Chapter 2 Solutions

Activities

Activity 2-1
No specific answer is required, but students should be able to repair a connection that has a corrupt TCP/IP configuration.

Activity 2-2
No specific answer is required, but students should be able to view the current IP address settings on a server.

Activity 2-3
No specific answer is required, but students should be able to view the current IP settings using the IPCONFIG utility.

Activity 2-4
No specific answer is required, but students should be able to configure alternative IP address information to be used when a DHCP server is unavailable.

Activity 2-5
No specific answer is required, but students should be able to use FTP to download a utility.

Activity 2-6
No specific answer is required, but students should be able to use Telnet to verify the functionality of an SMTP server.

Activity 2-7
No specific answer is required, but students should be able to connect to resources using TCP and UDP port numbers.

Activity 2-8
No specific answer is required, but students should be able to install Network Monitor to enable packet capturing.

Activity 2-9
No specific answer is required, but students should be able to capture and view TCP connection packets in Network Monitor.

Activity 2-10
No specific answer is required, but students should be able to capture and view UDP packets in Network Monitor.

Activity 2-11
No specific answer is required, but students should be able to test the functionality of a host using the ping command.

Activity 2-12
No specific answer is required, but students should be able to view the TTL of a ping packet.

Activity 2-13

No specific answer is required, but students should be able to view the contents of the ARP cache.

Review Questions

1. For what type of protocol is the development process controlled by a standards committee rather than any single company or individual?
Answer: A

2. Which of the following protocols is required for access to the Internet?
Answer: C

3. Which of the following network services is used by Active Directory for service location?
Answer: B

4. How many octets are in an IP address?
Answer: B

5. How many bits are in an octet?
Answer: C

6. Which of the following defines the part of an IP address that is the host ID and the part that is the network ID?
Answer: D

7. What is the default subnet mask for a Class C IP address?
Answer: C

8. A computer will use a default gateway if the destination IP address is on a different network. True or False?
Answer: True

9. Which of the following is another name for default gateway?
Answer: A

10. IP address 227.43.76.109 is an example of which of the following classes of IP addresses?
Answer: D

11. What was introduced to make Internet routing and the assignment of IP addresses more efficient?
Answer: D

12. How many octets are part of the host ID for the IP address 176.167.98.3/24?
Answer: 1

13. What type of server does a Windows client use to resolve NetBIOS names to IP addresses?
Answer: C

14. Which transport protocol establishes a connection with the remote host before sending data?
Answer: B

15. Which protocol supports the use of multicast groups?
Answer: E

16. Which of the following is not an application layer protocol?

Answer: C

17. Which network layer protocol is responsible for routing packets on the network?
Answer: C

18. ARP is used to resolve IP addresses to what?
Answer: B

19. When a packet crosses a router, what happens to the packet's TTL?
Answer: B

20. You ping a host that is on a remote subnet. When you view your ARP cache, which MAC address do you see for the remote host?
Answer: C

21. A network card operates at which layer of the IP stack?
Answer: D

22. Which of the following statements regarding TCP are false? (Choose all that apply.)
Answer: E

23. Which of the following statements regarding e-mail protocols are true? (Choose all that apply.)
Answer: A,C

24. Which port is used by HTTP?
Answer: E

25. Which transport layer protocol is most likely to be used for streaming media?
Answer: C

Case Projects

Case Project 2-1

The more likely configuration issues are:

- An incorrect IP address has been configured, therefore the server cannot communicate with other computers in the lab, or the default gateway.
- An incorrect default gateway has been configured, therefore the server cannot communicate outside the lab.
- An incorrect DNS server has been configured, therefore the host name utilities.arctic.local cannot be resolved to an IP address.
- An incorrect subnet mask has been configured, therefore this server is confused about which computers are on the local network and which computers are not. This is particularly likely because the default subnet mask for addresses on the 172.20.10.0 network would be 255.255.255.0 because it is a class B address.

Case Project 2-2

HTTP would be allowed for Web access. FTP would be allowed for file transfers. Telnet would be blocked to prevent hacking of internal Linux servers. SMTP would be allowed only for the mail server. POP3 and IMAP4 would be blocked since they are not required when using an internal e-mail server.

Case Project 2-3

When downloading from a web site you are using the HTTP application layer protocol. HTTP uses TCP as a transport layer protocol. TCP is a reliable protocol that will ensure that all packets reach their destination. Reliability is achieved by using a sliding window. A sliding window only sends a certain number of packets at a time then waits for acknowledgement that they were received. If a single packet is lost the entire process pauses until the packet is resent.

Since this is only happening for one web site and not all of them it appears to be a problem with the remote site and not the internal setup. Therefore no solution can be implemented internally.

Case Project 2-4

Twisted-pair cabling can be used by either Token Ring or Ethernet. Ethernet equipment is much cheaper and operates at faster speeds. This would be most appropriate in the offices.

Connectivity in the class would be easiest with 802.11b wireless. This would save the cost of installing cabling and allow the professors to be completely mobile. The 802.15 standard would not be appropriate because of its shorter range.

Chapter 2: TCP/IP Architecture

Objectives

After reading this chapter and completing the exercises students will be able to:

- Understand TCP/IP addressing
- Describe the overall architecture of TCP/IP
- Describe Application layer protocols
- Discuss Transport layer protocols
- Understand the role of various Internet layer protocols, including IP, ICMP, and ARP
- Understand Network Interface layer protocols

Introduction To TCP/IP

1. Transmission Control Protocol/Internet Protocol (TCP/IP) is the most commonly used network protocol suite in use today for the following reasons:

- It has wide vendor support
- It is an open protocol
- It provides access to Internet services

TCP/IP is automatically installed with Windows Server 2003 and cannot be removed.

Teaching Tip	Make sure students understand the fundamentals of TCP/IP so they are able to plan, manage and troubleshoot a Windows Server 2003 network.

Activity 2-1: Repairing a Network Connection

The purpose of this activity is to repair a connection that has a corrupt TCP/IP configuration.

IP Addresses

1. An IP address, like a mailing address for a house, is unique. The most common format for IP addresses is four numbers; each called octets, which are separated by periods. An example of an IP address is 192.168.5.66. Each octet in an IP address represents eight bits of information. If each octet is eight bits, then a full IP address of four octets is 32 bits long. When a computer works with an IP address, it is treated as a lump of 32 bits rather than four octets. The division into octets just makes it easier for people to use the addresses.

2. An IP address is composed of two parts: the network ID and the host ID. The network ID represents the network on which the computer is located. No two networks can have the same network ID or else routers cannot determine where to deliver packets that are addressed to that network ID. The host ID represents the individual computer on a network. No two computers on the same network can have the same host ID; however, two computers on different networks can have the same host ID. IP addresses that can be used on the Internet are assigned by an Internet service provider (ISP).

Subnet Masks

1. A subnet mask defines which part of its IP address is the network ID and which part is the host ID. Subnet masks are composed of four octets just like an IP address. The simplest subnet masks use only the two values of 0 and 255. Wherever there is a 255 in the subnet mask, that octet is part of the network ID. Wherever there is a 0 in the subnet mask, that octet is part of the host ID.

2. A computer uses its subnet mask to determine which network it is on and whether other computers with which it is communicating are on the same network or a different network. If two computers on the same network are communicating, then they can deliver packets directly to each other. If two computers are on different networks, they must use a router to communicate.

Teaching Tip	Make sure students understand why and how computers utilize subnet masks.

Default Gateway

1. Default gateway is another term for router. If a computer does not know how to deliver a packet, it gives the packet to the default gateway to deliver. This happens every time a computer needs to deliver a packet to a computer on a network other than its own.

2. Routers can distinguish multiple networks and how to move packets between them. Routers can also figure out the best path to use to move a packet between different networks.

3. A router has an IP address on every network to which it is attached. When a computer sends a packet to the router (default gateway) for further delivery, the address of the router must be on the same network as the computer, because computers can talk directly only to devices on their own network.

Activity 2-2: Viewing IP Address Configuration

The purpose of this activity is to view the current IP address settings on a server.

IP Address Classes

1. IP addresses are divided into five classes: A-E. The class of an IP address defines the default subnet mask of the device using that address. All of the IP address classes can be identified by the first octet of the address.

2. Class A addresses use eight bits for the network ID and 24 bits for the host ID. The value of the first octet is always in a range from 1 to 127. Class A networks are only assigned to very large companies and Internet providers.

3. Class B addresses use 16 bits for the network ID and 16 bits for the host ID. The value of the first octet ranges from 128 to 191. Class B networks are assigned to many larger organizations, such as governments, universities, and companies with several thousand users.

4. Class C addresses use 24 bits for the network ID and eight bits for the host ID. The value of the first octet ranges from 192 to 223. Although there are very many Class C networks, they have a relatively small number of hosts, and, thus, are suited only to smaller organizations.

5. Class D addresses are not divided into networks and they cannot be assigned to computers as IP addresses. Class D addresses are used for multicasting. The value of the first octet ranges from 224 to 239.

6. Multicast addresses are used by groups of computers. A packet addressed to a multicast address is delivered to each computer in the multicast group. This is better than a broadcast message because routers can be configured to allow multicast traffic to move from one network to another. In addition, all computers on the network process broadcasts, whereas only computers that are part of that multicast group process multicasts.

7. Class E addresses are considered experimental and are not used. The first octet of Class E addresses ranges from 240 to 255.

Teaching Tip	Make sure students understand the various types of IP address classes that are used for different types of business needs.

Classless Inter-domain Routing

1. Classful routing is when routers on the Internet use IP address classes to move packets. With classful routing, each Internet backbone router potentially needs to keep 2,097,152 entries in its routing table for Class C networks alone. As the number of Class C networks assigned grew, this became unsustainable. Classful routing wastes many IP addresses. If an organization needed 20 IP addresses, it required an entire Class C address. Out of the 254 hosts on a Class C network, 234 would be unused.

2. To make Internet routing and the assignment of IP addresses more efficient, classless interdomain routing (CIDR) was introduced. CIDR does not use the default subnet masks for routing. Instead, the subnet mask must be defined for each network. A definable subnet mask is more flexible and efficient because a single network can be subnetted and organizations assigned only a small part of a Class C network. CIDR also reduces the number of routing table entries that Internet backbone routers must hold. A single routing table entry can replace hundreds or thousands of entries for Class C networks.

Teaching Tip	Make sure students understand the benefits of classless routing over classful routing.

Reserved Addresses

1. There are a number of IP addresses and IP networks that are reserved for special purposes and either cannot be assigned to hosts or cannot be used on the Internet.

2. When packets need to be delivered to all computers on a network, they are addressed to a broadcast IP address. There are two different types of broadcast IP addresses: local and directed.

3. A packet addressed to a local broadcast address is delivered to all computers on a local network and is discarded by routers. The IP address 255.255.255.255 is a local broadcast; all address bits are set to 1.

4. A packet addressed to a directed broadcast address is a broadcast on a specific network. These packets can be routed to get to the network to which it is aimed. The IP address for a directed broadcast is composed of the network ID to which it is directed and then all host bits are set to 1. Routers can be configured to block directed broadcasts, but forwards them by default.

5. Any IP address with 127 as the first octet cannot be assigned to a host. These are referred to as loopback addresses. However, all of these addresses starting with 127 are actually the local host. If you ping 127.0.0.1, you are actually pinging the machine you are on.

DNS

1. Domain Name System (DNS) is essential to a Windows Server 2003 network. It is used to resolve host names to IP addresses, find domain controllers, and find e-mail servers. DNS is essential for Active Directory to work properly.

WINS

1. Windows Internet Naming Service (WINS) is used to resolve NetBIOS names to IP addresses. In addition, it stores information about services such as domain controllers. WINS is used primarily for backward compatibility with Windows NT and Windows 9x.

DHCP

1. Dynamic Host Configuration Protocol (DHCP) is an automated mechanism to assign IP addresses to clients. Automating this process avoids the problem of records being entered incorrectly. If a change needs to be made for the IP addressing information, you can simply change the information in the DHCP server.

Activity 2-3: Using IPCONFIG to View IP Configuration

1. The purpose of this activity is to view the current IP settings using the IPCONFIG utility.

Activity 2-4: Configuring an Alternative IP Configuration

1. The purpose of this activity is to configure alternative IP address information to be used when a DHCP server is unavailable.

Quick Quiz

1. An IP address is like a mailing address for a house in that it must be ___________________________.
   Answer: unique

2. A(n) ____________________________ mask defines which part of an IP address is the network ID and which part is the host ID.
   Answer: subnet

3. IP addresses can be divided into____________________________.
   Answer: classes

4. True or False: To make Internet routing more efficient CIDR was created.
   Answer: True

5. True or False: WINS is used to resolve host names to IP addresses.
   Answer: False

TCP/IP Architecture Overview

1. The TCP/IP model can be broken down into four layers: Application, Transport, Internet, and Network Interface:

- The Application layer provides access to network resources. It defines the rules, commands, and procedures that client software uses to talk to a service running on a server.
- The Transport layer is responsible for preparing data to be transported across the network. This layer breaks large messages into smaller packets of information and tracks whether they arrived at their final destination.
- The Internet layer is responsible for logical addressing and routing. IP addresses are logical addresses. Any protocol that is network-aware exists in this layer.
- The Network Interface layer consists of the network card driver and the circuitry on the network card itself.

2. The Open Systems Interconnection (OSI) reference model is an industry standard that is used as a reference point to compare different networking technologies and protocols.

Teaching Tip	Make sure students understand the four layer model of TCP/IP.

Application Layer Protocols

1. There are many Application layer protocols, each of which is associated with a client application and service. Some examples include: HTTP, FTP, Telnet, SMTP, POP3 and IMAP4.

HTTP

1. Hypertext Transfer Protocol (HTTP) is the most common protocol used on the Internet today. This is the protocol used by Web browsers and Web servers. HTTP defines the commands that Web browsers can send and how Web servers are capable of responding.

2. Many commands are defined as part of the protocol. Information can also be uploaded using the HTTP protocol. Some of the common methods for passing data from a Web server to an application are as follows:

- Common Gateway Interface (CGI)
- Internet Server Application Program Interface (ISAPI)
- Netscape Server Application Program Interface (NSAPI)

FTP

1. File Transfer Protocol (FTP) is a simple file-sharing protocol. It includes commands for uploading and downloading files, as well as requesting directory listings from remote servers. FTP is implemented in stand-alone FTP clients as well as in Web browsers.

Activity 2-5: Using FTP to Download a File

1. The purpose of this activity is to use the command line FTP client to download files.

Telnet

1. Telnet is a terminal emulation protocol that is primarily used to connect remotely to UNIX and Linux Systems. The Telnet protocol specifies how a telnet server and telnet client communicate. The most common reason to connect to a server via Telnet is to manage remotely UNIX or Linux systems.

2. All of the administration for these systems can be done through a character based interface. Telnet does not support a graphical user interface (GUI), only text. The telnet server controls the entire user environment, processes the keyboard input, and sends display commands back to the client. A telnet client is responsible only for displaying information on the screen and passing input to the server. There can be many telnet clients connected to a single server at one time.

SMTP

1. Simple Mail Transfer Protocol (SMTP) is used to send and receive e-mail messages between e-mail servers that are communicating. It is also used by e-mail client software, such as Outlook Express, to send messages to the server. SMTP is never used to retrieve e-mail from a server when you are reading it.

Activity 2-6: Using Telnet to Verify SMTP

1. The purpose of this activity is use Telnet to verify the functionality of an SMTP server.

POP3

1. Post Office Protocol version 3 (POP3) is the most common protocol used for reading e-mail messages. This protocol has commands to download messages and delete messages from the mail server. POP3 does not support sending messages. By default, most e-mail client software using POP3 copies all messages onto the local hard drive and erases them from the server. However, you can change the configuration so that messages can be left on the server. POP3 supports only a single inbox and does not support multiple folders for storage on the server.

IMAP4

1. Internet Message Access Protocol version 4 (IMAP4) is another common protocol used to read e-mail messages. The abilities of IMAP4 are beyond those of POP3. IMAP4 can download message headers only and allow you to choose which messages to download. In addition, IMAP4 allows for multiple folders on the server side to store messages.

Teaching Tip	Make sure students can distinguish between SMTP, POP3 and IMAP4.

Transport Layer Protocols

1. Transport layer protocols are responsible for getting data ready to move across the network. The most common task performed by Transport layer protocols is breaking entire messages down into packets.

2. Each Transport layer protocol has its own set of ports. When a packet is addressed to a particular port, the Transport layer protocol knows to which service to deliver the packet. The combination of an IP address and port number is referred to as a socket. A port number is like an apartment number for the delivery of mail. The network ID of the IP address ensures that the packet is delivered to the correct street

(network); the host ID ensures that the packet is delivered to the correct building (host); the Transport layer protocol and port number ensure that the packet is delivered to the proper apartment (service).

3. The two Transport layer protocols in the TCP/IP protocol are:
   a. Transmission Control Protocol (TCP)
   b. User Datagram Protocol (UDP).

Activity 2-7: Using Port Numbers

1. The purpose of this activity is to connect to resources using TCP and UDP port numbers.

TCP

1. Transmission Control Protocol (TCP) is the most commonly used Transport layer protocol. TCP is connection-oriented and reliable. TCP verifies that the remote host exists and is willing to communicate before starting the conversation. The establishment of a connection is a three-packet process between the source and destination host. It is often called a three-way handshake.

2. The SYN bit indicates that this packet is a request to negotiate a connection. This request includes parameters for the conversation such as the maximum packet size.

3. The ACK bit is an option in a packet that indicates this packet is a response to the first packet.

4. TCP is considered reliable because it tracks each packet and makes sure that it arrives at its destination. If a packet is lost or damaged as part of the communication process, then the packet is transmitted again. The overall process is called a sliding window. If a thousand packets are waiting to be sent as part of the communication process, not all of the packets are sent at once because it would be too difficult to track. Only a few packets are sent at a time. The number of packets is negotiated as part of the process of establishing the connection and is considered as being the size of the sliding window.

5. The sliding window cannot be moved past a packet that has not been received and acknowledged by the destination. If a packet goes missing, it must be retransmitted and acknowledged before the sliding window can move past that point. A common reason why there is a pause in the middle of large downloads from the Internet is that a packet has been lost and must be retransmitted before the conversation can continue. Being reliable and connection-oriented are generally desirable qualities. Consequently, TCP is the Transport layer protocol used for most Internet services. HTTP, FTP, SMTP, POP3, and IMAP4 all use TCP.

Activity 2-8: Installing Network Monitor

1. The purpose of this activity is to install Network Monitor to enable packet capturing.

Activity 2-9: Viewing a TCP Connection in Network Monitor

1. The purpose of this activity is to capture and view TCP connection packets in Network Monitor.

UDP

1. User Datagram Protocol (UDP) is not as common as TCP and is used for different services. UDP is connectionless and unreliable. UDP does not attempt to negotiate terms with a remote host before sending information. UDP simply sends the information. If any terms need to be negotiated, the Application layer protocol has to do it. There is no handshake for UDP. UDP does not track or guarantee delivery of packets between the source and destination. UDP just sends a stream of packets without waiting for acknowledgment. There is no sliding window for UDP.

2. UDP is the Transport layer protocol to use when you are unconcerned about missing packets or want to implement reliability in a special way. Streaming audio and video are in this category. If streaming audio were to pause and wait for missing packets to be sent again, then there could be long pauses in the sound. Most people prefer a small amount of static or silence to be inserted for the missing packet and for the rest of the audio track to continue to play. UDP does this because it does not keep track of packets that are missing or needing to be sent again. In the case of streaming audio, re-sent packets are handled by the Application layer protocol. Connectionless communication also makes sense when the amount of data being exchanged is very small. Using three packets to set up a connection for a two-packet conversation is very inefficient. The resolution of a DNS name is a two-packet communication process and is done via UDP.

Activity 2-10: Capturing UDP Packets in Network Monitor

1. The purpose of this activity is to capture and view UDP packets in Network Monitor.

TCP versus UDP

1. TCP is connection-oriented and reliable. TCP is like delivering a letter by registered mail. When the message is received, the sender receives notice that it arrived properly at its destination.

2. UDP is connectionless and unreliable. If you were to take the a single message and place it on several postcards, take all of the postcards and dump them in the mail box separately, then the likelihood is that the recipient would be able to put them in the proper order and understand the message. However, if one postcard was missing, it would be difficult for the recipient to understand the complete message.

Internet Layer Protocols

1. Internet layer protocols are responsible for all tasks related to logical addressing. An IP address is a logical address. Any protocol that is aware of other networks, as in how to find them and how to reach them, exists at this layer. Each Internet layer protocol is very specialized. They include: IP, RIP and OSPF, ICMP, IGMP, and ARP.

IP

1. Internet Protocol (IP) is responsible for the logical addressing of each packet created by the Transport layer. As each packet is built, IP adds the source and destination IP address to the packet. When a packet is received from the network, IP verifies that it is addressed to this computer. IP looks at the destination IP address of the packet to verify that it is the same as the IP address of the receiving computer, or a broadcast address of which this computer is a part.

RIP and OSPF

1. Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) are routing protocols responsible for defining how paths are chosen through the internetwork from one computer to another. They also define how routers can share information about the networks of which they are aware.

ICMP

1. Internet Control Messaging Protocol (ICMP) is used to send IP error and control messages between routers and hosts. The most common use of ICMP is the ping utility. The ping utility uses ICMP packets to test connectivity between hosts. Many firewalls are configured to block ICMP packets.

2. The Time Exceeded ICMP packet type indicates that a packet could not reach its destination because delivery took too long.

3. The Time to Live (TTL) of a packet is a combination of router hops and seconds. Each router that forwards a packet reduces the TTL of the packet by one. If it takes longer than 1 second to forward the packet, then the TTL is also reduced by one for each second that it is delayed.

Activity 2-11: Testing Host Functionality

1. The purpose of this activity is to test the functionality of a host using the ping command.

Activity 2-12: Viewing TTL

1. The purpose of this activity is to view the TTL of a ping packet.

IGMP

1. Internet Group Management Protocol (IGMP) is used for the management of multicast groups in the following ways:

- Hosts use IGMP to inform routers of their membership in multicast groups.
- Routers use IGMP to announce that their networks have members in particular multicast groups.

The use of IGMP allows multicast packets to be distributed only to routers that have interested hosts connected.

ARP

1. Address Resolution Protocol (ARP) is used to convert logical IP addresses to physical MAC addresses. This is an essential part of the packet delivery process. Network cards use a MAC address to filter irrelevant packets. When a packet is received, the network card verifies that the destination MAC address matches the MAC address of the network card or is a broadcast MAC address.

2. Data packets have four addresses:
-source IP address
-destination IP address
-source MAC address
-destination MAC address

3. When a packet is created, the source computer must find the MAC address of the destination computer based on the destination IP address. ARP uses a two-packet process to find the MAC address of the destination computer. The first packet is an ARP Request that is broadcast to all computers on the local network asking for the MAC address of the computer with the destination IP address. The destination computer sees this packet and sends an ARP Reply containing its MAC address. The sending computer can then create data packets using the destination MAC address.

4. The ARP_RARP section of the packet is the ARP information that is processed by ARP on the receiving computer. The most important information in this part of the packet is the Target’s Protocol Address. This is the IP address of the destination computer. If the Target’s Protocol Address matches the IP address of Computer B, then an ARP Reply packet is created. If the Target’s Protocol Address does not match the IP address of Computer B, then the packet is discarded.

5. The ETHERNET section of the packet contains the MAC address information used by network cards when analyzing whether the packet should be passed up to IP. In this packet, the source MAC address is the MAC address of Computer B and the destination MAC address is the MAC address of Computer A. The ARP_RARP section of the packet has the ARP information required by Computer A to create proper data packets. The Sender's Hardware Address is the MAC address that is required by Computer A.

6. If routers are forwarding packets, then the ARP process is modified. The first ARP Request is for the default gateway, then the ARP Response includes the MAC address of the router. The data packet is then built and sent to the router. The router removes and then replaces the source MAC address with its own and uses ARP to find the MAC address of the next router, if required, or the final destination host.

Activity 2-13: Viewing the ARP Cache

1. The purpose of this activity is for you to view the contents of the ARP cache and clear the cache to force the rebuilding of the cache information.

Network Interface Layer Protocols

1. Most of the common Network Interface layer protocols are defined by the Institute of Electrical and Electronics Engineers (IEEE). The IEEE has a system of numbered committees that each defines a different Network Interface layer protocol.

2. Ethernet is the most common Network Interface layer protocol used in corporate networks today. There are many different varieties of Ethernet, all of which use Carrier Sense Multiple Access/Collision Detection (CSMA/CD) for access control. The most common version of Ethernet is implemented with twisted-pair cabling at 100 Mbps.

3. Token Ring is an older technology created by IBM that was implemented in the late 1980s and early 1990s. It was commonly implemented with mainframe computers. This standard uses twisted-pair cabling and operates at 4 Mbps or 16 Mbps. The access method used is token passing.

4. Wireless LAN is one of the fastest growing network types. The 802.11b standard defines the most common wireless standard. It uses radio signals to send data at 11 Mbps. The maximum distance of 802.11b is approximately 300 feet indoors and up to 1000 feet outdoors. The 802.11g standard transfers data at 54 Mbps and is backward compatible with 802.11b.

5. The IEEE standard 802.15 defines the Physical layer portion of the Bluetooth standard. Bluetooth is a short-range wireless communication system with a maximum distance of approximately 30 feet and a maximum speed of 720 Kbps. This is a much shorter range and much slower data transfer rate than 802.11b. The IEEE 802.15 committee intends to increase this speed. Support for Bluetooth is built into many smaller devices that need to minimize energy consumption, such as Palm and Windows CE devices.

Quick Quiz

1. The four layers of the TCP IP model are: Application, Transport, Network Interface and ___________________________.
   Answer: Internet

2. ____________________________ is a simple file sharing protocol.
   Answer: FTP

3. ____________________________ is the most common protocol used for reading email messages.
   Answer: POP3

4. True or False: TCP is the most common protocol used for reading e-mail messages.
   Answer: True

5. True or False: IMAP4 is a common protocol used to send email messages.
   Answer: False

Class Discussion Topics

1. How does a computer utilize a subnet mask?

2. List the different types of IP address classes.

3. What is the difference between classful and classless routing?

4. What is the benefit of having a DHCP?

Additional Projects

1. You are a technology consultant hired to decide the type if IP address a company needs. Company # 1 is a large organization with over 100, 000 hosts and has asked that their network be subnetted to control traffic flow. Which IP address class would you recommend?

2. A computer installed with Windows Server 2003 is having trouble connecting to the internet. The connections look fine but you need to verify that the IP address exists and is valid before you do any additional troubleshooting. What steps would you take to verify the IP address for this machine?

Solutions to Additional Projects

1. Company # 1 requires a Class A IP address for the following reasons:
   a. Up to 16 million hosts can be serviced with this type of address
   b. It can be subnetted
   c. It is designed for large organizations

2. To check for an IP address using Windows Server 2003 perform the following steps:
   a. Click Start, point to Control Panel, point to Network Connections, right click on the specific network connection in question and click Support.
   b. View the connection status settings before resetting and performing other troubleshooting steps.

Chapter 2 Solutions

Lab 2.1 Review Question Answers

1. To view the Alternate Configuration tab, click the _____ option on the General tab of the Internet Protocol (TCP/IP) Properties dialog box.
   Answer: A
2. If a DHCP server offers a lease, what will be the result?
   Answer: A
3. When your computer obtains an automatic private IP address, which of the following options are not assigned. (Choose all that apply).
   Answer: C, D
4. When your computer obtains an Automatic private IP address, with which of the following subnets would your computer be able to communicate? (Choose all that apply.)
   Answer: D
5. In order to make TCP/IP configuration changes and to renew and release TCP/IP addresses, you need to belong to which of the following group(s). (Choose all that apply)
   Answer: A, C

Lab 2.2 Review Question Answers

1. In an ARP Request frame, which of the following is unknown?
   Answer: C
2. Static entries remain in the ARP cache ___. (Choose all that apply)
   Answer: A, D
3. Which of the following events cause an interface to be reinitiated? (Choose all that apply.)
   Answer: A, B, C, D, E
4. Which command would you use to remove static entries from the ARP cache?
   Answer: B
5. Which of the following statements are true? (Choose all that apply.)
   Answer: A, C, D

Lab 2.3 Review Question Answers

1. Which of the following best describes the functionality of the version of Network Monitor that comes with Windows Server 2003?
   Answer: B
2. Which of the following information can be found within a frame? (Choose all that apply.)

Answer: A, B, C, D

3. In Network Monitor you can create a ___ so that, if Network Monitor detects a particular set of conditions on the network, it can start a capture, end a capture, or start a program.
   Answer: D
4. To which group must you belong on the local computer to install Network Monitor?
   Answer: A
5. If you want to capture data from multiple local networks at the same time, which of the following best describes the actions you would take?
   Answer: B

Lab 2.4 Review Question Answers

1. Which of the following is true regarding local area connections?
   Answer: D
2. Which of the following is true? (Choose all that apply).
   An*swer: A, B*
3. Which of the following are examples of LAN connections? (Choose all that apply).
   Answer: A, B, C, D
4. Which of the following options can be viewed from the General tab in the Local Area Connection Status dialog box?
   Answer: D
5. If a local area connection icon displays on your taskbar with a red question mark, what does this indicate?
   Answer: B

Lab 2.5 Review Question Answers

1. What do you type in a command prompt window to exit the Netsh utility but to remain in the Command Prompt window?
   Answer: A
2. Which of the following can be configured using the Netsh interface ip command-line utility? (Choose all that apply).
   Answer: A, B, C, D
3. Which of the following would be the correct syntax to use with Netsh interface ip if you wanted to reset the Private connection to obtain both the IP address and the DNS server settings automatically?
   Answer: C
4. Which of the following would be the correct syntax to use with Netsh interface ip if you wanted to view the Internet Protocol (TCP/IP) configuration for the Private connection?
   Answer: B

5. On your computer, you haven't renamed the local area connection in the Network Connections folder. It is presently configured to obtain an IP address automatically; however, you want to add the DNS server configuration settings manually using the Netsh utility. Which of the following will allow you to configure a DNS server address of 192.168.1.10 for that connection?
   Answer: B