C) connector and the wire color codes for the T568A standard; (b) the wiring of the RJ-45 connector for the T568B standard (courtesy of StarTech.com).

Computer Communication

As mentioned in section 2-2, the CAT6/5e cable contains four twisted wire pairs. Figure 2-8 provides a picture of the four wire pairs. Figure 2-9 shows the signals and pin number assignments for the RJ-45 (8P8C) plug for CAT5e. Notice in Figure 2-9 that the Transmit Out signals are marked with a (+) and (-). The Receive In (+) and (-) signals are also marked in the same way. The (+) and (-) symbols are typical ways of indicating the positive and negative sides of a balanced wire pair. Recall from section 2-3, “Unshielded Twisted-Pair Cable,” that in a balanced mode of operation, neither signal line is at ground.



FIGURE 2-8 The four wire pairs of the CAT6/CAT5e.

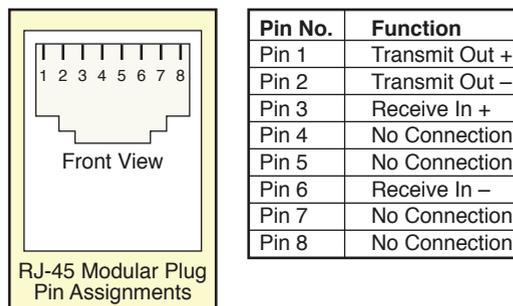


FIGURE 2-9 The pin assignments and signal names for the RJ-45 (8P8C) modular plug (CAT5e).

TX

Abbreviation for transmit

RX

Abbreviation for receive

For computers to communicate in a LAN, the transmit and receive pairs must be properly aligned. This means the transmit (**TX**) (+) and (-) signals must connect to the receive (**RX**) (+) and (-), as shown in Figure 2-10. Notice in Figure 2-10 that pins 1–2 of device A connect to pins 3–6 of device B. Pins 1–2 of device B connect to pins 3–6 of device A. This configuration is always valid when the data rates are 10Mbps or 100Mbps.

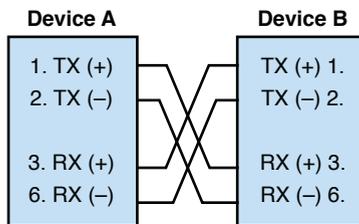
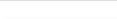


FIGURE 2-10 The proper alignment of the transmit and receive pairs in a CAT6/5e data link operating 10Mbps or 100Mbps.

In a LAN, the proper alignment of the transmit and receive pairs is managed by a switch or hub, not typically in the cable. Remember, in a star topology, all network communication travels through a switch or hub. You will see an “X” or “Uplink” on many of the switch and hub input ports, indicating that this is a cross-connected input. This means that transmit and receive pairs are internally swapped to maintain proper signal alignment of the TX and RX pairs. Even if the “X” or “Uplink” is missing, the switch or hub still properly aligns the TX and RX wire pairs. There is an exception to this on many switches and hubs. Some switches and hubs have an input port that can be selected to be “straight” or “crossed.” These ports are typically used in uplink applications when you connect a switch or hub to another switch or hub. If a device has a cross-connected port, then a straight-through cable is used because the device is providing the alignment. Just remember, proper alignment of the transmit and receive pair must be maintained for the computers to communicate. And a final note, if the wires are not properly connected, there won’t be a link light.

There is a difference with the signal names for the UTP cable when operating at 1Gbps and 10Gbps. At these higher data rates, the use of all four wire pairs is required and the data is bidirectional, which means the same wire pairs are being used for both transmitting and receiving data. Figure 2-11 shows the pin assignments and signal names.

Pin	1000 Mbps and 10 Gbps Color (T568A)	10/100 Mbps	1000 Mbps and 10 Gbps	Pin	1000 Mbps and 10 Gbps Color (T568B)	10/100 Mbps Signal	1000 Mbps Signal
1	 green/white	TX+	BI_DA+	1	 orange/white	TX+	BI_DA+
2	 Green	TX-	BI_DA-	2	 Orange	TX-	BI_DA-
3	 orange/white	RX+		3	 green/white	RX+	BI_DB+
4	 blue	-	BI_DC+	4	 blue	-	BI_DC+
5	 blue/white	-	BI_DC-	5	 blue/white	-	BI_DC-
6	 orange	RX-	BI_DB-	6	 green	RX-	BI_DB-
7	 brown/white	-	BI_DD+	7	 brown/white	-	BI_DD+
8	 brown	-	BI_DD-	8	 brown	-	BI_DD-

(a) The pin assignments and signal names for 1 Gbps and 10 Gbps (T568A).

(b) The pin assignments and signal names for 1 Gbps and 10 Gbps (T568B).

FIGURE 2-11 The pin assignments and signal names for 1Gbps and 10Gbps (T568A and T568B).

Straight-through and Crossover Patch Cables

Category 6/5e twisted-pair cables are used to connect networking components to each other in the network. These cables are commonly called *patch cables*. In this section, a technique for terminating CAT6/5e cables with RJ-45 (8P8C) modular plugs is demonstrated for two different configurations of patch cables, a straight-through and a crossover cable. In a **straight-through cable** the four wire pairs connect to the same pin numbers on each end of the cable. For example, pin 1 on one end connects to pin 1 on the other end. Figure 2-12 shows an example of the **wire-map** for a straight-through cable. A wire-map is a graphical or text description of the wire connections from pin to pin for a cable under test. Notice that in Figure 2-12 the transmit and receive pairs connect to the same connector pin numbers at each end of the cable, hence the name *straight* or *straight-through* cable.

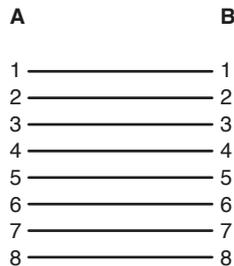


FIGURE 2-12 The wire-map for a straight-through cable.

Straight-through Cable

The wire pairs in the cable connect to the same pin numbers on each end

Wire-map

A graphical or text description of the wire connections from pin to pin

In some applications in 10/100Mbps data links, it is necessary to construct a cable where the transmit and receive wire pairs are reversed in the cable rather than by the switch or the hub. This cable configuration is called a **crossover cable**, which means the transmit pair of device A connects to the receive pair of device B, and the transmit pair of B connects to the receive pair of A. Figure 2-13 shows the wire-map for a crossover cable.

Crossover Cable

Transmit and receiver wire pairs are crossed

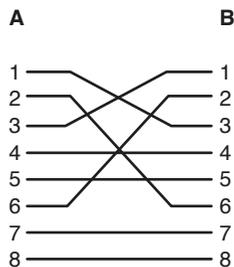


FIGURE 2-13 The wire-map for crossover cable 10/100Mbps links.

Note

The crossover cable diagram shown in Figure 2-13 is for 10/100Mbps. A gigabit crossover cable requires that all four wire-pairs be crossed. Although this is possible, it is not practical to make a gigabit crossover cable because of the limit on untwisted wire.

Terminating the CAT6 Horizontal Link Cable

This section presents the steps required for terminating a CAT6 cable using the AMP SL series termination procedure, AMP SL tool, CAT6 cable, and AMP SL Series AMP-TWIST-6S Category 6 modular jacks. In this example, an RJ-45 (8P8C) jack is used to terminate each end of the cable. One end connects to a wall plate in the network work area. The other end will terminate into a CAT6 RJ-45 (8P8C) patch panel, which is typically located in the LAN network closet.

The technical specifications and assembly requirements are more stringent with CAT6. This means that more care must be taken when terminating a CAT6 cable. However, advancements in the tools and connectors have actually made it easier to terminate CAT6 than it was with the old punch-down tools. The steps for terminating the CAT6 horizontal link cables are as follows:

1. Before terminating the cable, inspect the cable for any damage that might have occurred in installation. Examples of damage to look for include nicked or cut wires and possible stretching of the cable.
2. At the work area outlet end, add about one foot extra and cut the wire. Then coil the extra cable and insert it in the receptacle box. It is good to leave a little extra in case you make an error in installation and have to redo the termination. Remember, you can't splice a CAT6 cable. At the distribution end, you must route the cable and create a slack loop. A slack loop is simply extra cable looped at the distribution end that is used if the equipment must be moved. In

cases where you are having the cable pulled through ductwork or conduit by an installer, make sure you specify that extra cable length will be run. This will vary for each installation. Remember to allow for 5 meters in the telecommunications closet and allow for 5 meters in the work area.

3. Place a bend limiting strain relief boot on the cable, as shown in Figure 2-14(a). This is used in the last step to secure the RJ-45 (8P8C) jack. After placing the boot on the cable, you will need to strip approximately 3 inches of cable jacket from the UTP cable as shown in Figure 2-14(b). Be careful not to nick or cut the wires.



FIGURE 2-14 (a) Placing the bend-limiting strain relief boot on the cable and (b) stripping off 3 inches of jacket from the UTP cable.

4. Remove the jacket from the UTP cable. Bend the cable at the cut, as shown in Figure 2-15(a), and remove the jacket and expose the four wire pairs, as shown in Figure 2-15(b).

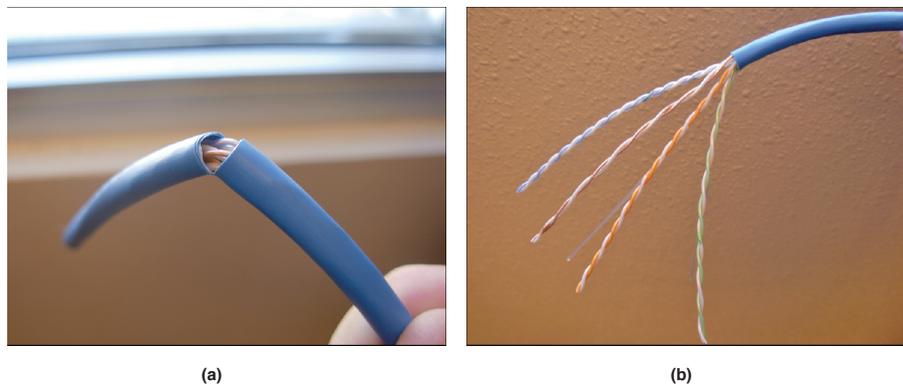


FIGURE 2-15 (a) Separating the cut jacket from the wire pairs and (b) removing of the jacket and exposing the four wire pairs.

5. Cut the plastic pull line and the string as shown in Figure 2-16(a). The plastic line adds strength to cable for pulling, and the string is used to remove extra cable jacket as needed. Place a lacing fixture on the cable, as shown in Figure 2-16(b), and sort the wires in either T568A or T568B color order.

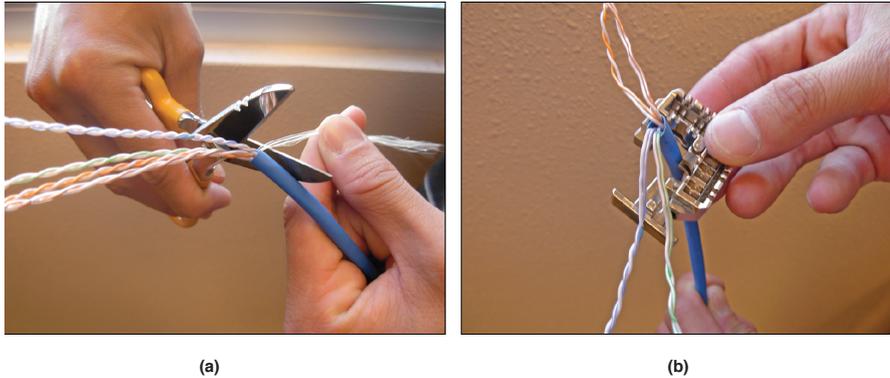


FIGURE 2-16 (a) Removing the plastic pull line and (b) placing the lacing tool on the cable with the color sorted cable pairs.

The sorted wire pairs are matched up with colors provided on the lacing fixture for 568A and 568B as shown in Figure 2-17.

6. Place the wires in the slots of the lacing tool as shown in Figure 2-18. The wire colors are matched to the proper order (T568A/T568B) displayed on the sides of the lacing tool.



FIGURE 2-17 The sides of the lacing tool showing the T568A and T568B wire color connections.

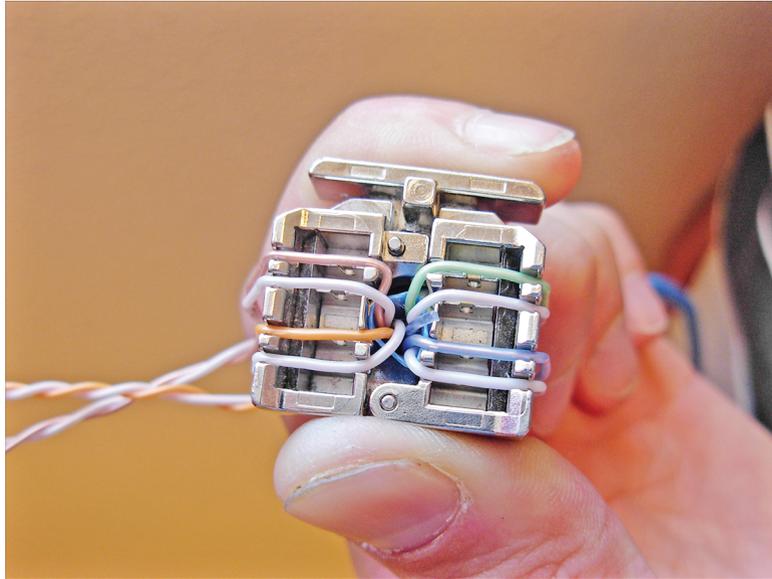
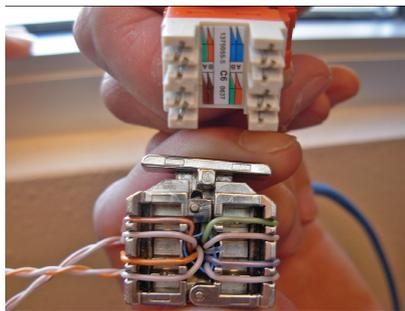
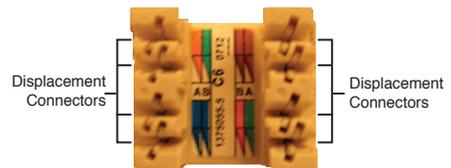


FIGURE 2-18 The routed cable wires on the lacing tool. The wire order shown is T568B.

7. Align an RJ-45 (8P8C) jack with the lacing fixture as shown in Figure 2-19(a). The RJ-45 jack must be properly aligned with the wires on the lacing fixture to maintain proper color order. Figure 2-19(b) provides a close-up picture of the AMP SL series AMP-TWIST-6S modular jack. This picture shows the locations of the displacement connectors on the modulator jack.
8. Insert the RJ-45 (8P8C) modular jack into the AMP SL tool as shown in Figure 2-20(a), and then insert the RJ-45 (8P8C) jack into the AMP SL tool as shown in Figure 2-20(b). Press the wires into the eight displacement connectors on the RJ-45 (8P8C) jack using the AMP SL tool as shown in Figure 2-20(c). This technique enables the pair twist to be maintained right up to the point of termination. In fact, the untwisted-pair length is less than or equal to 1/4 inch.



(a)



AMP SL Series AMP-TWIST-6S
Category 6 Modular Jack

(b)

FIGURE 2-19 (a) Aligning the RJ-45 (8P8C) jack and the lacing fixture and (b) a close-up view of the AMP-TWIST-6S CAT6 modular jack.

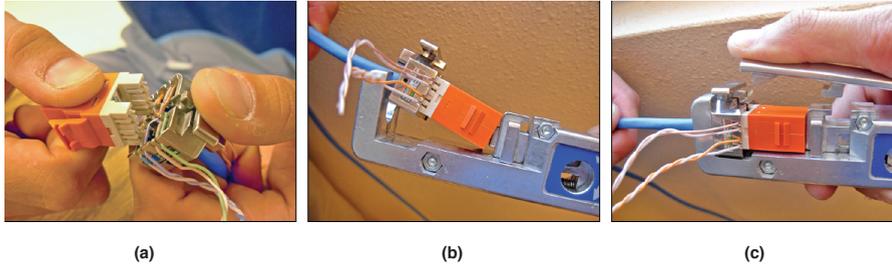
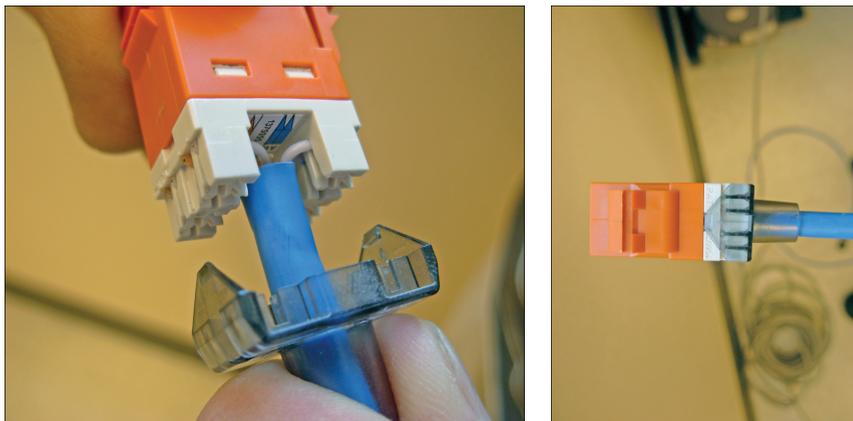


FIGURE 2-20 (a) Aligning the RJ-45 (8P8C) jack with the lacing tool; (b) inserting the RJ-45 (8P8C) jack and the lacing tool into the AMP SL tool; and (c) using the AMP SL tool to crimp the RJ-45 (8P8C) jack onto the eight displacement connectors and to cut the wires.

9. Connect the bend-limiting strain relief boot to the RJ-45 (8P8C) jack as shown in Figure 2-21(a). Figure 2-21(b) shows the completed termination.



(a) Connecting the bend-limiting strain relief boot to the RJ-45 jack. (b) The finished RJ-45 jack termination.

FIGURE 2-21 Connecting the bend-limiting strain relief boot to the RJ-45 (8P8C) jack.

Assembling the Straight-through CAT5e/5 Patch Cable

This section presents a technique for assembling a straight-through CAT5e/5 patch cable. In a straight-through patch cable, the wire pairs in the cable connect to the same pin numbers on each end of the CAT5e/5 patch cable. Figure 2-22 shows a CAT5e patch cable with RJ-45 (8P8C) modular plugs.

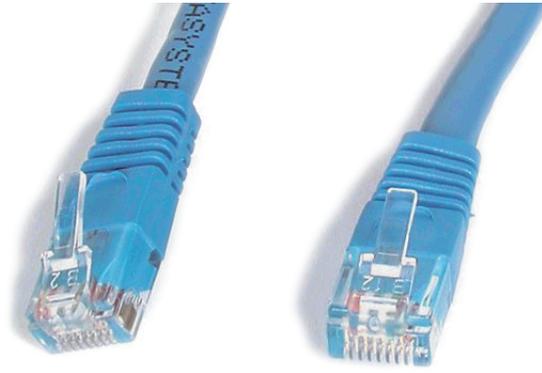


FIGURE 2-22 CAT5e patch cable with RJ-45 (8P8C) modular plugs (courtesy of StarTech.com).

The steps for making straight-through patch cables are as follows:

1. Before terminating the cable, inspect the cable for any damage that might have occurred in installation, such as nicked or cut wires and possible stretching of the cable.
2. Measure the cable to length, add about 6 inches extra, and cut the wire. It is good to have a little extra in case you make an error in installation and have to redo the termination. You can't splice CAT5e/5 twisted-pair cable!
3. Strip approximately 3/4 of an inch of the cable jacket from the end of the cable using a cable stripper. Figure 2-23 illustrates how to use a cable stripper. Notice that the stripper is positioned about 3/4 of an inch from the end of the cable. The cable insulation is removed by rotating the insulation stripper around the wire until the wire jacket is loose and easily removable. (Note: These tools must be periodically adjusted so that the blade cuts through the outer insulation only. If the blades are set too deep, they will nick the wires and the process must be repeated. The damaged portion of the cable must be cut away. Nicking the insulation of the twisted-pair wires is *not permitted!*)



FIGURE 2-23 An example of using the cable jacket stripper to remove the insulation.

4. Sort the wire pairs so that they fit into the connector and orient the wire in the proper order for either T568A or T568B as shown in Figures 2-24(a) and 2-24(b). Be careful to avoid creating a split pair connection. This happens when

a wire from one pair and a wire from another pair are used to make a connection. This potentially creates interference and crosstalk problems, thus preventing the cable to pass a certification test. This is discussed in section 2-5.

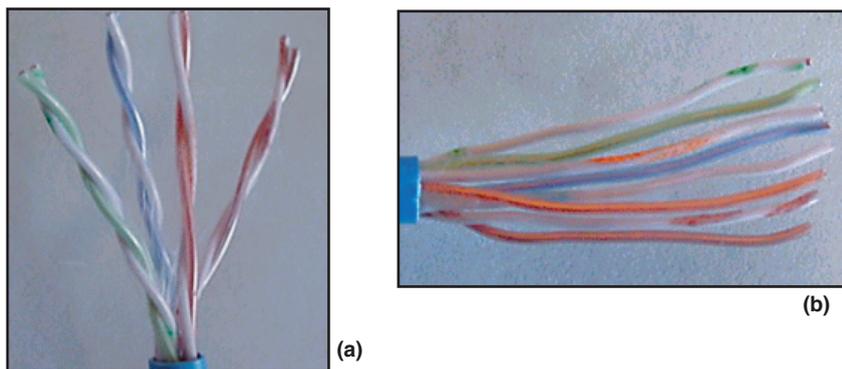


FIGURE 2-24 (a) Separating wire pairs; (b) orienting the wires.

5. Clip the wires so that they are even and insert the wires onto the RJ-45 (8P8C) modular plug as shown in Figure 2-25.



FIGURE 2-25 The clipped wires ready for insertion into the RJ-45 (8P8C) plug.

6. Push the wires into the connector until the ends of each wire can be seen through the clear end of the connector. (Note: Now is the time to verify that the wire order is correct.) The wires are visible through the plastic connector, as shown in Figure 2-26.



FIGURE 2-26 Wires pushed into the RJ-45 (8P8C) plug.

7. Use a crimping tool to crimp the wires onto the RJ-45 (8P8C) plug. The RJ-45 plug is inserted into the crimping tool until it stops as shown in Figure 2-27(a). Next, squeeze the handle on the crimping tool all the way until it clicks and releases (see Figure 2-27[b]). This step crimps the wire onto the insulation displacement connector pins on the RJ-45 (8P8C) jack.

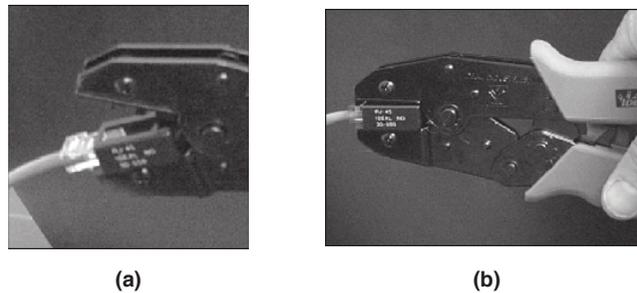


FIGURE 2-27 (a) Inserting the connector; (b) crimping the connector.

8. Repeat these steps for the other end of the twisted-pair cable.

The next step is to test the cable. These techniques and procedures are discussed in section 2-5.

Section 2-4 Review

This section has covered the following **Network+** Exam objectives.

- 1.5 Install and properly terminate various cable types and connectors using the appropriate tools

The steps for terminating CAT5 and CAT6 UTP cables have been presented. Make sure you understand the procedure and the purpose of the various tools required to terminate cables and a jack.

- 4.4 Given a scenario, troubleshoot and resolve common copper cable issues

The pin assignments and the signal names for wiring UTP cables have been presented. The proper alignment of the transmit and receive pairs was presented in Figure 2-10. This is an important concept. The concept of a split pair was also introduced.

- 5.4 Given a scenario, deploy the appropriate wired connectivity standard

This section has presented the T568A and T568B wiring schemes. It is very important that you know the wire colors and associated pin assignments.

Test Your Knowledge

1. The following is the color map and pin numbers for T568A:

Pin#	Wirecolor
1	White-Green
2	Blue
3	White-Orange
4	Green
5	White-Blue
6	Orange
7	White-Brown
8	Brown

True or False?

2. The following is the color map and pin numbers for T568B:

Pin#	Wirecolor
1	White-Orange
2	Orange
3	White-Green
4	Blue
5	White-Blue
6	Green
7	White-Brown
8	Brown

True or False?

3. How many wires are in a CAT5e/6 twisted-pair cable?
- 12 wires
 - 8 wires
 - 4 wires
 - 6 wires

2-5 CABLE TESTING AND CERTIFICATION

The issues and specifications for certifying CAT6 cable are presented in this section. All the parameters that are defined by the EIA/TIA 568B channel specifications are examined in this section. What about CAT7 and beyond? The specifications presented define the basis for most twisted-pair certification. CAT7 promises improved performance capability, and a good task would be to ask the student what the difference is for certifying CAT7 cable. Most likely the students will report that the cable and the connectors have improved performance specifications. The section concludes with examples of conducting CAT6 cable tests.

The need for increased data rates is pushing the technology of twisted-pair cable to even greater performance requirements and placing even greater demands on accurate testing of the cable infrastructure. The data speeds over twisted-pair copper cable are now at 10Gbps. The EIA/TIA 568B standard defines the minimum cable specifications for twisted-pair categories operating over bandwidths of 100MHz and at data rates up to 10Gbps.

The CAT6/5e designations are simply minimum performance measurements of the cables and the attached terminating hardware such as RJ-45 (8P8C) plugs, jacks, and patch panels. The **link** (the point from one cable termination to another) and the **full channel** (which consists of all the link elements from the hub or switch to the wall plate) must satisfy minimum **attenuation** loss and **near-end crosstalk (NEXT)** for a minimum frequency of 100MHz. Figure 2-28 shows a graphical representation of the link and the full channel. Table 2-4 lists the CAT5e, CAT6, CAT6A, CAT7, and CAT7A EIA/TIA 568B channel specifications.

Link

Point from one cable termination to another

Full Channel

Consists of all the link elements from the wall plate to the hub or switch

Attenuation (Insertion Loss)

The amount of loss in the signal strength as it propagates down a wire or fiber strand

Near-end Crosstalk (NEXT)

A measure of the level of crosstalk or signal coupling within the cable, with a high NEXT (dB) value being desirable

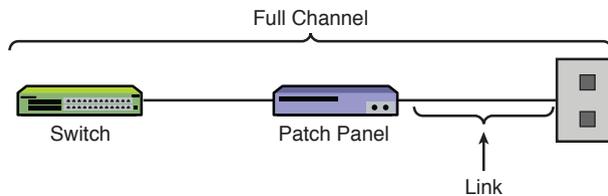


FIGURE 2-28 The link and channel areas for cable testing.

TABLE 2-4 EIA/TIA 568B CAT5e, CAT6, CAT6A, CAT7 and CAT7A Channel Specifications

Parameter	Category 5e	Category 6	Category 6A	Category 7/7A
Class	Class D	Class E	Class E _A	Class F/F _A
Bandwidth	100MHz	250MHz	500MHz	600MHz/1000MHz
Insertion Loss (dB)	24.0	21.3	20.9	20.8/20.3
NEXT Loss (dB)	30.1	39.9	39.9	62.9/65.0
PSNEXT Loss (dB)	27.1	37.1	37.1	59.9/62.0

Parameter	Category 5e	Category 6	Category 6A	Category 7/7A
ACR (dB)	6.1	18.6	18.6	42.1/46.1
PSACR (dB)	3.1	15.8	15.8	39.1/41.7
ACRF1 (ELFEXT) (dB)	17.4	23.3	23.3	44.4/47.4
(PSELFEXT) (dB)	14.4	20.3	20.3	41.1/44.4
Return Loss (dB)	10.0	12.0	12.0	12.0/12.0
* PANEXT Loss (dB)	n/s	n/s	60.0	n/s / 67.0
* PSAACRF (dB)	n/s	n/s	37.0	n/s / 52.0
* TCL (dB)	n/s	n/s	20.3	20.3/20.3
*ELTCTL (dB)	n/s	n/s	0.5	0/0
Propagation Delay (ns)	548	548	548	548/548
Delay Skew (ns)	50	50	50	30/30

*These parameters are discussed in section 2-6, “10 Gigabit Ethernet over Copper.”

The list that follows describes some of the parameters listed in Table 2-4:

- Attenuation (insertion loss):** This parameter defines the amount of loss in signal strength as it propagates down the wire. This is caused by the resistance of the twisted-pair cable, the connectors, and leakage of the electrical signal through the cable insulation. Attenuation also will increase with an increase in frequencies due to the inductance and capacitance of the cable. The cable test results will report a margin. Margin for attenuation (insertion loss) is defined as the difference between the measured value and the limit for the test. If the margin shows a negative value, the test has failed. A negative value is produced when the measured value is less than the limit. The limit for attenuation (insertion loss) for CAT6 is 21.3 dB, CAT6A is 20.9, CAT7 is 20.8, and CAT7a is 20.3. It is also important to note that UTP cables have a limit on how much the cable can be bent (bend radius). The limit on the bend radius is four times the outer jacket diameter. The reason for this is bends exceeding the limit can introduce attenuation loss.
- NEXT:** When current travels in a wire, an electromagnetic field is created. This field can induce a voltage in adjacent wires resulting in crosstalk. **Crosstalk** is what you occasionally hear on the telephone when you can faintly hear another conversation. Near-end crosstalk, or NEXT, is a measure of the level of crosstalk, or signal coupling within the cable. The measurement is called *near-end testing* because the receiver is more likely to pick up the crosstalk from the transmit to the receiver wire pairs at the ends. The transmit signal levels at each end are strong, and the cable is more susceptible to crosstalk at this point. Additionally, the receive signal levels have been attenuated due to normal cable path loss and are significantly weaker than the transmit signal. A high NEXT (dB) value is desirable.

Crosstalk
Signal coupling in a cable

Figure 2-29 graphically depicts NEXT. The dark gray area shows where the near-end crosstalk occurs. The margin is the difference between the measured

value and the limit. A negative number means the measured value is less than the limit, and therefore the measurement fails. Crosstalk is more problematic at higher data rates (for example, 1Gbps, 10Gbps). Figure 2-30 shows how CAT6 cable has a built-in separator to help minimize crosstalk among wire pairs. This separator is used to keep each wire pair at a minimum distance from other wire pairs. This addition reduces crosstalk at higher frequencies and helps provide improved signal bandwidth, and therefore it will support faster data rates. This addition also helps improve the far-end cross-talk. Note that not all cable manufacturers use the separator.

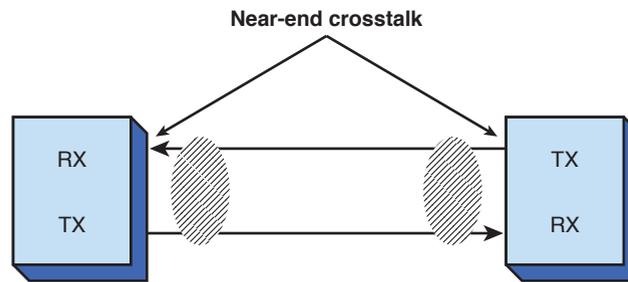


FIGURE 2-29 A graphical depiction of near-end crosstalk.

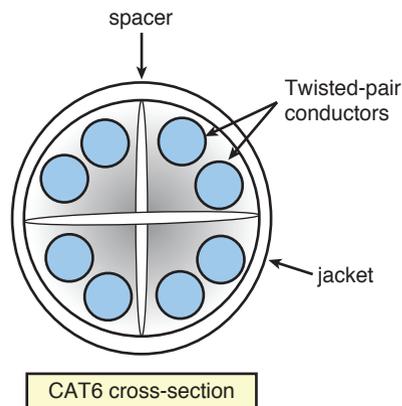


FIGURE 2-30 The cross-section of a CAT6 cable showing the separator used to minimize crosstalk problems.

- **Power Sum NEXT (PSNEXT):** The enhanced twisted-pair cable must meet four-pair NEXT requirements, called PSNEXT testing. Basically, power sum testing measures the total crosstalk of all cable pairs. This test ensures that the cable can carry data traffic on all four pairs at the same time with minimal interference. A higher PSNEXT value is desirable because it indicates better cable performance.

- **Equal Level FEXT (ELFEXT):** This measurement differs from NEXT in that the measurement is for the far end of the cable. Additionally, the ELFEXT measurement does not depend on the length of the cable. This is because ELFEXT is obtained by subtracting the attenuation value from the far-end crosstalk (**FEXT**) loss. Higher ELFEXT values (dB) indicate the signals at the far end of the cable are larger than the cross-talk measured at the far end. A larger ELFEXT (dB) value is desirable. A poor ELFEXT can result in data loss.
- **PSELFEXT:** Power sum ELFEXT that uses all four wire pairs to obtain a combined ELFEXT performance measurement. This value is the difference between the test signal level and the cross-talk measured at the far end of the cable. A higher PSELFEXT value indicates better cable performance.
- **ACR:** This measurement compares the signal level from a transmitter at the far end to the crosstalk measured at the near end. A larger ACR indicates that the cable has a greater data capacity and also indicates the cable's ability to handle a greater bandwidth. Essentially, it is a combined measurement of the quality of the cable. A higher ACR value (dB) is desirable.
- **PSACR:** Power sum ACR uses all four wire pairs to obtain the measure of the attenuation–crosstalk ratio. This is a measurement of the difference between PSNEXT and attenuation (insertion loss). The difference is measured in dB, and higher PSACR dB values indicate better cable performance.
- **Return loss:** An equally important twisted-pair cable measurement is return loss. This measurement provides a measure of the ratio of power transmitted into a cable to the amount of power returned or reflected. The signal reflection is due to impedance changes in the cable link and the impedance changes contributing to cable loss. Cables are not perfect, so there will always be some reflection. Examples of the causes for impedance changes are non-uniformity in impedance throughout the cable, the diameter of the copper, cable handling, and dielectric differences. A low return loss value (dB) is desirable.
- **Propagation delay:** This is a measure of the amount of time it takes for a signal to propagate from one end of the cable to the other. The delay of the signal is affected by the **nominal velocity of propagation (NVP)** of the cable. NVP is some percentage of the velocity of light and is dependent on the type of cable being tested. The typical delay value for CAT5/5e UTP cable is about 5.7 nsec per meter. The EIA/TIA specification allows for 548 nsec for the maximum 100-meter run for CAT5e, CAT6, CAT6a, CAT7, and CAT7A.
- **Delay skew:** This is a measure of the difference in arrival time between the fastest and the slowest signal in a UTP wire pair. It is critical in high-speed data transmission that the data on the wire pair arrive at the other end at the same time. If the wire lengths of different wire pairs are significantly different, then the data on one wire will take longer to propagate along the wire, hence arriving at the receiver at a different time and potentially creating distortion of the data and data packet loss. The wire pair with the shortest length will typically have the least delay skew.

Note

The power sum measurements are critical for high-speed data communication over UTP. It has also been shown that twisted-pair cable can handle gigabit data rates over a distance up to 100 meters. However, the gigabit data rate capability of twisted-pair requires the use of all four wire pairs in the cable, with each pair handling 250Mbps of data. The total bit rate is 4 X 250Mbps, or 1Gbps, hence the need to obtain the combined performance measurements of all four wire pairs.

Section 2-5 Review

This section has covered the following **Network+** Exam objectives.

4.2 Given a scenario, analyze and interpret the output of troubleshooting tools

This chapter presented an overview of testing the installed UTP cable. In this section, you learned the details of the EIA/TIA UTP specifications for many category types. You were also introduced to what the test parameters mean. Make sure you develop an understanding of each test parameter.

4.4 Given a scenario, troubleshoot and resolve common copper cable issues

This section has introduced some very important cable issue concepts. Make sure you have a good understanding of near-end, far-end crosstalk, attenuation, and distance limitation.

Test Your Knowledge

1. A full channel test tests all the link elements from the computer through the patch panel to the wall plate. True or False?
2. NEXT stands for Near End Cross Talk and a low dB value is desirable. True or False?
3. Signals travel in a cable at some percentage of the velocity of light. The term for this is called the nominal velocity of propagation. True or False?

2-6 10 GIGABIT ETHERNET OVER COPPER

Ethernet over copper is now available for 10Gbps (ten gigabit Ethernet). The increase in the required bandwidth for transporting a 10GB data transfer rate is placing increased demands on the copper cable as well as the hardware used for terminating the cable ends and for connecting to the networking equipment. Three improvements are required for transmitting the higher data bit rates over the copper cabling. These are

- Improve the cable so it can carry greater bandwidth.
- Improve the electronics used to transmit and receive (recover) the data.

- Utilize improvements in both the cable and electronics to facilitate greater bandwidths and distance.

Alien Crosstalk is an important issue at higher data rates such as with 10GBASE-T. Alien Crosstalk (AXT) is unwanted signal coupling from one permanent link to another. Basically this is the coupling of a signal from one 4-pair cable to another 4-pair cable.

Cable manufacturers are starting to offer CAT6 and higher grades of twisted-pair cable with foil over each of the four wire-pairs. The designation for this type of cable is foil twisted-pair (F/UTP). Have the students investigate the latest UTP cabling improvements.

Ethernet over copper is available for 10Mbps (Ethernet), 100Mbps (FastEthernet), 1000Mbps (gigabit Ethernet), and now 10Gbps (ten gigabit Ethernet). (Note that Mbps is “megabits per second.” Some literature writes this as Mb/s.) The increase in the required bandwidth for transporting a 10GB data transfer rate is placing increased demands on the copper cable as well as the hardware used for terminating the cable ends and for connecting to the networking equipment. There are three improvements required for transmitting the higher data bit rates over the copper cabling:

1. Improve the cable so it can carry greater bandwidth.
2. Improve the electronics used to transmit and receive (recover) the data.
3. Utilize improvements in both the cable and electronics to facilitate greater bandwidths and distance.

This section examines the changes in technology that are required to enable the transportation of ten gigabit data (**10GBASE-T**) over copper. The first part presents an overview of ten gigabit GB Ethernet over copper. The second part examines the modifications required to the technical specs (CAT6A and CAT7/7A) that are necessary for testing and certifying twisted-pair copper cable transporting ten gigabit data rates. The last section examines the issues of how the ten gigabit data is actually transmitted.

Overview

The standard for 10Gbps is **IEEE 802.3an-2006 10GBASE-T**. This standard was developed to support running 10Gbps data over twisted-pair cabling. The newer standard requires the bandwidth to be increased from 250MHz to 500MHz. Additionally, the new standard supports 10GB Ethernet up to 100 meters in cable length. At one time, most people assumed that higher data rates would be limited to fiber optics. While this is still true for lengthy runs (more than 100 meters) twisted-pair copper is finding its place in the horizontal runs from the telecommunications closet to the work area.

10GBASE-T

10Gbps over twisted-pair copper cable

IEEE 802.3an-2006 10GBASE-T

The standard for 10Gbps

Alien Crosstalk (AXT)

Unwanted signal coupling from one permanent link to another

PSANEXT

Power Sum Alien Near-End Cross-Talk

PSAACRF

Power Sum Alien Attenuation to Crosstalk Ratio

Alien Crosstalk

Alien Crosstalk is an important issue at higher data rates such as with 10GBASE-T. **Alien Crosstalk (AXT)** is unwanted signal coupling from one permanent link to another. Basically, this is the coupling of a signal from one 4-pair cable to another 4-pair cable. Figure 2-31 depicts the AXT from one 4-pair cable to another 4-pair cable. The other key measurements for 10GBASE-T are **NEXT (PSANEXT)**, **FEXT (PSAACRF)**, and Return Loss. PSANEXT (Power Sum Alien Near-End Cross-talk) and PSAACRF (Power Sum Alien Attenuation to Crosstalk Ratio) are new measurements for NEXT and FEXT that incorporate measures for Alien Crosstalk. Alien Crosstalk is considered to be the main electrical limiting parameter for 10G Ethernet. Alien Crosstalk causes disturbances in the neighboring cable. It is difficult for the electronics to cancel the AXT noise created; therefore, new cables have been developed to support the 10Gbps data rates. The newer cables have improved the cable separation, and new connectors have also been developed to help meet the required specifications to support 10G.

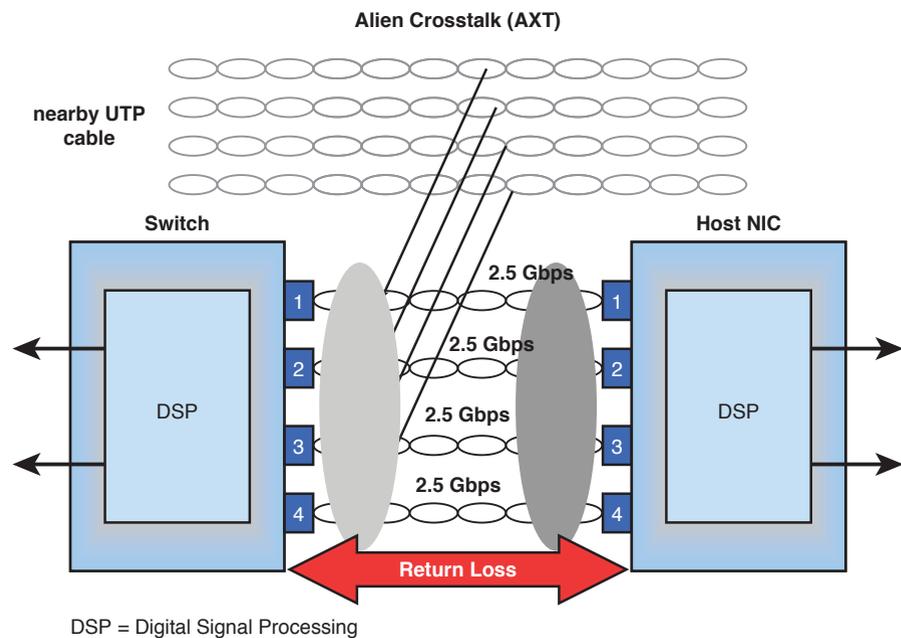


FIGURE 2-31 Alien Crosstalk from a neighboring 4-pair cable.

F/UTP

Foil over twisted-pair cabling

Cable manufacturers are starting to offer CAT6 and higher grades of twisted-pair cable with foil over each of the four wire-pairs. The designation for this type of cable is **F/UTP**. There are several advantages to using a shielded cable:

- A shielded cable offers better security because there is less chance that the data will radiate outside the cable.
- The foil shield helps improve noise immunity from EMI, radio frequency interference (RFI), and (most importantly) AXT.

Transmission of data over twisted-pair cabling relies on the signals being “balanced” over the wire pairs. The balance or symmetry of the signal over the wire pairs helps minimize unwanted leakage of the signal. There are two parameters now defined for CAT6 and better cabling that address the issue of balanced data. The first is **TCL (Transverse Conversion Loss)** and the other is **ELTCTL (Equal Level Transverse Conversion Transfer Loss)**. The TCL measurement is obtained by applying a common-mode signal to the input and measuring the differential signal level on the output. TCL is sometimes called **LCL (Longitudinal Conversion Loss)**. The ELTCTL value (expressed in dB) is the difference between the **TCTL (Transverse Conversion Transfer Loss)** and the differential mode insertion loss of the pair being measured. TCTL is the loss from a balanced signal at the near-end to the unbalanced signal at the far end.

The newer tests also require additional Power-Sum tests. These are **PSANEXT (Power-Sum Alien Near-End Cross-Talk)** and **PSAACRF (Power-Sum Alien Attenuation Cross-talk Ratio Far-end)**. These tests have been developed to help ensure cable compatibility with data transmission and reception that requires the use of all four wire-pairs. Both gigabit and ten gigabit require the use of all four wire pairs.

Signal Transmission

The 10GBASE-T system requires the use of all four wire pairs as shown in Figure 2-32. This system splits the 10Gbps of data into four 2.5Gbps data channels. This same technique is also used for 1000Mbps (1GB) data rates, except the 1000Mbps signal is split into four 250Mbps data channels. The system requires the use of signal conditioners and digital signal processing (DSP) circuits for both transmission and reception. The data transmission for ten gigabit uses a **multilevel encoding** technique as shown in Figure 2-33. The advantage of this type of encoding is the reduction in the required bandwidth required to transport the data.

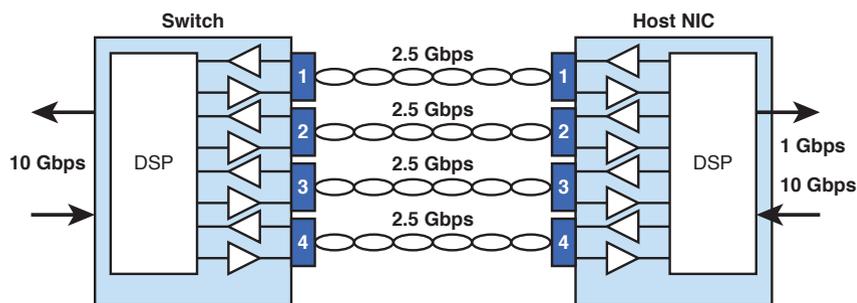


FIGURE 2-32 The four wire-pairs in UTP cabling required for transporting 10GBASE-T data. This same technique is used for 1000Mbps except the data rate for each of the four channels is 250Mbps.

TCL

Transverse Conversion Loss

ELTCTL

Equal Level Transverse Conversion Transfer Loss

LCL

Longitudinal Conversion Loss

TCTL

Transverse Conversion Transfer Loss

PSANEXT

Power-Sum Alien Near-End Crosstalk

PSAACRF

Power-Sum Alien Attenuation Cross-talk Ratio Far-End

Multilevel Encoding

Technique used to reduce in the required bandwidth required to transport the data

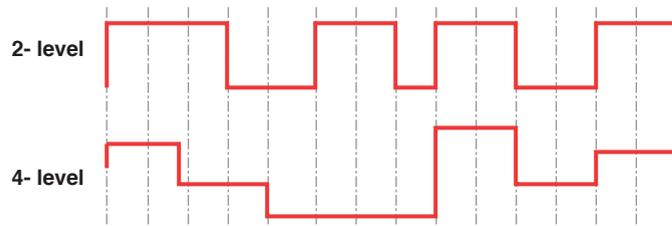


FIGURE 2-33 An example of multilevel encoding of the data streams to reduce the required bandwidth.

Hybrid Echo Cancellation Circuit

Removes the transmitted signal from the receive signal

10GBASE-T data transmission also requires the use of DSP Compensation Techniques. The DSP circuitry provides many functions, such as signal conditioning and echo cancellation. Anytime a signal is transmitted down a cable, part of the signal will be reflected. This reflection adds to overall signal degradation and limits the performance of the system. In 10GBASE-T, the transmit and receive signals are sharing the same wire pair. This is called full duplex transmission and requires the use of a device called a **hybrid echo cancellation circuit**. The hybrid circuit removes the transmitted signal from the receive signal.

The final issue with 10GBASE-T signal transmission is the performance of the cable. As mentioned previously, return loss, insertion loss, and crosstalk are all key limiting issues for 10GBASE-T. Crosstalk is the most important factor. The types of crosstalk observed are AXT, NEXT, FEXT, and ELFEXT. The cabling systems that will support 10GBASE-T operation with links up to 100 meters are CAT6 with the foil screen, augmented CAT6 (CAT6a), CAT7, and CAT7a.

Section 2-6 Review

This section has covered the following **Network+** Exam objectives.

5.4 Given a scenario, deploy the appropriate wired connectivity standard

This section has presented a look at the issue of running 10Gbps of data over UTP cable. This is based on the 10GBASE-T Ethernet standard. Probably one of the most important concepts associated with 10Gbps over twisted-pair is Alien Crosstalk, which is unwanted signal coupling from one permanent link to another.

Test Your Knowledge

- The term for unwanted signal coupling from one permanent link to another is
 - Near-end crosstalk
 - Alien Crosstalk**
 - Far-end crosstalk
 - None of these answers is correct.

2. 10GBASE-T requires the use of which of the following in the transmission of data over UTP?
 - a. The high data lines
 - b. Pins 4/5 7/8 only
 - c. All four wire pairs
 - d. 10G is not possible at 10G.

2-7 TROUBLESHOOTING CABLING SYSTEMS

This section presents some test results taken from several CAT6/5e cable tests. The objective is to acquaint the student with possible test results and problems he might encounter on the job.

This section examines some of the issues that the network administrator can have with both CAT6 and CAT5e cables tests. It is important that the network administrator monitor all parts of the cable installation, from pulling to terminating the cable ends. The reasons a cable fails a certification test can be due to multiple types of problems, such as with installation, cable stretching, and the cable failing to meet manufacturer specifications. These types of problems are discussed next, followed by a look at the certification reports for failures of both CAT6 and CAT5e.

Installation

If you obtain bad PowerSum measurements or NEXT or FEXT, there might be a problem with the installation. The certification report provided in Figure 2-34 indicates this cable does not pass CAT6 certification, as shown by the X in the upper-right corner of the certification report. This test indicates a “NEXT” failure, which is most likely due to a problem at the terminations. The most common error is the installer has allowed too much untwisted cable at the termination point. Remember, the twist on UTP cable must be maintained to less than 3/8 inch. At this point, the best thing is to go and inspect the terminations to see whether any terminations have too much untwisted cable and verify whether there is a procedure problem with the installation.

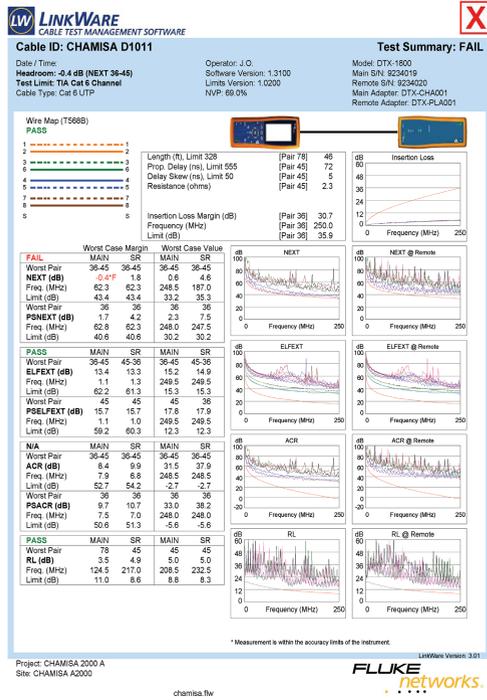


FIGURE 2-34 The DTX-1800 certification report: Failure due to termination problem.

Cable Stretching

It is important to avoid stretching of the UTP cable. Stretching of the cable is bad because it changes the electrical characteristics of the cable, increasing the attenuation and crosstalk. The maximum pulling tension is specified by the manufacturer data sheets, and the datasheet will list the maximum pulling tension put on a cable. The units for the pulling tension are expressed in lb-ft.

Cable Failing to Meet Manufacturer Specifications

Occasionally, manufacturers do experience problems with the cable failing to meet specifications. This could be due to a bad production run, and the result is that the cable does not meet minimum specifications. Repeated test failures with no apparent reason for the failure could indicate that the problem is with the cable. This rarely happens, but there is a possibility that there was a bad cable production run. As the manager, you need to isolate the source of the problem.

Figure 2-35 provides another CAT6 certification report, which indicates that the cable failed due to excessive insertion loss. Examination of the certification report shows that the cable length for pairs 7–8 is 311 ft. The maximum cable length for a permanent link is 295 ft. This cable run is too long for it to be certifiable.



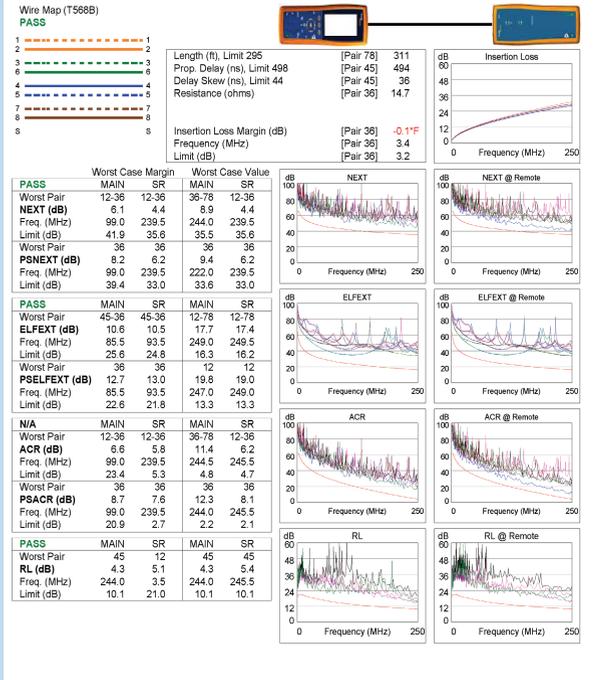
Cable ID: CHAMISA 2065

Test Summary: FAIL

Date / Time: Headroom: 4.4 dB (NEXT 12-36)
Test Limit: TIA Cat 6 Perm. Link
Cable Type: Cat 6 UTP

Operator: J.O. Software Version: 1.3100
Limits Version: 1.0200
NVP: 69.0%

Model: DTX-1800 Main S/N: 9234019
Remote S/N: 9234020
Main Adapter: DTX-PLA001
Remote Adapter: DTX-PLA001



Project: CHAMISA 2000 A
Site: CHAMISA A2000

chamisa.flw

FIGURE 2-35 The DTX-1800 certification report: Failure due to excessive insertion loss.

CAT5e Cable Test Examples

The next section presents some test results for several CAT5e cable tests. There are still many CAT5e horizontal cable runs already in place, and these runs support 100-Mbps data rates. Therefore, it is important for the network administrator to have a good understanding of certifying CAT5e links. The objective of this section is to acquaint the reader with possible CAT5e test results and problems they might encounter on the job. The procedures presented are the same for CAT6 except that the test mode of the cable analyzer must be set to CAT5e performance specifications. The testers used for conducting the CAT5e certification reports are the Fluke OMNIscanner and OMNIremote.

Test 1

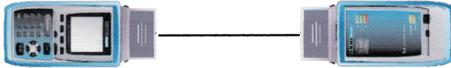
The first example presented is the test on a short patch cable. This shows that short patch cables can and should be tested. UTP cable testing is not restricted to long cables. The length of the wire pairs is about 3 feet. You also have a record that this cable meets CAT5e requirements. The test was conducted using the OMNIscanner.

The OMNISCANNER certification report verifies that the cable passes the CAT5e link test. Figure 2-36 shows the certification report, which indicates that the cable passed the test. This report shows that the cable length is 3 feet.



PASS

OMNISCANNER2 Certification Report

Circuit ID: Pre-cut	OMNISCanner	OMNIRemote
Project: TIA Project	50D99L00377	50E99L00037
Owner: OMNISCANNER 2	Adapter	Adapter
	CHAN 5/5E/6	CHAN 5/5E/6
Autotest: Cat 5E Link		
Cable: Cat 5E UTP		
NVP: 72		
Site: Las Cruces		
Building: Manufacturing		
Floor: 3rd		
Closet: 315A		
	Length (ft)	Limit 12 36 45 78
	Delay (ns):	(308) 3 3 3 3
	Resistance (Ohms):	(518) 4 4 4 4
		(—) — — — —
	Wiremap	Expected Actual
	OMNI:	12345678 12345678 Skew (ns): (45) 0
	Remote:	12345678 12345678 Bandwidth (MHz): ---

Attenuation				Overall Margin (dB)*		Return Loss				Overall Margin (dB)*	
Pairs	dB	Margin	MHz	OMNISCanner	OMNIRemote	Pairs	dB	Margin	MHz	OMNISCanner	OMNIRemote
12	0.3	21.0	97.4	19.9	---	12	23.8	11.4	90.7	23.4	11.2
36	0.4	20.1	90.7			36	23.2	10.4	80.8	22.5	11.0
45	0.4	21.0	97.4			45	23.1	10.1	74.7	24.2	11.0
78	0.3	19.9	88.4			78	23.9	11.5	91.3	24.1	12.0

NEXT				Overall Margin (dB)*		ACR				Overall Margin (dB)*	
Pairs	dB	Margin	MHz	OMNISCanner	OMNIRemote	Pairs	dB	Margin	MHz	OMNISCanner	OMNIRemote
12/36	62.5	18.7	19.6	3.0	---	12/36	---	---	---	---	---
12/45	59.2	21.8	48.6			12/45	---	---	---	---	---
12/78	93.1	33.1	1.2			12/78	---	---	---	---	---
36/45	50.5	8.6	25.9			36/45	---	---	---	---	---
36/78	56.0	13.3	23.2			36/78	---	---	---	---	---
45/78	51.6	14.6	51.6			45/78	---	---	---	---	---

ELFEXT				Overall Margin (dB)*		PSNEXT				Overall Margin (dB)*	
Pairs	dB	Margin	MHz	OMNISCanner	OMNIRemote	Pairs	dB	Margin	MHz	OMNISCanner	OMNIRemote
12/36	60.0	22.0	12.7	15.3	---	12	65.7	20.4	10.4	4.9	---
12/45	55.3	16.9	12.0			36	49.1	10.3	25.9	44.7	4.9
12/78	69.8	30.6	10.9			45	49.8	11.0	25.9	46.1	6.0
36/12	60.1	22.1	12.7			78	50.4	14.6	39.6	50.6	11.8
36/45	46.1	20.0	49.5								
36/78	64.2	28.2	16.0								
45/12	74.6	16.8	1.4								
45/36	76.7	20.3	1.6								
45/78	71.9	15.5	1.6								
78/12	85.3	30.4	1.9								
78/36	48.8	28.6	97.4								
78/45	73.0	15.3	1.4								

PSELFEXT				Overall Margin (dB)*		PSACR				Overall Margin (dB)*	
Pairs	dB	Margin	MHz	OMNISCanner	OMNIRemote	Pairs	dB	Margin	MHz	OMNISCanner	OMNIRemote
12	73.6	18.8	1.4	15.5	---	12	---	---	---	---	---
36	75.9	21.2	1.4			36	---	---	---	---	---
45	68.9	15.5	1.6			45	---	---	---	---	---
78	71.7	18.2	1.6			78	---	---	---	---	---

* Overall margin value is the worst margin for OMNI and Remote.

FIGURE 2-36 The certification report for Test 1 showing that the short jumper cable passes CAT5e link test.

Test 2

This shows the test on the same 3-foot cable used in Test 1; however, the cable no longer meets CAT5e requirements, as shown in Figure 2-37. The test results indicate

FAIL. In fact, careful inspection of the cable showed that it had been cut or nicked. This underscores the importance of documenting the network installation and having a record that the cable link was certified. Test 1 showed that the cable met specifications, but damage to the cable no longer enables it to meet CAT5e link specifications.

Inspection of the wire-map test results (see Figure 2-37) shows the cable failed, highlighted by the FAIL symbol in the upper-right corner of the certification report. In this test, the cable has failed a wire-map test. Not only is the text highlighted, but there is an exclamation preceding the text that indicates a failure. A quick check of the wire-map test shows that the number 4 wire was not detected at the remote.

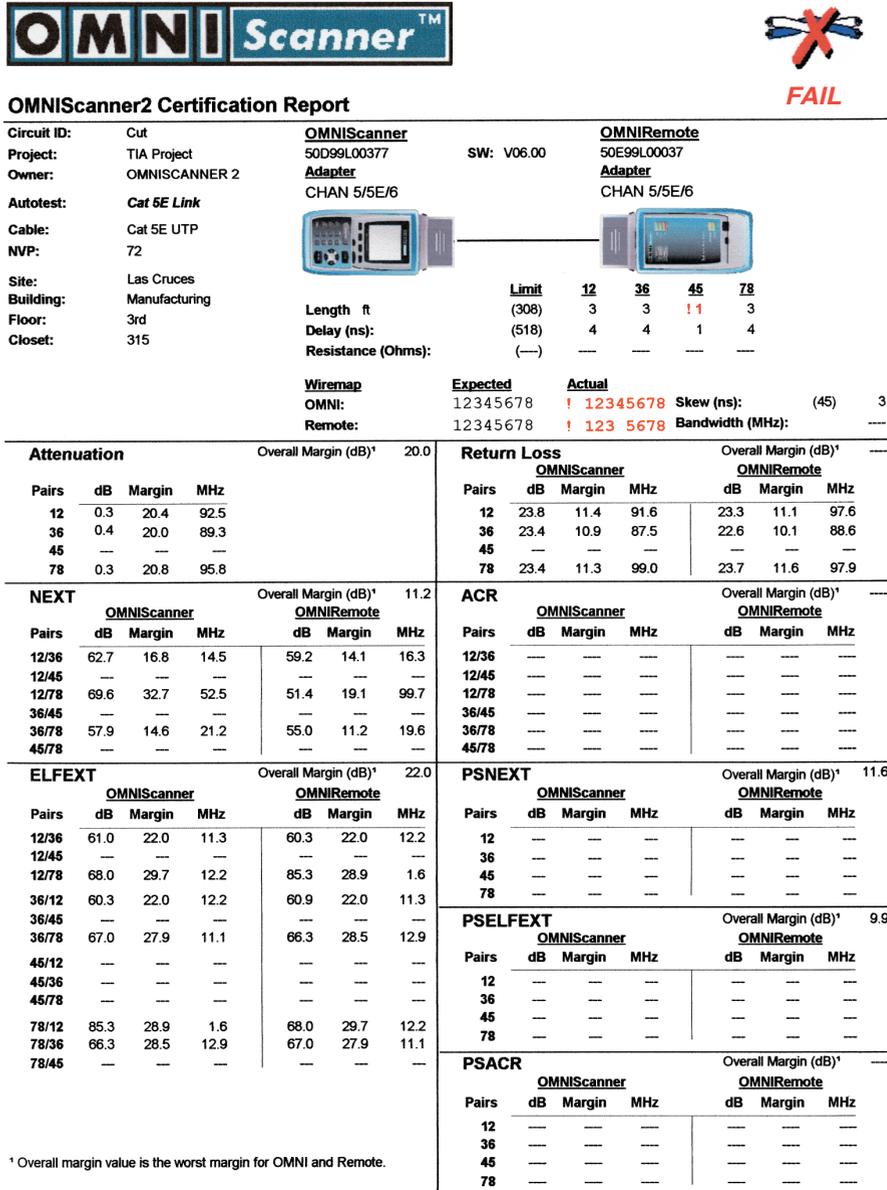


FIGURE 2-37 The results for Test 2 showing that the cable failed the CAT5e link test.

Test 3

This cable test (Figure 2-38) also generated a test result of FAIL. Examination of the attenuation and return-loss menu shows that the cable failed to meet CAT5e attenuation and return-loss specifications. The permitted attenuation in CAT5e cable is 24 dB. However, the 1–2 and 3–6 pairs have attenuation losses of 38.0 dB and 41.1 dB. Both cases greatly exceed the permitted maximum. An arrow points to these attenuation loss scores.

This cable also fails return loss for pairs 1–2 and 3–6. CAT5e cable permits 10 dB of return-loss. The tests show that the pairs fail the return-loss test at both the OMNIscanner and the remote test unit. This cable will fail a CAT5e certification based solely on attenuation or return loss. In fact, this cable also fails NEXT, ELFEXT, and PSELFEXT tests. Any of these failures are sufficient to not certify this cable.

Test 4

Figure 2-39 shows the certification report for the cable tested in Test 4. This cable test generated a test result of FAIL. Examination of the certification report shows the cable failed the delay skew. This cable exceeds the maximum allowed by EIA/TIA 568B. Additionally, this cable fails attenuation, ELFEXT, and PSELFEXT tests. No, the cable should not be certified.

The measured delay skew of 47 ns exceeds the tester setting of 45 ns. The EIA/TIA 568B standard permits a delay skew of 50 ns, so actually this cable meets delay skew requirements for CAT5e cable. The specification set on the tester actually exceeds the CAT5e requirements. Should the cable have been certified? Look at the length measurement for the 3–6 pair length. The cable is 1040 feet in length. Remember, the maximum cable length for a CAT5e cable run is 100 meters.



FAIL

OMNIScanner2 Certification Report

Circuit ID: Split Pairs	OMNIScanner	OMNIRemote
Project: TIA Project	50D99L00377	50E99L00037
Owner: OMNIScanner 2	Adapter	Adapter
Autotest: Cat 5E Link	CHAN 5/5E/6	CHAN 5/5E/6
Cable: Cat 5E UTP		
NVP: 72	Limit	12 36 45 78
Site: Las Cruces	Length ft	(308) 45 45 47 47
Building: Manufacturing	Delay (ns):	(518) 64 64 66 67
Floor: 3rd	Resistance (Ohms):	(—) — — — —
Closet: 315A	Wiremap	Expected Actual
	OMNI:	12345678 ! 12345678 Skew (ns): (45) 3
	Remote:	12345678 ! 12345678 Bandwidth (MHz): —

Attenuation				Overall Margin (dB) ¹ -19.5			Return Loss				Overall Margin (dB) ¹ -5.4						
Pairs	dB	Margin	MHz	OMNIScanner			OMNIRemote			Pairs	dB	Margin	MHz				
12	! 38.0	-16.4	99.4	12	! 10.6	-5.3	29.3	! 10.5	-5.3	29.5	36	! 10.4	-5.4	29.8	! 10.6	-5.2	29.3
36	! 41.1	-19.5	99.9	45	19.4	6.1	68.0	20.8	3.8	1.4	45	2.9	18.6	99.2	21.3	4.3	1.6
45	2.9	18.6	99.2	78	20.3	3.3	1.4	21.3	4.3	1.6	78	2.9	18.7	99.9			
78	2.9	18.7	99.9														

NEXT				Overall Margin (dB) ¹ -37.7			ACR				Overall Margin (dB) ¹ —		
Pairs	dB	Margin	MHz	OMNIScanner			OMNIRemote			Pairs	dB	Margin	MHz
12/36	! 22.3	-37.7	1.6	! 11.0	-36.4	11.8	12/36	—	—	—	—	—	—
12/45	56.6	5.4	6.8	54.2	3.5	7.3	12/45	—	—	—	—	—	—
12/78	69.8	9.9	1.9	70.2	10.9	2.1	12/78	—	—	—	—	—	—
36/45	39.4	4.9	74.1	56.1	3.9	5.9	36/45	—	—	—	—	—	—
36/78	68.2	9.6	2.3	68.7	9.4	2.1	36/78	—	—	—	—	—	—
45/78	59.5	15.5	19.0	57.3	13.2	19.0	45/78	—	—	—	—	—	—

ELFEXT				Overall Margin (dB) ¹ -30.1			PSNEXT				Overall Margin (dB) ¹ -34.7		
Pairs	dB	Margin	MHz	OMNIScanner			OMNIRemote			Pairs	dB	Margin	MHz
12/36	! 26.4	-30.1	1.6	! 26.6	-29.9	1.6	12	! 22.2	-34.7	2.1	! 11.0	-33.4	11.8
12/45	67.8	16.6	2.8	37.2	16.6	93.8	36	! 22.2	-34.7	2.1	! 11.0	-33.4	11.8
12/78	80.0	22.3	1.4	80.1	22.3	1.4	45	53.1	5.3	7.3	52.0	3.7	6.8
36/12	! 26.6	-29.9	1.6	! 26.4	-30.1	1.6	78	66.1	9.2	2.1	66.3	9.4	2.1
36/45	60.8	14.7	5.0	35.4	13.0	76.3							
36/78	79.9	22.2	1.4	57.9	21.2	14.7							
45/12	! 8.6	-11.4	99.4	! 10.4	-9.6	99.4							
45/36	! 1.9	-18.2	99.4	! 5.8	-14.2	99.9							
45/78	50.3	15.5	18.3	49.8	15.2	18.7							
78/12	! 14.4	-5.6	99.4	! 9.2	-10.9	99.4							
78/36	! 10.4	-9.7	99.9	23.3	3.3	99.9							
78/45	49.9	15.3	18.7	50.4	15.6	18.3							

PSELFEXT				Overall Margin (dB) ¹ -27.1			PSACR				Overall Margin (dB) ¹ —		
Pairs	dB	Margin	MHz	OMNIScanner			OMNIRemote			Pairs	dB	Margin	MHz
12	! 26.6	-26.8	1.6	! 26.4	-27.0	1.6	12	—	—	—	—	—	
36	! 26.4	-27.1	1.6	! 26.6	-26.9	1.6	36	—	—	—	—	—	
45	68.9	14.2	1.4	33.6	14.2	76.3	45	—	—	—	—	—	
78	72.0	17.3	1.4	72.1	17.4	1.4	78	—	—	—	—	—	

¹ Overall margin value is the worst margin for OMNI and Remote.

FIGURE 2-38 The Test 3 CAT5e link test showing failures with attenuation.



FAIL

OMNIScanner2 Certification Report

Circuit ID: Long Box	OMNIScanner	OMNIRemote
Project: TIA Project	50D99L00377	50E99L00037
Owner: OMNIScanner 2	Adapter	Adapter
	CHAN 5/5E/6	CHAN 5/5E/6
Autotest: Cat 5E Link		
Cable: Cat 5E UTP		
NVP: 72		
Site: Las Cruces		
Building: Manufacturing		
Floor: 3rd		
Closet: 315		
	Length ft	Limit 12 36 45 78
	Delay (ns):	(308) 1068 ! 1040 1050 1074
	Resistance (Ohms):	(518) 1508 ! 1469 1482 1516
		(---) --- --- --- ---
	Wiremap	Expected Actual
	OMNI:	12345678 12345678
	Remote:	12345678 12345678
		Skew (ns): (45) ! 47
		Bandwidth (MHz): ---
Attenuation	Overall Margin (dB)* -62.1	Return Loss Overall Margin (dB)* 4.9
Pairs dB Margin MHz		OMNIScanner OMNIRemote
12 ! 72.7 -52.8 86.4		Pairs dB Margin MHz dB Margin MHz
36 ! 74.5 -54.1 89.8		12 23.2 7.0 26.4 27.4 10.4 2.1
45 ! 80.4 -61.5 78.3		36 25.2 8.2 1.4 23.3 9.1 50.7
78 ! 82.4 -62.1 89.1		45 20.9 4.9 27.5 24.6 7.6 12.9
		78 25.4 8.4 2.3 24.6 8.6 28.0
NEXT	Overall Margin (dB)* 7.6	ACR Overall Margin (dB)* ---
Pairs dB Margin MHz	OMNIScanner OMNIRemote	Pairs dB Margin MHz dB Margin MHz
12/36 60.3 13.8 13.6 63.6 13.8 8.4		12/36 --- --- --- --- --- ---
12/45 44.1 10.1 78.5 53.8 15.7 44.1		12/45 --- --- --- --- --- ---
12/78 48.4 8.6 34.9 59.6 8.2 6.6		12/78 --- --- --- --- --- ---
36/45 66.1 8.1 2.5 62.6 7.6 3.9		36/45 --- --- --- --- --- ---
36/78 45.4 13.0 99.2 69.3 12.4 3.0		36/78 --- --- --- --- --- ---
45/78 63.8 13.0 7.3 69.4 16.9 5.7		45/78 --- --- --- --- --- ---
ELFEXT	Overall Margin (dB)* -21.1	PSNEXT Overall Margin (dB)* 9.4
Pairs dB Margin MHz	OMNIScanner OMNIRemote	Pairs dB Margin MHz dB Margin MHz
12/36 ! 5.1 -15.7 91.6 ! 7.5 -13.5 89.8		12 47.9 11.1 34.9 59.3 10.8 6.6
12/45 ! 9.6 -11.1 92.5 ! 4.4 -17.8 78.3		36 64.3 10.2 3.0 62.2 10.0 3.9
12/78 ! 3.0 -18.0 89.1 ! 0.6 -20.4 89.1		45 64.7 9.4 2.5 62.1 9.9 3.9
36/12 ! 13.0 -8.7 83.0 ! 11.2 -9.1 96.1		78 58.5 10.7 7.3 59.5 11.0 6.6
36/45 ! 1.4 -20.8 78.3 ! 5.6 -16.1 82.8		
36/78 ! 8.3 -12.6 90.4 ! 1.7 -19.4 89.1		
45/12 ! 7.7 -13.6 86.4 ! 8.3 -13.0 86.4		
45/36 ! 5.4 -16.3 82.8 ! 8.1 -13.5 82.8		
45/78 ! 1.3 -19.0 96.7 ! 1.3 -19.7 89.1		
78/12 ! 8.6 -13.1 83.0 ! 6.7 -14.9 83.0		
78/36 ! 4.7 -16.2 89.8 ! 7.6 -13.4 89.8		
78/45 ! 1.1 -21.1 78.3 ! 4.9 -17.2 78.3		
		PSELFEXT Overall Margin (dB)* -18.4
		Pairs dB Margin MHz dB Margin MHz
		12 ! 5.0 -13.3 86.4 ! 6.2 -12.4 83.0
		36 ! 1.3 -16.5 91.6 ! 3.4 -14.6 89.8
		45 ! 4.3 -14.9 78.3 ! 0.7 -18.4 78.3
		78 ! 0.3 -17.7 89.1 ! 0.8 -17.2 90.4
		PSACR Overall Margin (dB)* ---
		Pairs dB Margin MHz dB Margin MHz
		12 --- --- --- --- --- ---
		36 --- --- --- --- --- ---
		45 --- --- --- --- --- ---
		78 --- --- --- --- --- ---

* Overall margin value is the worst margin for OMNI and Remote.

FIGURE 2-39 A CAT5e link test showing failures with delay skew (Test 4).

Summary of CAT5e Cable Test Examples

This section has provided a few examples of CAT5e link tests. The objective has been to provide actual test data for various cable problems that might occur on the job. In the tests where a failure was detected, the tester displayed a failed screen, and the certification report identified the problem. The following is a summary of the tests:

- **Test 1:** The certification report shows a test result of PASS.
- **Test 2:** The certification report shows a test result of FAIL. The report shows the cable failed the wire-map test.
- **Test 3:** This cable test generated a test result of FAIL. Examination of the attenuation and return-loss shows that the cable failed to meet CAT5e attenuation and return-loss specifications. The cable also failed NEXT, ELFEXT, PSNEXT, and PSELFEXT tests.
- **Test 4:** The certification report shows the cable fails the CAT5e link test. Examination of the report shows the cable failed the delay skew measurement because the cable length exceeded the 100-meter maximum. The cable also fails attenuation, ELFEXT, and PSELFEXT tests.

The reasons for examining the test results is to find out why a cable fails a test. You need to know whether the problem is with your terminations, cable layout, or the way the cable is installed. Keeping a record of the cable tests will help you isolate recurring problems.

Tests 1 and 2 demonstrate the importance of keeping a record of tests. In this case, the cable was certified but later failed. The documentation provided by the certification report provides evidence that the cable was functioning properly and did meet CAT5e specifications.

Section 2-7 Review

This section has covered the following **Network+** Exam objectives.

1.5 Install and properly terminate various cable types and connectors using the appropriate tools

The certification exams require the use of sophisticated test gear to conduct the many tests needed to certify a cable.

4.4 Given a scenario, troubleshoot and resolve common cable issues

This section presents several examples of tests and possible problems that might be encountered. Some problems could be a result of poor installation, bad connectors, or bad cable, and the network administrator needs to have good documentation that each cable has been certified if possible.

Test Your Knowledge

1. Patch cables are too short to be tested. True or **False**?
2. A UTP certification report lists the following.

Pairs	12	36	45	78
Length	285	288	284	283

What do these results indicate?

- a. The test must be repeated.
 - b. Insufficient information to obtain an answer.
 - c. The cable length is too long.
 - d. **The cable passes the length test.**
3. A data problem is reported to the network administrator. The problem is found to be with the UTP network connection. Which steps could the network administrator have taken to isolate the problem? (Select two.)
- a. Visually inspect all UTP terminations.
 - b. **Run a cable test using a cable tester.**
 - c. **Use the **ping** command to verify network connectivity.**
 - d. Use pairs 4/5 7/8 to repair the connection.
 - e. Contact the installer of the UTP cable to obtain a certification report.

SUMMARY

This chapter introduced the basics of horizontal cabling and unshielded twisted-pair cable. The major topics the student should now understand include the following:

- Six subsystems of a structured cabling system
- The purpose of the telecommunication closet and the LAN work area
- The performance capabilities of CAT6/5e UTP
- The wiring color schemes for T568A and T568B
- The pin assignments for the RJ-45 (8P8C) modular plug
- The technical issues of copper over 10G Ethernet
- The procedures for testing a CAT6/5e link
- The procedures for troubleshooting a CAT6/5e link
- How to examine and use the test results provided by a CAT6/5e link certification report

QUESTIONS AND PROBLEMS

Section 2-2

1. What is an 8P8C connector?
 - a. Another term for an RJ-11 connector
 - b. Another term for an RJ-6 connector
 - c. Another term for an RJ-45 connector
 - d. Another term for RS-232
2. What do EIA and TIA stand for?

EIA: Electronics Industries Alliance

TIA: Telecommunication Industry Association
3. What are the three parts of the EIA/TIA 568B standard?

EIA/TIA-568-B.1 Commercial Cabling Standard

EIA/TIA-568-B.2 Twisted-pair Media

EIA/TIA-568-B.3 Optics Fiber Cabling Standard

4. Identify the six subsystems of a structured cabling system.
 1. Building Entrance
 2. Equipment Room
 3. Backbone Cabling
 4. Telecommunications Closet
 5. Horizontal Cabling
 6. Work Area
5. Which subsystem does permanent networking cabling within a building belong to?

Horizontal Cabling
6. What is a cross-connect?

It is a space where one or more cables connect to one or more cables or equipment.
7. What is the main cross-connect?

It is the point that usually connects two or more buildings.
8. The Telco and the ISP usually connect to what room in the campus network hierarchy?

Main cross-connect (MC)
9. What is the WO, and what is its purpose?

Workstation (WO): Outlet is the termination for the horizontal cross-connect.
10. The patch cable from a computer typically terminates into which of the following?
 - a. Jack in a wall plate
 - b. BNC connector
 - c. Thin net
 - d. RJ-11 modular plug
 - e. RG-59
11. What is the over all length limitation of an individual cable run from the telecommunications closet to a networking device in the work area?

100 meters
12. A general rule of thumb is to allow how many meters for the cable run from the telecommunications closet to the work area?

90 meters

Section 2-3

13. How many pins does an RJ-45 modular plug have?

8 pins

14. What is the difference in CAT 5 and CAT 5e?

CAT5e is an enhanced cable capable of carrying data at a rate of 1000 Mbps.

CAT5 is only good for 100 Mbps.

15. What is the data rate for Ethernet?

10 Mbps

16. What is the data rate for FastEthernet?

100 Mbps

17. What improvements will CAT6 and CAT7 cable provide?

Each provides improved bandwidth, which leads to improved data rates.

18. What is the data rate for gigabit Ethernet?

1000 Mbps

19. What is a benefit of using shielded twisted-pair cabling?

The shield reduces the potential for electromagnetic interference.

20. Which cable, UTP or STP, is preferred by the industry?

Testing shows little performance improvement using STP. The additional cable and installation cost do not justify its use in all cases; therefore, the industry usually recommends the use of UTP cable. However, this can change with higher data rates such as 10G.

Section 2-4

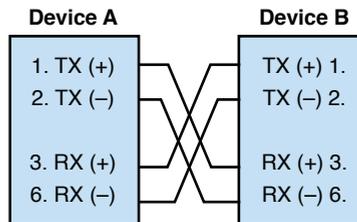
21. What are the color maps and pin number assignments for T568A and T568B?

T568A	T568B
1. White-Green	1. White-Orange
2. Green	2. Orange
3. White-Orange	3. White-Green
4. Blue	4. Blue
5. White-Blue	5. White-Blue
6. Orange	6. Green
7. White-Brown	7. White-Brown
8. Brown	8. Brown

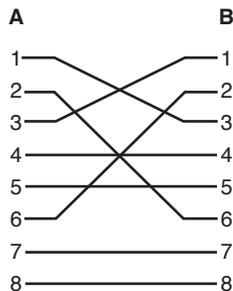
22. What is the difference between T568A and T568B?

Two different standards for wiring modular connectors.

23. How many wires are in a CAT6 twisted-pair cable?
8 wires
24. How many wire pairs are in a CAT6 twisted-pair cable?
4 pairs
25. In regards to a CAT6 cable, what pin numbers in an RJ-45 connector are used to carry data in a FastEthernet network?
TX(+)
TX(-)
RX(+)
RX(-)
26. What does an “X” on the input to a hub represent?
Indicates this is a cross-connected input.
27. Define the term cross-connected input.
Transmit and receive pairs are internally swapped to maintain proper alignment of the TX and RX pairs.
28. Draw a picture of properly aligned transmit and receive signal of a computer’s data link that is running Ethernet data rates.



29. What is the difference between “straight” and “cross-connected” input ports?
“Straight” =Tx----Tx Rx----Rx. “Crossed”= Tx----Rx Rx----Tx.
30. Draw the wire-map for a “cross-over” CAT6 UTP cable running FastEthernet.



31. Define a UTP link test.
Tests the cable from one cable termination to another.
32. Define a UTP full channel test.
Tests all the link elements from the hub or switch through the patch panel to the wall plate.
33. Define the term NEXT and what it measures.
Near End Crosstalk: A measure of the level of crosstalk within the cable.
34. A NEXT measurement of 59.5 dB is made on wire pairs 1–2/3–6. A next measurement of 51.8 dB is made on wire pairs 3–6/7–8. Which cable pairs have the best measure NEXT performance?
1–2/3–6. A high NEXT (dB) value is desirable.
35. Define Power-Sum measurements.
All four-wire pairs are used to obtain a combined performance measurement.
36. Define propagation delay.
Amount of time it takes a signal to propagate from one end of the cable to another.
37. Signals travel in a cable at some percentage of the velocity of light. What is the term for this?
NVP: nominal velocity of propagation.
38. Why is delay skew critical?
If the wire lengths of different wire pairs are significantly different, then the data on each wire will arrive at the receiver at a different time, potentially creating distortion of the data.
39. Why are power-sum measurements critical for high-speed data communication over UTP?
High-speed data communications (e.g., gigabit) requires the use of all four-wire pairs, hence the need to obtain the combined performance measurement of all four-wire pairs.
40. The expected + loss of a 20m UTP cable should be (greater than or less than) a 90m UTP cable?
Less than.
41. What is 8P8C, and what connector type is most associated with this?
8P8C (8 pin 8 connector); the RJ-45 plug and jack are the most common connectors.

42. What are the pin assignments for 1/10 Gbps?

Refer to Figure 2-11.

43. What is the purpose of a lacing tool?

This is used to properly align the wires for 568A/B and to make sure the untwisted wire is kept to a minimum.

Section 2-5

44. What is the limit on the bend radius for a UTP cable, and why is this important?

The limit is four times the diameter of the cable, and bends exceeding this can introduce attenuation loss.

45. Is a high PSNEXT measurement desirable?

Yes, this indicates better cable performance.

46. Define margin (dB) relative to cable measurements. What does it mean if the margin lists a negative value?

The margin indicates how many dB the measured value exceeds the limit. A negative value indicates the measurement is less than the limit.

Section 2-6

47. Define Alien Crosstalk and draw a picture of how this can happen.

Basically this is an unwanted signal coupling from one four-pair cable to another. See Figure 2-31 for an example of AXT.

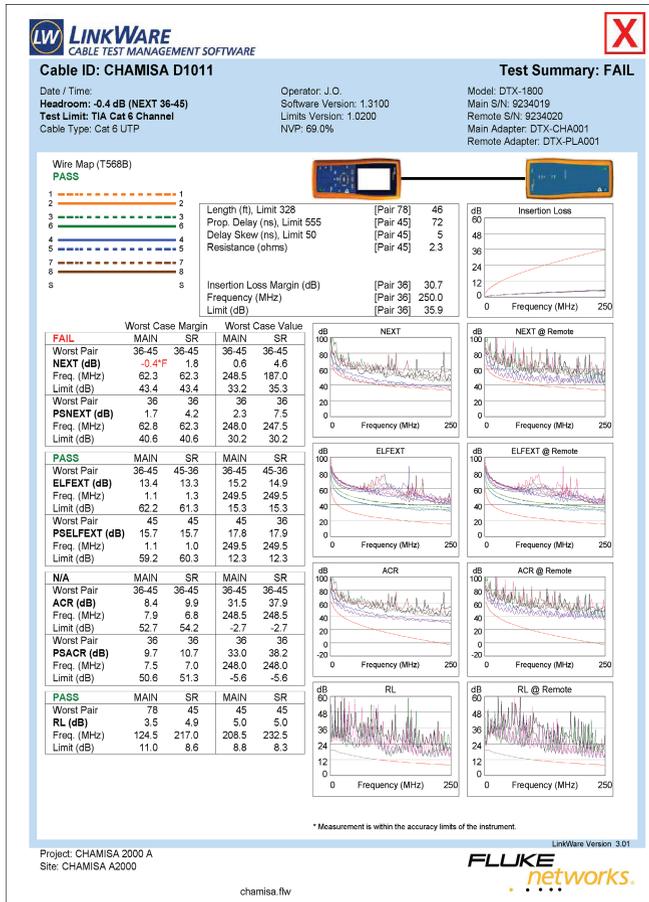
48. What is F/UTP, and what is its purpose?

This is foil over twisted-pair cabling, and it provides improved security and noise immunity.

49. Why is balance an issue in UTP cables, and what is TCL?

The balance or symmetry of the signal over the wire pairs helps to minimize unwanted leakage of the signal when transmitting gigabit data rates. TCL is Transverse Conversion Loss, and it measures the differential output signal given a common-mode signal on the input.

50. Answer the following questions for the certification report displayed here.



a. What is the length of pair 7-8?

46 ft.

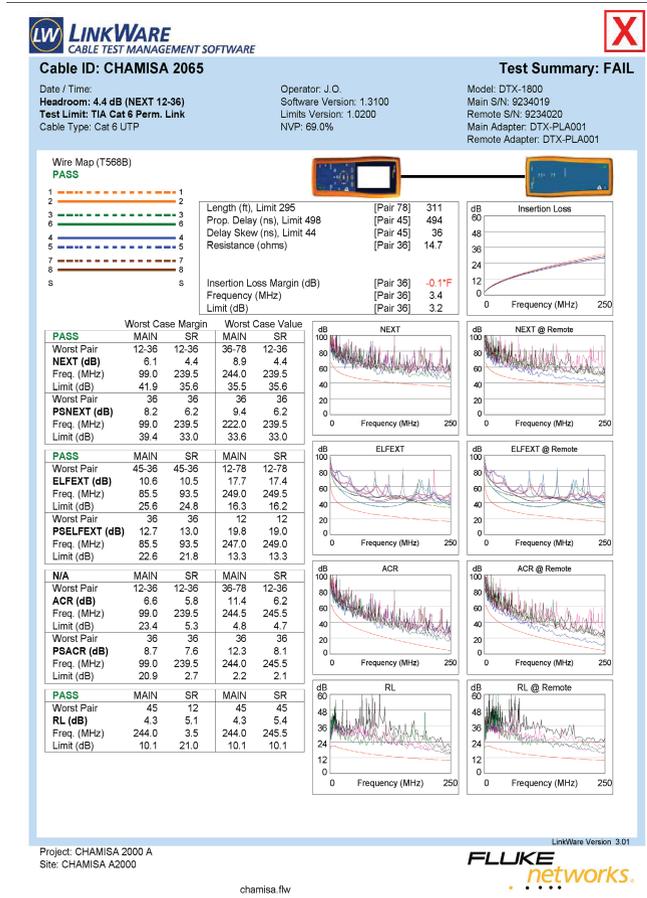
b. What is the length of pair 4-5?

72 ft.

c. Why did this cable fail the test?

Fails NEXT.

51. Answer the following questions for the certification report displayed here.



a. What is the length of wire pair 7–8?

311 ft. (exceeds the maximum length for a permanent link).

b. What is the delay skew for pair 4–5?

36 ns.

c. Why did this cable fail the wire-map test?

The cable is too long.

52. Answer the following questions for the certification report displayed here.




OMNIScanner2 Certification Report

Circuit ID: Grey 1	OMNIScanner	SW: V06.00	OMNIRemote
Project: TIA Project	SD:99,00377		SD:99,00377
Owner: OMNIScanner 2	Adapter		Adapter
Autotest: Cat 5E Link	CHAN 5/5E/6		CHAN 5/5E/6





Site: Las Cruces	Length ft	Limit	12	36	45	78
Building: Manufacturing	(308)	(308)	21	0	22	121
Floor: 3rd	Delay (ns):	(518)	30	0	31	30
Closet: 315	Resistance (Ohms):	(---)	---	---	---	---

Wiremap	Expected	Actual	
OMNI:	12345678	! 12345678	Skew (ns): (45) 31
Remote:	12345678	! 12547683	Bandwidth (MHz): ---

Attenuation				Overall Margin (dB)*		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12	1.5	19.7	96.1			
36	---	---	---			
45	---	---	---			
78	---	---	---			

Return Loss				Overall Margin (dB)*		
Pairs	dB	Margin	MHz	dB	Margin	MHz
12	19.2	6.9	94.3	19.0	6.7	95.6
36	---	---	---	---	---	---
45	---	---	---	---	---	---
78	---	---	---	---	---	---

NEXT						Overall Margin (dB)*			
Pairs	dB	Margin	MHz	dB	Margin	MHz	dB	Margin	MHz
12/36	---	---	---	---	---	---	---	---	---
12/45	---	---	---	---	---	---	---	---	---
12/78	---	---	---	---	---	---	---	---	---
36/45	---	---	---	---	---	---	---	---	---
36/78	---	---	---	---	---	---	---	---	---
45/78	---	---	---	---	---	---	---	---	---

ACR						Overall Margin (dB)*			
Pairs	dB	Margin	MHz	dB	Margin	MHz	dB	Margin	MHz
12/36	---	---	---	---	---	---	---	---	---
12/45	---	---	---	---	---	---	---	---	---
12/78	---	---	---	---	---	---	---	---	---
36/45	---	---	---	---	---	---	---	---	---
36/78	---	---	---	---	---	---	---	---	---
45/78	---	---	---	---	---	---	---	---	---

ELFEXT						Overall Margin (dB)*			
Pairs	dB	Margin	MHz	dB	Margin	MHz	dB	Margin	MHz
12/36	---	---	---	---	---	---	---	---	---
12/45	---	---	---	---	---	---	---	---	---
12/78	---	---	---	---	---	---	---	---	---
36/12	---	---	---	---	---	---	---	---	---
36/45	---	---	---	---	---	---	---	---	---
36/78	---	---	---	---	---	---	---	---	---
45/12	---	---	---	---	---	---	---	---	---
45/36	---	---	---	---	---	---	---	---	---
45/78	---	---	---	---	---	---	---	---	---
78/12	---	---	---	---	---	---	---	---	---
78/36	---	---	---	---	---	---	---	---	---
78/45	---	---	---	---	---	---	---	---	---

PSNEXT						Overall Margin (dB)*			
Pairs	dB	Margin	MHz	dB	Margin	MHz	dB	Margin	MHz
12	---	---	---	---	---	---	---	---	---
36	---	---	---	---	---	---	---	---	---
45	---	---	---	---	---	---	---	---	---
78	---	---	---	---	---	---	---	---	---

PSELFEXT						Overall Margin (dB)*			
Pairs	dB	Margin	MHz	dB	Margin	MHz	dB	Margin	MHz
12	---	---	---	---	---	---	---	---	---
36	---	---	---	---	---	---	---	---	---
45	---	---	---	---	---	---	---	---	---
78	---	---	---	---	---	---	---	---	---

PSACR						Overall Margin (dB)*			
Pairs	dB	Margin	MHz	dB	Margin	MHz	dB	Margin	MHz
12	---	---	---	---	---	---	---	---	---
36	---	---	---	---	---	---	---	---	---
45	---	---	---	---	---	---	---	---	---
78	---	---	---	---	---	---	---	---	---

* Overall margin value is the worst margin for OMNI and Remote.


Page 1

- a. Why did the cable fail the test?
- b. Draw the wire-map diagram for this cable.

There are multiple errors with cable wiring. The cable wire-map should show a straight-through connection, but it shows this:

- 1-1 5-7
- 2-2 6-6
- 3-5 7-8
- 4-4 8-3

Section 2-7

53. A UTP Certification report lists the following.

Pairs	12	36	45	78
Length	285	288	284	283

What do these results indicate? Select the correct answer.

- a. The test must be repeated.
 - b. Insufficient information to obtain an answer.
 - c. The cable length is too long.
 - d. **The cable passes the length test.**
54. A data problem is reported to the network administrator. The problem is found to be with the UTP network connection. What steps could the network administrator have taken to isolate the problem? (Select two.)
- a. Visually inspect all UTP terminations.
 - b. **Run a cable test using a cable tester.**
 - c. **Use the ping command to verify network connectivity.**
 - d. Use pairs 4/5 7/8 to repair the connection.
 - e. Contact the installer of the UTP cable to obtain a certification report.

CERTIFICATION QUESTIONS

55. A NEXT measurement of 59.5 dB is made on wire pairs 1-2/3-6. A NEXT measurement of 51.8 dB is made on wire pairs 3-6/7-8. Pairs 3-6/7-8 have the best NEXT performance measurement.
- a. True
 - b. **False**
56. In regards to CAT5e / CAT6 cable operating at half-duplex mode for Ethernet or FastEthernet, pins 1/2 3/6 are used to carry the data.
- a. **True**
 - b. False
57. A CAT5e / 6 link test, tests from one termination to another.
- a. True
 - b. **False**

58. Only two wire-pairs are used to obtain a proper Power Sum measurement.
- a. True
 - b. False
59. Delay skew is critical because if the wire lengths of different wire pairs are significantly different, the data will arrive at the receiver at a different time potentially creating distortion of the data.
- a. True
 - b. False
60. Which does permanent networking cabling within a building belong to?
- a. Vertical Cabling
 - b. Work Area
 - c. Equipment Room
 - d. None of these answers is correct.
61. How many pins does an RJ-45 modular plug have?
- a. 4
 - b. 6
 - c. 8
 - d. 16
 - e. None of these answers is correct.
62. Which of the following best defines horizontal cabling?
- a. Cabling that extends out from the telecommunications closet into the LAN work area.
 - b. Cabling that extends out from the work area into the LAN.
 - c. Cabling that extends out from the backbone into the LAN work area.
 - d. Cabling that extends out from the equipment room into the LAN work area.
 - e. None of these answers is correct.