Free Questions for N10-008 by go4braindumps

Shared by Conway on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Which of the following is a characteristic of the application layer?

Options:

A- It relies upon other layers for packet delivery.

B- It checks independently for packet loss.

C- It encrypts data in transit.

D- It performs address translation.

Answer:

A

Explanation:

The application layer is the highest layer of the OSI model, and it provides the interface between the user and the network. It does not handle the details of packet delivery, such as addressing, routing, error checking, or encryption. Those functions are performed by the

lower layers of the OSI model. The application layer only focuses on the format, content, and presentation of the data.

Question 2

Question Type: **MultipleChoice**

Which of the following most likely requires the use of subinterfaces?

Options:

A- A router with only one available LAN port

B- A firewall performing deep packet inspection

C- A hub utilizing jumbo frames

D- A switch using Spanning Tree Protocol

Answer:

A

Explanation:

Subinterfaces are logical divisions of a physical interface that allow a router to communicate with multiple networks using a single LAN port. Subinterfaces can have different IP addresses, VLANs, and routing protocols. They are useful for reducing the number of physical interfaces and cables needed, as well as improving network performance and security.

Subinterfaces - CompTIA Network+ N10-008 Domain 1.21 - YouTube1

CompTIA Network+ Certification Exam Objectives, page 92

Question 3

A network administrator needs to create an SVI on a Layer 3-capable device to separate voice and data traffic. Which of the following best explains this use case?

Options:

A- A physical interface used for trunking logical ports

B- A physical interface used for management access

C- A logical interface used for the routing of VLANs

D- A logical interface used when the number of physical ports is insufficient

Answer:

C

Explanation:

An SVI, or switched virtual interface, is a logical interface that is created on a Layer 3-capable device, such as a multilayer switch or a router. An SVI is associated with a VLAN and can be used to route traffic between different VLANs on the same device or across multiple devices. An SVI can also provide management access, security features, and quality of service (QoS) for the VLAN. An SVI is different from a physical interface, which is a port that connects to a physical device or network. A physical interface can be used for trunking, which is a method of carrying multiple VLANs over a single link, or for connecting to a single VLAN. An SVI is also different from a subinterface, which is a logical division of a physical interface that can be assigned to different VLANs.

VLANs and Trunking -- N10-008 CompTIA Network+ : 2.11

Switched Virtual Interfaces -- N10-008 CompTIA Network+ : 2.22

Question 4

A network manager wants to set up a remote access system for the engineering staff. Access to this system will be over a public IP and secured with an ACL.

Which of the following best describes this system?

Options:

A- VPN

B- Secure Shell

C- Jump server

D- API

Answer:

C

Explanation:

A jump server is a system that allows remote access to internal devices through a single, secure device on the public network. A jump server can be configured with an access control list (ACL) to limit who can access the system and what devices they can connect to. A jump server can also use secure protocols such as SSH or VPN to encrypt the communication between the remote user and the internal device. A jump server is different from a VPN, which creates a virtual private network between the remote user and the internal network. A jump server is also different from a secure shell, which is a protocol that allows remote command execution and file transfer. An API is an application programming interface that allows software components to interact with each other.

Other Network Appliances -- SY0-601 CompTIA Security+ : 3.31

Question 5

Question Type: **MultipleChoice**

A technician is concerned about unauthorized personnel moving assets that are installed in a data center server rack. The technician installs a networked

sensor that sends an alert when the server rack door is opened. Which of the following did the technician install?

Options:

A- Cipher lock

B- Asset tags

C- Access control vestibule

D- Tamper detection

Answer:

D

Explanation:

Tamper detection is a physical security feature that can alert the technician when someone opens the server rack door without authorization. Tamper detection sensors can be installed inside the equipment or on the rack itself, and they can send an alert via email, SMS, or other methods. Tamper detection can help prevent unauthorized access, theft, or damage to the network assets.

Physical Security -- N10-008 CompTIA Network+ : 4.51

Question 6

Question Type: **MultipleChoice**

A senior administrator has been directed to incorporate AAA services within a domain environment for regulatory compliance purposes. Which of the following standards

will enable the use of an AAA server in a domain environment?

Options:

A- 802.1Q

B- 802.1X

C- 802.3bt

D- 802.11h

Answer:

B

Explanation:

802.1X is a standard that enables the use of an AAA server in a domain environment by providing port-based network access control. 802.1X authenticates users or devices before granting them access to the network resources, and can also authorize them based on their roles or policies. 802.1X can work with different AAA protocols, such as RADIUS or TACACS+, to communicate with the AAA server.

CompTIA Network+ N10-008 Certification Study Guide, page 211

CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 382

Configuring AAA Services - Cisco3

Question 7

Question Type: MultipleChoice

After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect

take to troubleshoot the issue?

Options:

A- Check to see if the end connections were wrapped in copper tape before terminating.

B- Use passthrough modular crimping plugs instead of traditional crimping plugs.

C- Connect the RX/TX wires to different pins.

D- Run a speed test on a device that can only achieve 100Mbps speeds.

Answer:

A

Explanation:

Cat 8 keystones are shielded to prevent interference from external sources, but they also require proper grounding to avoid interference from within the cable. Wrapping the end connections with copper tape before terminating them is one way to ensure a good ground connection and reduce interference. Using passthrough modular crimping plugs, connecting the RX/TX wires to different pins, or running a speed test on a slow device are not relevant or effective steps to troubleshoot the issue.

CompTIA Network+ N10-008 Certification Study Guide, page 191

CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 362

CAT8 RJ45 Keystone Problem : r/HomeNetworking2

How to Terminate Cat8 Shielded Keystone Jacks3

Question 8

Question Type: MultipleChoice

A security engineer is trying to connect cameras to a 12-port PoE switch, but only eight cameras turn on. Which of the following should the engineer check first?

Options:

A- Ethernet cable type

B- Voltage

C- Transceiver compatibility

D- DHCP addressing

Answer:

B

Explanation:

The most likely reason why only eight cameras turn on is that the PoE switch does not have enough power budget to supply all 12 cameras. The engineer should check the voltage and wattage ratings of the PoE switch and the cameras, and make sure they are compatible and sufficient. The Ethernet cable type, transceiver compatibility, and DHCP addressing are less likely to cause this problem, as they would affect the data transmission rather than the power delivery.

CompTIA Network+ N10-008 Certification Study Guide, page 181

Question 9

Question Type: **MultipleChoice**

The network engineer receives a new router to use for WAN connectivity. Which of the following best describes the layer the network engineer should connect the new

router to?

Options:

A- Core

B- Leaf

C- Distribution

D- Access

Answer:

C

Explanation:

The distribution layer is the layer that connects the access layer to the core layer in a hierarchical network design. The distribution layer is responsible for routing, filtering, and policy enforcement between the LAN and the WAN. A router is a layer 3 device that can perform these functions and connect to different WAN technologies.

CompTIA Network+ N10-008 Certification Study Guide, page 151

CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 322

CompTIA Network+ N10-008 Exam Cram, page 233

Question 10

Question Type: **MultipleChoice**

Which of the following cables is the most appropriate to use when running bulk cables in ceilings?

Options:

A- Plenum

B- Coaxial

C- Ethernet

D- DAC

Answer:

A

Explanation:

Plenum cable is the most appropriate to use when running bulk cables in ceilings because it is designed to meet fire safety standards and reduce the risk of toxic smoke in plenum spaces, which are areas with air flow above or below floors.

Question 11

Question Type: **MultipleChoice**

A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User 3

and sees the Ethernet is properly connected. However, the network interface's indicator lights are not blinking on either the computer or the switch. Which of the following is

the most likely cause?

Options:

A- The switch failed.

B- The default gateway is wrong.

C- The port is shut down.

D- The VLAN assignment is incorrect.

Answer:

C

Explanation:

If the port is shut down, it means that the switch has disabled the port and is not sending or receiving any traffic on it. This would explain why the network interface's indicator lights are not blinking on either the computer or the switch, and why the user cannot access

resources on the network. The port could be shut down manually by the network administrator, or automatically by the switch due to security or error conditions.

Reference

Port shutdown is one of the common switch configuration options covered in Objective 2.3 of the CompTIA Network+ N10-008 certification exam1.

Port shutdown can cause the network interface's indicator lights to stop blinking2.

Port shutdown can prevent the user from accessing resources on the network3.

1: CompTIA Network+ Certification Exam Objectives, page 52: CompTIA Network+ N10-008: Switch not forwarding frames on trunked port33: Cable Management -- N10-008 CompTIA Network+ : 1.3