N10-008$^{\text{Q\&As}}$

CompTIA Network+

QUESTION 1

Lisa, a technician, is tasked to monitor various analog POTS lines for voice activity. Which of the following hardware tools would be used?

A. Butt set

B. Toner probe

C. Wire mapper

D. Cable certifier

Correct Answer: A

QUESTION 2

An organization recently connected a new computer to the LAN. The user is unable to ping the default gateway. Which of the following is the most likely cause?

A. The DHCP server is not available.

B. An RFC1918 address is being used

C. The VLAN is incorrect.

D. A static IP is assigned.

Correct Answer: A

The DHCP server is not available is the most likely cause of the issue where a new computer is unable to ping the default gateway. DHCP stands for Dynamic Host Configuration Protocol, which is a network protocol that automatically assigns IP addresses and other configuration parameters to clients on a network. The default gateway is the IP address of the router or device that connects a local network to other networks, such as the internet. Pinging is a network utility that tests the connectivity and reachability between two devices by sending and receiving echo packets. If the DHCP server is not available, the new computer will not be able to obtain an IP address or other configuration parameters, such as the default gateway, from the DHCP server. This will prevent the new computer from communicating with other devices on the network or the internet, resulting in ping failure.

QUESTION 3

Which of the following technologies allows traffic to be sent through two different ISPs to increase performance?

A. Fault tolerance

B. Quality of service

C. Load balancing

D. Port aggregation

Correct Answer: A

Load balancing is a technology that allows traffic to be sent through two different ISPs to increase performance. Load balancing is a process of distributing network traffic across multiple servers or links to optimize resource utilization, throughput, latency, and reliability. Load balancing can be implemented at different layers of the OSI model, such as layer 4 (transport) or layer 7 (application). Load balancing can also be used for outbound traffic by using multiple ISPs and routing protocols such as BGP (Border Gateway Protocol) to select the best path for each packet. References: https ://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/border-gateway-protocol-bgp/prod_white_paper0900aecd806c4eeb.html

QUESTION 4

A network administrator is required to ensure that auditors have read-only access to the system logs, while systems administrators have read and write access to the system logs, and operators have no access to the system logs. The network administrator has configured security groups for each of these functional categories. Which of the following security capabilities will allow the network administrator to maintain these permissions with the LEAST administrative effort?

A. Mandatory access control

B. User-based permissions

C. Role-based access

D. Least privilege

Correct Answer: C

Role-based access is a security capability that assigns permissions to users based on their roles or functions within an organization. It allows the network administrator to maintain these permissions with the least administrative effort, as they only need to configure the security groups for each role once and then assign users to those groups. Mandatory access control is a security capability that assigns permissions based on security labels or classifications, which requires more administrative effort to maintain. User-based permissions are a security capability that assigns permissions to individual users, which is not scalable or efficient for large organizations. Least privilege is a security principle that states that users should only have the minimum level of access required to perform their tasks, which is not a security capability by itself.

QUESTION 5

A rogue AP was found plugged in and providing Internet access to employees in the break room. Which of the following would be BEST to use to stop this from happening without physically removing the WAP?

A. Password complexity

B. Port security

C. Wireless client isolation

D. Secure SNMP

Correct Answer: B

Port security, would be the best option to use to stop the rogue AP in this scenario. Port security is a feature that can be used to limit the number of devices that can be connected to a switchport. By configuring port security on the switchport to which the rogue AP is connected, the network administrator can ensure that only authorized devices are able to connect to the network and receive an IP address. This would prevent unauthorized devices, such as the rogue AP, from providing Internet access to employees in the break room.

Latest N10-008 Dumps N10-008 Exam Questions N10-008 Braindumps