NETWORKING BASICS SOLUTIONS

1. Answer & Explanation

Answer: Option **D**

Explanation:

An IPv6 address is 128 bits long.

2. Answer & Explanation

Answer: Option **D**

Explanation:

Port Address Translation (PAT) allows a one-to-many approach to network address translation.

3. Answer & Explanation

Answer: Option **A**

Explanation:

Standard and extended access control lists (ACLs) are used to configure security on a router.

4. Answer & Explanation

Answer: Option **B**

Explanation:

The command to back up the configuration on a router is copy running-config startup-config.

5. Answer & Explanation

Answer: Option **D**

Explanation:

www.vtucs.com

Each device has 10 Mbps to the server

6. Answer & Explanation

Answer: Option **C**

Explanation:

IEEE 802.11B is 2.4GHz, but with a maximum of only 11Mbps. IEEE 802.11G is in the 2.4GHz range, with a top speed of 54Mbps.

7. Answer & Explanation

Answer: Option **A**

Explanation:

256 - 192 = 64. 64 + 64 = 128. 128 + 64 = 192. The subnet is 128, the broadcast address is 191, and the valid host range is the numbers in between, or 129-190.

8. Answer & Explanation

Answer: Option **D**

Explanation:

The command copy flash tftp will prompt you to back up an existing IOS in flash to a TFTP host.

9. Answer & Explanation

Answer: Option **A**

Explanation:

Network Control Protocol is used to help identify the Network layer protocol used in the packet.

www.vtucs.com

10. Answer & Explanation

Answer: Option **C**

Explanation:

The command line vty 0 4 places you in a prompt that will allow you to set or change your Telnet password.

11. Answer & Explanation

Answer: Option **C**

Explanation:

User Datagram Protocol is a connection network service at the Transport layer, and DHCP use

12. Answer & Explanation

Answer: Option **C**

Explanation:

The show ip interface command will show you if any outbound or inbound interfaces have an access list set.

13. Answer & Explanation

Answer: Option **B**

Explanation:

Hubs regenerate electrical signals, which are specified at the Physical layer.

14. Answer & Explanation

Answer: Option **B**

www.vtucs.com

Explanation:

The passive command, short for passive-interface, stops regular updates from being sent out an interface. However, the interface can still receive updates.

15. Answer & Explanation

Answer: Option **C**

Explanation:

ICMP is the protocol at the Network layer that is used to send messages back to an originating router.

16. Answer & Explanation

Answer: Option **B**

Explanation:

Every 2 seconds, BPDUs are sent out from all active bridge ports by default.

17. Answer & Explanation

Answer: Option **A**

Explanation:

By default, switches break up collision domains but are one large broadcast domain.

18. Answer & Explanation

Answer: Option **C**

Explanation:

The command line console 0 places you at a prompt where you can then set your console user-mode password.

www.vtucs.com

19. Answer & Explanation

Answer: Option **B**

Explanation:

To see the contents of all access lists, use the show access-lists command.

20. Answer & Explanation

Answer: Option **A**

Explanation:

Class A addressing provides 24 bits for host addressing.

21. Answer & Explanation

Answer: Option **A**

Explanation:

You should have only one root bridge per network.

22. Answer & Explanation

Answer: Option **C**

Explanation:

Link Control Protocol in the PPP stack provides dynamic addressing, authentication, and multilink.

23. Answer & Explanation

Answer: Option **D**

Explanation:

www.vtucs.com

Stub networks have only one connection to an internetwork. Only default routes can be set on a stub network or network loops may occur.

24. Answer & Explanation

Answer: Option **D**

Explanation:

The clock rate command is two words, and the speed of the line is in bps.

25. Answer & Explanation

Answer: Option **D**

Explanation:

Switches do not propagate VLAN information by default; you must configure the VTP domain. VLAN Trunking Protocol (VTP) is used to propagate VLAN information across a trunk link.

26. Answer & Explanation

Answer: Option **C**

Explanation:

VLANs break up broadcast domains at layer 2.

27. Answer & Explanation

Answer: Option **C**

Explanation:

The primary reason the OSI model was created was so that different networks could inter-operate.

www.ttucs.com

28. Answer & Explanation

Answer: Option **D**

Explanation:

Layer 2 switching creates individual collision domains.

29. Answer & Explanation

Answer: Option **B**

Explanation:

The show interface command shows the line, protocol, DLCI, and LMI information of an interface.

30. Answer & Explanation

Answer: Option **C**

Explanation:

ICMP is the protocol at the Network layer that is used to send echo requests and replies.

31. Answer & Explanation

Answer: Option **D**

Explanation:

The copy tftp flash command places a new file in flash memory, which is the default location for the Cisco IOS in Cisco routers.

32. Answer & Explanation

www.vtucs.com

Answer: Option **A**

Explanation:

The command erase startup-config deletes the configuration stored in NVRAM.

33. Answer & Explanation

Answer: Option **B**

Explanation:

VTP is not right because it has nothing to do with trunking except that it sends VLAN information across a trunk link. 802.1Q and ISL are used to configure trunking on a port.

www.vtucs.com

TCP/IP

1. Answer & Explanation

Answer: Option **B**

Explanation:

SMTP, HTTP and FTP use TCP.

2. Answer & Explanation

Answer: Option **B**

Explanation:

The four layers of the TCP/IP stack (also called the DoD model) are Application/Process, Host-to-Host, Internet, and Network Access. The Host-to-Host layer is equivalent to the Transport layer of the OSI model.

3. Answer & Explanation

Answer: Option **B**

Explanation:

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 Fs in hex, orFF: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.

4. Answer & Explanation

Answer: Option **C**

Explanation:

www.vtucs.com

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.

5. Answer & Explanation

Answer: Option **D**

Explanation:

Class A private address range is 10.0.0.0 through 10.255.255.255. Class B private address range is 172.16.0.0 through 172.31.255.255, and Class C private address range is 192.168.0.0 through 192.168.255.255.

6. Answer & Explanation

Answer: Option **C**

Explanation:

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

7. Answer & Explanation

Answer: Option **C**

Explanation:

The four layers of the DoD model are Application/Process, Host-to-Host, Internet, and Network Access. The Internet layer is equivalent to the Network layer of the OSI model.

8. Answer & Explanation

Answer: Option **A**

Explanation:

DHCP, SNMP, and TFTP use UDP.

www.vtucs.com

9. Answer & Explanation

Answer: Option **C**

Explanation:

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

10. Answer & Explanation

Answer: Option **A**

Explanation:

Both FTP and Telnet use TCP at the Transport layer; however, they both are Application layer protocols, so the Application layer is the best answer.

11. Answer & Explanation

Answer: Option **B**

Explanation:

To turn a binary number into decimal, you just have to add the values of each bit that is a 1. The values of 10011101 are 128, 16, 8, 4, and 1. 128 + 16 + 8 + 4 + 1 = 157.

Hexadecimal is a base-16 number system. The values of hexadecimal are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F-16 characters total, from which to create all the numbers you'll ever need. So, if 1001 in binary is 9, then the hexadecimal equivalent is 9. Since we then have 1101, which is 13 in binary, the hexadecimal answer is D and the complete hexadecimal answer is 0x9D.

12. Answer & Explanation

Answer: Option **C**

Explanation:

www.vtics.com

Internet Control Message Protocol (ICMP) is used to send error messages through the network, but they do not work alone. Every segment or ICMP payload must be encapsulated within an IP datagram (or packet).

13. Answer & Explanation

Answer: Option **B**

Explanation:

This seems like a hard question at first because it doesn't make sense. The listed answers are from the OSI model and the question asked about the TCP/IP protocol stack (DoD model). However, let's just look for what is wrong. First, the Session layer is not in the TCP/IP model; neither are the Data Link and Physical layers. This leaves us with the Transport layer (Host-to-Host in the DoD model), Internet layer (Network layer in the OSI), and Application layer (Application/Process in the DoD).

14. Answer & Explanation

Answer: Option **B**

Explanation:

Although Telnet does use TCP and IP (TCP/IP), the question specifically asks about layer 4, and IP works at layer 3. Telnet uses TCP at layer 4.

15. Answer & Explanation

Answer: Option **B**

Explanation:

ICMP is used for diagnostics and destination unreachable messages. ICMP is encapsulated within IP datagrams, and because it is used for diagnostics, it will provide hosts with information about network problems.

16. Answer & Explanation

www.vtucs.com

Answer: Option **C**

Explanation:

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.

17. Answer & Explanation

Answer: Option **B**

Explanation:

Address Resolution Protocol (ARP) is used to find the hardware address from a known IP address.

18. Answer & Explanation

Answer: Option **D**

Explanation:

DNS uses TCP for zone exchanges between servers and UDP when a client is trying to resolve a hostname to an IP address.

19. Answer & Explanation

Answer: Option **C**

Explanation:

The range of a Class B network address is 128-191. This makes our binary range10xxxxxx.

www.vtucs.com

IP ROUTING

1. Answer & Explanation

Answer: Option **A**

Explanation:

Although answer D almost seems right, it is not; the mask is the mask used on the remote network, not the source network. Since there is no number at the end of the static route, it is using the default administrative distance of 1.

2. Answer & Explanation

Answer: Option **B**

Explanation:

The debug ip rip command is used to show the Internet Protocol (IP) Routing Information Protocol (RIP) updates being sent and received on the router.

3. Answer & Explanation

Answer: Option **C**

Explanation:

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.

4. Answer & Explanation

Answer: Option **C**

Explanation:

The network 10.0.0.0 cannot be placed in the next router's routing table because it already is at 15 hops. One more hop would make the route 16 hops, and that is not valid in RIP networking.

www.vtucs.com

5. Answer & Explanation

Answer: Option **A**

Explanation:

A split horizon will not advertise a route back to the same router it learned the route from.

6. Answer & Explanation

Answer: Option **C**

Explanation:

The (config-router)#passive-interface command stops updates from being sent out an interface, but route updates are still received.

7. Answer & Explanation

Answer: Option **B**

Explanation:

When a routing update is received by a router, the router first checks the administrative distance (AD) and always chooses the route with the lowest AD. However, if two routes are received and they both have the same AD, then the router will choose the one route with the lowest metrics, or in RIP's case, hop count.

8. Answer & Explanation

Answer: Option **C**

Explanation:

You cannot have 16 hops on a RIP network by default. If you receive a route advertised with a metric of 16, this means it is inaccessible.

www.vtucs.com

9. Answer & Explanation

Answer: Option **A**

Explanation:

Since the routing table shows no route to the 192.168.22.0 network, the router will discard the packet and send an ICMP destination unreachable message out interface FastEthernet 0/0, which is the source LAN where the packet originated from.

10. Answer & Explanation

Answer: Option **C**

Explanation:

Static routes have an administrative distance of 1 by default. Unless you change this, a static route will always be used over any other found route. IGRP has an administrative distance of 100, and RIP has an administrative distance of 120, by default.

11. Answer & Explanation

Answer: Option **D**

Explanation:

Another way to avoid problems caused by inconsistent updates and to stop network loops is route poisoning. When a network goes down, the distance-vector routing protocol initiates route poisoning by advertising the network with a metric of 16, or unreachable (sometimes referred to as infinite).

12. Answer & Explanation

Answer: Option **C**

Explanation:

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

www.vtucs.com

13. Answer & Explanation

Answer: Option **B**

Explanation:

RIP has an administrative distance (AD) of 120, while IGRP has an administrative distance of 100, so the router will discard any route with a higher AD than 100.

14. Answer & Explanation

Answer: Option **C**

Explanation:

RIPv2 uses the same timers and loop-avoidance schemes as RIPv1. Split horizon is used to stop an update from being sent out the same interface it was received on. Holddown timers allow time for a network to become stable in the case of a flapping link.

15. Answer & Explanation

Answer: Option **C**

Explanation:

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

16. Answer & Explanation

Answer: Option **B**

Explanation:

IGRP uses bandwidth and delay of the line, by default, to determine the best path to a remote network. Delay of the line can sometimes be called the cumulative interface delay.

www.vtucs.com

17. <u>Answer & Explanation</u>

Answer: Option **D**

Explanation:

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 0.0.0.0mask and then specify the next hop, as in option A. Or you can use 0.0.0.0 0.0.0.0and use the exit interface instead of the next hop. Finally, you can use option D with theip default-network command.

www.vtucs.com

SECURITY

1. Answer & Explanation

Answer: Option **C**

Explanation:

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.

2. Answer & Explanation

Answer: Option **C**

Explanation:

To apply an access list, the proper command is ip access-group 101 in.

3. Answer & Explanation

Answer: Option **B**

Explanation:

Standard IP access lists use the numbers 1-99 and 1300-1999 and filter based on source IP address only. Option C is incorrect because the mask must be in wildcard format.

4. Answer & Explanation

Answer: Option **C**

Explanation:

The range of 192.168.160.0 to 192.168.191.0 is a block size of 32. The network address is 192.168.160.0 and the mask would be 255.255.224.0, which for an access list must be a wildcard format of 0.0.31.255. The 31 is used for a block size of 32. The wildcard is always one less than the block size.

www.vtics.com

5. Answer & Explanation

Answer: Option **D**

Explanation:

The only command that shows which access lists have been applied to an interface isshow 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.

6. Answer & Explanation

Answer: Option **D**

Explanation:

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.

7. Answer & Explanation

Answer: Option **D**

Explanation:

First, you must know that a /20 is 255.255.240.0, which is a block size of 16 in the third octet. Counting by 16s, this makes our subnet 48 in the third octet, and the wildcard for the third octet would be 15 since the wildcard is always one less than the block size.

8. Answer & Explanation

Answer: Option **C**

Explanation:

www.vtucs.com

Only the show ip interface command will tell you which interfaces have access lists applied. show access-lists will not show you which interfaces have an access list applied.

9. Answer & Explanation

Answer: Option **C**

Explanation:

Using a named access list just replaces the number used when applying the list to the router's interface. ip access-group Blocksales in is correct.

10. Answer & Explanation

Answer: Option **B**

Explanation:

First, you must know that a /21 is 255.255.248.0, which is a block size of 8 in the third octet. Counting by eight, this makes our subnet 144 in the third octet, and the wildcard for the third octet would be 7 since the wildcard is always one less than the block size.

11. Answer & Explanation

Answer: Option **D**

Explanation:

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

12. Answer & Explanation

Answer: Option **A**

Explanation:

www.vtucs.com

First, you must know that a /19 is 255.255.224.0, which is a block size of 32 in the third octet. Counting by 32, this makes our subnet 192 in the third octet, and the wildcard for the third octet would be 31 since the wildcard is always one less than the block size.

13. Answer & Explanation

Answer: Option **C**

Explanation:

The extended access list ranges are 100-199 and 2000-2699, so the access-list number of 100 is valid. Telnet uses TCP, so the protocol TCP is valid. Now you just need to look for the source and destination address. Only the third option has the correct sequence of parameters. Answer B may work, but the question specifically states "only" to network 192.168.10.0, and the wildcard in answer B is too broad.

14. Answer & Explanation

Answer: Option **C**

Explanation:

The show access-lists command will allow you to view the entire contents of all access lists, but it will not show you the interfaces to which the access lists are applied.

15. Answer & Explanation

Answer: Option **A**

Explanation:

The first thing to check in a question like this is the access-list number. Right away, you can see that the second option is wrong because it is using a standard IP access-list number. The second thing to check is the protocol. If you are filtering by upper-layer protocol, then you must be using either UDP or TCP; this eliminates the fourth option. The third and last answers have the wrong syntax.

www.vtucs.com

16. Answer & Explanation

Answer: Option **B**

Explanation:

The wildcard 0.0.0.0 tells the router to match all four octets. This wildcard format alone can be replaced with the host command.

17. Answer & Explanation

Answer: Option **D**

Explanation:

Extended IP access lists use numbers 100-199 and 2000-2699 and filter based on source and destination IP address, protocol number, and port number. The last option is correct because of the second line that specifies permit ip any any. (I used 0.0.0.0 255.255.255.255, which is the same as the any option.) The third option does not have this, so it would deny access but not allow everything else.

18. Answer & Explanation

Answer: Option **C**

Explanation:

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.

19. Answer & Explanation

Answer: Option **C**

Explanation:

www.vtues.com

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

www.vtucs.com

WIRELESS TECHNOLOGIES

1. Answer & Explanation

Answer: Option **D**

Explanation:

The IEEE 802.11a standard runs in the 5GHz RF range.

2. Answer & Explanation

Answer: Option **D**

Explanation:

The IEEE 802.11b standard provides the lowest data rate at 1Mbps, but it also has the longest distance, which is about 350 feet.

3. Answer & Explanation

Answer: Option **A**

Explanation:

The IEEE 802.11a standard provides a maximum data rate of up to 54Mbps, but you need to be close to the access point, somewhere around 65 to 75 feet.

4. Answer & Explanation

Answer: Option **C**

Explanation:

The IEEE 802.11b and IEEE 802.11g standards both run in the 2.4GHz RF range.

www.vtics.com

5. Answer & Explanation

Answer: Option **B**

Explanation:

Each AP in a mesh network runs the Adaptive Wireless Path Protocol (AWPP). This protocol allows RAPs to communicate with each other to determine the best path back to the wired network via the RAP.

6. Answer & Explanation

Answer: Option **D**

Explanation:

The IEEE 802.11g standard provides a maximum data rate of up to 54Mbps.

7. Answer & Explanation

Answer: Option **D**

Explanation:

The IEEE 802.11a standard provides a maximum data rate of up to 54Mbps.

8. Answer & Explanation

Answer: Option **A**

Explanation:

The IEEE 802.11b standard provides 3 non-overlapping channels.

9. Answer & Explanation

Answer: Option **B**

www.vtucs.com

Explanation:

The IEEE 802.11a standard provides up to 12 non-overlapping channels.

10. Answer & Explanation

Answer: Option **B**

Explanation:

The split-MAC architecture allows the splitting of 802.11 protocol packets between the Cisco LWAPP-based AP, which handles real-time portions of the protocol, and the WLAN controller, which handles those items that are not time sensitive.

11. Answer & Explanation

Answer: Option **C**

Explanation:

The IEEE 802.11b standard provides a maximum data rate of up to only 11Mbps, and you can be around 150 feet, maybe farther, depending on conditions.

12. Answer & Explanation

Answer: Option **B**

Explanation:

The IEEE 802.11g standard provides a maximum data rate of up to 54Mbps, but you need to be close to the access point, somewhere around 90 to 100 feet.

13. Answer & Explanation

Answer: Option **B**

Explanation:

www.vtucs.com

The IEEE 802.11a standard's lowest data rate is 6Mbps, but it can run from a distance of about 175 feet.

14. Answer & Explanation

Answer: Option **C**

Explanation:

The IEEE 802.11h standard provides an addition 11 channels to the 802.11a standard's 12 non-overlapping channel for a total of 23 non-overlapping channels.

15. Answer & Explanation

Answer: Option **B**

Explanation:

The IEEE 802.11b standard provides a maximum data rate of up to 11Mbps.

16. Answer & Explanation

Answer: Option **A**

Explanation:

Extended Service Set ID means that you have more than one access point and they all are set to the same SSID and all are connected together in the same VLAN or distribution system so users can roam.

17. Answer & Explanation

Answer: Option **B**

Explanation:

www.vtucs.com

The Cisco Unified Wireless Solution is a great product, but you must purchase specialized devices. Cisco managed access points and a controller are the devices you need to purchase to run the Unified Wireless Solution.

18. Answer & Explanation

Answer: Option **C**

Explanation:

The IEEE 802.11b and IEEE 802.11g standards both run in the 2.4GHz RF range.

19. Answer & Explanation

Answer: Option **A**

Explanation:

The IEEE 802.11g standard provides 3 non-overlapping channels.

20. Answer & Explanation

Answer: Option **C**

Explanation:

The IEEE 802.11g standard's lowest data rate is 6Mbps, but it can run from a distance of about 300 feet.

www.vtucs.com

WIDE AREA NETWORKS

1. Answer & Explanation

Answer: Option **C**

Explanation:

It is very important to remember when studying the CCNA exam objectives, and when configuring Frame Relay with point-to-point subinterfaces, that you do not put an IP address on the physical interface.

2. Answer & Explanation

Answer: Option **C**

Explanation:

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

3. Answer & Explanation

Answer: Option **D**

Explanation:

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.

4. Answer & Explanation

Answer: Option **C**

Explanation:

If you have a Cisco router on one side of a Frame Relay network and a non-Cisco router on the other side, you would need to use the Frame Relay encapsulation type of IETF. The default is

www.vtucs.com

Cisco encapsulation, which means that a Cisco router must be on both sides of the Frame Relay network.

5. Answer & Explanation

Answer: Option **A**

Explanation:

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, though it typically is not used anymore since PPP is so efficient.

6. Answer & Explanation

Answer: Option **C**

Explanation:

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.

7. Answer & Explanation

Answer: Option **C**

Explanation:

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.

8. Answer & Explanation

Answer: Option **C**

Explanation:

www.vtucs.com

The show frame-relay ? command provides many options, but the options available in this question are lmi, pvc, and map.

9. Answer & Explanation

Answer: Option **D**

Explanation:

In a modern network, hybrid fibre-coaxial (HFC) is a telecommunications industry term for a network that incorporates both optical fiber and coaxial cable to create a broadband network.

10. Answer & Explanation

Answer: Option **C**

Explanation:

Frame Relay, by default, is a non-broadcast multi-access (NBMA) network, which means that broadcasts, such as RIP updates, will not be forwarded across the link by default.

11. Answer & Explanation

Answer: Option **C**

Explanation:

A 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.

12. Answer & Explanation

Answer: Option **D**

Explanation:

www.vtucs.com

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.

13. Answer & Explanation

Answer: Option **A**

Explanation:

ATM is the Data-Link layer protocol that's typically used over the DSL layer 1 connection from the CPE and terminated at what's known as the DSLAM-an ATM switch that contains DSL interface cards, or ATU-Cs.

14. Answer & Explanation

Answer: Option **A**

Explanation:

Clocking on a serial interface is always provided by the CSU/DSU (DCE device). However, if you do not have a CSU/DSU in your nonproduction test environment, then you need to supply clocking with the clock rate command on the serial interface of the router with the DCE cable attached.

15. Answer & Explanation

Answer: Option **B**

Explanation:

If you have a router in your Frame Relay network that does not support IARP, you must create Frame Relay maps on your router, which provide known DLCI-to-IP address mappings.

16. Answer & Explanation

Answer: Option **A**

www.vtucs.com

Explanation:

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.

17. <u>Answer & Explanation</u>

Answer: Option **C**

Explanation:

PPPoE encapsulates PPP frames in Ethernet frames and uses common PPP features like authentication, encryption, and compression. PPPoA is used for ATM.

www.vtucs.com

NETWORK ADDRESS TRANSLATION

1. Answer & Explanation

Answer: Option **B**

Explanation:

As in 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.

2. Answer & Explanation

Answer: Option **A**

Explanation:

The command show ip nat translations will show you the translation table containing all the active NAT entries.

3. Answer & Explanation

Answer: Option **A**

Explanation:

As in 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.

4. Answer & Explanation

Answer: Option **C**

Explanation:

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

www.vtucs.com

5. **Answer & Explanation**

Answer: Option **B**

Explanation:

Instead of the netmask command, you can use the prefix-length <length>statement.

6. **Answer & Explanation**

Answer: Option **C**

Explanation:

In order for NAT to provide translation services, you must have ip nat inside and ip nat outside configured on your router's interfaces.

7. **Answer & Explanation**

Answer: Option **B**

Explanation:

The show ip nat statistics command displays a summary of the NAT configuration as well as counts of active translation types, hits to an existing mapping, misses (causing an attempt to create a mapping), and expired translations.

8. **Answer & Explanation**

Answer: Option **B**

Explanation:

The host on the global network before translation is considered to be an outside local host.

9. **Answer & Explanation**

www.vtics.com

Answer: Option **C**

Explanation:

The host on the private network after translation is considered to be an inside global host.

10. Answer & Explanation

Answer: Option **C**

Explanation:

You can configure NAT three ways on a Cisco router: static, dynamic, and NAT Overload (PAT).

11. Answer & Explanation

Answer: Option **C**

Explanation:

The command debug ip nat will show you in real time the translations occurring on your router.

12. Answer & Explanation

Answer: Option **A**

Explanation:

The most popular use of NAT is if you want to connect to the Internet and you don't want hosts to have global (real) IP addresses, but option B and D are correct as well.

13. Answer & Explanation

Answer: Option **D**

Explanation:

www.vtucs.com

NAT is not perfect, but there are some advantages. It conserves global addresses, which allow us to add millions of hosts to the Internet without "real" IP addresses. This provides flexibility in our corporate networks. NAT can also allow you to use the same subnet more than once in the same network without overlapping networks.

14. Answer & Explanation

Answer: Option **A**

Explanation:

The host on the private network before translation is considered to be an inside local host.

15. Answer & Explanation

Answer: Option **A**

Explanation:

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.

16. Answer & Explanation

Answer: Option **D**

Explanation:

The host on the global network after translation is considered to be an outside global host.

17. Answer & Explanation

Answer: Option **B**

Explanation:

www.vtucs.com

The command ip nat pool <name> creates the pool that hosts can use to get onto the global Internet. What makes option B correct is that the range 171.16.10.65 through 171.16.10.94 includes 30 hosts, but the mask has to match 30 hosts as well, and that mask is 255.255.255.224. Option C is wrong because the pool name has a lower case "T" in the pool name. Pool name's are case sensitive.

18. Answer & Explanation

Answer: Option **D**

Explanation:

The command clear ip nat translations * will clear all the active NAT entries in your translation table.

www.vtucs.com

IPv6

1. Answer & Explanation

Answer: Option **B**

Explanation:

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.

2. Answer & Explanation

Answer: Option **A**

Explanation:

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

3. Answer & Explanation

Answer: Option **A**

Explanation:

To enable OSPFv3, you enable the protocol as with RIPng. The command string is ipv6ospf <process-id> area <area-id>.

4. Answer & Explanation

Answer: Option **B**

Explanation:

RIPng uses the multicast IPv6 address of FF02::9. If you remember the multicast addresses for IPv4, the numbers at the end of each IPv6 address are the same.

www.vtucs.com

5. Answer & Explanation

Answer: Option **B**

Explanation:

In order to shorten the written length of an IPv6 address, successive fields of zeros may be replaced by double colons. In trying to shorten the address further, leading zeros may also be removed. Just as with IPv4, a single device's interface can have more than one address; with IPv6 there are more types of addresses and the same rule applies. There can be link-local, global unicast, and multicast addresses all assigned to the same interface.

6. Answer & Explanation

Answer: Option **B**

Explanation:

It's pretty simple to enable RIPng for IPv6. You configure it right on the interface where you want RIP to run with the ipv6 router rip number command.

7. Answer & Explanation

Answer: Option **B**

Explanation:

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

8. Answer & Explanation

Answer: Option **D**

Explanation:

Adjacencies and next-hop attributes now use link-local addresses, and OSPFv3 still uses multicast traffic to send its updates and acknowledgments with the addresses FF02::5for OSPF

www.vtucs.com

routers and FF02::6 for OSPF designated routers. These are the replacements for 224.0.0.5 and 224.0.0.6, respectively.

9. Answer & Explanation

Answer: Option **A**

Explanation:

EIGRPv6's multicast address stayed very near the same. In IPv4 it was 224.0.0.10; now it is FF02::A (A=10 in hexadecimal notation).

10. Answer & Explanation

Answer: Option **B**

Explanation:

Unlike RIPng and OSPFv3, you need to configure EIGRP both from global configuration mode and from interface mode, and you have to enable the command with the no shutdown command.

11. Answer & Explanation

Answer: Option **C**

Explanation:

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.

12. Answer & Explanation

Answer: Option **D**

Explanation:

www.vtucs.com

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 were designed as a replacement for site-local addresses.

13. Answer & Explanation

Answer: Option **C**

Explanation:

Anycast addresses identify multiple interfaces, which is the same as multicast; however, the big difference is that the anycast packet is only delivered to one address, the first one it finds defined in the terms of routing distance. This address can also be called one-to-one-of-many.

14. Answer & Explanation

Answer: Option **C**

Explanation:

The loopback address with IPv4 is 127.0.0.1. With IPv6, that address is ::1.

15. Answer & Explanation

Answer: Option **C**

Explanation:

IPv4 addresses are 32 bits long and are represented in decimal format. IPv6 addresses are 128 bits long and represented in hexadecimal format.

www.vtucs.com