Answers to Review Questions

1. C. Proxy ARP can help machines on a subnet reach remote subnets without configuring routing or a default gateway.

2. C. Dynamic Host Configuration Protocol (DHCP) is used to provide IP information to hosts on your network. DHCP can provide a lot of information, but the most common is IP address, subnet mask, default gateway, and DNS information.

3. C. A Class C network address has only 8 bits for defining hosts: $2^8 - 2 = 254$.

4. A, B. A client that sends out a DHCP Discover message in order to receive an IP address sends out a broadcast at both layer 2 and layer 3. The layer 2 broadcast is all *F*s in hex, or FF:FF:FF:FF:FF:FF. The layer 3 broadcast is 255.255.255.255, which means all networks and all hosts. DHCP is connectionless, which means it uses User Datagram Protocol (UDP) at the Transport layer, also called the Host-to-Host layer.

5. A, E. Telnet has been around as long as networking and there is no cost to implement Telnet services on your network. However, all data is sent in a clear text format and both the sending and receving devices must have telnet services running.

6. A, C, F. DHCP, SNMP, and TFTP use UDP. SMTP, FTP, and HTTP use TCP.

7. C, D, E. Telnet, File Transfer Protocol (FTP), and Trivial FTP (TFTP) are all Application layer protocols. IP is a Network layer protocol. Transmission Control Protocol (TCP) is a Transport layer protocol.

8. C. The encapsulation method is data, segment, packet, frame, bit.

9. A, C. When a virtual circuit is created, windowing is used for flow control and acknowledgment of data.

10. A, C, E, G. Routers provide packet switching, packet filtering, internetwork communication, and path selection.

Answers to Review Questions

1. Answer:C. Explanation:To manage a switch remotely, you must set an IP address under the management VLAN, which is, by default, `interface vlan 1`. Then, from global configuration mode, you set the default gateway with the `ip default-gateway` command.

2. Answer:C. Explanation:Switches flood all frames that have an unknown destination address. If a device answers the frame, the switch will update the MAC address table to reflect the location of the device.

3. Answer:C. Explanation:Since the source MAC address is not in the MAC address table, the switch will add the source address and the port it is connected to into the MAC address table and then forward the frame to the outgoing port.

4. Answer:A. Explanation:802.1w is the also called Rapid Spanning-Tree Protocol. It is not enabled by default on Cisco switches, but it is a better STP to run since it has all the fixes that the Cisco extensions provide with 802.1d.

5. Answer:D. Explanation:If the Spanning-Tree Protocol is not running on your switches and you connect them together with redundant links, you will have broadcast storms and multiple frame copies

6. Answer:C. Explanation:The command `show mac address-table` will display the forward/filter table, also called a CAM table on a switch.

7. Answer:D. Explanation:If you have a server or other devices connected into your switch that you're totally sure won't create a switching loop if STP is disabled, you can use something called `portfast` on these ports. Using it means that the port won't spend the usual 50 seconds to come up while STP is converging.

8. Answer:A. Explanation:A switch can have multiple MAC addresses associated with a port. In the graphic, a hub is connected to port Fa0/1, which has two hosts connected.

9. Answer:A, B, C, D. Explanation:Switches, unlike bridges, are hardware based. Cisco says its switches are wire speed and provide low latency, and I guess they are low cost compared to their prices in the 1990s.

10. Answer:B. Explanation:Since the destination MAC address is in the MAC address table (forward/filter table), it will send it out port Fa0/3 only.

Answers to Review Questions

1. D. A point-to-point link uses only two hosts. A /30, or 255.255.255.252, mask provides two hosts per subnet.

2. A, E. First, if you have two hosts directly connected, as shown in the graphic, then you need a crossover cable. A straight-through cable won't work. Second, the hosts have different masks, which puts them in different subnets. The easy solution is just to set both masks to 255.255.255.0 (/24).

3. A. A /28 is a 255.255.255.240 mask. Let's count to the ninth subnet (we need to find the broadcast address of the eighth subnet, so we need to count to the ninth subnet). Starting at 16 (remember, the question stated that we will not use subnet zero so we start at 16, not 0)16, 32, 48, 64, 80, 96, 112, 128, 144. The eighth subnet is 128 and the next subnet is 144, so our broadcast address of the 128 subnet is 143. This makes the host range 129-142.] 142 is the last valid host.

4. C. A /28 is a 255.255.255.240 mask. The first subnet is 16 (remember that the question stated not to use subnet zero), and the next subnet is 32, so our broadcast address is 31. This makes our host range 17–30. 30 is the last valid host.

5. C. To test the local stack on your host, ping the loopback interface of 127.0.0.1.

6. B. Unlike unicast addresses, global unicast addresses are meant to be routed.

7. A. Packets addressed to a unicast address are delivered to a single interface. For load balancing, multiple interfaces can use the same address.

8. C. Link-local addresses are meant for throwing together a temporary LAN for meetings or a small LAN that is not going to be routed but needs to share and access files and services locally.

9. D. These addresses are meant for nonrouting purposes like link-local, but they are almost globally unique, so it is unlikely they will have an address overlap. Unique local addresses where designed as a replacement for site-local addresses

10. B. Packets addressed to a multicast address are delivered to all interfaces identified by the multicast address, the same as in IPv4. It is also called a one-to-many address. You can always tell a multicast address in IPv6 because multicast addresses always start with FF.

Answers to Review Questions

1. A, E. There are actually three different ways to configure the same default route, but only two are shown in the answer. First, you can set a default route with the 0.0.0.0 0.0.0.0 mask and then specify the next hop, as in answer A. Or you can use 0.0.0.0 0.0.0.0 and use the exit interface instead of the next hop. Finally, you can use answer E with the `ip default-network` command.

2. B, E. Classful routing means that all hosts in the internetwork use the same mask. Classless routing means that you can use Variable Length Subnet Masks (VLSMs) and can also support discontiguous networking.

3. B, C. The distance-vector routing protocol sends its complete routing table out all active interfaces on periodic time intervals. Link-state routing protocols send updates containing the state of their own links to all routers in the internetwork.

4. B. `Debug ip rip` is used to show the Internet Protocol (IP) Routing Information Protocol (RIP) updates being sent and received on the router.

5. C. RIPv2 is pretty much just like RIPv1. It has the same administrative distance and timers and is configured just like RIPv1.

6. E. Explanation: To copy the IOS to a backup host, which is stored in flash memory by default, use the `copy flash tftp` command.

7. B. Explanation: The command `traceroute` (`trace` for short), which can be issued from user mode or privileged mode, is used to find the path a packet takes through an internetwork and will also show you where the packet stops because of an error on a router.

8. C. Explanation: Since the configuration looks correct, you probably didn't screw up the copy job. However, when you perform a copy from a network host to a router, the interfaces are automatically shut down and need to be manually enabled with the `no shutdown` command.

9. B. Explanation: The `show flash` command will provide you with the current IOS name and size, and the size of flash memory.

10. D. Explanation: The command `copy tftp flash` will allow you to copy a new IOS into flash memory on your router.

Answers to Review Questions

1. C. The IEEE 802.11b and IEEE 802.11b both run in the 2.4GHz RF range.
2. D. The IEEE 802.11a standard runs in the 5GHz RF range.
3. C. The IEEE 802.11b and IEEE 802.11b both run in the 2.4GHz RF range.
4. C. WPA2 uses the Advanced Encryption Standard (AES) known as the Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) protocol (CCMP).
5. A . The IEEE 802.11g standard provides three non-overlapping channels
6. A. The IEEE 802.11b standard provides three non-overlapping channels
7. B. The IEEE 802.11a standard provides up to 12 non-overlapping channels.
8. D. The IEEE 802.11a standard provides a maximum data rate of up to 54Mbps.
9. D. The IEEE 802.11g standard provides a maximum data rate of up to 54Mbps.
10. B. The IEEE 802.11b standard provides a maximum data rate of up to 11Mbps

Answers to Review Questions

1. B. Users who would normally be blocked by an ACL can just bring up a browser to get through the firewall and then authenticate on a TACACS+ or RADIUS server.

2. C. Context-based Access Control (CBAC's) job is to scrutinize any and all traffic that's attempting to come through the firewall so it can find out about and control the state information for TCP and UDP sessions. And it uses that very information it's gathered to determine whether to create a temporary pathway into the firewall's access lists.

3. A. Reflexive ACLs filter IP packets depending upon upper-layer session information, and they often permit outbound traffic to pass but place limitations on inbound traffic. You can't define reflexive ACLs with numbered or standard IP ACLs, or any other protocol ACLs for that matter.

4. D. Dynamic ACLs first drop the Telnet connection that the user initiated and replace it with a single-entry dynamic ACL that's appended to the extended ACL already in place. This causes traffic to be allowed through for a specific amount of time.

5. A, C. The four typical types of denial of service attacks are TCP SYN flood, ping of death, Tribe Flood Network and Stacheldraht.

6. A. Application layer attacks commonly zero in on well-known holes in the software that's typically found running on servers. Favorite targets include FTP, sendmail, and HTTP.

7. C. Backdoors are simply paths leading into a computer or network. Through simple invasions, or via more elaborate "Trojan horse" code, bad guys can use them as inroads into a specific host or even a network.

8. B. Bad guys use something called a rootkit to probe, scan, and then capture data on a strategically positioned computer that's poised to give them "eyes" into entire systems.

9. D. Denial of service attacks are attacks that makes a service unavailable by overwhelming the system that normally provides it, and there are several different versions.

10. A, B. The two types of security appliances that you'll typically find on a network that provide security are intrusion prevention systems (IPS), which prevent intrusions, hopefully, and intrusion detection systems (IDS), which only detect them and tells you about it.

Answers to Review Questions

1. C. To place an access list on an interface, use the `ip access-group` command in interface configuration mode.

2. D. When trying to find the best answer to an access-list question, always check the access-list number and then the protocol. When filtering to an upper-layer protocol, you must use an extended list, numbers 100–199 and 2000–2699. Also, when you filter to an upper-layer protocol, you must use either `tcp` or `udp` in the protocol field. If it says `ip` in the protocol field, you cannot filter to an upper-layer protocol. SMTP uses TCP.

3. D. If you add an access list to an interface and you do not have at least one `permit` statement, then you will effectively shut down the interface because of the implicit `deny any` at the end of every list.

4. C. Telnet access to the router is restricted by using either a standard or extended IP access list inbound on the VTY lines of the router. The command `access-class` is used to apply the access list to the VTY lines.

5. C. A Cisco router has rules regarding the placement of access lists on a router interface. You can place one access list per direction for each layer 3 protocol configured on an interface.

6. D. The only command that shows which access lists have been applied to an interface is `show ip interface Ethernet 0`. The command `show access-lists` displays all configured access lists, and `show ip access-lists` displays all configured IP access lists, but neither command indicates whether the displayed access lists have been applied to an interface.

7. A. As with access lists, you must configure your interfaces before NAT will provide any translations. On the inside networks, you would use the command `ip nat inside`. On the outside interface, you will use the command `ip nat outside`.

8. B. As with access lists, you must configure your interfaces before NAT will provide any translations. On the inside networks, you would use the command `ip nat inside`. On the outside interface, you will use the command `ip nat outside`.

9. C. Another term for port address translation is NAT Overload because that is the command used to enable port address translation.

10. A, C, E. NAT is not perfect and can cause some issues in some networks, but most networks work just fine. NAT can cause delays and troubleshooting problems, and some applications just won't work.

Answers to Review Questions

1. C. The command `debug ppp authentication` will show you the authentication process that PPP uses between point-to-point connections.

2. C. The key is "there are no free ports" on your router. Only Frame Relay can provide a connection to multiple locations with one interface, and in an economical manner no less.

3. A. If you have a serial port configured with multiple DLCIs connected to multiple remote sites, split horizon rules stop route updates received on an interface from being sent out the same interface. By creating subinterfaces for each PVC, you can avoid the split horizon issues when using Frame Relay.

4. C, D, E. Ethernet and Token Ring are LAN technologies and cannot be configured on a serial interface. PPP, HDLC, and Frame Relay are layer 2 WAN technologies that are typically configured on a serial interface.

5. D. PPP is your only option, as HDLC and Frame Relay do not support these types of business requirements. PPP provides dynamic addressing, authentication using PAP or CHAP, and callback services.

6. A, B. Please do not freak out because ATM is an answer to this question. ATM is not covered in depth on the CCNA exam. PPP is mostly used for dial-up (async) services, but ATM could be used as well, although it typically is not used anymore, since PPP is so efficient.

7. E. This is an easy question because the Remote router is using the default HDLC serial encapsulation and the Corp router is using the PPP serial encapsulation. You should go to the Remote router and set that encapsulation to PPP or change the Corp router back to the default of HDLC.

8. C. Even though the IP addresses don't look correct, they are in the same subnet, so answer B is not correct. The question states that you can ping the other side, so the PVC must be up—answer A can't be correct. You cannot configure IARP, so only answer C can be correct. Since a Frame Relay network is a non-broadcast multi-access network by default, broadcasts such as RIP updates cannot be sent across the PVC unless you use the broadcast statement at the end of the `frame-relay map` command.

9. D. IPSec is an industry-wide standard suite of protocols and algorithms that allows for secure data transmission over an IP-based network that functions at the layer 3 Network layer of the OSI model.

10. C. A *virtual private network (VPN)* allows the creation of private networks across the Internet, enabling privacy and tunneling of non-TCP/IP protocols. A VPN can be set up across any type of link.