5.7.2 Module 5: Network Fundamentals Quiz (Answers)

itexamanswers.net/5-7-2-module-5-network-fundamentals-quiz-answers.html

September 14, 2021

DevNet Associate 5.7.2 Module 5: Network Fundamentals Quiz (Answers)

1. Which statement describes the ping and tracert commands?

- **Tracert shows each hop, while ping shows a destination reply only.**
- Tracert uses IP addresses; ping does not.
- Both ping and tracert can show results in a graphical display.
- Ping shows whether the transmission is successful; tracert does not.

Explanation: The **ping** utility tests end-to-end connectivity between the two hosts. However, if the message does not reach the destination, there is no way to determine where the problem is located. On the other hand, the **traceroute** utility (**tracert** in Windows) traces the route a message takes from its source to the destination. **Traceroute** displays each hop along the way and the time it takes for the message to get to that network and back.

2. Which IPv6 address is most compressed for the full FE80:0:0:0:2AA:FF:FE9A:4CA3 address?

- FE80:::0:2AA:FF:FE9A:4CA3
- FE8::2AA:FF:FE9A:4CA3
- FE80::0:2AA:FF:FE9A:4CA3
- FE80::2AA:FF:FE9A:4CA3

Explanation: When an IPv6 address is being compressed, the :: can be used to replace a recurring set of 0s only once.

3. Which command can be used on Linux and MAC hosts to get IP addressing information?

- networksetup -getinfo
- ipconfig
- ip address
- **ifconfig**

Explanation: Network administrators typically view the IP addressing information on Windows hosts by issuing the **ipconfig** command, and on Linux and Mac hosts by issuing the **ifconfig** command. The **networksetup -getinfo** command is used on Mac hosts to

verify IP settings. The **ip address** command is used on Linux hosts to display IP addresses and properties.

4. What type of IPv6 address is FE80::1?

- global unicast
- loopback
- **link-local**
- multicast

Explanation: Link-local IPv6 addresses start with FE80::/10, which is any address from FE80:: to FEBF::. Link-local addresses are used extensively in IPv6 and allow directly connected devices to communicate with each other on the link they share.

5. Which two statements are true about NTP servers in an enterprise network? (Choose two.)

- There can only be one NTP server on an enterprise network.
- NTP servers control the mean time between failures (MTBF) for key network devices.
- **NTP servers at stratum 1 are directly connected to an authoritative time source.**
- All NTP servers synchronize directly to a stratum 1 time source.
- **NTP servers ensure an accurate time stamp on logging and debugging information.**

Explanation: Network Time Protocol (NTP) is used to synchronize the time across all devices on the network to make sure accurate timestamping on devices for managing, securing and troubleshooting. NTP networks use a hierarchical system of time sources. Each level in this hierarchical system is called a stratum. The stratum 1 devices are directly connected to the authoritative time sources.

6. A small-sized company has 30 workstations and 2 servers. The company has been assigned a group of IPv4 addresses 209.165.200.224/29 from its ISP. The two servers must be assigned public IP addresses so they are reachable from the outside world. What technology should the company implement in order to allow all workstations to access services over the Internet simultaneously?

- static NAT
- dynamic NAT
- DHCP
- **port address translation**

Explanation: The company allocated only 6 usable host public addresses. Two public addresses should be assigned to the two servers. Since the four remaining public addresses are not enough for the 30 clients, NAT must be implemented for internal workstations to access the Internet. Therefore, the company should use PAT, also known as NAT with overload. DHCP can be used to dynamically assign internal private IP addresses to the workstations, but cannot provide the NAT service required.

7. Which statement describes a stateful firewall?

- **It can determine if the connection is in the initiation, data transfer, or termination phase.**
- It can expand the number of IP addresses available and can hide network addressing design.
- It can filter packets based on information at Layers 3, 4, 5 and 7 of the OSI reference model.
- It can only filter packets based on limited Layer 3 and 4 information.

Explanation: Basic packet filtering firewalls can only filter based on Layer 3 and sometimes basic Layer 4 information. An application gateway firewall, or proxy firewall, can filter based on information in the upper layers such as the application layer. A NAT firewall can expand the number of available IP addresses on the network.

8. Which impact does adding a Layer 2 switch have on a network?

- an increase in the number of dropped frames
- **an increase in the size of the broadcast domain**
- an increase in the size of the collision domain
- an increase in the number of network collisions

Explanation: Adding a Layer 2 switch to a network increases the number of collision domains and increases the size of the broadcast domain. Layer 2 switches do not decrease the amount of broadcast traffic, do not increase the amount of network collisions and do not increase the number of dropped frames.

9. Data is being sent from a source PC to a destination server. Which three statements correctly describe the function of TCP or UDP in this situation? (Choose three.)

- **The source port field identifies the running application or service that will handle data returning to the PC.**
- **The UDP destination port number identifies the application or service on the server which will handle the data.**
- **UDP segments are encapsulated within IP packets for transport across the network.**

- TCP is the preferred protocol when a function requires lower network overhead.
- The TCP source port number identifies the sending host on the network.
- The TCP process running on the PC randomly selects the destination port when establishing a session with the server.

Explanation: Layer 4 port numbers identify the application or service which will handle the data. The source port number is added by the sending device and will be the destination port number when the requested information is returned. Layer 4 segments are encapsulated within IP packets. UDP, not TCP, is used when low overhead is needed. A source IP address, not a TCP source port number, identifies the sending host on the network. Destination port numbers are specific ports that a server application or service monitors for requests.

10. What is the function of the MIB element as part of a network management system?

- to send and retrieve network management information
- to change configurations on SNMP agents
- **to store data about a device**
- to collect data from SNMP agents

Explanation: The Management Information Base (MIB) resides on a networking device and stores operational data about the device. The SNMP manager can collect information from SNMP agents. The SNMP agent provides access to the information.

11. Which two devices allow hosts on different VLANs to communicate with each other? (Choose two.)

- **Layer 3 switch**
- hub
- Layer 2 switch
- repeater
- **router**

Explanation: Members of different VLANs are on separate networks. For devices on separate networks to be able to communicate, a Layer 3 device, such as a router or Layer 3 switch, is necessary.

12. What is obtained when ANDing the address 192.168.65.3/18 with its subnet mask?

- 192.168.32.0
- **192.168.64.0**
- 192.168.0.0
- 192.168.16.0

Explanation: The value of the IP address 192.168.65.3 in binary is 11000000.10101000.01001110.00000011. The value of the subnet mask in binary is 11111111.11111111.11000000.00000000. When ANDing the two, the result is 11000000.10101000.01000000.00000000, which in turn converts into 192.168.64.0.