APPENDIX B

Exercise Answers

Chapter 1 Exercises

1. The network used exclusively by the University of Texas is an example of a *campus area network* (CAN). Note that LAN and MAN are also appropriate responses.
2. What are the names of the layers in the OSI reference model?
   - Layer 7 — Application
   - Layer 6 — Presentation
   - Layer 5 — Session
   - Layer 4 — Transport
   - Layer 3 — Network
   - Layer 2 — Data Link
   - Layer 1 — Physical
3. List at least five applications and/or utilities that use TCP/IP.
   - Telnet
   - FTP

- SMTP
- POP
- SNMP

4. What are the two types of network relationships?
   - Connectionless
   - Connection-oriented
5. Explain the difference between a client/server network relationship and a client/server database system.

   In both cases, the server provides the data requested by a client, but in a database system, the client node has to use its own resources to format and view the data retrieved.
6. What is the 1822 protocol?

   Specifies the method to connect a host computer to an ARPANET router.
7. What are the three types of standards? Do a search on the Internet to see if you can find at least one of each standard type.
   - Proprietary
   - Open
   - De facto
8. The 802.11n standard supports an operating frequency of *2.4 GHz* and *5 GHz*. The maximum data rate for 802.11n is *600 Mbps*. 802.11n reaches a maximum indoor range of *70 meters* and an outdoor range of 250 meters.
9. True or false: The Application layer of the OSI model concerns itself with the application/user interface on a PC.

   True
10. In this chapter, we listed seven reasons why TCP/IP has grown to be the ''method of choice.'' What are these seven reasons?
    - Routing
    - Addressing
    - Name resolution
    - Operates on many types of networks
    - Connection-oriented

- Open standards
- Application support

Chapter 2 Exercises

1. Modem is short for modulator/demodulator.
2. A *LAN (local area network)* is a network where network devices are located within close proximity to each other.
3. CSMA/CD is an acronym for *Carrier Sense Multiple Access with Collision Detection* and is associated with a network using a *bus* network topology.
4. Which network topology allows for orderly network access for the stations connected to that network?

   Token Ring
5. What two standards define a CSMA/CD network?
   - IEEE 802.3
   - Ethernet
6. Name three media types that can be used to interconnect devices located on a LAN.
   - Wire
   - Fiber optic
   - Wireless
7. What is the major characteristic of 10BASE-T cable?

   Unshielded twisted pair (UTP)
8. A personal computer (PC) requires a *network interface card (NIC)* to be connected to a local area network (LAN).
9. FDDI is an acronym for *Fiber Distributed Data Interface*, which is often used to construct citywide networks called *metropolitan area networks (MANs)*.
10. POTS is an acronym for *plain old telephone system*.
11. A dialup service that connects to a digital network is *integrated services digital network (ISDN)*.

12. What technology can be used to create a point-to-point network connection over the Internet?

    VPN (virtual private network)

Chapter 3 Exercises

1. Explain what ''10 half or 100 full?'' means to you, what the difference between 10 half and 100 full is, and list pros and cons of each.
    - 10 half is 10Mbps at half-duplex. It is slower and prone to collisions.
    - 100 full is 100Mbps at full-duplex. It is faster and not prone to collisions
2. List three types of interfaces and three types of adaptors.

    Interfaces:

    - The network interface controller (NIC).
    - The point at the boundary of a LAN, which connects the LAN to an outside network, is another type of network interface.
    - In Layer 3 environments, *interface* is often the term used to describe a network connection and really isn't considered hardware.

    Adaptors:

    - The network interface controller (NIC)
    - Virtual adaptor
    - Physical adaptor
3. Why is an NIC card considered both an interface and an adaptor?

    The NIC card adapts to the computer, allowing it to have an interface to the network.
4. List three examples of flash memory:
    - Memory cards for cell phones
    - Memory cards for digital cameras
    - Memory cards for video game systems
    - PCMCIA type 1 memory cards
    - PCMCIA type 2 memory cards
    - PCMCIA type 3 memory cards
    - Personal computer system BIOS chip

5. List the PDU for each of the OSI layers.

Layer	**PDU**
Application	Data
Presentation	Data
Session	Data
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bit

6. What is the difference between volatile and nonvolatile memory?

   Volatile memory content is erased when power is removed. Nonvolatile memory retains its contents whether power is on or off.

7. What is the difference between STP and UTP cabling?

   STP has a shield around the twisted pairs, whereas UTP has no shield.

8. Explain when you would want to use MMF cables instead of SMF cables. Next, explain in what instances SMF cabling would be preferred over MMF cabling.

   SMF cables are thinner than MMF cables. This is because SMF cables are designed to carry a single beam of light. Because there are not multiple beams involved, the SMF cable is more reliable and supports greater distances and a bandwidth much higher than MMF cables. The bulk cost of SMF cabling is much less expensive than the MMF cabling. MMF cabling is made for shorter distances. Unlike SMF, there are multiple beams of light, so the distance and speed is less. Granted, supporting data rates of up to 10 Gbps for distances as far as 300 meters is nothing to sneeze at. Because of the additional modes, MMF cabling is able to carry much more data at any given time.

9. Define *modulation*.

   The process of manipulating a waveform to create a signal that sends a message that needs to be communicated. In data communications, modulation is performed by a node that converts a digital signal to an analog signal, in order to be communicated over a phone line.

10. What does a router use to determine the best path to a destination?

    Routing table

Chapter 4 Exercises

1. If you have a network-capable PC, try using a few of the network utilities discussed in this chapter.
2. Open a DOS window by running `cmd` from Start ➪ Run and enter the command `ipconfig` and note what is displayed.
3. Issue the command `ipconfig /all` and note what is displayed.
4. If your network allows your PC to access the Internet, execute this command `tracert <insert your favorite website URL>` and hit the Return key. Note the results. You may want to repeat this to other Internet addresses.
5. To display information about all the interfaces on a Unix computer, which command would need to be issued?

   `netstat`
6. What is used on the Internet to find the numeric address of a computer host that resides on the Internet?

   DNS server
7. True or false: Floppy disks are the fastest form of magnetic media.

   False
8. True or false: AT&T is the sole provider for the Unix operating system.

   False
9. Can you name at least one Linux distribution?

   Red Hat, SUSE, Ubuntu
10. If a microprocessor designer wanted to allow his newest chip design to access a greater amount of memory space, what might he do to accomplish this?

    Increase the number of address bits available

Chapter 5 Exercises

1. What are the four layers of the TCP/IP reference model?
   - Network interface layer
   - Internet layer
   - Transport layer
   - Application layer

2. Name four Application layer protocols that we discussed in this chapter.
   - DNS (Domain Name System)
   - SNMP (Simple Network Management Protocol)
   - FTP (File Transfer Protocol)
   - TFTP (Trivial File Transfer Protocol)
   - SMTP (Simple Mail Transfer Protocol)
   - NFS (Network File System)
   - TNP (Telecommunications Network Protocol)
   - SSH (Secure Shell)
3. Explain the structure of the DNS hierarchy.

   DNS names are organized hierarchically, with an unnamed root at the top, then what are known as top-level domain (TLD) names next, followed by second-level domain, and, finally, one or more subdomains.
4. What are the five PDU types that are used by SNMP?
   - GetRequest
   - GetNextRequest
   - SetRequest
   - GetResponse
   - Trap
5. What is the purpose of FTP?

   The File Transfer Protocol (FTP) allows users to access an FTP server and transfer files to and from the server.
6. Why does TFTP not perform many of the functions that FTP does?

   TFTP is a simple file transfer protocol designed to transfer boot-up files for diskless nodes.
7. What is a daemon?

   A daemon is an application or a process that is running on a server for the purpose of providing client and server access and communication.
8. What are the four control characters used by Telnet for option negotiation and their meanings?
   - WILL — Used when the sender wants to enable an option
   - WONT — Used when the sender wants to disable an option
   - DO — Used when the sender wants the receiver to enable an option

- DON'T — Used when the sender wants the receiver to disable an option

9. TCP is a *connection-oriented* protocol, whereas UDP is a *connectionless* protocol
10. What are the three main reporting functions that we said are performed by ICMP?
    - Error reporting
    - Testing and troubleshooting
    - Informational reporting

Chapter 6 Exercises

1. What does the acronym CSMA/CD mean?

   Carrier Sense Multiple Access with Collision Detection.
2. What form of communications eliminates the need for collision detection?

   Full-duplex
3. When you choose not to configure an Ethernet port's speed and duplex mode what are you relying on?

   Autonegotiation
4. What is needed when setting up VLAN networking?

   The ability to tag frames
5. What is a source address? What is a destination address?

   A source address is the address of the network node that is transmitting the frame. A destination address is the address of the network node that the frame is intended for.
6. What is the maximum number of bytes the Data field can contain in an Ethernet frame? What is the minimum number of data bytes?

   The maximum number of bytes in the Data field is 1500. The minimum number is 46 bytes.

Chapter 7 Exercises

1. True or false: The only type of node that is used on a FDDI ring is a FDDI concentrator.

   False

2. The three levels of operation within the X.25 protocol suite are:
   - Physical level
   - Link level
   - Packet level
3. In X.25, *S-frames* are used to pass control data, such as transmission requests, status reporting, *I-frame* receipt acknowledgements, and termination requests.
4. What are the three main components used by PPP?
   - The PPP encapsulation method.
   - The PPP link control protocol (LCP)
   - The PPP network control protocol (NCP)
5. What is the difference between a DTE and a DCE in an X.25 network?

   The DTE are the user nodes (endpoint nodes), while the DCE is the entry to the cloud (network nodes).
6. What are the Session layer protocols that are used in the AppleTalk protocol suite?
   - AppleTalk DataStream Protocol (ADSP) — A connection-oriented protocol that provides a data channel for the host nodes.
   - AppleTalk Session Protocol (ASP) — ASP maintains and manages higher level sessions.
   - Printer Access Protocol (PAP) — Maintains and manages virtual connections to printers, print servers, and other server types.
   - Zone Information Protocol (ZIP) — Used to manage network numbers and AppleTalk zone names.
7. What does the acronym ISDN stand for?

   Integrated services digital network
8. What is the frame relay local management interface (LMI) used for?

   LMI is used to provide link status updates pertaining to PVCs between a DTE and the local DCE. One of the functions performed by LMI is status inquiries that are sent out periodically (normally 10 seconds) to test to see if a link is up. If the inquiry does not receive a reply, it assumes the link is down. These inquiries are known as *keepalives*. LMI will also send out updates pertaining to the status of all the links in a frame relay network, provide information about PVC changes, and ensure that IP multicast is functioning.

9. What is a constant bit rate (CBR)?

   A constant bit rate means that the bandwidth required to pass the data is always available.

10. The *Link Control Protocol (LCP)* is the foundation protocol of the PPP protocol suite.

Chapter 8 Exercises

1. List in order from highest to lowest the upper layers of the OSI model, also indicating their layer number.
   - Application Layer — Layer 7
   - Presentation Layer — Layer 6
   - Session Layer — Layer 5

2. An application that runs on a user's workstation and communicates over a network with an appropriate application that is running on a server is considered to be what type of application?

   Client/server

3. Which protocol is considered to be a connection-based protocol?

   TCP (Transmission Control Protocol)

4. What functionality can be used to disguise addresses from a private address space to be seen on the Internet?

   NAT (Network Address Translation)

5. List the three private address spaces that may be used and are considered to be not routable over the Internet.
   - 10.X.X.X
   - 172.16.X.X
   - 192.168.X.X

6. Name an Application layer protocol that can be used to perform file transfers over the network.

   FTP (File Transfer Protocol)

7. What is the protocol that resolves IP addresses to hardware addresses?

   ARP (Address Resolution Protocol)

Chapter 9 Exercises

1. What are the two ISO/IRC standards that define recommendations for the transport layer?

   ISO/IEC 8072 and ISO/IEC 8073

2. What are the two types of transport service?

   - Connectionless
   - Connection-oriented

3. From the following list, fill in the class function in the following table.

   - Multiplexing class
   - Error detection and recovery class
   - Simple class
   - Error recovery and multiplexing class
   - Basic error recovery class

Class Name	**Class Function**
Class 0	Simple class
Class 1	Basic error recovery class
Class 2	Multiplexing class
Class 3	Error recovery and multiplexing class
Class 4	Error detection and recovery class

4. Match the type with the correct description:

   - Type C — Network connections that maintain an unacceptable rate of residual errors
   - Type A — Network connections that maintain both an acceptable rate of signaled errors and residual errors
   - Type B — Network connections that maintain an acceptable rate of residual errors and an unacceptable rate of signaled errors

5. Define *upward multiplexing*.

   Multiple Transport layer signals to a single network signal

6. Define *downward multiplexing*.

   Multiple network signals to a single transport signal

7. Explain how a three-way handshake works.
    1. The originating node will send a request known as a *SYN* to the destination node.
    2. The destination node will let the originating node know that it has received the SYN request by sending back a *SYN-ACK* message.
    3. The originating node will respond to the SYN-ACK by sending back an *ACK* message.
8. List four Transport layer protocols.
    - ATP (AppleTalk Transaction Protocol)
    - DCCP (Datagram Congestion Control Protocol)
    - NetBEUI
    - RTP (Realtime Transport Protocol)
    - TCP (Transmission Control Protocol)
    - UDP (User Datagram Protocol)

Chapter 10 Exercises

1. Name the type of network service being used for each of the following:
    - HTTP — Connection-oriented
    - FTP — Connection-oriented
    - Mail — Connectionless
    - Telnet — Connection-oriented
2. A client/server application is considered to be what type of network service?

    Connection-oriented
3. What is a TLD and can you name a few?

    TLD is a top-level domain and is usually the suffix of a URL such as .com, .gov, .edu, or .net.
4. How is the MTU size determined?

    MTU is determined by taking the maximum packet size allowed to cross the network medium being used and subtracting the size of the frame's header and the remainder is the maximum payload size or MTU.

5. What does NAT accomplish?

   NAT enables the use of non-routable addresses to be used on a private network that can be used to translate out network requests to the Internet using a public IP address that the requestor's source address has been translated to.

6. Name two network tools that can be used to troubleshoot a network problem.

   `ping` and `traceroute`

Chapter 11 Exercises

1. How is a jam signal used in a CSMA/CD environment?

   A jam signal in CSMA/CD is a message to all other nodes that a collision has occurred and they should stop transmitting.

2. How is a jam signal used in a CSMA/CA environment?

   A jam signal lets all the other nodes know that the node is ready to transmit data.

3. An unnumbered frame type is used with which type of LLC?

   LLC-1, LLC-2, and LLC-3

4. Find the MAC address of your PC's NIC card. Once you have found it, take the OUI and look it up on the IEEE website. What is the information that is listed for that particular OUI?

   User-dependent results

5. What are the three fields in an LLC PDU, and what do they do?

   - Destination Service Access Point (DSAP) — This is used to identify the LLC that is supposed to receive the PDU.
   - Source Service Access Point (SSAP) — This is used to identify the LLC that is supposed to send the PDU.
   - Control — The control field provides sequencing data, command information, and responses to requests. Note that any or all of these can be used in any combination.

6. How many bits are in an IEEE 802 MAC address?

   There are 48 bits in an IEEE 802 MAC address.

7. What are the two error checking methods used at the Data Link layer?
   - Parity checking
   - CRC
8. What does full-duplex Ethernet use for flow control?

   PAUSE frames or the PAUSE function.
9. What is the functional difference between a bridge and a Layer 2 switch?

   There is no functional difference between a bridge and a switch. That's right! None! Nada! Zero! Zip! *Switch* is nothing more than a marketing term that came out in the 1990s.

Chapter 12 Exercises

1. What are the three layers of the hierarchical design model?
   - The access layer
   - The distribution layer
   - The core layer
2. In this chapter, we listed six benefits of the hierarchical model. List these.
   - Easy design replication
   - Easy expandability of the network
   - Provides redundancy
   - Increased network performance
   - Better security
   - Easy to manage and maintain
3. This question is actually broken down into questions about the 5-4-3 rule. Refer to Figure A-1 for these questions.

   a. Does this network comply with the 5-4-3 rule?
   - Yes

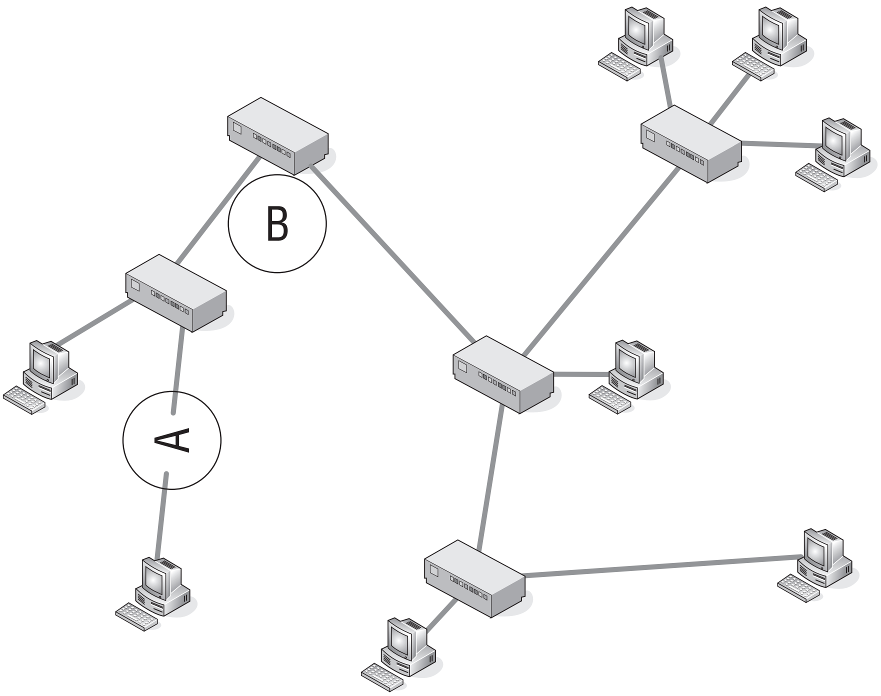

Figure A-1

b. Identify what A and B represent in the diagram.

- A = Segment
- B = Repeater

4. How many possible spanning tree states are there and what are they?

   There are five spanning tree port states:

- Disabled
- Blocking
- Listening
- Learning
- Forwarding

5. In this chapter, we discussed that a spanning tree port can be in a learning state. Why do you think that this is required instead of the port becoming active and just forwarding the frame?

   Having a port wait before forwarding data will prevent the alternative that is offered by the switched default behavior, which is to flood the frame for destinations that the port does not know about.

6. A port in a *learning* state is one that is *learning* paths to destinations and is preparing to forward the frame.

7. What is the purpose of the distribution layer of the hierarchical network?

   The distribution layer is the middleman between the access layer and the core. Data received from the access layer is sent to the core to be routed to the destination. Broadcast domains are separated at this layer with the implementation of virtual LANs (VLANs). Security is also a function that is implemented at this layer.

8. True or false: When the switch receives a frame, it will ‘‘tag’’ the frame with the VLAN identifier from where the data came from. This process is known as *implicit tagging*.

   False

9. What are the VLAN types we discussed in this chapter?

   - Port-based VLANs
   - MAC-based VLANs
   - Protocol-based VLANs
   - IP subnet-based VLANs

10. Take a look at Figure A-2 and then identify the appropriate layer of the hierarchical design model.

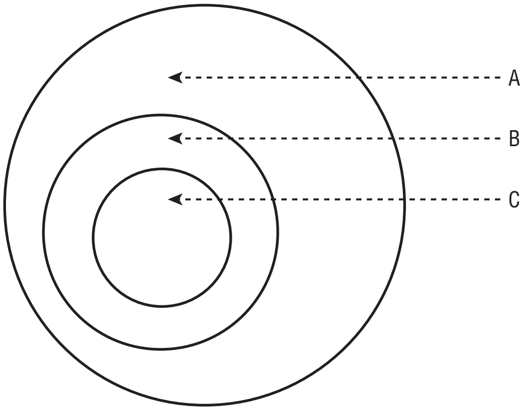

Figure A-2

- The letter *A* in the example represents the *access* layer.
- The letter *B* in the example represents the *distribution* layer.
- The letter *C* in the example represents the *core* layer.

Chapter 13 Exercises

The exercise in the chapter has no right or wrong answers. The important part is that you understand design planning concepts. If Rich and Jim get motivated enough, we will roll out a website with some more exercises. If not, there are many steps that you can take to create your own exercises.

Within Appendix A, there are some more direct questions pertaining to the chapter.

Chapter 14 Exercises

1. How would you best protect network elements that are located in a remote area away from the network operations center?

   Secure the area and keep it under lock and key.
2. Name a service that can provide not only user authentication but determine the amount of time a user has been logged in.

   RADIUS
3. What is a digital signature associated with?

   Certificates
4. Which tunneling protocol was first supported with Microsoft's Windows 95 operating system?

   PPTP

Chapter 15 Exercises

1. Which protocol can be used to monitor devices on a network?

   SNMP — Simple Network Management Protocol
2. Where would an SNMP agent be found?

   Embedded within a network-connected device
3. What would cause an alert to be displayed on an NMS workstation?

   A network-connected device that is being monitored to set an SNMP trap.

4. How would packets on a network be captured and inspected?

   With packet-capturing software loaded on a computer or a packet sniffer device.

Chapter 16 Exercises

1. For each item on the following list, identify the layer of the OSI reference model that item applies to.
   - Damaged cables — Layer 1
   - Dirty fiber — Layer 1
   - Excessive signal attenuation — Layer 1
   - Insufficient bandwidth — Layer 1
   - Denial-of-service (DoS) attack — Layer 2
   - Electrical interference — Layer 1
   - Wireless interference — Layer 1
   - Damaged interface — Layer 1
   - Dirty interface — Layer 1
   - Configuration error — Layer 2, Layer 3
   - Authentication issues — Layer 3
   - Excessive utilization — Layer 2
   - Excessive errors — Layer 2
   - VLAN configuration error — Layer 2, Layer 3
   - Class of Service issue — Layer 2
2. In the following example, explain why there is a missing hop.

```
C:\>tracert 207.215.79.16

Tracing route to www.testshow.com [207.215.79.16]
over a maximum of 30 hops:

1   1 ms  <10 ms  <10 ms 192.168.1.1
2   7 ms    7 ms    6 ms c-3-0-ubr01.boston.cast.net [43.16.12.1]
3   9 ms    8 ms    7 ms ge-1-37-ur01.boston.cast.net [43.16.12.193]
4    *       *       *    Request timed out.
5   7 ms    7 ms    7 ms po-24-ur01.boston.cast.net [43.16.12.161]
```

   In the example, there is a missing hop because the router 43.16.12.193 was unable to reach the preferred next hop and took an alternate path.

3. True or false: The UDP connection state is one of the fields displayed with the `netstat` utility.

   False. UDP is connectionless, so there is no such thing as a connection state. TCP is the connection state that is displayed with the `netstat` command.

4. Network *cable* testers are devices that are used to check the integrity of the cabling in the LAN.

5. List three options that can be used with the `arp` command in windows, and what each one does.

   - `-a` — Displays current ARP entries by interrogating the current protocol data. If `inet_addr` is specified, the IP and physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
   - `-g` — Same as `-a`.
   - `inet_addr` — Specifies an Internet address.
   - `-N if_addr` — Displays the ARP entries for the network interface specified by `if_addr`.
   - `-d` — Deletes the host specified by `inet_addr`. `inet_addr` may be wildcarded with * to delete all hosts.
   - `-s` — Adds the host and associates the Internet address `inet_addr` with the physical address `eth_addr`. The physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.
   - `eth_addr` — Specifies a physical address.
   - `if_addr` — If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

6. The network analyzer is also known as a *sniffer*.

7. What are three ways you can baseline your network? Explain details for each of these.

   - **Traffic analyzer** — The traffic analyzer (also known as a network analyzer, packet analyzer, packet sniffer, or just sniffer) can be an application or a specialized node that is used to capture data being transmitted on the network. Each packet is captured and can be manipulated and sorted by RFC, protocol, statistics, or whatever specifications are set by the user. The data can be organized and set to graphs or any other form supported by the analyzer and set by the user.

- **Statistical graphing with the management station** — SNMP management stations usually have the ability to record statistical data and record the data in reports and graphs. Maintaining such information can be useful in determining abnormal conditions within the catenet.
- **Determine thresholds that need to be maintained** — Know your LAN. Test and analyze traffic patterns, traffic capacity limits, overall throughput operation, routing path costs, Physical layer well-being, etc. Keep the results on hand for reference when an issue occurs. Not only can this assist in alerting you to abnormal operations, it can offer proof of the abnormal operations should you need to bring in a vendor for assistance in troubleshooting an issue. Understanding peak traffic periods, protocol usage statistics, average throughput, and normal traffic patterns is important in understanding problems that occur in the network and resolving them quickly and effectively.

8. What command can be used in a Windows environment that will provide you with detailed information about the current TCP/IP settings of your PC?

```
ipconfig /all
```

9. From your PC, open up a traffic analyzer and point it to the interface of your PC. Issue a constant ping to www.richardbramante.com (`ping www.richardbramante.com -t`). Next, disable your network connection. What do you notice in your trace?

   This exercise is mainly for the reader to get a better feel for data collection and process recognition. The main thing we are looking for in the answer to this question is the ARP processes that start when the connection is down, and then the route-learning processes that occur until the connection is recovered.

10. This chapter listed eight quick checks that you can do when you are having issues within a VLAN. What are they?

- Is there any maintenance going on at the time?
- Have there been any recent changes that may have created the issue?
- Verify the configurations of the bridges.
- Check statistics. Review logs and traces. Utilize `show` and `debug` commands that are available and are applicable.
- Is this a new configuration? Make sure that all necessary configuration parameters are set correctly.

- Are the VLANs configured correctly? Make sure that all VLAN rules were followed. Have there been any changes made? Did someone delete a VLAN?
- Are tagging rules applied correctly?
- Is there a routing issue that is preventing devices within the VLAN from communicating with other devices?

Appendix A Exercises

1. What is an Internet service provider (ISP)?

   Internet service providers (ISPs) provide the gateway to the Internet for their customers and information is shared.

2. *An internet* is often confused with *the Internet*, but an internet is not necessarily part of the Internet.
3. What is an extranet?

   An extranet is an intranet that is opened up to allow outside users

4. In a client/server network relationship, the *server* stores data that is used by the users of the organizational LAN.
5. List three examples of a shared network resource.
   - Printers
   - Modem
   - Scanner
   - Data files
   - Applications
   - Storage
6. What is a network protocol?

   A protocol is a standard (or set of standards) that governs the rules to follow for setting up a data connection, communication between endpoints once the connection is set, and transferring data between those endpoints.

7. What is the name of the ARPA subgroup that was set up to focus on research pertaining to anything that related to computing?

   The Information Processing Techniques Office (IPTO)

8. What are the four locations that made up the original ARPANET?
   - Stanford Research Institute

- University of California, Los Angeles
- University of California, Santa Barbara
- University of Utah

9. The National Science Foundation Network (NSFNET) was developed originally to allow researchers access to five supercomputers. Where were these supercomputers located?
   - Cornell University
   - Pittsburgh Supercomputing Center
   - Princeton University
   - University of Illinois
   - University of California, San Diego
10. A *proprietary* standard is a standard that is developed and owned by a specific vendor.
11. What is a de facto standard?

    A de facto standard is a standard that began as a proprietary standard and then grew to a standard that is used by pretty much everyone.
12. ANSI is the organization that represents the United States in working with the global community on discussions relating to two important global standards organizations. Name these standards organizations.
    - International Organization for Standardization (ISO)
    - International Electrotechnical Commission (IEC)
13. A *working group* is a team of IEEE professionals brought together to work on new research activities.
14. IEEE 802.3 identifies which IEEE working group?

    Ethernet Working Group
15. IEEE 802.11 is the standard for *wireless LAN technology*.
16. What functions are performed at the Presentation layer?
    - Encryption services
    - Decryption services
    - Data compression services
    - Data decompression services
    - Translation services
17. Network File System (NFS) is a data format that is used at the *Session* layer.

18. Open Shortest Path First (OSPF) is an example of a *Network* layer protocol.

19. Point-to-Point Protocol (PPP) is an example of a *Data Link* layer protocol.

20. What are the reasons why we said that TCP/IP has grown into the ''method of choice''? Explain each of the reasons you list.

    - **Routing** — TCP/IP was designed to route data from node to node of networks of variable sizes and complexities. TCP/IP is not worried about the status of nodes in the network, it is concerned about the networks that it should know about. Various protocols that are within the TCP/IP protocol suite manage data flow between networks.
    - **Addressing** — And guess what is built into TCP/IP? That's right, IP. IP provides a way for a node to identify other nodes within a network and deliver data to any endpoint node that it has been made aware of.
    - **Name resolution** — TCP/IP provides name resolution as a way to map an IP address (10.10.10.10) to an actual name (`networkz.org`). Can you imagine how tough it would be to remember the IP addresses of all of the websites that you needed to know about? Name resolution really helps.
    - **Doesn't discount the lower layers** — Although TCP/IP operates at the upper layers (Layer 3 and above), it does have the ability to operate at the lower levels as well. This means that for most LANs and WLANs, and some MANs and WANs, TCP/IP is able to work with multiple networks of these types and connect them to each other with TCP/IP.
    - **Open standards** — TCP/IP was mainstreamed to give different nodes the capability to communicate with one another. The open standards that TCP/IP contains are available to anyone. These standards are determined through the RFC process that we discuss in Section 1.3.9.
    - **Talking endpoint to endpoint** — TCP/IP provides a way for one endpoint to speak directly with another endpoint, regardless of any nodes that are in between. It is as if the endpoints were directly connected to one another, even when they are not physically connected to a common network. Thanks to TCP/IP, both the originating and the destination nodes can exchange connection acknowledgements directly with one another.

- **Application support** — TCP/IP provides protocols that provide a commonality among end user applications. Often when an application that utilizes TCP/IP is developed, many of the functions required for the application are already common with any node supporting TCP/IP.

21. Using the terms listed under the table, place them in the appropriate spaces.

Diagnostic Utilities	General Purpose Utilities	Services Utilities
Address Resolution Protocol (ARP)	File Transfer Protocol (FTP)	TCP/IP print server
ipconfig	Line Printer Daemon (LPD)	Web server
Line Printer Daemon (LPD)	Remote Copy Protocol (RCP)	File Transfer Protocol Server
netstat	Remote Shell (RSH)	E-mail server
nslookup	Telnet	Domain name server
ping	Trivial File Transfer Protocol (TFTP)	
route		
tracert		

22. A LAN may consist of computers, printers, storage devices, and other shared devices or services available to a group of users within a *(any term that defines a local or a limited distance is a correct answer)* geographical area.

23. What does the term *sneakernet* refer to?

    The term *sneakernet* refers to the days when data was copied on a floppy disk and then transported by an individual to the destination PC.

24. What are the three main IEEE standards that are primarily associated with traditional LANs?

    - IEEE 802.2 Logical Link Control
    - IEEE 802.3 CSMA/CD Access Method and Physical Layer Specifications
    - IEEE 802.5 Token Ring Access Method and Physical Layer Specifications

25. The Media Access Control sublayer provides *addressing* and *channel* control.

26. What was the name of the company that introduced Token Ring technology? When it was introduced, what was the operating speed?

    When Token Ring was first introduced by IBM it possessed a speed of 4 Mbps, thus not offering any advantage over CSMA/CD networks.

27. What are the two notable differences between the IBM and IEEE 802.5 specifications for Token Ring?

    - The number of nodes on a ring is up to 260 nodes per IBM specification, and the IEEE 802.5 standard limits it to a maximum of 250 nodes.
    - Source routing IBM allows up to 8 fields for route designation when source routing is employed, while the IEEE 802.5 standard allows for a maximum of 14 fields.

28. True or false: Both IEEE 802.3 and Ethernet are CSMA/CD network standards that are fully compatible with each other.

    False — Although both are network standards, the two are not fully compatible with each other.

29. Fill in the missing information in the following two tables.

DB9 Pin Assignment

Signal	**Pin**
Receive +	1
Receive –	6
Transmit +	9
Transmit –	5

RJ-45 Pin Assignment

Signal	**Pin**	**Wire Color**
Receive +	4	White with orange stripe
Receive –	5	Orange with white stripe
Transmit +	6	White with blue stripe
Transmit –	3	Blue with white stripe

30. IBM Token Ring used cabling of different types to be used in different environments. Connect the appropriate type with its description below.

    A. This type consists of two parallel pairs. The wires in this cable are untwisted and have a maximum length of 50 meters. The primary purpose of this wire is to be used in installations requiring the cable to run under carpeting.

    B. This type consists of multimode fiber optic cable used to extend the token ring network and used to interconnect optical repeaters.

    C. This type consists of two shielded twisted pairs. It is considered a low cost short distance cable with a maximum length of 45 meters and is often used for MAU-to-MAU interconnection.

    D. This type is a lower cost alternative to Type 1 cable with a maximum length of 65 meters. It consists of two pairs of shielded twisted pairs.

    E. This type consists of two shielded twisted pairs as can be found in Type 1 cable and four unshielded twisted pairs as can be found in Type 3 cable.

    - Type 2 — E
    - Type 5 — B
    - Type 6 — C
    - Type 8 — A
    - Type 9 — D

31. Although this protocol is closely related to Token Ring, it is not officially considered part of the Token Ring family. Name this protocol.

    Fiber Distributed Data Interface (FDDI)

32. Define the following bus network terms:

    - **Collision detection** — Provided by circuitry designed to detect collisions on the bus network. If a collision is detected, the transceiver notifies the transmitting function that a collision has occurred and then it broadcasts a jamming signal on the network to notify other systems connected to the bus network that a collision has occurred. The LAN is then allowed to settle before the resumption of transmissions on to the bus.
    - **Heartbeat** — Generation of a short signal to inform the main adapter that the transmission was successful and collision free. Although it is specified in the 802.3 standard and the

Ethernet standard, it is rarely used as many adapters confuse this signal with the signal that signifies a collision has occurred.

- **Jabber** — The function that allows the transceiver to cease transmission if the frame being transmitted exceeds the specified limit of 1518 bytes. This helps prevent a malfunctioning system or adapter from flooding the LAN with inappropriate data.
- **Monitor** — This function monitors LAN traffic by prohibiting transmit functions while receive and collision functions are enabled. It does not generate any traffic onto the LAN.

33. A star topology is implemented with the use of *hubs* and UTP cables terminated with *RJ-45* plugs.

34. Fill in the blanks in the following table:

Pin	Ethernet	IEEE 802.3
1	Ground	Ground Control In
2	Collision Detected +	Control In A
3	Transmit +	Data Out A
4	Ground	Data In
5	Receive +	Data In A
6	Voltage	Common
7	Control	Out A
8	Ground	Control Out
9	Collision Detected –	Control In B
10	Transmit –	Data Out B
11	Ground	Data Out
12	Receive –	Data In B
13	Power	
14	Power Ground	
15	Control	Out B

35. What are the two types of duplex? What are the differences?

Duplex is either half duplex or full duplex. The difference between the two is that full-duplex devices are capable of both transmitting and receiving at the same time, whereas half-duplex devices are either in transmit or receive mode but never both simultaneously.

36. Fault *tolerance* is built into the dual-ring FDDI network.

37. What is POTS? What is it used for?

    POTS stands for plain old telephone service. It refers to the use of voice-grade telephone lines to form a point-to-point data connection.

38. What type of a node is required in order for two LANs to be able to communicate using the ISDN protocol?

    LAN-to-LAN connectivity with ISDN can best be accomplished with the use of ISDN routers.

39. Explain the two most commonly used ISDN services.

    - Basic rate — Provides two B channels of 64 Kbps and a single D channel of 16Kbps.
    - Primary rate — Provides 23 B channels of 64 Kbps and a single D channel of 64 Kbps for U.S.- and Japan-based subscribers. Subscribers in Europe and Australia are provided with 30 B channels.

40. A full T1 line provides *24* channels each with *64Kbps* of bandwidth.

41. Fill in the blanks in the following table:

decimal	**binary**
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
10	1010

42. What is RAM?

    Random access memory (RAM) is memory that is available for data storage and access, regardless of the order in which it is stored. Information stored in RAM is accessible until it is cleared out or the device it is being used on is shut down.

43. The type of RAM that is used by most PCs today is called *dynamic random access memory (DRAM)*.

44. Define the following:

- **Read-only memory (ROM)** — Memory that is configured and set by the manufacturer. It contains device systems software that is necessary for the proper operation of the device.
- **Programmable read-only memory (PROM)** — A memory chip that can be written to only once. This will allow someone other than the manufacturer to write data onto the PROM. Just like ROM, the data is there forever. In order to write the data onto the memory chip, a device known as a PROM programmer (PROM burner) is used.
- **Erasable programmable read-only memory (EPROM)** — A memory chip that can be written to and store data that may need to be overwritten at some point. The data on the EPROM is erased by UV light and then can be reprogrammed with a PROM burner.
- **Electrically erasable programmable read-only memory (EEPROM)** — A memory chip that can be written to and store data that may need to be overwritten at some point. The data on the EEPROM is erased by an electrical charge and then can be reprogrammed with a PROM burner.

45. What is the difference between a PDU and an SDU?

The PDU specifies the data that is to be transmitted to the peer layer at the receiving end. The SDU can be considered the PDU payload.

46. In order for communication to take place between nodes, one end of the connection must be a *DCE* and the other a *DTE*.

47. What are the four IP address network classes? Explain each one.

- **Class A** — Class A addresses are identified by a number from 1 to 126 in the first octet. In Class A addresses, the first octet identifies the network and the remaining three octets identify the host. These addresses are normally assigned to larger networks.
- **Class B** — Class B addresses are identified by a number from 128 to 191 in the first octet. In Class B addresses, the first two octets identify the network and the last two identify the host. These addresses are normally assigned to medium size networks.
- **Class C** — Class C addresses are identified by a number from 192 to 223 in the first octet. In Class C addresses, the first three octets identify the network while the last octet identifies the host. These addresses are normally assigned to small to medium size networks.
- **Class D** — Class D addresses are a little different from the other Classes. Class D addresses are used for multicasting. These addresses always begin with the first 4 bits being 1110 and the

remaining 29 bits identifying the catenet in which the multicast message is to be sent.

48. The main types of network cables are *twisted pair*, *fiber optic*, and *coaxial*.

49. What are the four primary colors of cabling used in twisted pair?

    - Blue
    - Brown
    - Green
    - Orange

50. True or false: Twisted pair cabling is used in Ethernet and Token Ring networks.

    True

51. What are the types of twisted pair cabling? What are the differences in the types?

    - **UTP (unshielded twisted pair)** — UTP cabling is the type of copper cabling that is used the most in networks today. UTP cables consist of two or more pairs of conductors that are grouped within an outer sleeve. UTP cable is often referred to as Ethernet cable, because Ethernet is the predominant technology that uses UTP cable. UTP cabling is cheap, but does not offer protection from electrical interference. Additionally, bandwidth is limited with UTP in comparison with some of the other cable types.
    - **STP (shielded twisted pair)** — STP cabling is a type of copper cabling that is used in networks where fast data rates are required. STP cables consist of two or more pairs of conductors that are grouped together and then an additional metal shield wraps around the twisted pairs, forming an additional barrier to help protect the cabling. Finally, all of the cables are grouped together and a final outer sleeve is placed over the wiring. STP cables are also referred to as Ethernet cables. STP cables provide additional protection to the internal copper, thus data rates are increased and more reliable. The conductors that are grouped together can be shielded as individual pairs (in other words, each pair will have its own shield), or all pairs can be shielded as a group.

52. What are the two types of fiber optic cabling? Explain each.

    - **Single-mode fiber optical cabling** — SMF cables are thinner than MMF cables. This is because SMF cables are designed to carry a single beam of light. Because there are not multiple beams involved, the SMF cable is more reliable and supports greater distances and a much higher bandwidth than MMF cables. The bulk cost of SMF cabling is much less expensive than MMF cabling.

- **Multi-mode fiber optical cabling** — MMF cabling is made for shorter distances. Unlike SMF, there are multiple beams of light, so the distance and speed are less. Granted, supporting data rates of up to 10 Gbps for distances as far as 300 meters is nothing to sneeze at. Because of the additional modes, MMF cabling is able to carry much more data at any given time.

53. The *network interface controller (NIC)* is a hardware card that allows a PC to participate in passing and receiving data on a network.

54. A network *concentrator* is a node that is able to multiplex signals and then transmit them over a single transmission medium.

55. What is the name for the node type that is similar to a Ethernet hub, but is used in Token Ring networks?

    Media access unit (MAU)

56. What is the name of the Layer 2 device that supports and performs the same basic function of joining network segments within the LAN?

    Layer 2 switch or a bridge

57. What is the name of the node that operates at Layer 3 of the OSI reference model?

    Router

58. A *Layer 3 switch* is a node that allows the wire speed technologies that are used by Layer 2 and the tools that are needed to route packets at Layer 3.

59. *Layer 3* switches have the ability to control the flow of data by implementing what is known as *class of service (COS)*, which provides for packet queuing into classes of service to ensure that data with a higher priority is attended to before data with a lower priority.

60. Name at least three types of network servers that are used in a LAN.

    - Print server
    - File server
    - Network server
    - FTP server
    - Mail server
    - Fax server
    - List server
    - Proxy server

61. The portion of a computer that receives data and instructions and manipulates and acts on the received data in a controlled manner is known as what?

    The central processing unit (CPU)

62. True or false: Data can never be stored on magnetic media because the magnet will erase all data.

    False — The memory storage area can be constructed of various storage nodes anywhere from semiconductor to magnetic media.

63. The address space of a node can be determined by taking the number 2 and raising it to the power of the number of address bits that are generated by the CPU. That being said, calculate the following (the first one is done for you):

    - 16 address bits = 2^{16}(65,536)
    - 20 address bits = 2^{20}(1,048,576)
    - 24 address bits = 2^{24}(16, 777,216)
    - 32 address bits = 2^{32}(4,294,967,296)

64. Hard drives are usually mounted within a computer's case, but today, with USB ports, many drives are sold as *external* drives communicating between the drive and computer over the USB port.

65. On personal computers, input/output connections are in the form of ports dedicated to either *serial* or *parallel* data communications.

66. What is the most basic form of an operating system?

    A file manager

67. In the world today, there are two main GUI-based operating systems that are in use by most people. What are they?

    - Microsoft Windows
    - Mac OS X

68. As the need for PC connectivity rose, the most common design of network operating systems was the *client/server* implementation

69. True or false: One of the early network operating systems, Microsoft Networking, utilized an IPX/SPX protocol stack to provide communications over its network.

    False — Novell utilized an IPX/SPX protocol stack to provide communications over its network.

70. True or false: The problem with TCP/IP networks is that a workstation can only have a single session running at a time with any server on the network.

False — The majority of today's networks are TCP/IP-based networks that have a wide range of various applications running over them. A workstation may have multiple sessions to various servers on the network simultaneously.

71. What is peer-to-peer networking?

    Peer-to-peer networking is where one computer can share data and resources with another computer.

72. True or false: To perform peer-to-peer networking, some sort of application program is required.

    True

73. List the NetBIOS primitives that are associated with the session service and what each of them does.

    - Call — Opens a session to a remote computer using its NetBIOS name
    - Listen — Listens for session requests using NetBIOS name
    - Hang Up — Ends a session that had been previously established
    - Send — Sends a packet to the computer that a session had been established with
    - Send No ACK — Similar to Send but does not require a returned acknowledgement that the packet was received
    - Receive — Waits for the arrival of a packet from a computer a session has been established with

74. For each of the following statements, give the corresponding operating system name. The first one has been completed as an example.

    A. The operating system that was first developed by AT&T Bell Labs as a multiuser operating system.

    Unix

    B. This operating system was designed more for the desktop environment even though it will run on larger computers.

    Linux

    C. Newer versions of this operating system come with configuration utility programs that assist with the network settings and configuration.

    Unix

    D. This operating system has many similarities and commonalities to Unix.

Linux and Sun Solaris

E. Can be configured with a text editor.

Linux and Unix

F. This operating system was initially designed to handle many users connected simultaneously and all sitting in front of a character-based terminal.

Unix

G. Sun initially developed this operating system for their Sun SPARC workstations.

Sun Solaris

H. This operating system is a flat file operating system; most of the configuration files are in readable text.

Unix

I. This operating system provides strong networking tools to allow it to be interconnected not only to the local LAN but the Internet.

Sun Solaris

75. Developers of networking protocols adhere to a *layered* approach.

76. Name the layers of the TCP/IP reference model and list what the responsibility is of each layer.

- **Network interface layer** — The network interface layer corresponds to the Physical and Data Link layers of the OSI reference model. This layer is also often referred to as the link layer or the data link layer. The network interface layer is responsible for the device drivers and hardware interfaces that connect a node to the transmission medium.
- **Internet layer** — The Internet layer corresponds to the Network layer of the OSI reference model. This layer is also known as the network layer. The Internet layer is responsible for the delivery of packets through a network. All routing protocols (RIP, OSPF, IP, etc.) are members of this layer. Nodes that perform functions at this layer are responsible for receiving a datagram, determining where to send it, and then forwarding it toward the destination. When a node receives a datagram that is destined for the node, this layer is responsible for determining the forwarding method for information that is in the packet. Finally, this layer contains protocols that send and receive error messages and control messages as required.
- **Transport layer** — The transport layer corresponds to the Transport layer of the OSI reference model. There are two primary

protocols that operate at this layer. These are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). This layer serves the application layer and is responsible for data flow between two or more nodes within a network.

- **Application layer** — The application layer corresponds to the Application, Presentation, and Session layers of the OSI reference model. Users initiate a process that will use an application to access network services. Applications work with protocols at the transport layer in order to pass data in the form needed by the transport protocol chosen. On the receiving end, the data is received by the lower layers and passed up to the application for processing for the destination end user. This layer concerns itself with the details of the application and its process and not so much about the movement of data. This is what separates this upper layer from the lower three.

77. What is the name of the protocol that allows for e-mail communications and at which layer does it operate?

    The name of the protocol is the Simple Mail Transfer Protocol (SMTP) and it is an Application layer protocol.

78. True or false: Secure Shell is an Application layer protocol.

    True

79. *Domain* names are names that are assigned to URLs on the Internet.

80. Make sure that you have a connection to the Internet, then use the `ping` command to find the IP address for the following domains. Write down your results.

    - www.cnn.com ____________
    - www.yahoo.com ____________
    - www.wiley.com ____________
    - www.google.com ____________
    - www.richardbramante.com ____________

    Because IP addresses can change, the blanks have been left blank. The important thing is that you were able to get an IP address using the `ping` command.

81. What does the acronym gTLD stand for?

    Generic top-level domain

82. What type of organization or business would use the following gTLDs?

    - .biz — Restricted for use by businesses

- .com — Intended for use by commercial organizations
- .edu — Post-secondary educational institutions
- .gov — Restricted for use by the United States federal, state, and local governments.
- .jobs — Sites related to employment
- .mil — The United States military
- .net — Miscellaneous
- .org — Miscellaneous organizations

83. What is the name of the protocol that runs between nodes for the purpose of sharing management information pertaining to the managed system?

    The Simple Network Management Protocol (SNMP) is a protocol that runs between an SNMP manager and an SNMP client, also known as an SNMP managed system, for the purpose of sharing management information pertaining to the managed system.

84. What are the three message types that can be sent from the SNMP manager to the SNMP agents?

    - GetRequest
    - GetNextRequest
    - SetRequest

85. A *management information base (MIB)* is a database that contains manageable objects and variables of these objects pertaining to a network node, for the purpose of node management within a network.

86. The formal language used by SNMP is *Abstract Syntax Notation 1 (ASN.1)*.

87. What is an object identifier (OID)?

    An OID is a series of sequential integers that are separated by dots. The OID defines the path to the sought object.

88. Name some of the improvements that were introduced by SNMPv2.

    - Security
    - SNMP manager to SNMP manager communication
    - Improved performance
    - Confidential sessions
    - Additional protocol support
    - Improvements in the way trap PDUs are handled

89. Which version of the SNMP protocol is considered the official one?

    The Simple Network Management Protocol version 3 (SNMPv3) is considered the official standard and is the one that will be developed upon if there are any updates or enhancements needed at some point in the future.

90. What is the name of the protocol that provides the capability for users to access an FTP server and transfer files to and from the server?

    FTP (File Transfer Protocol)

91. Fill in the correct FTP command in the following table.

Command	**Function**
ascii	Sets the file transfer mode to ASCII.
binary	Sets the file transfer mode to binary.
cd	Changes to another directory.
close	Terminates a connection.
delete	Removes a file.
get	Places a copy of a file on the remote node onto a specified directory on the local node.
hash	Used to monitor the file transfer process. For every 1028 bytes received, a # will be placed on the screen.
help	Gets a list of available FTP commands.
?	Gets information about commands.
ls	Lists the names of the files in the current directory.
mget	Used to copy more than one file from the remote node to the local node.
mkdir	Makes a new directory.
mput	Used to copy more than one file from the local node to the remote node.
put	Used to copy a file from the local node to the remote node.
pwd	Used to determine the directory path to the current directory.
quit	Terminates the FTP session.
rename	Renames a file or directory.
rmdir	Removes a directory and any subdirectories, if applicable.

92. True or false: There is no difference in between the TFTP and FTP protocols. They have different names because they were developed by different companies, but they are exactly the same in function.

    False — TFTP uses UDP while FTP uses TCP. TFTP uses UDP because it is less chatty than the FTP protocol. TFTP does not have all of the functions that are available with FTP. This is because TFTP is a simple file transfer protocol designed to transfer boot-up files for diskless nodes. With TFTP, users are not able to browse directories, make directory changes, list files or directories, and are limited in terms of the files they can access.

93. Using the SMTP protocol, an SMTP client has a total of five message types that are sent to an SMTP server. Following is a list of these message types. Define the purpose of each one.

    - HELO — Used by the client to identify itself to the server
    - MAIL — Identifies the end user that is sending the message
    - RCPT — Identifies the end user that the message is being sent to
    - DATA — The contents of the message
    - QUIT — Terminates the session

94. Developed originally by Sun Microsystems, this protocol allows end users access to files that are stored remotely as if the files were local to the end user's workstation. What is the name of this protocol?

    NFS (Network File System)

95. What are the three modes of operation used by Telnet clients and servers?

    - Half-duplex mode
    - Character mode
    - Line mode

96. SSH utilizes *public key cryptography*, which is used to provide cryptographic keys to authenticate remote nodes and users.

97. What are the two most popular Transport layer protocols?

    - UDP (User Datagram Protocol)
    - TCP (Transmission Control Protocol)

98. Name at least three Application layer protocols that use TCP.

    - FTP
    - Telnet

- SMTP
- DNS
- POP3
- HTTP
- DNS
- IMAP

99. Name at least three Application layer protocols that use UDP.
    - DNS
    - BOOTP/DHCP
    - TFTP
    - SNMP
    - RIP
    - NFS

100. Name at least five Internet layer protocols.
    - IP
    - IGMP
    - ICMP
    - ARP
    - RIP
    - OSPF
    - BGP
    - IPSec

101. What is the name of the protocol that allows for operating system access for diskless nodes?

    BOOTP (Bootstrap Protocol)

102. Define the following:
    - **Routing protocol** — Refers to the protocols that perform functions that allow the routing of packets between routers. RIP, OSPF, BGP, etc., are examples of routing protocols. This is sometimes confused with a routed protocol, which is not the same thing.
    - **Routed protocol** — Refers to protocols that participate in transmitting data between nodes within a network. Telnet, SNMP, IP, etc., are all examples of a routed protocol. Routed protocols are sometimes incorrectly termed routing protocols.

- **Gateway** — Refers to the entry point for an entity. A computer that provides access to a network area is a gateway. A network that provides access to a network is a gateway. Many applications have gateways that allow information sharing. The node that connects the LAN to the Internet (or any other network type) is a gateway.
- **Interior gateway protocol (IGP)** — A routing protocol that operates within an AS. RIP and OSPF are IGPs.
- **Exterior gateway protocol (EGP)** — BGP is often called an EGP, although the EGP protocol was the predecessor to BGP for IP routing between AS's.
- **Static routing** — Refers to IP routing information that is manually configured on a node by a system administrator.
- **Dynamic routing** — Refers to IP routing information that is learned by the node through a routing protocol, such as RIP.

103. What is the speed of the following Ethernet types?
    - 10BASE-T — 10 Mbps
    - Fast Ethernet — 100 Mbps
    - Gig Ethernet — 1000 Mbps
104. Ethernet nodes using UTP cabling fall into one of two component types. What are those?
    - DTE (data terminal equipment)
    - DCE (data communications equipment)
105. What is a straight-through cable?

    A straight-through cable is a cable where the wire will run to the same number on each end of the cable (i.e., pin 1 on one end would be connected to pin 1 on the other end).
106. True or false: A straight-through cable can be wired with either the T568A or T568B wiring scheme as long as both ends of the cable are wired exactly the same using the same wiring pin-out.

    True
107. A *crossover* Ethernet cable must have one plug wired with the T568A wiring scheme and the other plug wired following the T568B wiring pin-out.
108. What is the major difference between the OSI reference model and the IEEE 802.3 model?

There is a close similarity between the ISO OSI model and IEEE 802.3 model with the difference being at the Data Link layer of the OSI model

109. What is a frame check sequence?

A frame check sequence is a 4-byte field that contains a 32-bit CRC checksum (cyclical redundancy check) value, which is calculated and inserted by the sending network node and is used by the receiving network node to validate the received frame. Both the sending and receiving nodes calculate the CRC value by using the data contained within the Destination Address, Source Address, Frame Length/Type, and Data fields.

110. Define the following:

- **Carrier sense** — All network nodes continuously listen on the network media to determine if there are gaps in frame transmission on the media.
- **Multiple access** — All network nodes are able to transmit any time they determine that the network media is quiet.
- **Collision detection** — When two network nodes transmit at the same time, the data streams from both nodes interfere and a collision occurs. The network nodes involved must be capable of detecting that a collision has occurred while they were attempting to transmit a frame. Upon detecting that a collision occurred at the time they were transmitting a frame, both nodes will cease transmission of the frame and back off. They will wait a period of time determined by the back-off algorithm before again attempting to transmit the frame.

111. Fill in the missing information in the following table:

Half-Duplex Operational Limitations

Parameters	10 Mbps	100 Mbps	1000 Mbps
Minimum frame size	64	64	520
Maximum collision diameter with UTP cable	100 meters	100 meters	100 meters
Maximum collision diameter with repeaters	2500 meters	205 meters	200 meters
Maximum number of repeaters in network path	5	2	1

112. What is frame bursting, and when was it introduced?

The standard for CSMA/CD Ethernet for Gigabit Ethernet added the capability for frame bursting. Frame bursting is the capability of a Gigabit Ethernet network interface's Media Access Control to transmit a burst of frames without releasing the access to the network media.

113. *Full-duplex* transmission is the capability of a network node to transmit and receive simultaneously.

114. *Hubs* are nodes that are actually considered part of the Physical layer since they are not decision making devices. They basically provide the interconnectivity on the physical level for network nodes.

115. *Autonegotiation* is the capability of a network interface to negotiate the communication parameters to be used between it and the port it is connected to.

116. True or false: Network administrators don't have to worry about traffic patterns on the network.

False — When administering large network installations it is important to understand the traffic patterns present on the network.

117. What does the acronym VLAN stand for?

Virtual local area network

118. What is the name of the LAN protocol that was once popular in the majority of active LANs and is now used as an embedded standard to serve networks that control technologies such as automation services, transportation, robotics, gaming, and other similar network types?

Attached Resource Computer Network (ARCnet)

119. *StarLAN* technology is, for the most part, the predecessor to what we all know as Ethernet.

120. What is the name of the corporation that developed Token Ring technology?

Token Ring network technology was developed by IBM in the late 1970s.

121. True or false: Unshielded twisted pair (UTP) cables became the preferred medium used by Token Ring technologies. This is because it was less bulky than shielded twisted pair (STP) cables and was also less expensive than STP.

True — Token Ring originally operated on STP cabling, but converted to UTP cabling in the 1990s. This was greatly appreciated by the networking community as it offered a cheaper and less bulky medium.

122. What is the name of the first technology that could operate at 100 Mbps?

    Fiber Distributed Data Interface (FDDI)

123. What advantages are there in using optical fiber as the primary transmission medium within a network?

    - Performance
    - Greater distances
    - Faster transmission speed
    - Reliability
    - Data security

124. *Copper Distributed Data Interface (CDDI)* is the FDDI protocol over twisted pair medium instead of fiber.

125. Define the following FDDI node types:

    - **Single attachment station (SAS)** — Connects to the FDDI ring through a single connector. The connector has an input port and an output port. Data is received on the input port and is sent to the downstream neighbor via the output port. The SAS connects to a concentrator and then to the primary ring only.
    - **Single attached concentrator (SAC)** — Like the SAS, the SAC concentrator connects to only the primary ring. The connection is made through another concentrator.
    - **Dual attachment station (DAS)** — Connects to the FDDI ring through two connectors (each with an input and an output port). Can connect directly to the ring or through a concentrator.
    - **Dual attached concentrator (DAC)** — A concentrator that connects to both rings.

126. The Digital Equipment Company (Digital) developed and released the first version of the *Digital Equipment Company Network (DECnet)* protocol in the mid-1970s.

127. What are the levels of the XNS model and what layer does each level correspond to on the OSI layered model?

    - Level 0 — Roughly corresponds to the OSI Layers 1 and 2.
    - Level 1 — Roughly corresponds to the OSI Layer 3.
    - Level 2 — Roughly corresponds to the OSI Layers 3 and 4.
    - Level 3 — Roughly corresponds to the OSI Layers 6 and 7.
    - Level 4+ — Roughly corresponds to the OSI Layer 7.

128. The *Internetwork Packet Exchange (IPX)* protocol is one that is normally found within networks that have nodes that are running the Novell NetWare operating system.

129. In order to support multiple protocol datagrams, there are three main components that are used by PPP. What are they?

- PPP encapsulation method
- PPP Link Control Protocol (LCP)
- PPP Network Control Protocol (NCP)

130. The Link Access Procedure, Balanced (LAPB) is the *X.25* link-level protocol that ensures reliable, error-free packet framing and data communication management.

131. Match the ATM adaptation layer type to its appropriate function.

A. This AAL type supports both connectionless and connection-oriented data transmission. This AAL type is used to transmit non-SMDS packets.

B. This AAL type supports VBR transmissions.

C. This AAL type supports CBR transmissions.

D. This AAL type supports both connectionless and connection-oriented data transmission. This AAL type is used to transmit switched multimegabit data services (SMDS) packets.

- AAL1 — C
- AAL2 — B
- AAL3 — D
- AAL4 — D
- AAL5 — A

132. AppleTalk is a protocol suite that was developed by the Apple computer company. AppleTalk was developed specifically to be integrated with new *Macintosh* computers to allow for resource sharing on a network.

133. There are two services used in ISDN to determine bandwidth availability for an end network. These are *basic rate interface (BRI)* and *primary rate interface (PRI)*.

134. The upper layers of the OSI reference model are utilized by software programs to send and receive data over a network.

135. True or false: One of the great things about mail servers is that they do not have to perform any authentication, as such authentication is only performed by a RADIUS server.

False — Mail servers may have to perform user authentication to ensure security and user privacy. The determination on whether the mail server will perform such actions is made by the network administrators.

136. The *time-to-live* field is an 8-bit field that indicates how many seconds a packet can live on the Internet.

137. DMZ is the acronym for what?

Demilitarized zone

138. FTP and SMTP are upper-layer protocols that reside within which layer of the TCP/IP model?

The Application layer of the TCP/IP model contains the upper-level protocols of the TCP/IP protocol suite such as FTP (File Transport Protocol) and SMTP (Simple Mail Transfer Protocol).

139. The following table contains some common Application layer protocols. Complete the missing parts of the table.

Mnemonic	Port(s)	Description
DHCP	67 and 68	Dynamic Host Configuration Protocol provides the means for network clients to obtain an IP address, default gateway IP address, and Domain Name System server addresses.
FTP	20 and 21	File Transfer Protocol is used to transfer files between an FTP client workstation and an FTP server. Port 20 is for data and port 21 is used for control signaling between server and client.
HTTP	80	Hypertext Transfer Protocol is used to transfer Hypertext information over the Internet. The most familiar application use for hypertext information retrieval is a web browser.
SNMP	161	Simple Network Management Protocol is used to manage and monitor network devices over the local network and Internet.
Telnet	23	Telecommunications Network Protocol is used over the local network and Internet to establish terminal sessions between a client computer and a server.

140. True or false: Port numbers range from 0 to 65,535, but for the most part the first 1024 (0 to 1023 decimal or 0x03FF hexadecimal) are considered to be the well-known ports.

   True

141. Explain `traceroute`.

   `traceroute` returns replies from each hop that it crosses to reach a particular targeted network node. Usually, it will try to reach a target in a given number of hops. The customary maximum hop count is 30 hops. It is a good indication if the packet is traveling in the right direction.

142. *OSPF* is a dynamic routing protocol used to move packets from network segment to network segment.

143. True or false: Port 0 is normally reserved, but its use is allowed as a valid source port in transmissions where the transmitting network node does not require a response from the receiving network node.

   True

144. What is the standard that defines the recommended services provided by the OSI Transport layer while working with the Network layer to serve the needs of protocols that are used at the Session layer?

   ISO/IEC 8072

145. What is the standard that sets the recommendations to be followed by nodes (entities) within a network that are utilizing the services of the OSI Transport layer?

   ISO/IEC 8073

146. There are two types of transport service. What are they?

   Connection-oriented and connectionless

147. What are the two data units that operate at the Transport layer?

   - Transport protocol data unit (TPDU)
   - Transport service data unit (TSDU)

148. Match the correct transport service class with its class function.

   A. Error recovery and multiplexing class

   B. Multiplexing class

   C. Simple class

   D. Error detection and recovery class

   E. Basic error recovery class

   - Class 0 — C
   - Class 1 — E

- Class 2 — B
- Class 3 — A
- Class 4 — D

149. The purpose of the Transport layer is to provide end-to-end delivery of data from one *application* to another.

150. Explain how a three-way handshake works.

- Step 1 — The originating node will send a request known as a SYN to the destination node.
- Step 2 — The destination node will let the originating node know that it has received the SYN request by sending back a SYN-ACK message.
- Step 3 — The originating node will respond to the SYN-ACK by sending back an ACK message.

151. True or false: The term *connectionless* can be misleading as connectionless protocols require a connection before they can transmit data.

False — Connectionless protocols do not require a connection; a transmitting device simply sends data as soon as it has data that is ready to be sent.

152. TCP is a *connection-oriented* protocol, whereas UDP is a *connectionless* protocol.

153. In a connection-oriented environment, *congestion* control and *flow* control are two mechanisms that are used to maintain control over the transmission of data.

154. SMTP mail servers will deliver e-mail to the *SMTP mail* server servicing a particular domain.

155. http://www.mydomainname.com is an example of a *URL*.

156. True or false: Unlike IP addresses, domain names do not have to be unique.

False — As with IP addresses, domain names also need to be unique.

157. What protocol is primarily a method of moving packets of data across networks consisting of various mediums, seamlessly delivering these packets solely based on destination address?

IP (Internet Protocol)

158. What version of IP allows for 4,294,967,296 unique addresses?

IPv4

159. What would the binary number look like for the IP address 192.168.15.85?

 11000000.10101000.00001111.01010101

160. The real thrust of moving to *IPv6* is the larger address space that it provides, with 128 bits dedicated to address space.

161. What is the name of the protocol that provides a means of messaging when a sent datagram is not able to be received by a destination node?

 Internet Control Message Protocol, an essential part of the TCP/IP Internet protocol suite.

162. The `traceroute` command is used to trace the path from the sending network node to the receiving network node on a network hop-to-hop basis.

163. What is the name of the protocol that makes use of authentication and encryption to establish a secure connection between endpoint network nodes?

 Internet Protocol Security (IPSec)

164. In this chapter, we discussed certain expectations that each LAN should meet. We called them the highs and the lows. What are these? Define them.

 - **High throughput** — The data throughput is simply the rate of error-free delivery for messages within a network.
 - **High total bandwidth** — Bandwidth is the available capacity of the physical or wireless channel and network nodes provided for the delivery of data messages in the LAN.
 - **Low delays** — No delays is optimal, but unlikely. Delays will occur, but the goal is to have as few as possible.
 - **Low error rate** — The amount of errors that you see in the network needs to stay as low as possible.

165. A collision causes datagrams to be *dropped*, but it doesn't necessarily mean that the data can't be recovered in some way.

166. In a token bus configuration, there is a central node called a *MAU* or a *MSAU*. This device is similar to an Ethernet hub, but it has a computer chip that provides the logical ring that the end nodes are concerned with.

167. Define the following:

 - **Carrier Sense Multiple Access (CSMA)** — Allows multiple nodes to be attached to a shared network. Prior to transmission, the nodes listen to see if the shared channel is busy and transmit when they sense that the channel is not busy. ''Carrier sense'' simply means that a node is listening to see if it can detect an unused channel. If the node senses that there is a busy channel, it will defer transmission of its data until the channel is idle. ''Multiple access'' defines the fact that there are multiple nodes accessing the shared medium to transmit data.

- **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)** — This is an enhanced version of the CSMA protocol in that it adds collision avoidance as a function. In this type of network, collisions are avoided because the station will not transmit data when it senses the channel is busy. The node listens to the channel for a defined amount of time and when the node is ready to send data, it sends a jam signal, which lets all of the other nodes know that the node is ready to transmit data.
- **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** — This is an enhanced version of the CSMA protocol in that it adds collision detection as a function. The collision detection function allows the transmitting node to be able to monitor the channel for other transmissions. If while transmitting a frame the node detects a signal coming from another node, it terminates the transmission, sends out a signal known as a jam signal, and then tries to send the frame again. There are different ways for collisions to be detected, depending on the shared media that is being used. The most popular and most often used CSMA/CD protocol is Ethernet.

168. A *jam signal* in CSMA/CD is a message to all other nodes that a collision has occurred and that they should stop transmitting.

169. Match the LLC type with the correct answer.

    A. This LLC type is used for connectionless services.

    B. This LLC type is used for connection-oriented services.

    C. This LLC type is used for acknowledgments in conjunction with connectionless services.

    - LLC Type 1 (LLC-1) — A
    - LLC Type 2 (LLC-2) — B
    - LLC Type 3 (LLC-3) — C

170. Define the following:

    - **Destination service access point (DSAP)** — This is used to identify the LLC that is supposed to receive the PDU.

- **Source service access point (SSAP)** — This is used to identify the LLC that is supposed to send the PDU.
- **Control** — The control field provides sequencing data, command information, and responses to requests. Note that any or all of these can be used in any combination.

171. The *Subnetwork Access Protocol (SNAP)* is a protocol that is used in conjunction with LLC-1 for the purpose of upward multiplexing to more upper-layer protocols than what is available with the standard LLC 8-bit SAP fields.

172. True or false: The LLC sublayer is responsible for interfacing between the MAC sublayer and the Physical layer.

     False — The MAC sublayer is responsible for interfacing between the LLC sublayer and Layer 1, the Physical layer.

173. The IEEE 802 *MAC* address is a 48-bit address that is used to identify the network adaptor for a particular node or interface in the network.

174. What is the name for the portion of a frame that contains the source and destination MAC addresses for interfaces that are involved in a communication stream?

     The MAC header

175. True or false: Multicasting is the act of sending a message to multiple nodes.

     True

176. What is the function of the following well-known MAC addresses?
     - 01:80:C2:00:00:00 — Spanning tree BPDU
     - 09:00:4E:00:00:02 — Novell IPX
     - CF:00:00:00:00:00 — Ethernet configuration test
     - 09:00:2B:00:00:0F — DEC LAT

177. Frames are either *fixed-length* or *bit-oriented* PDUs

178. *CRC* is a function that is used to detect common errors that may occur during data transmission.

179. Ethernet uses what are known as *PAUSE* frames for flow control within Ethernet LANs.

180. Explain the following:
     - **Source route bridging** — This type of bridging is used in a source-routed catenet. In a source-routed catenet, the path to a destination is determined by the end nodes and not the bridge

itself. An example of an environment that uses source route bridging is Token Ring.

- **Transparent bridging** — This is the type of bridging that is used in Ethernet (and others). In a transparent bridging environment, the bridge makes the path determinations and the end nodes are not aware of decisions that are being made. They simply throw the data to the bridge and leave the decision making up to it.

181. True or false: A bridge is a device that operates much like a repeater or a hub, but it makes data forwarding decisions that bridge traffic from one network segment to another.

    True

182. True or false: When a bridge receives a frame that is destined for a multicast address, the bridge will forward the frame to all of the ports, including the port on which it is received.

    False — When a bridge receives a frame that is destined for a multicast address, the bridge will forward the frame to all of the ports *except* the port on which it is received.

183. Which of the following is *not* a type of organizational LAN?

    The Internet

184. What are examples of external considerations that need to be made when designing a network?

    - Consideration needs to be given to WAN interfacing, as well as interfacings with LANs that are within your realm of control.
    - Make sure you know about any government regulations and that you are in compliance with them.
    - What are your competitors using/doing? What network type would you like to have and who out there did it right? What did they do?
    - What potential technological growth is out there, and will your proposed design be prepared to support it?

185. Developing a project *scope* is important in the early phases of network design.

186. The *hierarchical* design models are the most commonly used in most high-speed LANs today.

187. In a hierarchical design model, there are three layers. What are they?

    - The access layer
    - The distribution layer
    - The core layer

188. What are three WAN protocols that can be used to connect a LAN to remote sites?

- Frame relay
- ISDN
- Leased lines

189. The *distribution* layer is the middleman between the access layer and the core.

190. The *core* layer is the backbone of the LAN and often provides connectivity to WANs as well as Internet services.

191. Explain some of the benefits of using a hierarchical model.

- Design replication — Once you have a working model, you can simply change the addressing schemes and design the next network expansion based on the way the original design was configured.
- Expandability — As the network grows, it is very simple to introduce additional nodes into the topology. Future growth planning is a breeze.
- Redundancy — Redundancy from the access layer to the core layer is very important in high speed LANs. When a node fails, you have to have another node picking up the pieces until the node comes back on line.
- Better performance — Nodes that operate in the hierarchical model are able to maintain close to wire speed transmissions to all of the nodes they support.
- Security — Access control security is provided at the access layer. The distribution layer can support advanced security that meets the security needs of the LAN
- Easy to manage and maintain — Because of the scalability of the hierarchical design model, the network is easy to manage and maintain. A layered approach to troubleshooting helps in finding the source or a network connectivity issue. Additional nodes can be installed fairly simply, and configurations can be built from existing configurations, thus saving time and money. Over time, the hierarchical model will pay for itself in money saved due to the ease of maintaining and managing the LAN.

192. Explain the maximum allowed in each level of the 5-4-3-2-1 design model.

- 5 — This is the number of *segments* allowed in total.

- 4 — This is the number of *repeaters* used to join the segments together.
- 3 — This is the maximum number of segments in total that have nodes that are *active*.
- 2 — This is the maximum number of segments in total that are *not active*.
- 1 — This is the number of *collision domains*.

193. The *bus* topology is the most often used topology in LANs.

194. What are the advantages to the bus topology?

- Easy to install
- Easy to extend
- Less expensive to implement

195. What are the disadvantages to the bus topology?

- There is a limitation to the distance a cable can go without a repeater.
- There is a limit to the number of nodes that can be supported.
- It can experience sluggishness in performance when there are heavy traffic loads.
- Security risks exist because all stations can hear what the others are saying on the shared channel.

196. What are the advantages to the star topology?

- Better performance
- Easy to troubleshoot
- High scalability of the network through the central node

197. What are the disadvantages of a star topology?

- Too much dependency on the central node
- May be complex to manage
- Wiring may become cumbersome

198. What are the advantages of a ring topology?

- No need to have a mechanism to ensure collision-free datagram passing
- Can expand to cover a greater number of nodes than some of the other topology types
- Fairly simple to maintain

199. What are the disadvantages of a ring topology?

   - A failure with one node on the ring may cause an outage to all connected nodes.
   - Any maintenance (e.g., adding a node, making a change to a node, removing a node) would affect all of the nodes that connect to the ring.
   - Some of the hardware required to implement a ring is more expensive than Ethernet network cards and nodes.
   - Under normal traffic load, a ring is much slower than other topologies.

200. The *ring* topology is used for Token Ring and FDDI LANs.

201. The *concentrator* used within a LAN is either a hub or an MAU that allows the combination of data transmissions for a group of nodes.

202. The *bridge*, or *Layer 2 switch*, is a LAN node that operates at Layer 2 of the OSI reference model.

203. What is the name of the traditional network node that operates at Layer 3 of the OSI reference model?

   A router

204. Why is a Layer 3 switch preferred over a traditional router in high-speed LANs?

   The Layer 3 switch is preferred over a router because routing decisions are hardware based and thus are much faster than those done by traditional routers.

205. List five terms that are used to define a switch that operates at Layer 4-7 of the OSI model.

   - Layer 4-7 switch
   - Web switch
   - Application switch
   - Content switch
   - VPN switch

206. Explain what each type of switch does.

   - Cut-through — In cut-through operations, the switch reads the header of the datagram as it is received on a port. Once the switch determines the port that reaches the destination, the datagram is sent to the port and on to its destination. There is no storing of data in a cut-through environment. There are also no options for error checking or control because the cut-through switch only reads the header for an address and sends the datagram on.

- Store and forward — In store and forward operations, the switch stores the data and does error checking on the datagram before it sends the datagram off toward its destination port. Although this will make the transfer of datagrams slower than with a cut-through switch, the data is delivered reliably.

207. Which of the following is a false statement?

   C. A loop only occurs when there is no redundancy built into the network.

208. What is the name of the public standard protocol that was developed to control loops in a catenet?

   Spanning Tree Protocol (STP)

209. What are the possible port states used by STP?

   - Disabled
   - Blocking
   - Listening
   - Learning
   - Forwarding

210. The standard that covers link aggregation is *IEEE 802.1ad*, the Link Aggregation Control Protocol (LACP).

211. What are some benefits of link aggregation?

   - Increase link capacity
   - High link availability
   - Often can be done with existing hardware

212. What are some disadvantages of link aggregation?

   - Requires additional interfaces on each end
   - Higher potential of configuration errors
   - May require device driver updates to ensure compatibility with link aggregation

213. What are some benefits of creating VLANs within your LAN?

   - Better performance. Only VLAN members receive multicasts.
   - Members of a group no longer have to physically be located close to the group.

- Administration is easier. Changes to any work area can be done with simple configuration change.
- Increased security. Only nodes within a VLAN will have access to data.
- No need for a router in order to separate the broadcast domain.

214. What are the four types of VLANs?
    - Port-based VLANs
    - MAC-based VLANs
    - Protocol-based VLANs
    - IP subnet–based VLANs

215. What are the two types of network management nodes and what function does each type perform?
    - Network management agent — An entity (typically a combination of software and hardware) within a node that is responsible for gathering network management information and reporting it to a network management station as appropriate.
    - Network management station — A node that communicates with network management agents throughout a network. Typically it comprises a workstation operated by a network administrator, equipped with network management and other relevant applications software.

216. True or false: Good network planning begins with a top-down approach.

    True

217. There is a natural dividing line as far as planning goes; one involves a *current* network infrastructure and the other a totally new design.

218. In Chapter 13, we discussed some fixed costs that you should consider when planning the network. What are these?
    - Hardware
    - Cabling
    - Any initial installation fees

219. In Chapter 13, we discussed some recurring costs that you should consider when planning the network. What are these?
    - Access fees (monthly telecommunications charges)
    - Support contracts (usually billed out annually)
    - In-house support staff

- Energy needs
- Routine maintenance

220. Which is the best answer to the following statement?

Many companies these days lump __________ under the IT (Information Technology) umbrella.

C. Computer operations, network operations, and all other telecommunications.

221. What is a false floor?

A false floor is a raised floor made up of individual panels that are normally two-foot squares (two feet on each side). They are installed over a framework that looks like a giant matrix before the tiles are laid in. Usually, the facility is wired under the flooring before the tiles are placed down.

222. What is a DMZ?

DMZ is the acronym for demilitarized zone. It has been adopted by the networking world to mean an area not directly connected to any other network segment.

223. VPN remote users have a VPN *client* on their PCs which is configured to access the company's VPN access gateway router.

224. True or false: The distribution from the network operations area to each floor is accomplished by using redundant STP cabling to provide a high-speed path for the network traffic coming from each floor.

False — The distribution from the network operations area to each floor is accomplished using *a high-speed fiber optic link* to provide a high-speed path for the network traffic coming from each floor.

225. List the items that should be included in the final documentation of a network.

- Complete network diagrams with IP addressing
- Equipment lists with location
- Description of each type of network equipment used in the network
- Troubleshooting guides for each type of network equipment being used in the network
- List containing support information for each manufacturer of the network equipment used within the network
- A collection location for all warranty statements for all new equipment deployed within the network
- A collection location for all support contracts from the original equipment or other third-party support organizations

- A collection location of all equipment manuals for the network equipment deployed in the network
- Wiring diagrams for each panel deployed about the network
- A collection location for the information dealing with Internet service providers and other telecommunications providers, including data and voice
- A collection location for all license keys that may be required for any of the equipment in the network
- Maintenance/trouble log (used for ongoing support)
- A collection location of all contact information for all staff responsible for the maintenance of the network

226. *Infrastructure* refers to the structural components within a facility in support of the network architecture.

227. What does WEP stand for?

WEP is an acronym for wired equivalent privacy. This is used by the wireless components within the network for authentication using a shared key. It is only used to prevent unintended use of the network from those users not permitted to access the network's resources.

228. In a networking environment, what is the area that should be restricted and controlled access at all times?

The network operations area

229. True or false: The security practices used in a home LAN are sufficient for all large corporate LANs.

False — In large networks with a wide range of network services and resources, there is a need to restrict some users to only portions of the network that are required by their function within the organization. There is the possibility of multiple authentication services within the same organization. There may be servers within the network that may not rely on network authentication and request a user ID and password from users when they try to gain access to that server.

230. A *firewall* is placed in the path in front of the Intranet web server to analyze the network traffic that is being directed toward it.

231. True or false: Depending upon the size of the network, constantly monitoring every node of a network can be overwhelming.

True

232. True or false: It is bad practice to document the network from a security perspective.

False — To ensure the network from a security perspective requires full documentation as the network currently exists. The documentation should include network diagrams with network address schemes being used and the physical locations of the equipment and cabling being used to make up the network.

233. Name three methods of authentication.

- Lightweight Directory Access Protocol (LDAP)
- Remote Authentication Dial In User Service (RADIUS)
- Certificates

234. True or false: The process of network authentication can be simple as a user ID and password.

True

235. What are the four most commonly used elements in an LDAP?

- Users
- Groups
- Filters
- Services

236. When a RADIUS client passes a user's authentication credentials to the RADIUS server, the server will respond with one of three responses. What are these responses and what does each mean?

- Access Reject — User is denied all access to network resources.
- Access Challenge — User needs to provide additional information.
- Access Accept — User is granted access.

237. The use of *digitally signed certificates* came into use as a security method used to ensure the entities on opposite ends of a communication channel are who they claim to be.

238. *IPSec* is a suite of protocols used for securing Internet communications.

239. True or false: To have a successful help desk implementation, there is a need for someone to pick up the telephone.

True

240. In a large organization, there are usually groups of dedicated individuals who support certain aspects of the network. What are they?

- PC support
- Server support
- Network support

- Telecommunications support
- User base support

241. True or false: Monitoring network performance for larger networks is a manual, time-consuming process.

False — Monitoring network performance for larger networks is an automated process.

242. In any organization, the security group would have a broad range of activities that deal with all aspects of network *security*.

243. The *network* support group is responsible for the distribution of network services over the network.

244. What is the logistics group responsible for?

Logistics involves overseeing the inventory on hand as spares and accounting for all devices deployed in the network. It is the department responsible for logging of the new incoming stock as well as the units that have been returned to the manufacturer for repair.

245. What are three activities that are considered network maintenance?

- Revision control measures
- Corrective measures
- Preventive measures

246. The SNMP *agent* is software that communicates with a network management station (NMS) to answer queries from the station.

247. Each element has its own unique *OID*, which provides information on the object or is an object that will take a variable setting to configure the unit.

248. True or false: Packet capture nodes and programs can return some statistical information if you are investigating traffic patterns or performance issues on a network segment.

True

249. SNMP uses a *community* setting to group a number of devices to be monitored within the *community*.

250. Name at least five of the common LAN issues that we mentioned in Chapter 16.

- Damaged cables
- Dirty fiber
- Excessive signal attenuation
- Insufficient bandwidth

- Denial-of-service (DoS) attack
- Electrical interference
- Wireless interference
- Damaged nodes
- Damaged interface
- Dirty interface
- Configuration error
- Authentication issues
- Excessive utilization
- Excessive errors
- VLAN configuration error
- Class-of-service issue
- Quality-of-service issue

251. When you are notified of a network issue, what are some of the first questions you should start considering?

- How many users are affected?
- Is there only one user having the issue, or are there several individuals?
- Is the problem an expected one? If so, do you have an action plan?
- Have you seen the issue before?
- What is the impact to the LAN? In other words, what nodes are affected?
- How many domains are affected?

252. The *proactive* approach beats the *reactive* approach.

253. Which of the following is a good proactive step you can take to help keep the network from going down and to recover quickly when it does?

- Shared knowledge
- Proper tools
- Ensure the proper individuals are trained appropriately
- Hardware spares
- *All of the above*

254. The ping is an ICMP echo request/reply that determines whether a node is *reachable*, the *round-trip* time for the process to complete, any

packet loss percentages, and a statistical *summary* for a given remote node.

255. True or false: By default, the `ping` command will send four ICMP requests and will expect four replies.

True

256. The *`netstat`* utility by default displays both incoming and outgoing network connections.

257. Network cable testers are devices that are used to check the integrity of the *cabling* in the LAN.

258. Name a few things that you should investigate when troubleshooting a node that is having problems.

- Node configuration(s)
- Event logs (as well as any other logs that may be available)
- Check the status of the interfaces of the node
- Check the memory usage statistics
- Capture any vendor recommended documentation
- Screen shots that may provide insight about the problem

259. What are the steps in the logical, eight-step troubleshooting model that we discussed in Chapter 16?

- Define the problem.
- Consider the possibilities.
- Determine the issue.
- Find a possible solution.
- Test the possible solution.
- Develop an action plan.
- Implement the action plan.
- Monitor the results.

260. As redundant as it may seem, what are the layers of the OSI reference model, and what is performed at each layer?

- Application layer — Provides services used by applications (the transfer of files and messages, authentication, name lookups, etc.) within the network.
- Presentation layer — Ensures that information received by one host can be read by that host.
- Session layer — Sets up, manages, and ends application sessions.

- Transport layer — Ensures the transmission of data from one endpoint to another.
- Network layer — Provides a path from endpoint to endpoint.
- Data Link layer — Provides for a way to transport data over a physical link.
- Physical layer — Determines the specifications for the operations of the physical links between network devices.

261. What are some common Layer 1 issues that can occur in a network?
    - Damaged cables
    - Dirty fiber
    - Excessive signal attenuation
    - Insufficient bandwidth
    - Electrical interference
    - Wireless interference
    - Damaged interface
    - Dirty interface
    - Configuration error
    - Denial-of-service (DoS) attack
    - VLAN configuration error
    - Class-of-service issue
    - Excessive utilization
    - Excessive errors
    - VLAN issue
    - Spanning tree issue
    - MAC address table issue
    - Hardware compression issue
    - Software compression issue
    - VRRP issue
262. What are some things that you should look for in each of the following layers?
    - Layer 4 — At this layer, you want to focus on whether TCP or UDP is operating as intended. Take a sniffer trace and see if there are acknowledgements being sent in response to requests. Also, you will want to check if fragmentation is working as intended. Finally,

check if there are any filters or QOS parameters that may be affecting the flow of data.

- Layer 5 — Things to look for at this layer are whether the session layer protocols are receiving errors while trying to communicate. A sniffer trace can be viewed to determine if the protocols are behaving correctly.
- Layer 6 — At this layer, the encryption, formatting, and compression of data occurs. Is data being encrypted and/or decrypted appropriately? Are encryption configuration settings correct? Are the correct data formats in use? Another concern at this layer is whether a VPN tunnel is operating as it is configured to do.
- Layer 7 — Concerns at the final layer are whether applications are working correctly. Sometimes a version of a standard may support new features, and older clients may no longer interoperate with the new versions. Also, end users may still try to connect to a server with the incorrect client and this, of course, will cause the user not to connect.

263. What are three of the symptoms that indicate a duplex mismatch?
    - FCS/CRC errors
    - Runt datagrams
    - Late collisions

264. A failure in spanning tree usually creates a *loop* within the area that the spanning tree group covers.

265. What are three common ways to find out you have a loop within the LAN?
    - System statistics
    - Sniffer trace
    - Because everyone is reporting issues