IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **N10-006**

Title : CompTIA Network+ Certification

Version : Demo

1.A technician needs to limit the amount of broadcast traffic on a network and allow different segments to communicate with each other.
Which of the following options would satisfy these requirements?
A. Add a router and enable OSPF.
B. Add a layer 3 switch and create a VLAN.
C. Add a bridge between two switches.
D. Add a firewall and implement proper ACL.
Answer: B
Explanation:
We can limit the amount of broadcast traffic on a switched network by dividing the computers into logical network segments called VLANs.
A virtual local area network (VLAN) is a logical group of computers that appear to be on the same LAN even if they are on separate IP subnets. These logical subnets are configured in the network switches. Each VLAN is a broadcast domain meaning that only computers within the same VLAN will receive broadcast traffic.
Toallow different segments (VLAN) to communicate with each other, a router is required to establish a connection between the systems. We can use a network router to route between the VLANs or we can use a 'Layer 3' switch. Unlike layer 2 switches that can only read the contents of the data-link layer protocol header in the packets they process, layer 3 switches can read the (IP) addresses in the network layer protocol header as well.

2.The network install is failing redundancy testing at the MDF. The traffic being transported is a mixture of multicast and unicast signals.
Which of the following would BEST handle the rerouting caused by the disruption of service?
A. Layer 3 switch
B. Proxy server
C. Layer 2 switch
D. Smart hub
Answer: A
Explanation:
The question states that the traffic being transported is a mixture of multicast and unicast signals. There are three basic types of network transmissions: broadcasts, which are packets transmitted to every node on the network; unicasts, which are packets transmitted to just one node; and multicasts, which are packets transmitted to a group of nodes. Multicast is a layer 3 feature of IPv4 & IPv6. Therefore, we would need a layer 3 switch (or a router) to reroute the traffic. Unlike layer 2switches that can only read the contents of the data-link layer protocol header in the packets they process, layer 3 switches can read the (IP) addresses in the network layer protocol header as well.

3.Which of the following network devices use ACLs to prevent unauthorized access into company systems?
A. IDS
B. Firewall
C. Content filter
D. Load balancer

Answer: B
Explanation:
A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls arefrequently used to prevent unauthorized Internet users from accessing privatenetworks connected to the Internet, especially intranets. Firewalls use ACLs (access control lists) to determine which traffic is allowed through the firewall. All traffic entering or leaving the intranet passes through the firewall, which examines each message and blocks or allows the message depending on rules specified in the ACL. The rules in the ACL specify which combinations of source IP address, destination address in IP port numbers are allowed.

4.Which of the following is used to define how much bandwidth can be used by various protocols on the network?
A. Traffic shaping
B. High availability
C. Load balancing
D. Fault tolerance
Answer: A
Explanation:
If a network connection becomes saturated to the point where there is a significant level of contention, network latency can rise substantially.
Traffic shaping is used to control the bandwidth used by network traffic. In a corporate environment, business-related traffic may be given priority over other traffic. Traffic can be prioritized based on the ports used by the application sending the traffic. Delayed traffic is stored in a buffer until the higher priority traffic has been sent.

5.Which of the following is used to authenticate remote workers who connect from offsite? (Select TWO).
A. OSPF
B. VTP trunking
C. Virtual PBX
D. RADIUS
E. 802.1x
Answer: D,E
Explanation:
D: A RADIUS (Remote Authentication Dial-in User Service) server is a server with a database of user accounts and passwords used as a central authentication database for users requiring network access. RADIUS servers are commonly used by ISP’s to authenticate their customer’s Internet connections. Remote users connect to one or more Remote Access Servers. The remote access servers then forward the authentication requests to the central RADIUS server.
E: 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a network.
802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client that wishes to attach to the network. The authenticator is a network device,such as an Ethernet switch, wireless access point or in this case, a remote access server and the authentication server is the RADIUS server.