Free Questions for N10-008

Shared by Conway on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A support agent receives a report that a remote user's wired devices are constantly disconnecting and have slow speeds. Upon inspection, the support agent sees that the user's coaxial modem has a signal power of -97dB Which of the following should the support agent recommend to troubleshoot the issue?

Options:

A- Removing any splitters connected to the line
B- Switching the devices to wireless
C- Moving the devices closer to the modern
D- Lowering the network speed

Answer:

A

Explanation:

A splitter is a device that divides a coaxial cable into two or more branches, allowing multiple devices to share the same cable connection. However, a splitter also reduces the signal strength and quality of the cable, which can affect the performance and reliability of the devices connected to it. A signal power of -97dB is very low and indicates a weak or poor cable signal, which can cause constant disconnections and slow speeds.

The support agent should recommend removing any splitters connected to the line and connecting the coaxial modem directly to the cable outlet. This can help to improve the signal power and quality of the cable, and thus enhance the performance and reliability of the wired devices. Alternatively, the support agent can also suggest using a signal amplifier or booster, which is a device that increases the signal strength and quality of the cable, to compensate for the signal loss caused by the splitter.

The other options are not correct because they are not the best recommendations to troubleshoot the issue. They are:

Switching the devices to wireless. Switching the devices to wireless may not solve the issue, as the wireless connection may also depend on the cable signal and quality. Moreover, switching the devices to wireless may introduce other problems, such as interference, security, or compatibility issues, that can affect the performance and reliability of the devices.

Moving the devices closer to the modem. Moving the devices closer to the modem may not solve

the issue, as the problem is not related to the distance between the devices and the modem, but to the signal power and quality of the cable. Moreover, moving the devices closer to the modem may not be feasible or convenient for the user, depending on the layout and setup of the location.

Lowering the network speed. Lowering the network speed may not solve the issue, as the problem is not related to the bandwidth or capacity of the network, but to the signal power and quality of the cable. Moreover, lowering the network speed may degrade the user experience and satisfaction, as the user may not be able to access or use the network services or applications as expected.

Reference 1:Network+ (Plus) Certification | CompTIA IT Certifications 2:What is a Coaxial Splitter? - Definition from Techopedia 3:What is a Signal Amplifier? - Definition from Techopedia

Question 2

Question Type: MultipleChoice

A technician is troubleshooting a SQL database connection. After remotely connecting to the end client, the technician tests basic connectivity. Which of the following ports is available to connect via command-line interface?

Options:

A- 143
B- 445
C- 993
D- 1521

Answer:

D

Explanation:

The correct port available for connecting to a SQL database via command-line interface isD. 1521. Port 1521 is the default port for Oracle Database connections using the Oracle Net Services (SQL*Net) protocol.

Port 143: This is used for IMAP (Internet Message Access Protocol) communication.

Port 445: This is used for Microsoft's SMB (Server Message Block) protocol (file and printer

sharing).

Port 993: This is used for secure IMAP (IMAPS) communication.

Port 1521: This is the default port for Oracle Database connections using the Oracle Net Services (SQL*Net) protocol.

Question 3

Question Type: MultipleChoice

An engineer recently installed a new distribution switch and connected two servers provisioned with the following IPs: 192.168.17.20 and 192.168.17.30. The servers cannot connect to the Internet, but they can reach themselves. The engineer observes that the distribution switch has the following setup:

```
interface VLAN 100
IP address 192.168.17.5 255.255.255.0
```

The engineer is able to reach the core router 192.168.17.1 from the distribution switch. Which of the following is the most likely cause of this issue?

Options:

A- A routing loop has occurred.
B- The subne1 mask is Incorrect.
C- The servers are not configured with default gateway.
D- There is an improper Layer 1 connection between the router and the ISP modem.

Answer:

C

Explanation:

The servers can communicate with each other but not the internet, indicating local network connectivity is fine. The distribution switch's VLAN and IP configuration are correct, and the engineer can reach the core router, suggesting the issue is not with the switch or the router. The most likely cause is that the servers do not have a default gateway configured, which is necessary for traffic to leave the local network and reach the internet.

Question 4

Question Type: MultipleChoice

A network administrator is adding a new wired IoT device to the internal network. The only devices that will be communicating are the HVAC system and the IoT device. Which of the following should the network administrator do?

Options:

A- Set up a secure VM.
B- Implement a reverse proxy.
C- Set up the guest network isolation.
D- Configure a dedicated VLAN.

Answer:

D

Explanation:

When adding a new wired IoT device that will only communicate with the HVAC system, it is best practice to configure a dedicated VLAN. This isolates the traffic between the IoT device and the HVAC system from the rest of the network, enhancing security and network efficiency.

CompTIA Network+ N10-008 Full Course for Beginners - Configuring SOHO Networks4

Network+ (Plus) Certification | CompTIA IT Certifications

Question 5

Question Type: MultipleChoice

A company wants to mitigate unauthorized physical connectivity after implementing a hybrid work schedule. Which of the following will the company most likely configure?

Options:

A- Intrusion prevention system
B- DHCP snooping

C- ARP inspection
D- Port security

Answer:

D

Explanation:

Port security is a feature that allows network administrators to limit the number of devices that can connect to a switch port, based on the MAC address of the device. This can prevent unauthorized physical connectivity by blocking any device that is not on the allowed list or exceeding the maximum number of devices per port. Port security can also trigger an action, such as shutting down the port or sending an alert, when a violation occurs.Reference:CompTIA Network+ N10-008 Cert Guide - O'Reilly Media, Chapter 14: Securing a Basic Network, page 512

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

A company receives a cease-and-desist order from its ISP regarding prohibited torrent activity. Which of the following should be implemented to comply with the cease-and-desist order?

Options:

A- MAC security
B- Content filtering
C- Screened subnet
D- Perimeter network

Answer:

B

Explanation:

Content filtering is a technique that blocks or allows access to certain types of web content, based on predefined criteria or policies. Content filtering can be used to comply with the cease-and-desist order by preventing users from accessing torrent sites or downloading torrent files, which are often used for illegal file sharing or piracy. Content filtering can also protect the network from malware, phishing, or inappropriate content.Reference:CompTIA Network+ N10-008 Cert Guide - O'Reilly Media, Chapter 14: Securing a Basic Network, page 520

Question 8

Question Type: MultipleChoice

Which of the following fields are negotiated during the three-way-handshake process? (Select three).

Options:

A- Sequence number
B- MTU
C- Window size
D- MSS
E- TTL
F- Flags
G- Acknowledgment number
H- CRC

Answer:

A, C, G

Explanation:

During the TCP three-way handshake process, the following fields are negotiated:

A . Sequence number: Initial sequence numbers are established during the handshake to keep track of the segments in the communication.

C . Window size: This determines the amount of data that can be sent before receiving an acknowledgment.

G . Acknowledgment number: This confirms receipt of the data and also indicates the next expected byte.

The other options are not negotiated during the three-way handshake:

B . MTU (Maximum Transmission Unit): This is determined at the network layer and is not negotiated during the handshake.

D . MSS (Maximum Segment Size): This is communicated during the handshake but not negotiated; it's declared by the sender to inform the receiver of the maximum segment size it can handle.

E . TTL (Time To Live): This is set in each IP packet to limit its lifespan and is not negotiated during the handshake.

F- Flags: Specific flags are used during the handshake (SYN and ACK), but they are not ''negotiated'' per se.

H) CRC (Cyclic Redundancy Check): This is used for error-checking in frames at the data link layer and is not part of the three-way handshake.

Question 9

Question Type: MultipleChoice

Which of the following best describes the purpose of an access control vestibule?

Options:

A- To mitigate an on-path attack
B- To mitigate tailgating
C- To mitigate phishing
D- To mitigate snooping

Answer:

B

Explanation:

An access control vestibule, also known as a mantrap, is a physical security access control system that consists of a small space with two sets of interlocking doors. The first set of doors must close before the second set opens, preventing unauthorized individuals from following authorized individuals into facilities with controlled access. This activity, also known as tailgating, results in unauthorized access to the facility. An access control vestibule can help deter and detect tailgating attempts, as well as provide a containment area while authorization for physical access is verified.

Reference

Access Control Vestibules: Types and Peculiarities

Mantrap (access control)

PE-3 (8): Access Control Vestibules

Question 10

Question Type: MultipleChoice

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 11

Question Type: MultipleChoice

Which of the following combinations of single cables and transceivers will allow a server to have 40GB of network throughput? (Select two).

Options:

A- SFP+
B- SFP
C- QSFP+
D- Multimode
E- Cat 6a
E- Cat5e

Answer:

C, D

Explanation:

QSFP+ is a type of transceiver that supports 40 gigabit Ethernet (40GbE) over four lanes of 10 gigabit Ethernet (10GbE) each. QSFP+ stands for quad small form-factor pluggable plus, and it is a compact and hot-swappable module that plugs into a QSFP+ port on a network device. QSFP+ transceivers can support various types of cables and connectors, such as direct attach copper (DAC), active optical cable (AOC), or fiber optic cable.

Multimode is a type of fiber optic cable that supports multiple modes of light propagation within the core. Multimode fiber optic cable can carry higher bandwidth and data rates than single-mode fiber optic cable, but over shorter distances. Multimode fiber optic cable is commonly used for short-reach applications, such as within a data center or a campus network. Multimode fiber optic cable can be paired with QSFP+ transceivers to achieve 40GbE connectivity.

The other options are not correct because they do not support 40GbE. They are:

SFP+. SFP+ is a type of transceiver that supports 10 gigabit Ethernet (10GbE) over a single lane. SFP+ stands for small form-factor pluggable plus, and it is a compact and hot-swappable module that plugs into an SFP+ port on a network device. SFP+ transceivers can support various types of cables and connectors, such as direct attach copper (DAC), active optical cable (AOC), or fiber optic cable. However, SFP+ transceivers cannot support 40GbE by themselves, unless they are used in a breakout configuration with a QSFP+ transceiver.

SFP. SFP is a type of transceiver that supports 1 gigabit Ethernet (1GbE) over a single lane. SFP stands for small form-factor pluggable, and it is a compact and hot-swappable module that plugs into an SFP port on a network device. SFP transceivers can support various types of cables and connectors, such as twisted-pair copper, coaxial cable, or fiber optic cable. However, SFP transceivers cannot support 40GbE by themselves, unless they are used in a breakout configuration with a QSFP+ transceiver.

Cat 6a. Cat 6a is a type of twisted-pair copper cable that supports 10 gigabit Ethernet (10GbE) over distances up to 100 meters. Cat 6a stands for category 6 augmented, and it is an enhanced version of Cat 6 cable that offers better performance and reduced crosstalk. Cat 6a cable can be

paired with 10Gbase-T transceivers to achieve 10GbE connectivity. However, Cat 6a cable cannot support 40GbE by itself, unless it is used in a breakout configuration with a QSFP+ transceiver.

Cat 5e. Cat 5e is a type of twisted-pair copper cable that supports 1 gigabit Ethernet (1GbE) over distances up to 100 meters. Cat 5e stands for category 5 enhanced, and it is an improved version of Cat 5 cable that offers better performance and reduced crosstalk. Cat 5e cable can be paired with 1000base-T transceivers to achieve 1GbE connectivity. However, Cat 5e cable cannot support 40GbE by itself, unless it is used in a breakout configuration with a QSFP+ transceiver.

Reference 1:QSFP+ - an overview | ScienceDirect Topics 2:Multimode Fiber - an overview | ScienceDirect Topics 3:Network+ (Plus) Certification | CompTIA IT Certifications 4:SFP+ - an overview | ScienceDirect Topics 5:SFP - an overview | ScienceDirect Topics 6:Cat 6a - an overview | ScienceDirect Topics 7: [Cat 5e - an overview | ScienceDirect Topics]

P2P exams

P2P exams

To Get Premium Files for N10-008 Visit
https://www.p2pexams.com/products/n10-008

For More Free Questions Visit
https://www.p2pexams.com/comptia/pdf/n10-008

