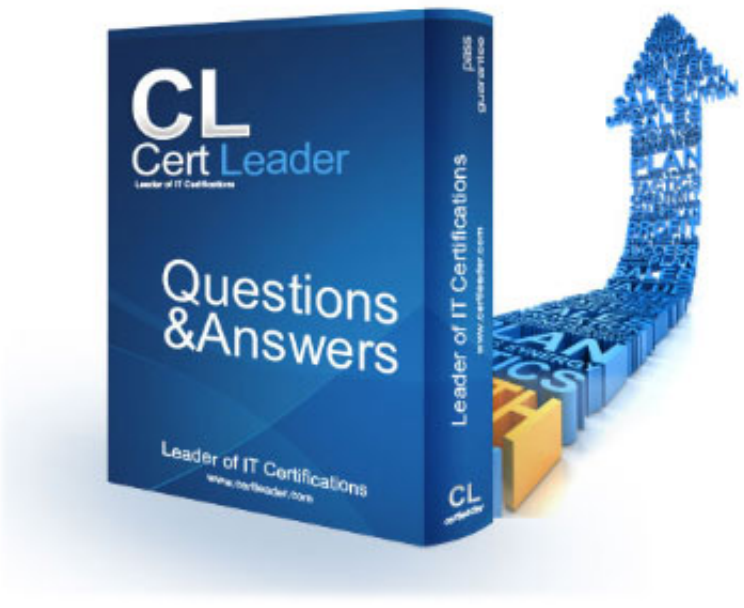
N10-009 Dumps

CompTIA Network+ Exam

https://www.certleader.com/N10-009-dumps.html



NEW QUESTION 1
- (Topic 3)
During an incident, an analyst sends reports regularly to the investigation and leadership teams. Which of the following best describes how Pll should be safeguarded during an incident?

A. Implement data encryption and store the data so only the company has access.
B. Ensure permissions are limited to the investigation team and encrypt the data.
C. Implement data encryption and create a standardized procedure for deleting data that is no longer needed.
D. Ensure the permissions are open only to the company.

Answer: C

Explanation:
PII stands for Personally Identifiable Information, which is any data that can be used to identify, contact, or locate a specific individual, such as name, address, phone number, email, social security number, and so on. PII should be safeguarded during an incident to protect the privacy and security of the individuals involved, and to comply with the legal and ethical obligations of the organization. One way to safeguard PII during an incident is to implement data encryption, which is a process of transforming data into an unreadable format that can only be accessed by authorized parties who have the decryption key. Data encryption can prevent unauthorized access, modification, or disclosure of PII by malicious actors or third parties. Another way to safeguard PII during an incident is to create a standardized procedure for deleting data that is no longer needed, such as after the incident is resolved or the investigation is completed. Deleting data that is no longer needed can reduce the risk of data breaches, data leaks, or data theft, and can also save storage space and resources. A standardized procedure for deleting data can ensure that the data is erased securely and completely, and that the deletion process is documented and audited.
References
? 1: CompTIA Network+ N10-008 Certification Study Guide, page 304-305
? 2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 13
? 3: CompTIA Network+ N10-008 Certification Practice Test, question 5
? 4: Data Encryption – N10-008 CompTIA Network+ : 3.1

NEW QUESTION 2
- (Topic 3)
A company's publicly accessible servers are connected to a switch between the company's ISP-connected router and the firewall in front of the company network. The firewall is stateful, and the router is running an ACL. Which of the following best describes the area between the router and the firewall?

A. Untrusted zone
B. Screened subnet
C. Trusted zone
D. Private VLAN

Answer: B

Explanation:
A screened subnet is a network segment that is isolated from both the internal and external networks by firewalls or routers. It is used to host publicly accessible servers that need some protection from external attacks, but also need to be separated from the internal network for security reasons.
References
? 1: Seven-Second Subnetting – N10-008 CompTIA Network+ : 1.4
? 2: CompTIA Network+ Study Guide: Exam N10-008, 5th Edition, page 56
? 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 22

NEW QUESTION 3
- (Topic 3)
A Chief Information Officer wants to monitor network breaching in a passive, controlled manner. Which of the following would be best to implement?

A. Honeypot
B. Perimeter network
C. Intrusion prevention system
D. Port security

Answer: A

Explanation:
A honeypot is a decoy system that is designed to attract and trap hackers who attempt to breach the network. A honeypot mimics a real system or network, but contains fake or non- sensitive data and applications. A honeypot can be used to monitor network breaching in a passive, controlled manner, as it allows the network administrator to observe the hacker’s behavior, techniques, and tools without compromising the actual network or data. A honeypot can also help to divert the hacker’s attention from the real targets and collect forensic evidence for further analysis or prosecution.

NEW QUESTION 4
- (Topic 3)
A company is moving to a new building designed with a guest waiting area that has existing network ports. Which of the following practices would BEST secure the network?

A. Ensure all guests sign an NDA.
B. Disable unneeded switchports in the area.
C. Lower the radio strength to reduce Wi-Fi coverage in the waiting area.
D. Enable MAC filtering to block unknown hardware addresses.

Answer: B

Explanation:
One of the best practices to secure the network would be to disable unneeded switchports in the guest waiting area. This will prevent unauthorized users from

connecting to the network through these ports. It's important to identify which switchports are not in use and disable them, as this will prevent unauthorized access to the network. Other practices such as ensuring all guests sign an NDA, lowering the radio strength to reduce Wi-Fi coverage in the waiting area and enabling MAC filtering to block unknown hardware addresses are not as effective in securing the network as disabling unneeded switchports. Enforcing an NDA with guests may not stop a malicious user from attempting to access the network, reducing the radio strength only limits the Wi-Fi coverage, and MAC filtering can be easily bypassed by hackers.

NEW QUESTION 5
- (Topic 3)
Which of the following is the best action to take before sending a network router to be recycled as electronic waste?

A. Turn on port security.
B. Shred the switch hard drive.
C. Back up and erase the configuration.
D. Remove the company asset ID tag.

Answer: C

Explanation:
Before disposing of a network router, it is important to back up and erase the configuration to prevent unauthorized access to sensitive data and network settings. A network router may contain information such as passwords, IP addresses, firewall rules, VPN settings, and other network parameters that could be exploited by hackers or malicious users. By backing up the configuration, you can preserve the network settings for future reference or reuse. By erasing the configuration, you can wipe out the data and restore the router to its factory default state.

NEW QUESTION 6
- (Topic 3)
Which of the following documents is MOST likely to be associated with identifying and documenting critical applications?

A. Software development life-cycle policy
B. User acceptance testing plan
C. Change management policy
D. Business continuity plan

Answer: D

Explanation:
A business continuity plan (BCP) is a document that outlines the procedures and strategies to ensure the continuity of critical business functions in the event of a disaster or disruption. A BCP is most likely to be associated with identifying and documenting critical applications that are essential for the organization's operations and recovery. A BCP also defines the roles and responsibilities of the staff, the backup and restore processes, the communication channels, and the testing and maintenance schedules.
References: Network+ Study Guide Objective 5.2: Explain disaster recovery and business continuity concepts.

NEW QUESTION 7
- (Topic 3)
While troubleshooting a network, a VoIP systems engineer discovers a significant inconsistency in the amount of time required for data to reach its destination and return. Which of the following terms best describes this issue?

A. Bandwidth
B. Latency
C. Jitter
D. Throughput

Answer: C

Explanation:
Jitter is the variation in the delay of data packets over a network. It is caused by factors such as network congestion, routing changes, packet loss, or improper queuing. Jitter affects the quality of VoIP calls because it can cause gaps, distortion, or out-of-order delivery of voice data. Jitter can be measured by the difference between the expected and actual arrival times of packets2. To reduce jitter, VoIP systems use buffers to store and reorder packets before playing them back. However, too much buffering can also increase latency, which is the total time it takes for data to travel from one point to another3.
References2 - VoIP Troubleshooting: 5 Fixes for Common Connection Issues - Nextiva3 - Troubleshooting VoIP — Is it You or the Network? - PingPlotter

NEW QUESTION 8
- (Topic 3)
Which of the following combinations of single cables and transceivers will allow a server to have 40GB of network throughput? (Select two).

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

Answer: CD

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.
References1: QSFP+ - an overview | ScienceDirect Topics2: Multimode Fiber - an overview | ScienceDirect Topics3: Network+ (Plus) Certification | CompTIA IT Certifications4: SFP+ - an overview | ScienceDirect Topics5: SFP - an overview | ScienceDirect Topics6: Cat 6a - an overview | ScienceDirect Topics7: [Cat 5e - an overview | ScienceDirect Topics]

NEW QUESTION 9
- (Topic 3)
Which of the following is the most accurate NTP time source that is capable of being accessed across a network connection?

A. Stratum 0 device
B. Stratum 1 device
C. Stratum 7 device
D. Stratum 16 device

Answer: B

Explanation:
NTP (Network Time Protocol) is a protocol that synchronizes the clocks of network devices with a reference time source. NTP uses a hierarchical system of time sources, called strata, to distribute the time information. A stratum 0 device is the most accurate time source, such as an atomic clock or a GPS receiver, but it is not directly accessible across a network connection. A stratum 1 device is a network device that is directly connected to a stratum 0 device, such as a dedicated NTP server or a router with a GPS antenna, and it acts as a primary time server for other network devices. A stratum 2 device is a network device that synchronizes its time with a stratum 1 device, and so on. The higher the stratum number, the lower the accuracy and reliability of the time source. A stratum 16 device is a network device that has no valid time source and is considered unsynchronized.
References:
? Part 1 of current page talks about how Bing is your AI-powered copilot for the web and provides various examples of how it can help you with different tasks, such as writing a joke, creating a table, or summarizing research. However, it does not mention anything about NTP or time sources.
? Part 2 of current page shows the search results for “ai powered search bing chat”, which include web, image, and news results. However, none of these results seem to be relevant to the question, as they are mostly about Bing’s features, products, or announcements, not about NTP or time sources.
? Therefore, I cannot find the answer or the explanation from the current page. I have to use my own knowledge and information from other sources to verify the answer and provide a short but comprehensive explanation. I will cite these sources using numerical references.
? : CompTIA Network+ Certification Exam Objectives, Version 8.0, Domain 2.0: Infrastructure, Objective 2.5: Given a scenario, implement network time synchronization, Subobjective 2.5.1: NTP, https://www.comptia.jp/pdf/comptia- network-n10-008-exam-objectives.pdf
? : Network Time Protocol (NTP), https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back- issues/table-contents-58/154-ntp.html
? : How NTP Works, https://www.meinbergglobal.com/english/info/ntp.htm

NEW QUESTION 10
- (Topic 3)
A network administrator would like to purchase a device that provides access ports to endpoints and has the ability to route between networks. Which of the following would be BEST for the administrator to purchase?

A. An IPS
B. A Layer 3 switch
C. A router
D. A wireless LAN controller

Answer: B

NEW QUESTION 10
- (Topic 3)
A customer connects a firewall to an ISP router that translates traffic destined for the internet. The customer can connect to the internet but not to the remote site. Which of the following will verify the status of NAT?

A. tcpdump
B. nmap
C. ipconfig
D. tracert

Answer: A

Explanation:
tcpdump is a command-line tool that can capture and analyze network traffic on a given interface. tcpdump can verify the status of NAT by showing the source and destination IP addresses of the packets before and after they pass through the ISP router that translates traffic destined for the internet. tcpdump can also show the NAT protocol and port numbers used by the router. nmap, ipconfig, and tracert are not suitable tools for verifying the status of NAT, as they do not show the IP

address translation process.
References
? 1: Network Address Translation – N10-008 CompTIA Network+ : 1.4
? 2: CompTIA Network+ N10-008 Certification Study Guide, page 95-96
? 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 16
? 4: CompTIA Network+ N10-008 Certification Practice Test, question 7

NEW QUESTION 12
- (Topic 3)
A network technician wants to find the shortest path from one node to every other node in the network. Which of the following algorithms will provide the FASTEST convergence time?

A. A static algorithm
B. A link-state algorithm
C. A distance-vector algorithm
D. A path-vector algorithm

Answer: B

Explanation:
A link-state algorithm is a routing algorithm that uses information about the state of each link in the network to calculate the shortest path from one node to every other node. A link-state algorithm requires each router to maintain a complete map of the network topology and exchange link-state advertisements with its neighbors periodically or when a change occurs. A link-state algorithm uses a mathematical formula called Dijkstra's algorithm to find the shortest path based on the link costs. A link-state algorithm provides the fastest convergence time because it can quickly detect and adapt to network changes. References: [CompTIA Network+ Certification Exam Objectives], [Link-state routing protocol - Wikipedia]

NEW QUESTION 13
- (Topic 3)
Which of the following attacks utilizes a network packet that contains multiple network tags?

A. MAC flooding
B. VLAN hopping
C. DNS spoofing
D. ARP poisoning

Answer: B

NEW QUESTION 17
- (Topic 3)
A company is considering shifting its business to the cloud. The management team is concerned at the availability of the third-party cloud service. Which of the following should the management team consult to determine the promised availability of the cloud provider?

A. Memorandum of understanding
B. Business continuity plan
C. Disaster recovery plan
D. Service-level agreement

Answer: D

Explanation:
A Service-level agreement (SLA) is a document that outlines the responsibilities of a cloud service provider and the customer. It typically includes the agreed-upon availability of the cloud service provider, the expected uptime for the service, and the cost of any downtime or other service interruptions. Consulting the SLA is the best way for the management team to determine the promised availability of the cloud provider. Reference: CompTIA Cloud+ Study Guide, 6th Edition, page 28.

NEW QUESTION 19
- (Topic 3)
A network administrator is adding a new switch to the network. Which of the following network hardening techniques would be BEST to use once the switch is in production?

A. Disable unneeded ports
B. Disable SSH service
C. Disable MAC filtering
D. Disable port security

Answer: A

NEW QUESTION 21
- (Topic 3)
A network technician wants to deploy a new wireless access point to reduce user latency. Currently, the organization has the following deployed:
Which of the following channels should the new device broadcast on?

A. Channel 3
B. Channel 9
C. Channel 10
D. Channel 11

Answer: D

Explanation:
The best channel for a new wireless access point is one that does not overlap with the existing channels used by other devices. Overlapping channels can cause interference and degrade the performance of the wireless network. According to the web search results, the 2.4 GHz band has 11 channels in the U.S., but only channels 1, 6, and 11 are non- overlapping. Since the existing devices are using channels 1 and 6, the new device should use channel 11 to avoid adjacent-channel interference12
References1: Why Channels 1, 6 and 11? | MetaGeek 2: How to Choose the Best Wi-Fi Channels for Your Network - Lifewire

NEW QUESTION 25
- (Topic 3)
A customer is hosting an internal database server. None of the users are able to connect to the server, even though it appears to be working properly. Which of the following is the best way to verify traffic to and from the server?

A. Protocol analyzer
B. nmap
C. ipconfig
D. Speed test

Answer: A

Explanation:
A protocol analyzer is the best way to verify traffic to and from the server. A protocol analyzer, also known as a packet sniffer or network analyzer, is a tool that captures and analyzes the network packets that are sent and received by a device. A protocol analyzer can show the source and destination IP addresses, ports, protocols, and payload of each packet, as well as any errors or anomalies in the network communication. A protocol analyzer can help troubleshoot network connectivity issues by identifying the root cause of the problem, such as misconfigured firewall rules, incorrect routing, or faulty network devices12.
To use a protocol analyzer to verify traffic to and from the server, the customer can follow these steps:
? Install a protocol analyzer tool on a device that is connected to the same network
as the server, such as Wireshark3 or Microsoft Network Monitor4.
? Select the network interface that is used to communicate with the server, and start capturing the network traffic.
? Filter the captured traffic by using the IP address or hostname of the server, or by using a specific port or protocol that is used by the database service.
? Analyze the filtered traffic and look for any signs of successful or failed connection attempts, such as TCP SYN, ACK, or RST packets, or ICMP messages.
? If there are no connection attempts to or from the server, then there may be a problem with the network configuration or device settings that prevent the traffic from reaching the server.
? If there are connection attempts but they are rejected or dropped by the server, then there may be a problem with the server configuration or service settings that prevent the traffic from being accepted by the server.
The other options are not the best ways to verify traffic to and from the server. nmap is a tool that can scan a network and discover hosts and services, but it cannot capture and analyze the network packets in detail. ipconfig is a command that can display and configure the IP settings of a device, but it cannot monitor or test the network communication with another device. Speed test is a tool that can measure the bandwidth and latency of a network connection, but it cannot diagnose or troubleshoot specific network problems.

NEW QUESTION 27
- (Topic 3)
In which of the following components do routing protocols belong in a software-defined network?

A. Infrastructure layer
B. Control layer
C. Application layer
D. Management plane

Answer: B

Explanation:
A software-defined network (SDN) is a network architecture that decouples the control plane from the data plane and centralizes the network intelligence in a software controller. The control plane is the part of the network that makes decisions about how to route traffic, while the data plane is the part of the network that forwards traffic based on the control plane's instructions. The control layer is the layer in an SDN that contains the controller and the routing protocols that communicate with the network devices. The control layer is responsible for managing and configuring the network devices and providing them with the necessary information to forward traffic. References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 378)

NEW QUESTION 30
- (Topic 3)
A network engineer designed and implemented a new office space with the following characteristics:

Building construction type:	Brick
Layout:	10,764sq ft (1,000sq m) commercial office space
Users:	50
Servers:	2
Laptops:	50

One month after the office space was implemented, users began reporting dropped signals when entering another room and overall poor connections to the 5GHz network. 'which of the following should the engineer do to best resolve the issue?

A. use non-overlapping channels
B. Reconfigure the network to support 2.4GHz_
C. Upgrade to WPA3.
D. Change to directional antennas-

Answer: D

Explanation:
The best solution to resolve the issue of dropped signals and poor connections to the 5GHz network is to change to directional antennas. Directional antennas are antennas that focus the wireless signal in a specific direction, increasing the range and strength of the signal. Directional antennas are suitable for environments where there are obstacles or interference that can weaken or block the wireless signal. In the image, the office space has several walls and doors that can reduce the signal quality of the 5GHz network, which has a shorter wavelength and higher frequency than the 2.4GHz network. By using directional antennas, the network engineer can aim the wireless signal towards the desired areas and avoid the signal loss caused by the walls and doors. References: CompTIA Network+ N10-008 Certification Study Guide, page 76; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-19.

NEW QUESTION 35
- (Topic 3)
Which of the following topologies is designed to fully support applications hosted in on- premises data centers, public or private clouds, and SaaS services?

A. SDWAN
B. MAN
C. PAN
D. MPLS

Answer: A

NEW QUESTION 40
- (Topic 3)
A network administrator is configuring a new switch and wants to connect two ports to the core switch to ensure redundancy. Which of the following configurations would meet this
requirement?

A. Full duplex
B. 802.1Q tagging
C. Native VLAN
D. Link aggregation

Answer: D

Explanation:
Link aggregation is a technique that allows multiple physical ports to be combined into a single logical channel, which provides increased bandwidth, load balancing, and redundancy. Link aggregation can be configured using protocols such as Link Aggregation Control Protocol (LACP) or static methods.
References
? Link aggregation is one of the common Ethernet switching features covered in Objective 2.3 of the CompTIA Network+ N10-008 certification exam1.
? Link aggregation can be used to connect two ports to the core switch to ensure redundancy23.
? Link aggregation can be configured using LACP or static methods23.
1: CompTIA Network+ Certification Exam Objectives, page 5 2: Interface Configurations – N10-008 CompTIA Network+ : 2.3 3: CompTIA Network+ N10-008 Cert Guide, Chapter 11, page 323

NEW QUESTION 41
- (Topic 3)
A network administrator is preparing new switches that will be deployed to support a network extension project. The lead network engineer has already provided documentation to ensure the switches are set up properly Which of the following did the engineer most likely provide?

A. Physical network diagram
B. Site survey reports
C. Baseline configurations
D. Logical network diagram

Answer: C

Explanation:
Baseline configurations are the standard settings and parameters that are applied to network devices, such as switches, routers, firewalls, etc., to ensure consistent performance, security, and functionality across the network. Baseline configurations can include aspects such as IP addresses, VLANs, passwords, protocols, access lists, firmware versions, etc. Baseline configurations are usually documented and updated regularly to reflect any changes or modifications made to the network devices.
The lead network engineer most likely provided baseline configurations to the network administrator to ensure that the new switches are set up properly and in accordance with the network design and policies. Baseline configurations can help to simplify the deployment process, reduce errors and inconsistencies, and facilitate troubleshooting and maintenance.
The other options are not correct because they are not the most likely documentation that the lead network engineer provided to the network administrator. They are:
? Physical network diagram. A physical network diagram is a graphical representation of the physical layout and connections of the network devices and components, such as cables, ports, switches, routers, servers, etc. A physical network diagram can help to visualize the network topology, identify the locations and distances of the devices, and plan for cabling and power requirements. However, a physical network diagram does not provide the specific settings and parameters that need to be configured on the network devices, such as the switches.
? Site survey reports. A site survey report is a document that summarizes the findings and recommendations of a site survey, which is a process of assessing the suitability and readiness of a location for installing and operating network devices and components. A site survey report can include aspects such as environmental conditions, power and cooling availability, security and safety measures, interference and noise sources, signal coverage and quality, etc. A site survey report can help to identify and resolve any potential issues or challenges that may affect the network performance and reliability. However, a site survey report does not provide the specific settings and parameters that need to be configured on the network devices, such as the switches.
? Logical network diagram. A logical network diagram is a graphical representation of the logical structure and functionality of the network devices and components, such as subnets, IP addresses, VLANs, protocols, routing, firewall rules, etc. A logical network diagram can help to understand the network design, architecture, and policies, as well as the data flow and communication paths between the devices. However, a logical network diagram does not provide the specific settings and parameters that need to be configured on the network devices, such as the switches.
References1: Network+ (Plus) Certification | CompTIA IT Certifications2: What is a Baseline Configuration? - Definition from Techopedia3: What is a Physical

Network Diagram? - Definition from Techopedia4: What is a Site Survey? - Definition from Techopedia5: [What is a Logical Network Diagram? - Definition from Techopedia]

NEW QUESTION 46
- (Topic 3)
While setting up a new workstation, a technician discovers that the network connection is only 100 full duplex (FD), although it is connected to a gigabit switch. While reviewing the interface information in the switch CLI, the technician notes the port is operating at IOOFD but Shows many RX and TX errors. The technician moves the computer to another switchport and experiences the same issues.
Which of the following is MOST likely the cause of the low data rate and port errors?

A. Bad switch ports
B. Duplex issues
C. Cable length
D. Incorrect pinout

Answer: B

NEW QUESTION 48
- (Topic 3)
Which of the following architectures is used for FTP?

A. Client-server
B. Service-oriented
C. Connection-oriented
D. Data-centric

Answer: A

Explanation:
FTP (File Transfer Protocol) is a client-server based protocol, meaning that the two computers involved communicate with each other in a request-response pattern. The client sends a request to the server and the server responds with the requested data. This type of architecture is known as client-server, and it is used for many different types of applications, including FTP. Other architectures, such as service-oriented, connection- oriented, and data-centric, are not used for FTP.

NEW QUESTION 50
- (Topic 3)
A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks does the technician need to install?

A. 110
B. 66
C. Bix
D. Krone

Answer: A

Explanation:
A 110 block is a type of punch-down block that is used to distribute Ethernet to multiple computers in an office. A punch-down block is a device that connects one group of wires to another group of wires by using a special tool that pushes the wires into slots on the block. A 110 block is a non-proprietary standard that supports up to Category 6 cabling and can be used for voice or data applications. References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 64)

NEW QUESTION 55
- (Topic 3)
A technician is deploying a new SSID for an industrial control system. The control devices require the network to use encryption that employs TKIP and a symmetrical password to connect. Which of the following should the technician configure to ensure compatibility with the control devices?

A. WPA2-Enterprise
B. WPA-Enterprise
C. WPA-PSK
D. WPA2-PSK

Answer: C

Explanation:
"WPA uses Temporal Key Integrity Protocol (TKIP) for enhanced encryption. TKIP uses RC4 for the encryption algorithm, and the CompTIA Network+ exam may reference TKIP-RC4 in a discussion of wireless."
" WPA2 uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) for integrity checking and Advanced Encryption Standard (AES) for encryption. On the Network+ exam, you might find this referenced as simply CCMP-AES"

NEW QUESTION 58
- (Topic 3)
A security engineer is trying to determine whether an internal server was accessed by hosts on the internet. The internal server was shut down during the investigation Which of the following will the engineer review to determine whether the internal server had an unauthorized access attempt?

A. The server's syslog
B. The NetFlow statistics
C. The firewall logs
D. The audit logs on the core switch

Answer: A

NEW QUESTION 62
- (Topic 3)
Which of the following ports is a secure protocol?

A. 20
B. 23
C. 443
D. 445

Answer: C

Explanation:
This is the port number for HTTPS, which stands for Hypertext Transfer Protocol Secure. HTTPS is a secure version of HTTP, which is the protocol used to communicate between web browsers and web servers. HTTPS encrypts the data sent and received using SSL/TLS, which are cryptographic protocols that provide authentication, confidentiality, and integrity. HTTPS is commonly used for online transactions, such as banking and shopping, where security and privacy are important

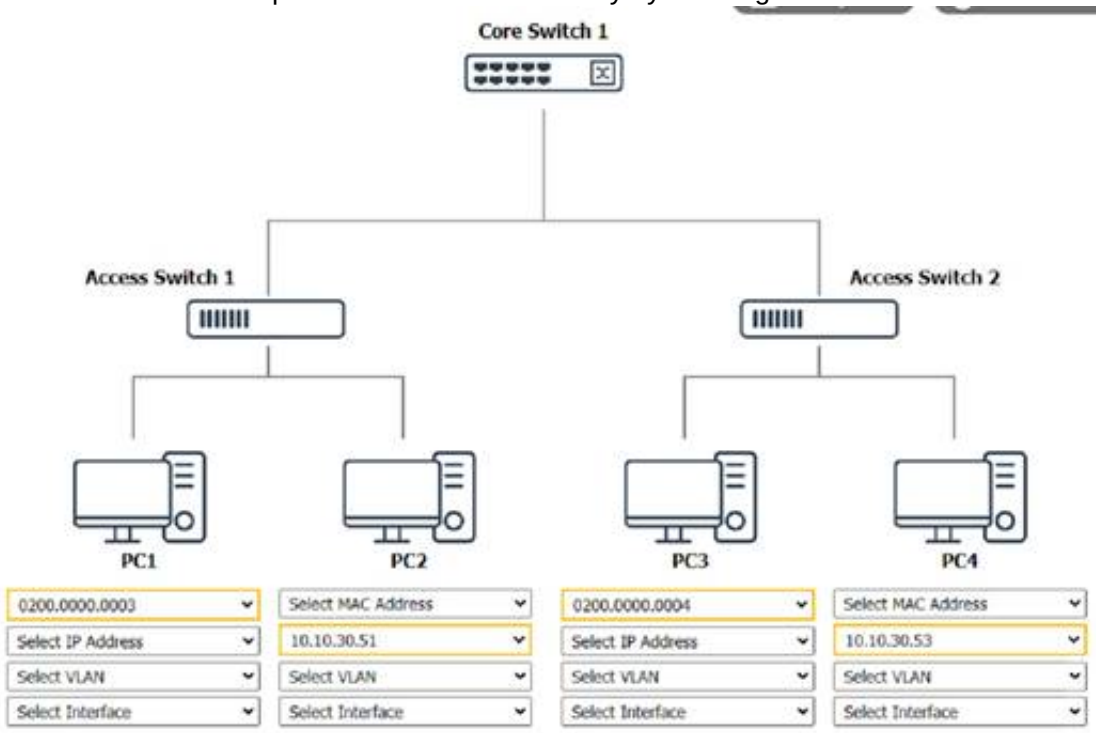
NEW QUESTION 64
- (Topic 3)
Users are reporting intermittent Wi-Fi connectivity in specific parts of a building. Which of the following should the network administrator check FIRST when troubleshooting this issue? (Select TWO).

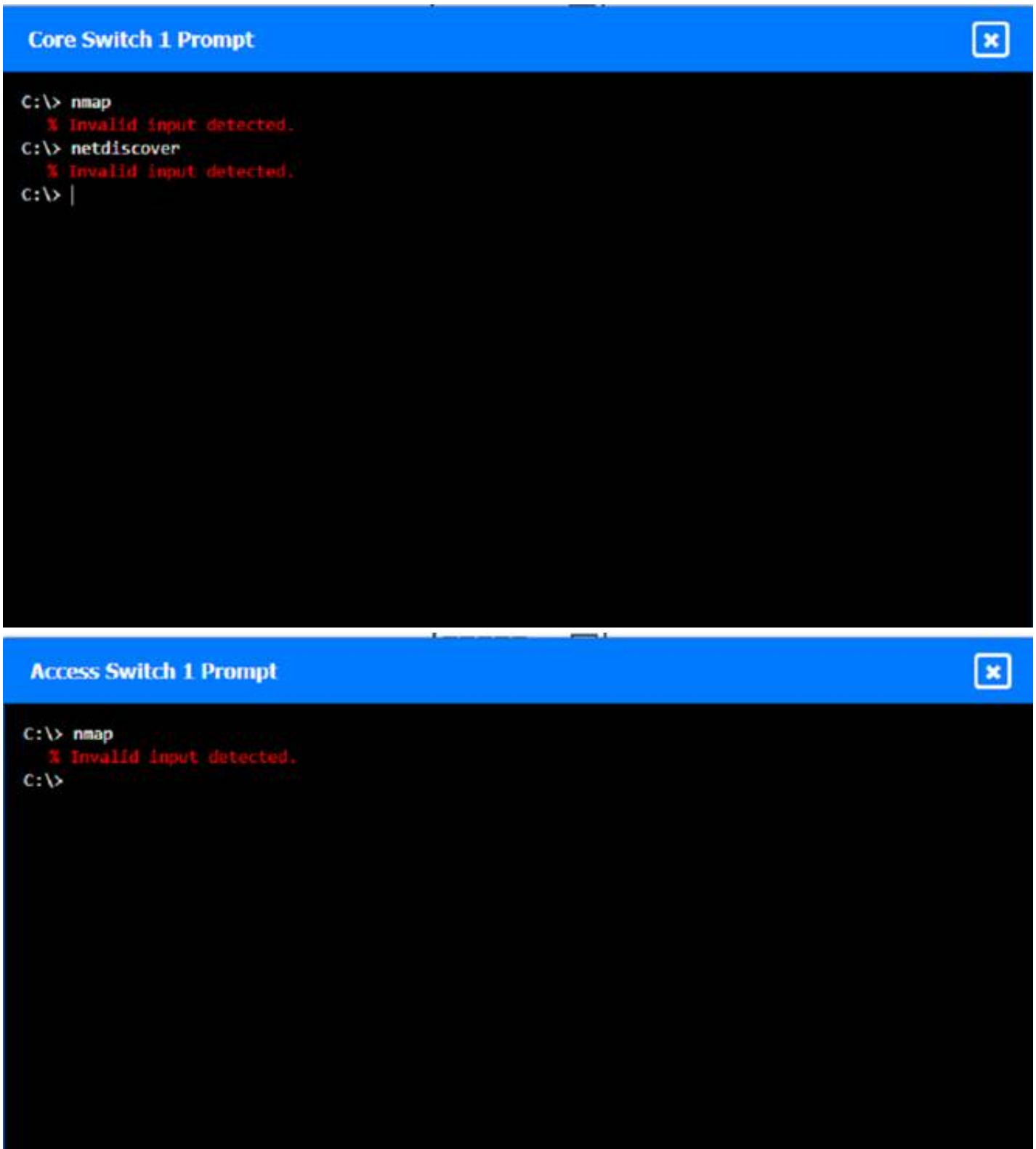
A. Site survey
B. EIRP
C. AP placement
D. Captive portal
E. SSID assignment
F. AP association time

Answer: AC

Explanation:
This is a coverage issue. WAP placement and power need to be checked. Site survey should be done NEXT because it takes a while.

NEW QUESTION 68
SIMULATION - (Topic 3)
A network technician was recently onboarded to a company. A manager has
tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.
Instructions:
Click on each switch to perform a network discovery by entering commands into the terminal. Fill in the missing information using drop-down menus provided.





A. Mastered
B. Not Mastered

Answer: A

Explanation:
(Note: Ips will be change on each simulation task, so we have given example answer for the understanding)
To perform a network discovery by entering commands into the terminal, you can use the following steps:
? Click on each switch to open its terminal window.
? Enter the command show ip interface brief to display the IP addresses and statuses of the switch interfaces.
? Enter the command show vlan brief to display the VLAN configurations and assignments of the switch interfaces.
? Enter the command show cdp neighbors to display the information about the neighboring devices that are connected to the switch.
? Fill in the missing information in the diagram using the drop-down menus provided. Here is an example of how to fill in the missing information for Core Switch 1:
? The IP address of Core Switch 1 is 192.168.1.1.
? The VLAN configuration of Core Switch 1 is VLAN 1: 192.168.1.0/24, VLAN 2: 192.168.2.0/24, VLAN 3: 192.168.3.0/24.
? The neighboring devices of Core Switch 1 are Access Switch 1 and Access Switch 2.
? The interfaces that connect Core Switch 1 to Access Switch 1 are GigabitEthernet0/1 and GigabitEthernet0/2.
? The interfaces that connect Core Switch 1 to Access Switch 2 are GigabitEthernet0/3 and GigabitEthernet0/4.
You can use the same steps to fill in the missing information for Access Switch 1 and Access Switch 2.

NEW QUESTION 73
- (Topic 3)
A help desk technician is concerned that a client's network cable issues may be causing intermittent connectivity. Which of the following would help the technician determine if this is the issue?

A. Run the show interface command on the switch
B. Run the tracerouute command on the server
C. Run iperf on the technician's desktop
D. Ping the client's computer from the router
E. Run a port scanner on the client's IP address

Answer: A

Explanation:
To determine if a client's network cable issues may be causing intermittent connectivity, the help desk technician can run the show interface command on the switch.
This command allows the technician to view the status and statistics of the various interfaces on the switch, including the physical link status and the number of transmitted and received packets. If the interface is experiencing a large number of errors or dropped packets, this could indicate a problem with the network cable or with the connection between the client's device and the switch.
"Cisco routers and switches have a show interfaces IOS command that provides interface statistics/status information, including link state (up/down), speed/duplex, send/receive traffic, cyclic redundancy checks (CRCs), and protocol packet and byte counts."

NEW QUESTION 77
- (Topic 3)
Which of the following documents dictates the uptimes that were agreed upon by the involved parties?

A. MOU
B. BYOD
C. SLA
D. NDA

Answer: C

Explanation:
An SLA (Service Level Agreement) is a document that defines the expected level of service and performance guaranteed by a service provider to a customer. It usually specifies metrics such as uptime, availability, reliability, response time, and compensation or penalties for not meeting the agreed standards. An SLA is a way of ensuring that both parties are clear about their roles and responsibilities, and that the customer receives the quality of service they paid for.

NEW QUESTION 82
- (Topic 3)
A company is designing a SAN and would like to use STP as its medium for communication. Which of the following protocols would BEST suit me company's needs?

A. SFTP
B. Fibre Channel
C. iSCSI
D. FTP

Answer: B

Explanation:
A SAN also employs a series of protocols enabling software to communicate or prepare data for storage. The most common protocol is the Fibre Channel Protocol (FCP), which maps SCSI commands over FC technology. The iSCSI SANs will employ an iSCSI protocol that maps SCSI commands over TCP/IP.
STP (Spanning Tree Protocol) is a protocol used to prevent loops in Ethernet networks, and it is not a medium for communication in a storage area network (SAN). However, Fibre Channel is a protocol that is specifically designed for high-speed data transfer in SAN environments. It is a dedicated channel technology that provides high throughput and low latency, making it ideal for SANs. Therefore, Fibre Channel would be the best protocol for the company to use for its SAN. SFTP (Secure File Transfer Protocol), iSCSI (Internet Small Computer System Interface), and FTP (File Transfer Protocol) are protocols used for transferring files over a network and are not suitable for use in a SAN environment.

NEW QUESTION 87
- (Topic 3)
A network technician is having issues connecting an IoT sensor to the internet The WLAN settings were enabled via a custom command line, and a proper IP address assignment was received on the wireless interlace. However, when trying to connect to the internet, only HTTP redirections are being received when data Is requested. Which of the following will point to the root cause of the Issue?

A. Verifying if an encryption protocol mismatch exists.
B. Verifying If a captive portal is active for the WLAN.
C. Verifying the minimum RSSI for operation in the device's documentation
D. Verifying EIRP power settings on the access point.

Answer: C

Explanation:
A captive portal is a web page that is displayed to a user before they can access the internet or other network resources. This is often used in public or guest networks to present users with a login or terms and conditions page before they can access the internet. If a captive portal is active on the WLAN, it would explain why the IoT sensor is only receiving HTTP redirections when trying to connect to the internet.

NEW QUESTION 88
- (Topic 3)
A network administrator wants to test the throughput of a new metro Ethernet circuit to verify that its performance matches the requirements specified m the SLA. Which of the following would BEST help measure the throughput?

A. iPerf
B. Ping
C. NetFlow
D. Netstat

Answer: A

NEW QUESTION 91
- (Topic 3)
Which of the following layers of the OSI model has new protocols activated when a user moves from a wireless to a wired connection?

A. Data link
B. Network
C. Transport
D. Session

Answer: A

Explanation:
"The Data Link layer also determines how data is placed on the wire by using an access method. The wired access method, carrier-sense multiple access with collision detection (CSMA/CD), was once used by all wired Ethernet networks, but is automatically disabled on switched full-duplex links, which have been the norm for decades. Carrier- sense multiple access with collision avoidance (CSMA/CA) is used by wireless networks, in a similar fashion."

NEW QUESTION 94
- (Topic 3)
A network team is getting reports that air conditioning is out in an IDF. The team would like to determine whether additional network issues are occurring. Which of the following should the network team do?

A. Confirm that memory usage on the network devices in the IDF is normal.
B. Access network baseline data for references to an air conditioning issue.
C. Verify severity levels on the corporate syslog server.
D. Check for SNMP traps from a network device in the IDF.
E. Review interface statistics looking for cyclic redundancy errors.

Answer: D

Explanation:
"Baselines play an integral part in network documentation because they let you monitor the network's overall performance. In simple terms, a baseline is a measure of performance that indicates how hard the network is working and where network resources are spent. The purpose of a baseline is to provide a basis of comparison. For example, you can compare the network's performance results taken in March to results taken in June, or from one year to the next. More commonly, you would compare the baseline information at a time when the network is having a problem to information recorded when the network was operating with greater efficiency. Such comparisons help you determine whether there has been a problem with the network, how significant that problem is, and even where the problem lies."

NEW QUESTION 99
- (Topic 3)
All packets arriving at an interface need to be fully analyzed. Which of me following features should be used to enable monitoring of the packets?

A. LACP
B. Flow control
C. Port mirroring
D. NetFlow exporter

Answer: D

Explanation:
Port mirroring is a feature that can be used to enable monitoring of all packets arriving at an interface. This feature is used to direct a copy of all traffic passing through the switch to a monitoring device, such as a network analyzer. This allows the switch to be monitored with the network analyzer in order to identify any malicious or suspicious activity. Additionally, port mirroring can be used to troubleshoot network issues, such as latency or poor performance.

NEW QUESTION 101

- (Topic 3)
Which of the following disaster recovery metrics describes the average length of time a piece of equipment can be expected to operate normally?

A. RPO
B. RTO
C. MTTR
D. MTBF

Answer: D

Explanation:
MTBF is the disaster recovery metric that describes the average length of time a piece of equipment can be expected to operate normally. MTBF stands for mean time between failures, which is a measure of the reliability and availability of a device or system. MTBF is calculated by dividing the total operating time by the number of failures that occurred during that time. MTBF indicates how often a device or system fails and how long it can run without interruption. A higher MTBF means a lower failure rate and a longer operational life span. References: [CompTIA Network+ Certification Exam Objectives], What Is Mean Time Between Failures (MTBF)? | Definition & Examples | Forcepoint

NEW QUESTION 105
- (Topic 3)
A network administrator is troubleshooting a connectivity performance issue. As part of the troubleshooting process, the administrator performs a traceout from the client to the server, and also from the server to the client. While comparing the outputs, the administrator notes they show different hops between the hosts. Which of the following BEST explains these findings?

A. Asymmetric routing
B. A routing loop
C. A switch loop
D. An incorrect gateway

Answer: C

NEW QUESTION 109
- (Topic 3)
Which of the following would be used to enforce and schedule critical updates with supervisory approval and include backup plans in case of failure?

A. Business continuity plan
B. Onboarding and offboarding policies
C. Acceptable use policy
D. System life cycle
E. Change management

Answer: A

NEW QUESTION 111
- (Topic 3)
To comply with an industry regulation, all communication destined to a secure server should be logged and archived on a storage device. Which of the Mowing can be configured to fulfill this requirement?

A. QoS traffic classification
B. Port mirroring
C. Flow control
D. Link Aggregation Control Protocol

Answer: B

NEW QUESTION 115
- (Topic 3)
An organization has a security staff shortage and must prioritize efforts in areas where the staff will have the most impact. In particular, the focus is to avoid expending resources on identifying non-relevant events. A security analyst is reviewing web server logs and sees the following:

```
202.180.155.1 - [14/Jan/2021:04:12:28 -0200] "GET /img/us.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:28 -0200] "GET /img/org.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:29 -0200] "GET /img/org2.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:29 -0200] "GET /img/org3.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:30 -0200] "GET /img/org4.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:31 -0200] "GET /img/directors.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:31 -0200] "GET /img/directors2.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:32 -0200] "GET /img/directors3.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:33 -0200] "GET /img/directors4.gif" 404 295
```

Which of the following should the analyst recommend?

A. Configuring the web server log to filter out 404 errors on image files
B. Updating firewall rules to block 202.180.155.1
C. Resyncing the network time server and monitoring logs for future anomalous behavior
D. Checking with the penetration testing team to see if the team ran any scans on January 14, 2021

Answer: A

Explanation:
This answer will help the organization to avoid expending resources on identifying non- relevant events, as the 404 errors on image files are not indicative of any

security threat or issue, but rather a misconfiguration or a broken link on the web server. The 404 errors on image files are also very frequent and repetitive, as shown by the web server log, which can clutter the log and make it harder to spot any relevant events. By filtering out these errors, the analyst can focus on more important events and reduce the noise in the log. The other answers are not as good as A, because they either do not address the problem of identifying non-relevant events, or they are based on incorrect assumptions or information. For example:
? B. Updating firewall rules to block 202.180.155.1 is not a good answer, because the IP address 202.180.155.1 is not doing anything malicious or suspicious, but rather requesting image files that do not exist on the web server. Blocking this IP address will not improve the security of the web server, but rather create unnecessary firewall rules and possibly deny legitimate access to the web server.
? C. Resyncing the network time server and monitoring logs for future anomalous behavior is not a good answer, because there is no evidence that the network time server is out of sync or causing any problems. The web server log shows that the entries are all within a few minutes of each other, which is normal and expected. Resyncing the network time server will not help the analyst to identify non-relevant events, but rather waste time and resources on an unrelated task.
? D. Checking with the penetration testing team to see if the team ran any scans on January 14, 2021 is not a good answer, because the web server log does not show any signs of a penetration test or a scan. The log shows only 404 errors on image files, which are not typical of a penetration test or a scan, which would usually target different types of files, ports, or vulnerabilities. Checking with the penetration testing team will not help the analyst to identify non-relevant events, but rather distract the analyst from the actual events and possibly create false alarms.
https://www.professormesser.com/network-plus/n10-008/n10-008-video/general-network-troubleshooting-n10-008/

NEW QUESTION 119
- (Topic 3)
Which of the following cloud deployment models involves servers that are hosted at a company's property and are only used by that company?

A. Public
B. Private
C. Hybrid
D. Community

Answer: B

Explanation:
A private cloud deployment model involves servers that are hosted at a company’s property and are only used by that company. A private cloud provides exclusive access and control over the cloud resources to the company, as well as higher security and privacy. However, a private cloud also requires more investment and maintenance from the company, compared to other cloud deployment models1

NEW QUESTION 120
- (Topic 3)
An infrastructure company is implementing a cabling solution to connect sites on multiple continents. Which of the following cable types should the company use for this project?

A. Cat 7
B. Single-mode
C. Multimode
D. Cat 6

Answer: B

Explanation:
Single-mode fiber is a type of optical fiber that has a small core diameter and allows only one mode of light to propagate. This reduces signal attenuation and increases transmission distance, making it suitable for long-distance communication networks.
Single-mode fiber can carry data over thousands of kilometers without requiring repeaters or amplifiers. Single-mode fiber is also immune to electromagnetic interference and has a higher bandwidth than multimode fiber. Therefore, single-mode fiber is the best cable type for connecting sites on multiple continents.
References: [CompTIA Network+ Certification Exam Objectives], [Single-mode optical fiber - Wikipedia]
Single-mode fiber optic cable uses a single ray of light to transmit data. This allows it to achieve very low attenuation and high bandwidth.
Multimode fiber optic cable uses multiple rays of light to transmit data. This results in higher attenuation and lower bandwidth than single-mode cable.
Twisted pair copper cable uses two insulated copper wires to transmit data. It is less expensive than fiber optic cable, but it has higher attenuation and lower bandwidth. When choosing a cable type for a long-distance application, it is important to consider the following factors:
? Attenuation: The amount of signal loss that occurs over the length of the cable.
? Bandwidth: The amount of data that can be transmitted over the cable per second.
? Cost: The cost of the cable and installation.
Single-mode fiber optic cable is the best choice for long-distance applications because it
has the lowest attenuation and highest bandwidth of any cable type. However, it is also the most expensive cable type.

NEW QUESTION 122
- (Topic 3)
An engineer needs to verity the external record tor SMTP traffic. The engineer logged in to the server and entered the nslookup command. Which of the following commands should the engineer send before entering the DNS name?

A. set type=A
B. is -d company-mail.com
C. set domain=company.mail.com
D. set querytype=Mx

Answer: D

NEW QUESTION 126
- (Topic 3)
A network administrator received a report staling a critical vulnerability was detected on an application that is exposed to the internet. Which of the following Is the appropriate NEXT step?

A. Check for the existence of a known exploit in order to assess the risk
B. Immediately shut down the vulnerable application server.

C. Install a network access control agent on the server.
D. Deploy a new server to host the application.

Answer: A

Explanation:
The appropriate next step in this situation would be to check for the existence of a known exploit in order to assess the risk. This is important because it will help the network administrator determine the severity of the vulnerability and the potential impact it could have on the organization. Once the network administrator has assessed the risk, they can then take appropriate action to address the vulnerability. This might include patching the application, deploying a new server to host the application, or implementing other security measures to mitigate the risk. It is generally not advisable to immediately shut down the vulnerable application server, as this could disrupt business operations and cause significant downtime. Similarly, installing a network access control agent on the server may not be the most effective solution, as it would not address the underlying vulnerability.

NEW QUESTION 129
- (Topic 3)
Which of the following is a valid alternative to maintain a deployed proxy technology while saving physical space in the data center by moving the network service to the virtualization infrastructure?

A. NFV
B. SDWAN
C. Networking as code
D. VIP

Answer: A

Explanation:
The valid alternative to maintain a deployed proxy technology while saving physical space in the data center by moving the network service to the virtualization infrastructure is NFV (Network Function Virtualization). NFV is a technique that allows network functions, such as proxies, firewalls, routers, or load balancers, to be implemented as software applications running on virtual machines or containers. NFV reduces the need for dedicated hardware devices and improves scalability and flexibility of network
services. References: CompTIA Network+ N10-008 Certification Study Guide, page 440; The Official CompTIA Network+ Student Guide (Exam N10-008), page 16-11.
NFV can be used to virtualize a wide variety of network functions, including proxy servers. By virtualizing proxy servers, organizations can save physical space in the data center and
improve the scalability and efficiency of their networks.
To virtualize a proxy server using NFV, an organization would need to deploy a virtualization platform, such as VMware ESXi or Microsoft Hyper-V. The organization would then need to install a virtual proxy server appliance on the virtualization platform.
Once the virtual proxy server appliance is installed, it can be configured and used just like a physical proxy server.
NFV is a relatively new technology, but it is quickly gaining popularity as organizations look for ways to improve the efficiency and scalability of their networks.

NEW QUESTION 130
- (Topic 3)
A device is connected to a managed Layer 3 network switch. The MAC address of the device is known, but the static IP address assigned to the device is not. Which of the following features of a Layer 3 network switch should be used to determine the IPv4 address of the device?

A. MAC table
B. Neighbor Discovery Protocol
C. ARP table
D. IPConfig
E. ACL table

Answer: C

Explanation:
The ARP table is a database that is used by a device to map MAC addresses to their corresponding IP addresses. When a device sends a packet to another device on the same network, it uses the MAC address of the destination device to deliver the packet. The ARP table allows the device to determine the IP address of the destination device based on its MAC address.

NEW QUESTION 134
- (Topic 3)
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?

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.
References:
? Physical Security – N10-008 CompTIA Network+ : 4.51

NEW QUESTION 136
- (Topic 3)

Following the implementation of a BYOO policy. some users in a high-density environment report slowness over the wireless connection. Some wireless controller reports indicate high latency and airtime contention. Which of the following is the most probable root cause?

A. The AP is configured with 2.4GHz frequency, which the new personal devices do not support.
B. The AP is configured with 2.4GHz frequency without band-steering capabilities.
C. The AP is configured with 5Ghz frequency with band-steering capabiäties.
D. The AP is configured with 5Ghz frequenc
E. which the new personal devices do not support

Answer: B

Explanation:
Band-steering is a feature that allows an AP to steer dual-band capable clients to the less congested 5GHz frequency, leaving the 2.4GHz frequency for legacy clients. Without band- steering, the AP may have more clients competing for the same channel on the 2.4GHz frequency, resulting in high latency and airtime contention.
References:
? According to the CompTIA Network+ Certification Exam Objectives, one of the topics covered in the exam is “Given a scenario, use appropriate wireless technologies and configurations”. One of the subtopics is “Band steering” 1.
? According to the PoliFi: Airtime Policy Enforcement for WiFi paper, “Band steering allows the access point to disable the 2.4 GHz band from probing the client device, so it responds only to the 5 GHz band, reducing the congestion on the 2.4 GHz band while taking advantage of the faster 5GHz band to improve user’s network experience.” 2.
? According to the Aruba Air Slice Tech Brief, “Air Slice minimizes airtime contention and efficiently groups Wi-Fi 6 and non-Wi-Fi 6 client devices to guarantee bit rate, and provide bounded latency and jitter simultaneously.” 3.

NEW QUESTION 140
- (Topic 3)
A technician is configuring a static IP address on a new device in a newly created subnet. The work order specifies the following requirements:
• The IP address should use the highest address available in the subnet.
• The default gateway needs to be set to 172.28.85.94.
• The subnet mask needs to be 255.255.255.224.
Which of the following addresses should the engineer apply to the device?

A. 172.28.85.93
B. 172.28.85.95
C. 172.28.85.254
D. 172.28.85.255

Answer: A

Explanation:
https://www.tunnelsup.com/subnet-calculator/
IP Address: 172.28.85.95/27 Netmask: 255.255.255.224
Network Address: 172.28.85.64
Usable Host Range: 172.28.85.65 - 172.28.85.94
Broadcast Address: 172.28.85.95

NEW QUESTION 142
- (Topic 3)
A network administrator installed a new data and VoIP network. Users are now experiencing poor call quality when making calls. Which of the following should the administrator do to increase VoIP performance?

A. Configure a voice VLAN.
B. Configure LACP on all VoIP phones.
C. Configure PoE on the network.
D. Configure jumbo frames on the network.

Answer: A

Explanation:
"Benefits of Voice VLAN
It ensures that your VoIP (Voice over Internet Phone) devices do not have to contend directly with all the broadcasts and other traffic from the data VLAN. A voice VLAN can simplify network configuration in some circumstances."
https://community.fs.com/blog/auto-voip-vs-voice-vlan-what-s-the-difference.html Jumbo Frames
"When jumbo frames on a VoIP/UC network are enabled, it can cause the same kind of
delay to your network transmissions."
"VoIP uses will always not benefit from jumbo frame, as VoIP like gaming, is latency and time sensitive. Jumbo Frame for Internet Purpose: You will not see any performance boost as the files that came across the internet does not support jumbo frame."
https://www.ankmax.com/newsinfo/1358641.html#:~:text=VoIP%20uses%20will%20always
%20not,does%20not%20support%20jumbo%20frame.
"To summarize this general best practice guide, you should NOT enable jumbo frame feature as a general home user."

NEW QUESTION 143
- (Topic 3)
A technician is equipped with a tablet, a smartphone, and a laptop to troubleshoot a switch with the help of support over the phone. However, the technician is having issues interconnecting all these tools in troubleshooting the switch. Which Of the following should the technician use to gain connectivity?

A. PAN
B. WAN
C. LAN
D. MAN

Answer: A

Explanation:
A PAN stands for Personal Area Network and it is a type of network that connects devices within a small range, such as a few meters. A PAN can use wireless technologies such as Bluetooth or Wi-Fi to interconnect devices such as tablets, smartphones, and laptops. A technician can use a PAN to gain connectivity among these tools and troubleshoot the switch.
References: Network+ Study Guide Objective 1.2: Explain devices, applications, protocols and services at their appropriate OSI layers.

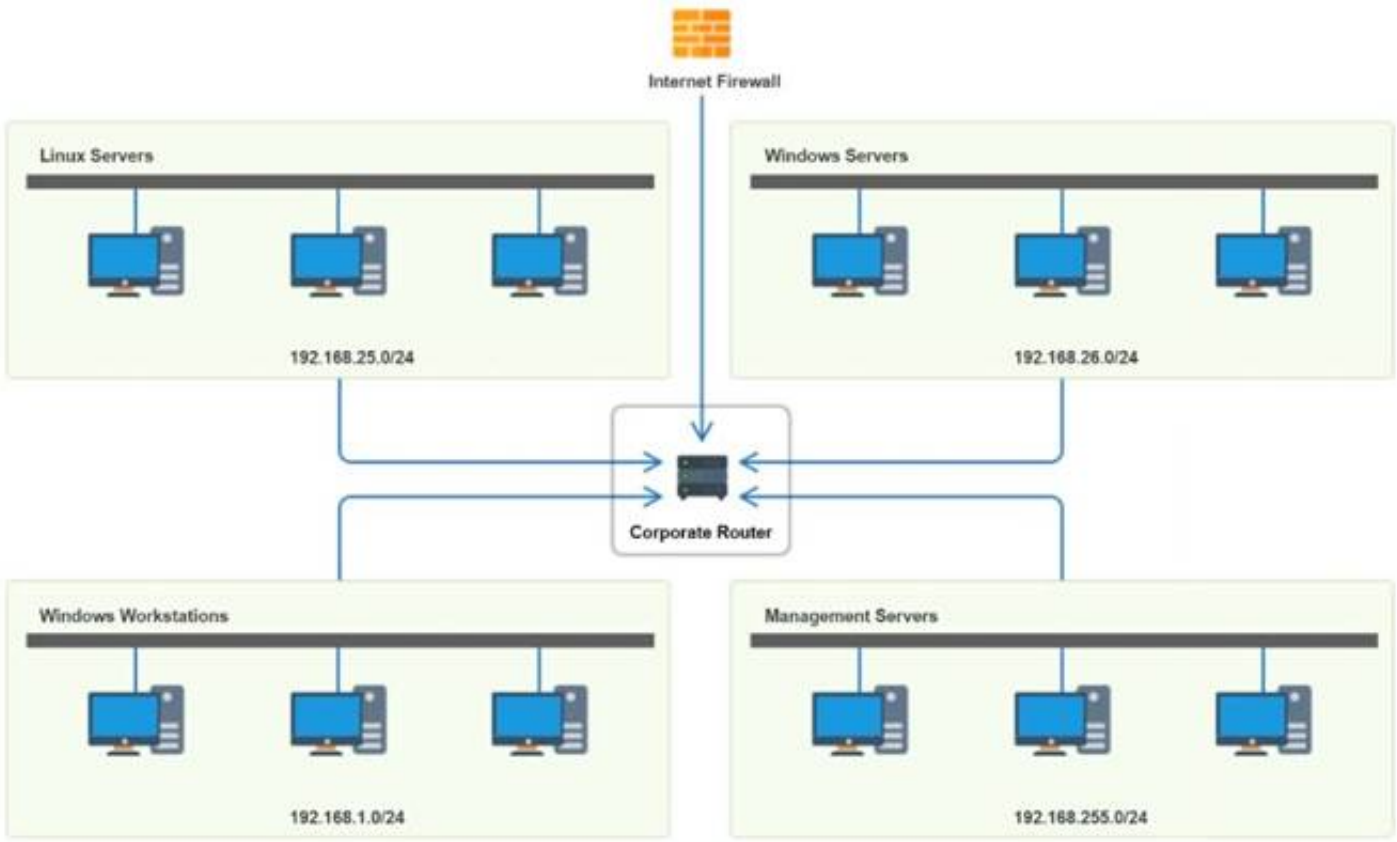
NEW QUESTION 146
- (Topic 3)
Which of the following describes when an active exploit is used to gain access to a network?

A. Penetration testing
B. Vulnerability testing
C. Risk assessment
D. Posture assessment
E. Baseline testing

Answer: A

Explanation:
Penetration testing is a type of security testing that is used to assess the security of a system or network by actively exploiting known vulnerabilities. It is used to simulate an attack on the system and identify any weaknesses that may be exploited by malicious actors. As stated in the CompTIA Security+ Study Guide, "penetration testing is a type of security assessment that attempts to gain unauthorized access to networks and systems by exploiting security vulnerabilities."

NEW QUESTION 150
SIMULATION - (Topic 3)
You have been tasked with implementing an ACL on the router that will:
* 1. Permit the most commonly used secure remote access technologies from the management network to all other local network segments
* 2. Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.
* 3. Prohibit any traffic that has not been specifically allowed.
INSTRUCTIONS
Use the drop-downs to complete the ACL
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Router Access Control List

Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	Any	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Router Access Control List

Rule	Source	Destination	Protocol	Service	Action
1	192.168.255.0	192.168.26.0	TCP	SSH	Allow
2	192.168.255.0	192.168.25.0	TCP	SSH	Allow
3	192.168.255.0	192.168.1.0	TCP	SSH	Allow
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0	Any	TCP	RDP	Deny
7	192.168.1.0	Any	TCP	VNC	Deny
8	192.168.1.0	Any	Any	Any	Allow
9	Any	Any	Any	Any	Deny

NEW QUESTION 154
- (Topic 3)
A desktop support department has observed slow wireless speeds for a new line of laptops using the organization's standard image. No other devices have experienced the same issue. Which of the following should the network administrator recommend troubleshooting FIRST to resolve this issue?

A. Increasing wireless signal power
B. Installing a new WAP
C. Changing the protocol associated to the SSID
D. Updating the device wireless drivers

Answer: D

Explanation:
Wireless drivers can affect the performance and compatibility of your wireless connection5. If only a new line of laptops using the organization’s standard image has experienced slow wireless speeds, it could be that their wireless drivers are outdated or incompatible with the network. Updating the device wireless drivers could resolve this issue.
Wireless drivers play an important role in the performance of a wireless connection, as they control how the device interacts with the wireless network. If the laptops in question are using an outdated version of the wireless driver, it could be causing the slow speeds. The network administrator should recommend updating the device wireless drivers first to see if this resolves the issue.

NEW QUESTION 156
- (Topic 3)
A network security engineer is responding to a security incident. The engineer suspects that an attacker used an authorized administrator account to make configuration changes to the boundary firewall. Which of the following should the network security engineer review?

A. Network traffic logs
B. Audit logs
C. Syslogs
D. Event logs

Answer: B

Explanation:
Audit logs are records of the actions performed by users or processes on a system or network device. They can provide information about who made what changes, when, and why. Audit logs are essential for detecting and investigating security incidents, as well as for ensuring compliance with policies and regulations. Audit logs can help the network security engineer to identify the source of the unauthorized configuration changes to the boundary firewall, as well as the scope and impact of the changes.
References1 - Changes to Cyber Essentials requirements – April 2021 update2 - 8 Firewall Best Practices for Securing the Network3 - How to secure your network boundaries with a firewall

NEW QUESTION 157
- (Topic 3)
A company with multiple routers would like to implement an HA network gateway with the least amount of downtime possible. This solution should not require changes on the gateway setting of the network clients. Which of the following should a technician configure?

A. Automate a continuous backup and restore process of the system's state of the active gateway.
B. Use a static assignment of the gateway IP address on the network clients.
C. Configure DHCP relay and allow clients to receive a new IP setting.
D. Configure a shared VIP and deploy VRRP on the routers.

Answer: D

Explanation:

The open standard protocol Virtual Router Redundancy Protocol (VRRP) is similar to HSRP, the differences mainly being in terminology and packet formats. In VRRP, the active router is known as the master, and all other routers in the group are known as backup routers. There is no specific standby router; instead, all backup routers monitor the status of the master, and in the event of a failure, a new master router is selected from the available backup routers based on priority

NEW QUESTION 158
- (Topic 3)
A network security administrator needs to monitor the contents of data sent between a secure network and the rest of the company. Which of the following monitoring methods will accomplish this task?

A. Port mirroring
B. Flow data
C. Syslog entries
D. SNMP traps

Answer: A

Explanation:
Port mirroring is a method of monitoring network traffic by copying the data packets from one port to another port on the same switch or router. This allows the network security administrator to analyze the contents of the data sent between different networks without affecting the performance or security of the original traffic. Port mirroring can be configured to capture all traffic or only specific types of traffic, such as VLANs, protocols, or IP addresses.
References:
? Port Mirroring - CompTIA Network+ N10-008 Domain 3.1 - YouTube1
? CompTIA Network+ Certification Exam Objectives, page 142

NEW QUESTION 159
- (Topic 3)
Which of the following most likely occurs when an attacker is between the target and a legitimate server?

A. IP spoofing
B. VLAN hopping
C. Rogue DHCP
D. On-path attack

Answer: D

Explanation:
An on-path attack (also known as a man-in-the-middle attack) is a type of security attack where the attacker places themselves between two devices (often a web browser and a web server) and intercepts or modifies communications between the two1. The attacker can then collect information as well as impersonate either of the two agents. For example, an on-path attacker could capture login credentials, redirect traffic to malicious sites, or inject malware into legitimate web pages.
The other options are not correct because they describe different types of attacks:
•IP spoofing is the practice of forging the source IP address of a packet to make it appear as if it came from a trusted or authorized source2.
•VLAN hopping is a technique that allows an attacker to access a VLAN that they are not authorized to access by sending packets with a modified VLAN tag3.
•Rogue DHCP is a scenario where an unauthorized DHCP server offers IP configuration parameters to clients on a network, potentially causing network disruption or redirection to malicious sites4.
References
2: Understanding Targeted Attacks: What is a Targeted Attack? 3: Types of attacks - Security on the web | MDN
1: What is an on-path attacker? | Cloudflare
4: [What is a Rogue DHCP Server? - Definition from Techopedia]

NEW QUESTION 163
- (Topic 3)
After router and device configurations are applied, internet access is not possible. Which of the following is the most likely cause?

A. The Ethernet interface was configured with an incorrect IP address.
B. The router was configured with an incorrect loopback address.
C. The router was configured with an incorrect default gateway.
D. The serial interface was configured with the incorrect subnet mas

Answer: C

Explanation:

The default gateway is the IP address of the router that connects a network to the internet or another network. The default gateway is usually configured on the devices that need to access the internet or other networks, such as PCs, servers, or routers. If the router was configured with an incorrect default gateway, it would not be able to forward packets to the correct destination, and internet access would not be possible.
The other options are not the most likely causes of the issue. The Ethernet interface is the physical port that connects a device to a network using a cable. If the Ethernet interface was configured with an incorrect IP address, it would cause a problem with the local network connectivity, not the internet access. The loopback address is a special IP address that refers to the device itself, usually used for testing or troubleshooting purposes. If the router was configured with an incorrect loopback address, it would not affect the internet access, as the loopback address is not used for routing packets to other networks. The serial interface is another type of physical port that connects a device to a network using a serial cable, often used for WAN connections. If the serial interface was configured with the incorrect subnet mask, it would cause a problem with the WAN connectivity, not the internet access, as the subnet mask is used to determine the network and host portions of an IP address.
ReferencesWhat is a Default Gateway? | HowStuffWorksWhat is an Ethernet Interface? - Definition from TechopediaWhat is a Loopback Address? - Definition from TechopediaWhat is a Serial Interface? - Definition from Techopedia

NEW QUESTION 167
- (Topic 3)
After a firewall replacement, some alarms and metrics related to network availability stopped updating on a monitoring system relying on SNMP. Which of the following should the network

administrator do first?

A. Modify the device's MIB on the monitoring system.
B. Configure syslog to send events to the monitoring system.
C. Use port mirroring to redirect traffic to the monitoring system.
D. Deploy SMB to transfer data to the monitoring syste

Answer: A

Explanation:

SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a monitoring system and provide information about their status, performance, and configuration. SNMP relies on MIBs (Management Information Bases), which are collections of objects that define the types of information that can be accessed or modified on a device1.
When a firewall replacement occurs, the new firewall may have a different MIB than the old one, which means that the monitoring system may not be able to recognize or interpret the data sent by the new firewall. This can cause some alarms and metrics related to network availability to stop updating on the monitoring system. To fix this, the network administrator should modify the device’s MIB on the monitoring system, so that it matches the MIB of the new firewall and can correctly process the SNMP data2.
The other options are not relevant to the issue. Configuring syslog to send events to the monitoring system would not affect the SNMP data, as syslog is a different protocol that sends log messages from network devices to a central server. Using port mirroring to redirect traffic to the monitoring system would not help, as port mirroring is a technique that copies traffic from one port to another for analysis or troubleshooting purposes, but does not change the format or content of the traffic. Deploying SMB to transfer data to the monitoring system would not work, as SMB is a protocol that allows file sharing and access between network devices, but does not support SNMP data.
ReferencesGrafana & Prometheus SNMP: advanced network monitoring guideConfiguring Windows Systems for Monitoring with SNMP - ScienceLogic

NEW QUESTION 171
- (Topic 3)
A network consultant is installing a new wireless network with the following specifications:
5GHz
1,300Mbps 20/40/80MHz
Which of the following standards should the network consultant use?

A. 802.11a
B. 802.11ac
C. 802.11b
D. 802.11n

Answer: B

NEW QUESTION 175
- (Topic 3)
A technician is configuring a wireless access point in a public space for guests to use. Which of the following should the technician configure so that only approved connections are
allowed?

A. Geofencing
B. Captive portal
C. Secure SNMP
D. Private VLANs

Answer: B

Explanation:

A captive portal is a web page that requires users to authenticate or accept terms of service before they can access the internet through a wireless access point. A captive portal can be used to control who can use the wireless network, limit the bandwidth or time of usage, or display advertisements or information. A captive portal is a common feature of public wireless networks, such as those in hotels, airports, cafes, or libraries. A captive portal can prevent unauthorized or malicious users from accessing the network or consuming network resources.
ReferencesPublic Wireless Access Points Definition | Law InsiderAre Public Wi-Fi Networks Safe? What You Need To Know

NEW QUESTION 177
- (Topic 3)
A network engineer has added a new route on a border router and is trying to determine if traffic is using the new route. Which of the following commands should the engineer use?

A. ping
B. arp
C. tracert
D. route

Answer: C

Explanation:

The tracert command is a network diagnostic tool that traces the route of packets from the source host to the destination host. It displays the IP addresses and hostnames of the routers along the path, as well as the time taken for each hop. The tracert command can be used to determine if traffic is using the new route by comparing the output before and after adding the route. If the new route is effective, the tracert command should show a different or shorter path to the destination host.
ReferencesNetworking Commands For Troubleshooting Windows - GeeksforGeeksNine Switch Commands Every Cisco Network Engineer Needs to Know

NEW QUESTION 180
- (Topic 3)
Which of the following ports should a network administrator enable for encrypted log-in to a network switch?

A. 22
B. 23
C. 80
D. 123

Answer: A

Explanation:
Port 22 is used by Secure Shell (SSH), which is a protocol that provides a secure and encrypted method for remote access to hosts by using public-key cryptography and challenge-response authentication. SSH can be used to log in to a network switch and configure it without exposing the credentials or commands to eavesdropping or tampering. Port 23 is used by Telnet, which is an insecure and plaintext protocol for remote access. Port 80 is used by HTTP, which is a protocol for web communication. Port 123 is used by NTP, which is a protocol for time synchronization

NEW QUESTION 184
- (Topic 3)
A medical building offers patients Wi-Fi in the waiting room. Which of the following security
features would be the BEST solution to provide secure connections and keep the medical data protected?

A. Isolating the guest network
B. Securing SNMP
C. MAC filtering
D. Disabling unneeded switchports

Answer: A

NEW QUESTION 187
- (Topic 3)
A customer runs a DNS lookup service and needs a network technician to reconfigure the network to improve performance. The customer wants to ensure that servers are accessed based on whichever one is topographically closest to the destination. If the server does not respond, then the next topographically closest server should respond Which of the following does the technician need to configure to meet the requirements?

A. Multicast addressing
B. Anycast addressing
C. Broadcast addressing
D. Unicast addressing

Answer: B

Explanation:
Anycast addressing is a network addressing and routing methodology in which a single destination address has multiple routing paths to two or more endpoint destinations. Routers will select the desired path on the basis of number of hops, distance, lowest cost, latency measurements or based on the least congested route. Anycast addressing is designed to provide high availability and low latency for services that have multiple instances across the world, such as DNS servers. By using anycast addressing, the customer can ensure that servers are accessed based on whichever one is topographically closest to the destination. If the server does not respond, then the next topographically closest server should respond. References: [CompTIA Network+ Certification Exam Objectives], [Anycast - Wikipedia]

NEW QUESTION 188
- (Topic 3)
Which of the following would be increased by adding encryption to data communication across the network?

A. Availability
B. Integrity
C. Accountability
D. Confidentiality

Answer: D

Explanation:
Confidentiality is the property of preventing unauthorized access or disclosure of data. Encryption is a method of transforming data into an unreadable format that can only be decrypted by authorized parties who have the correct key. Encryption can increase the confidentiality of data communication across the network by making it harder for attackers to intercept or eavesdrop on the data. References: Network+ Study Guide
Objective 4.1: Summarize the purposes of physical security devices. Subobjective: Encryption.

NEW QUESTION 190
- (Topic 3)
An organization has experienced an increase in malicious spear-phishing campaigns and wants to mitigate the risk of hyperlinks from inbound emails.
Which of the following appliances would best enable this capability?

A. Email protection gateway
B. DNS server
C. Proxy server
D. Endpoint email client
E. Sandbox

Answer: A

Explanation:
An email protection gateway is an appliance that can filter and block malicious emails and attachments before they reach the recipients. An email protection gateway can mitigate the risk of hyperlinks from inbound emails by scanning the links for malicious content, rewriting the links to point to a safe domain, or blocking the links altogether. An email protection gateway can also perform other functions such as spam filtering, antivirus scanning, encryption, and data loss prevention. A DNS server, a proxy server, an endpoint email client, and a sandbox are not appliances that can enable this capability, as they have different purposes and functions.
References
? 1: CompTIA Network+ N10-008 Certification Study Guide, page 304
? 2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 15
? 3: CompTIA Network+ N10-008 Certification Practice Test, question 5
? 4: Email Protection Gateway – N10-008 CompTIA Network+ : 3.2

NEW QUESTION 191
- (Topic 3)
An international company is transferring its IT assets including a number of WAPs from the United States to an office in Europe for deployment. Which of the following considerations should the company research before Implementing the wireless hardware?

A. WPA2 cipher
B. Regulatory Impacts
C. CDMA configuration
D. 802.11 standards

Answer: B

Explanation:
When transferring IT assets, including wireless access points (WAPs), from one country to another, it's important to research the regulatory impacts of the move. Different countries have different regulations and compliance requirements for wireless devices, such as frequency bands, power levels, and encryption standards. Failing to comply with these regulations can result in fines or other penalties.

NEW QUESTION 193
- (Topic 3)
A hacker used a packet sniffer on the network to capture the hardware address of the server. Which of the following types of attacks can the hacker perform now?

A. Piggybacking
B. MAC spoofing
C. Evil twin
D. VLAN hopping

Answer: B

Explanation:
MAC spoofing is a technique that allows a hacker to change the media access control (MAC) address of their network interface card (NIC) to impersonate another device on the network. By capturing the hardware address of the server, the hacker can spoof their MAC address to match the server's and bypass any MAC-based security measures, such as MAC filtering or MAC authentication. MAC spoofing can also be used to perform man-in- the-middle attacks, where the hacker intercepts and alters the traffic between two devices on the network. References: CompTIA Network+ N10-008 Cert Guide, Chapter 7, Section 7.3

NEW QUESTION 194
- (Topic 3)
Which of the following OSI model layers is where a technician would view UDP information?

A. Physical
B. Data link
C. Network
D. Transport

Answer: D

NEW QUESTION 195
- (Topic 3)
A network technician is investigating why a core switch is logging excessive amounts of data to the syslog server. The running configuration of the switch showed the following logging information:

```
ip ssh logging events
logging level debugging
logging host 192.168.1.100
logging synchronous
```

Which of the following changes should the technician make to BEST fix the issue?

A. Update the logging host IP
B. Change lo asynchronous logging.
C. Stop logging SSH events.
D. Adjust the logging level.

Answer: D

Explanation:
The logging level is set to debugging, which is the most verbose and detailed level of logging. This means that the switch will send a lot of information to the syslog

server, which can cause excessive network traffic and storage consumption. To fix the issue, the technician should adjust the logging level to a lower value, such as informational or warning, which will reduce the amount of data logged

NEW QUESTION 199
- (Topic 3)
A network technician is selecting new network hardware, and availability is the main concern. Which of the following availability concepts should the technician consider?

A. RTO
B. MTTR
C. MTBF
D. RPO

Answer: A

Explanation:
The availability concept that the network technician should consider when selecting new network hardware is RTO (Recovery Time Objective). RTO is a metric that defines the maximum acceptable time for restoring a system or service after a disruption or failure. RTO is based on the impact and cost of downtime for the business and its customers. RTO helps determine the level of redundancy and backup needed for network hardware to ensure high availability and minimize downtime. References: CompTIA Network+ N10-008 Certification Study Guide, page 346; The Official CompTIA Network+ Student Guide (Exam N10-008), page 13-9.

NEW QUESTION 204
- (Topic 3)
Two users on a LAN establish a video call. Which of the following OSI model layers ensures the initiation coordination, and termination of the call?

A. Session
B. Physical
C. Transport
D. Data link

Answer: A

Explanation:
The OSI model layer that ensures the initiation, coordination, and termination of a video call is the session layer. The session layer is responsible for establishing, maintaining, and terminating communication sessions between two devices on a network.

NEW QUESTION 205
- (Topic 3)
A network technician needs to install patch cords from the UTP patch panel to the access switch for a newly occupied set of offices. The patch panel is not labeled for easy jack identification. Which of the following tools provides the easiest way to identify the appropriate patch panel port?

A. Toner
B. Laptop
C. Cable tester
D. Visual fault locator

Answer: A

Explanation:
A toner is a tool that generates an audible signal that can be traced by a probe. A network technician can use a toner to identify the appropriate patch panel port by connecting the toner to one end of the patch cord and using the probe to scan the patch panel until the signal is detected. A toner is the easiest way to identify the patch panel port when the patch panel is not labeled, as it does not require a laptop, a cable tester, or a visual fault locator.
A toner can also be used to locate breaks or shorts in a cable, or to verify continuity. References:
? Using a Toner and Probe - CompTIA Network+ Certification (N10-008): The Total Course Video
? CompTIA Network+ Certification Exam Objectives, page 141

NEW QUESTION 210
- (Topic 3)
A network security engineer is investigating a potentially malicious Insider on the network. The network security engineer would like to view all traffic coming from the user's PC to the switch without interrupting any traffic or having any downtime. Which of the following should the network security engineer do?

A. Turn on port security.
B. Implement dynamic ARP inspection.
C. Configure 802.1Q.
D. Enable port mirroring.

Answer: D

Explanation:
Port mirroring is a feature that allows a network switch to copy the traffic from one or more ports to another port for monitoring purposes. Port mirroring can be used to analyze the network traffic from a specific source, destination, or protocol without affecting the normal operation of the network. Port mirroring can also help to detect and troubleshoot network problems, such as performance issues, security breaches, or policy violations.
The other options are not correct because they do not meet the requirements of the question. They are:
? Turn on port security. Port security is a feature that restricts the number and type of devices that can connect to a switch port. Port security can help to prevent unauthorized access, MAC address spoofing, or MAC flooding attacks. However, port security does not allow the network security engineer to view the traffic from the user's PC to the switch.
? Implement dynamic ARP inspection. Dynamic ARP inspection (DAI) is a feature

that validates the ARP packets on a network and prevents ARP spoofing attacks. DAI can help to protect the network from man-in-the-middle, denial-of-service, or data interception attacks. However, DAI does not allow the network security engineer to view the traffic from the user's PC to the switch.
? Configure 802.1Q. 802.1Q is a standard that defines how to create and manage
virtual LANs (VLANs) on a network. VLANs can help to segment the network into logical groups based on function, security, or performance. However, 802.1Q does not allow the network security engineer to view the traffic from the user's PC to the switch.
References1: Port Mirroring - an overview | ScienceDirect Topics2: Network+ (Plus) Certification | CompTIA IT Certifications3: Port Security - an overview | ScienceDirect Topics4: Dynamic ARP Inspection - an overview | ScienceDirect Topics5: 802.1Q - an overview | ScienceDirect Topics

NEW QUESTION 213
- (Topic 3)
Which of the following would enable a network technician to implement dynamic routing?

A. An IPS
B. A bridge
C. A Layer 3 switch
D. A hub

Answer: C

NEW QUESTION 214
- (Topic 3)
The results of a recently completed site survey indicate a significant, undesired RSSI in the parking lot and other exterior areas near the like to mitigate access to the wireless network in exterior access areas. The current access point settings are listed in the following table:

Name	Power	Antenna type	Channel	SSID	Passphrase
AP1	High	Omnidirectional	1	Corp01	P$ssw0rd
AP2	Medium	Omnidirectional	6	Corp01	P$ssw0rd
AP3	Medium	Directional	9	Corp01	P$ssw0rd

Which of the following is the BEST step for the technician to take to resolve the issue?

A. Reconfigure AP2 and AP3 for non-overlapping channels
B. Implement directional antennas on AP1 and AP2.
C. Raise the power settings on AP2 and AP3.
D. Change the SSID on AP1 and AP2.

Answer: B

Explanation:
Implementing directional antennas on AP1 and AP2 is the best step for the technician to take to resolve the issue of undesired RSSI in the parking lot and other exterior areas near the building. RSSI stands for received signal strength indicator, which is a measure of how well a device can receive a wireless signal from an access point (AP). An AP is a device that provides wireless connectivity to a network. An antenna is a device that radiates or receives electromagnetic waves. A directional antenna is an antenna that focuses the wireless signal in a specific direction, resulting in higher gain and longer range. By using directional antennas on AP1 and AP2, which are located near the exterior walls of the building, the technician can reduce the wireless signal leakage to the outside areas and improve the wireless coverage inside the building. References: [CompTIA Network+ Certification Exam Objectives], What Is RSSI and How Does It Affect Wireless Networks?, Directional Antennas: Everything You Need to Know

NEW QUESTION 215
- (Topic 3)
A technician knows the MAC address of a device and is attempting to find the device's IP address. Which of the following should the technician look at to find the IP address? (Select TWO).

A. ARP table
B. DHCP leases
C. IP route table
D. DNS cache
E. MAC address table
F. STP topology

Answer: BE

NEW QUESTION 217
- (Topic 3)
A systems administrator wants to use the least amount of equipment to segment two departments that nave cables terminating in the same room. Which of the following would allow this to occur?

A. A load balancer
B. A proxy server
C. A Layer 3 switch
D. A hub
E. A Layer 7 firewall
F. The RSSI was not strong enough on the link

Answer: D

NEW QUESTION 220
- (Topic 3)
Which of the following can be used to decrease latency during periods of high utilization of a firewall?

A. Hot site
B. NIC teaming
C. HA pair
D. VRRP

Answer: B

Explanation:
NIC Teaming, also known as load balancing and failover (LBFO), allows multiple network adapters on a computer to be placed into a team for the following purposes:
(https://www.bing.com/search?q=what+is+nic+teaming+used+for%3F&form=QBLH&sp=- 1&pq=what+is+nic+teaming+used+for&sc=10-28&qs=n&sk=&cvid=13882A9A9B584D8099F4ABCAD034E821&ghsh=0&ghacc=0&ghpl=)

NEW QUESTION 223
- (Topic 3)
An engineer is designing a network topology for a company that maintains a large on- premises private cloud. A design requirement mandates internet-facing hosts to be partitioned off from the internal LAN and internal server IP ranges. Which of the following defense strategies helps meet this requirement?

A. Implementing a screened subnet
B. Deploying a honeypot
C. Utilizing network access control
D. Enforcing a Zero Trust model

Answer: A

Explanation:
A screened subnet is a network topology that uses two firewalls to isolate a segment of the network from both the internal LAN and the internet. The screened subnet, also known as a demilitarized zone (DMZ), hosts the internet-facing servers that need to be accessible from outside the network, such as web servers, mail servers, or DNS servers. The first firewall, also known as the external firewall, filters the traffic between the internet and the DMZ, allowing only the necessary ports and protocols to pass through. The second firewall, also known as the internal firewall, filters the traffic between the DMZ and the internal LAN, allowing only authorized and secure connections to access the internal resources. This way, the screened subnet provides a layer of protection for both the internet-facing hosts and the internal LAN from potential attacks12.
The other options are not defense strategies that help meet the design requirement of partitioning off the internet-facing hosts from the internal LAN and internal server IP ranges. Deploying a honeypot is a deception technique that lures attackers to a fake system or network that mimics the real one, in order to monitor their activities and collect information about their methods and motives. However, a honeypot does not isolate or protect the internet-facing hosts from the rest of the network3. Utilizing network access control is a security method that enforces policies on who or what can access the network resources, based on factors such as identity, role, device type, location, or time. However, network access control does not create a separate segment for the internet-facing hosts from the internal LAN. Enforcing a Zero Trust model is a security paradigm that assumes no trust for any entity inside or outside the network, and requires continuous verification and validation of every request and transaction. However, a Zero Trust model does not necessarily imply a specific network topology or architecture for separating the internet-facing hosts from the internal LAN.

NEW QUESTION 227
- (Topic 3)
A network administrator needs to change where the outside DNS records are hosted.
Which of the following records should the administrator change at the registrar to accomplish this task?

A. NS
B. SOA
C. PTR
D. CNAME

Answer: A

Explanation:
NS stands for Name Server, and it is a DNS record that specifies which servers are authoritative for a domain. The registrar is the entity that manages the domain registration and delegation, and it maintains the NS records for each domain. To change where the outside DNS records are hosted, the network administrator needs to change the NS records at the registrar to point to the new DNS servers that will host the outside DNS records.
References:
? DNS Record Types – N10-008 CompTIA Network+ : 1.61
? CompTIA Network+ N10-008 Cert Guide, page 1472

NEW QUESTION 230
- (Topic 3)
A technician is investigating an issue with connectivity at customer's location. The technician confirms that users can access resources locally but not over the internet The technician theorizes that the local router has failed and investigates further. The technician's testing results show that the route is functional: however, users still are unable to reach resources on the internal. Which of the following describes what the technician should do NEXT?

A. Document the lessons learned
B. Escalate the issue
C. identify the symptoms.
D. Question users for additional information

Answer: C

Explanation:
According to the CompTIA Network+ troubleshooting model123, this is the first step in troubleshooting a network problem. The technician should gather

information about the current state of the network, such as error messages, device status, network topology, and user feedback. This can help narrow down the scope of the problem and eliminate possible causes.

NEW QUESTION 231
- (Topic 3)
A user returns to the office after working remotely for an extended period. The user is reporting limited access to the office wireless network and the inability to reach company resources on the network. The user connected to the guest network, ensured all patches were applied, and checked to make sure software was up to date. Which of the following is most likely the cause of the issue?

A. The laptop drivers need to be updated to support a new wireless infrastructure.
B. The wireless passphrase has been cycled and needs to be updated.
C. The NAC appliance has labeled the laptop as non-complaint.
D. The WAP transmit power is too low and cannot complete user authentication.

Answer: C

Explanation:
A network access control (NAC) appliance is a device that checks the enrollment and compliance state of devices that try to access the network resources. It can deny, quarantine, or restrict the access of non-compliant devices based on predefined policies1. A device can be considered non-compliant if it does not meet the security requirements, such as having the latest patches, antivirus signatures, firewall settings, or encryption standards. In this scenario, the user's laptop may have been labeled as non-compliant by the NAC appliance because it was out of sync with the network policies after working remotely for a long time. The user connected to the guest network, which is usually less secure and isolated from the corporate network, and updated the patches and software, but that may not be enough to satisfy the NAC appliance. The user may need to enroll the device again, or contact the IT support to resolve the issue.
References1 - Network access control integration with Microsoft Intune | Microsoft Learn

NEW QUESTION 235
- (Topic 3)
Which of the following describes the ability of a corporate IT department to expand its cloud-hosted VM environment with minimal effort?

A. Scalability
B. Load balancing
C. Multitenancy
D. Geo-redundancy

Answer: A

Explanation:
Scalability is the ability of a corporate IT department to expand its cloud- hosted virtual machine (VM) environment with minimal effort. This allows IT departments to quickly and easily scale up their cloud environment to meet increased demand. Scalability also allows for the efficient use of resources, as IT departments can quickly and easily scale up or down as needed.

NEW QUESTION 240
- (Topic 3)
Which of the following should be used to associate an IPv6 address with a domain name?

A. AAAA
B. A
C. SOA
D. TXT

Answer: A

Explanation:
An AAAA record is a type of DNS record that maps a domain name to an IPv6 address. It is similar to an A record, which maps a domain name to an IPv4 address, but it uses a 128-bit address instead of a 32-bit one. An AAAA record allows a domain name to be resolved by both IPv4 and IPv6 clients, and it is necessary for accessing websites and services that use IPv6.

NEW QUESTION 242
- (Topic 3)
Classification using labels according to information sensitivity and impact in case of unauthorized access or leakage is a mandatory component of:

A. an acceptable use policy.
B. a memorandum of understanding.
C. data loss prevention,
D. a non-disclosure agreement.

Answer: C

Explanation:
Data loss prevention (DLP) is a set of tools and processes that aim to prevent unauthorized access or leakage of sensitive information. One of the components of DLP is data classification, which involves labeling data according to its information sensitivity and impact in case of unauthorized disclosure. Data classification helps to identify and protect the most critical and confidential data and apply appropriate security controls and policies. References: Network+ Study Guide Objective 5.1: Explain the importance of policies, processes and procedures for IT governance. Subobjective: Data loss prevention.

NEW QUESTION 247
- (Topic 3)
An organization has a guest network with a network IP range of 192.168.1.0/28 using a DHCP pool. One visitor reported difficulties connecting and configured a static IP address. Following this action, another visitor reported intermittent connection issues. Which of the following is the most likely reason?

A. Address pool exhaustion
B. Duplicate IP addresses
C. Misconfigured default gateway
D. Incorrect subnet mask

Answer: B

Explanation:
A duplicate IP address occurs when two devices on the same network have the same IP address assigned to them. This can cause intermittent connection issues, as the network devices may not be able to distinguish between the two conflicting devices. A duplicate IP address can be caused by a visitor manually configuring a static IP address that is already in use by another device on the guest network. The network IP range of 192.168.1.0/28 has only 14 usable host addresses, so the chances of a duplicate IP address are higher than a larger network.
References
? 1: Troubleshooting IP Configurations – CompTIA Network+ N10-006 – 4.6
? 2: Troubleshooting Duplicate IP Addresses - CompTIA Network+ N10-005: 2.5
? 3: Network Address Translation – N10-008 CompTIA Network+ : 1.4

NEW QUESTION 252
- (Topic 3)
An attacker targeting a large company was able to inject malicious A records into internal name resolution servers. Which of the following attack types was MOST likely used?

A. DNS poisoning
B. On-path
C. IP spoofing
D. Rogue DHCP

Answer: A

NEW QUESTION 256
- (Topic 3)
Logs show an unauthorized IP address entering a secure part of the network every night at 8:00 pm. The network administrator is concerned that this IP address will cause an issue to a critical server and would like to deny the IP address at the edge of the network. Which of the following solutions would address these concerns?

A. Changing the VLAN of the web server
B. Changing the server's IP address
C. Implementing an ACL
D. Instating a rule on the firewall connected to the web server

Answer: D

NEW QUESTION 257
- (Topic 3)
An organization is interested in purchasing a backup solution that supports the organization's goals. Which of the following concepts would specify the maximum duration that a given service can be down before impacting operations?

A. MTTR
B. RTO
C. MTBF
D. RPO

Answer: B

Explanation:
The maximum duration that a given service can be down before it impacts operations is often referred to as the Recovery Time Objective (RTO). RTO is a key consideration in any backup and disaster recovery plan, as it determines how quickly the organization needs to be able to recover from a disruption or failure. It is typically expressed in terms of time, and it helps to inform the design and implementation of the backup solution. For example, if an organization has a critical service that must be available 24/7, it may have a very low RTO, requiring that the service be restored within a matter of minutes or even seconds. On the other hand, if the service can be down for a longer period of time without significantly impacting operations, the organization may have a higher RTO. When selecting a backup solution, it is important to consider the organization's RTO requirements and ensure that the solution is capable of meeting those needs. A solution that does not meet the organization's RTO requirements may not be sufficient to ensure the availability of critical services in the event of a disruption or failure.

NEW QUESTION 259
- (Topic 3)
Several end users viewing a training video report seeing pixelated images while watching. A network administrator reviews the core switch and is unable to find an immediate cause. Which of the following BEST explains what is occurring?

A. Jitter
B. Bandwidth
C. Latency
D. Giants

Answer: A

Explanation:
"Jitter is the loss of packets due to an overworked WAP. Jitter shows up as choppy conversations over a video call, strange jumps in the middle of an online game—pretty much anything that feels like the network has missed some data. Latency is when data stops moving for a moment due to a WAP being unable to do the work. This manifests as a Word document that stops loading, for example, or an online file that stops downloading."

NEW QUESTION 260
- (Topic 3)
Which of the following best describes what an organization would use port address translation for?

A. VLANs on the perimeter
B. Public address on the perimeter router
C. Non-routable address on the perimeter router
D. Servers on the perimeter

Answer: B

Explanation:
The best answer is B. Public address on the perimeter router.
Port address translation (PAT) is a function that allows multiple users within a private network to make use of a minimal number of IP addresses. Its basic function is to share a single IP public address between multiple clients who need to use the Internet publicly. It is an extension of network address translation (NAT)1.
PAT works by creating dynamic NAT mapping, in which a global (public) IP address and a unique port number are selected. The router keeps a NAT table entry for every unique combination of the private IP address and port, with translation to the global address and a unique port number2.
Therefore, an organization would use PAT for having a public address on the perimeter router, which can be shared by many hosts on the private network using different port numbers. This can reduce the bandwidth consumption and cost of the organization's internet connection, as well as provide some security benefits by hiding the internal network structure3.
The other options are not correct because:
? VLANs on the perimeter are not related to PAT, as they are used to segment the network into logical groups based on different criteria, such as function, security, or performance4.
? Non-routable address on the perimeter router would not allow the organization to access the Internet or the cloud, as non-routable addresses are not valid on the public network and cannot be translated by PAT5.
? Servers on the perimeter are not a reason to use PAT, as servers usually have static IP addresses and do not need to share a public address with other hosts. Servers on the perimeter may use NAT, but not PAT, to map their private IP addresses to a public IP address2.

NEW QUESTION 265
- (Topic 3)
A false camera is installed outside a building to assist with physical security. Which of the following is the device assisting?

A. Detection
B. Recovery
C. Identification
D. Prevention

Answer: A

NEW QUESTION 268
- (Topic 3)
A network administrator is preparing answers for an annual risk assessment that is required for compliance purposes. Which of the following would be an example of an internal threat?

A. An approved vendor with on-site offices
B. An infected client that pulls reports from the firm
C. A malicious attacker from within the same country
D. A malicious attacker attempting to socially engineer access into corporate offices

Answer: A

Explanation:
Insider threat= insider threat is defined as the threat that an employee or a contractor will use his or her authorized access, wittingly or unwittingly, to do harm

NEW QUESTION 269
- (Topic 3)
A systems operator is granted access to a monitoring application, configuration application,
and timekeeping application. The operator is denied access to the financial and project management applications by the system's security configuration. Which of the following BEST describes the security principle in use?

A. Network access control
B. Least privilege
C. Multifactor authentication
D. Separation of duties

Answer: D

NEW QUESTION 274
- (Topic 3)
Which of the following OSI model layers are responsible for handling packets from the sources to the destination and checking for errors? (Select two).

A. Physical
B. Session
C. Data link
D. Network
E. Presentation
F. Application

Answer: CD

Explanation:
The data link and network layers are responsible for handling packets from the source to the destination and checking for errors. The data link layer is the second layer of the OSI model, which is a conceptual framework that describes how different network functions are organized and interact. The data link layer is responsible for providing reliable and efficient data transmission between two adjacent nodes on a network. The data link layer uses frames as its unit of data, and adds a header and a trailer to each frame that contain information such as source and destination MAC addresses, frame type, and error detection code. The data link layer can check for errors by using techniques such as parity check, checksum, or cyclic redundancy check (CRC). The network layer is the third layer of the OSI model, which is responsible for providing logical addressing and routing of packets across different networks. The network layer uses packets as its unit of data, and adds a header to each packet that contains information such as source and destination IP addresses, protocol type, and hop count. The network layer can check for errors by using techniques such as Internet Control Message Protocol (ICMP), which can send and receive error messages or diagnostic information. References: [CompTIA Network+ Certification Exam Objectives], Data Link Layer - an overview | ScienceDirect Topics, Network Layer - an overview | ScienceDirect Topics

NEW QUESTION 275
- (Topic 3)
A public, wireless ISP mounts its access points on top of traffic signal poles. Fiber-optic cables are installed from a fiber switch through the ground and up the pole to a fiber-copper media converter, and then connected to the AP. In one location, the switchport is showing sporadic link loss to the attached AP. A similar link loss is not seen at the AP interface. The fiber-optic cable is moved to another unused switchport with a similar result. Which of the following steps should the assigned technician complete NEXT?

A. Disable and enable the switchport.
B. Clean the fiber-optic cable ends.
C. Replace the media converter.
D. Replace the copper patch cord.

Answer: B

Explanation:
Fiber-optic cables are cables that use light signals to transmit data over long distances at high speeds. Fiber-optic cables are sensitive to dirt, dust, moisture, or other contaminants that can interfere with the light signals and cause link loss or signal degradation. To troubleshoot link loss issues with fiber-optic cables, one of the steps that should be completed next is to clean the fiber-optic cable ends with a lint-free cloth or a specialized cleaning tool. Cleaning the fiber-optic cable ends can remove any dirt or debris that may be blocking or reflecting the light signals and restore the link quality.

NEW QUESTION 279
- (Topic 3)
Which of the following most likely determines the size of a rack for installation? {Select two).

A. KVM size
B. Switch depth
C. Hard drive size
D. Cooling fan speed
E. Outlet amperage
F. Server height

Answer: BF

Explanation:
The size of a rack for installation depends on several factors, such as the available space, the power and cooling requirements, and the dimensions of the equipment to be installed. Two of the most important dimensions to consider are the switch depth and the server height. Switch depth refers to the length of the switch from front to back, which determines how much space is needed inside the rack. Server height refers to the vertical space occupied by the server, which is measured in rack units (RU) or U. One rack unit is equal to 1.75 inches. The height of the rack should be able to accommodate the total number of rack units needed for the servers and other devices, as well as some extra space for cable management and airflow. References: CompTIA Network+ N10-008 Cert Guide, Chapter 2, Section 2.5

NEW QUESTION 282
- (Topic 3)
Which or the following devices and encapsulations are found at me data link layer? (Select TWO)

A. Session
B. Frame
C. Firewall
D. Switch
E. Packet
F. Router

Answer: BD

Explanation:
The data link layer is responsible for defining the format of data on the network and providing physical transmission of data. Devices that operate at this layer include switches and network interface cards (NICs). Encapsulations that are used at this layer include frames, which are units of data that contain a header, payload, and trailer. Frames are used to identify the source and destination of data on the network and to perform error detection. References: CompTIA Network+ N10-008 Certification Study Guide, page 9; The Official CompTIA Network+ Student Guide (Exam N10-008), page 1-6.

NEW QUESTION 285
- (Topic 3)
A network administrator needs to provide remote clients with access to an internal web application. Which of the following methods provides the highest flexibility and compatibility while encrypting only the connection to the web application?

A. Clientless VPN
B. Virtual desktop
C. Virtual network computing
D. mGRE tunnel

Answer: A

Explanation:
A clientless VPN is a method of providing remote clients with access to an internal web application without installing any additional software or dedicated VPN client on their devices. Instead, users access the VPN through a web browser, utilizing a web portal or gateway provided by the VPN service. This method provides the highest flexibility and compatibility, as it supports various operating systems and devices, and encrypts only the connection to the web application, not the entire traffic of the device.

NEW QUESTION 286
- (Topic 3)
A network administrator is connecting two Layer 2 switches in a network These switches must transfer data in multiple networks. Which of the following would fulfill this requirement?

A. Jumbo frames
B. 802. IQ tagging
C. Native VLAN
D. Link aggregation

Answer: B

Explanation:
The technique that would fulfill the requirement of transferring data in multiple networks is 802.1Q tagging. 802.1Q tagging is a method of adding a tag or identifier to Ethernet frames that indicate which VLAN (Virtual Local Area Network) they belong to. VLANs are logical subdivisions of a network that allow devices in different physical locations or segments to communicate as if they were in the same network. VLANs improve network performance, security, and management by reducing broadcast traffic, isolating sensitive data, and grouping devices by function or department. By using 802.1Q tagging, two Layer 2 switches can exchange data from multiple VLANs over a single trunk link, without mixing or losing the VLAN information. References: CompTIA Network+ N10-008 Certification Study Guide, page 64; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-12.

NEW QUESTION 289
- (Topic 3)
At which of the following OSI model layers does routing occur?

A. Data link
B. Transport
C. Physical
D. Network

Answer: D

NEW QUESTION 290
- (Topic 3)
Which of the following is the physical security mechanism that would MOST likely be used to enter a secure site?

A. A landing page
B. An access control vestibule
C. A smart locker
D. A firewall

Answer: B

Explanation:
An access control vestibule is a physical security mechanism that consists of a small room or chamber with two doors, one leading to the outside and one leading to the secure site. The doors are controlled by an electronic system that verifies the identity and authorization of the person entering before allowing access to the next door. A landing page is a web page that appears when a user clicks on a link or advertisement. A smart locker is a physical security mechanism that allows users to store and retrieve items using a code or biometric authentication. A firewall is a network security device that monitors and filters incoming and outgoing traffic based on predefined rules. References: [CompTIA Network+ Certification Exam Objectives], Domain 4.0 Network Operations, Objective 4.1: Explain the importance of documentation and diagrams, Subobjective: Physical security devices (locks, cameras, etc.)

NEW QUESTION 292
- (Topic 3)
Given the following Information:

Connection	Cable length	Cable type	Configuration
PC A to switch 1	394ft (120m)	Cat 5	Straight through
Switch 1 to switch 2	3.3ft (1m)	Cat 6	Crossover
Switch 2 to PC B	16ft (5m)	Cat 5	Straight through

Which of the following would cause performance degradation between PC A and PC B'?

A. Attenuation
B. Interference
C. Decibel loss
D. Incorrect pinout

Answer: D

NEW QUESTION 295
- (Topic 3)
Which of the following is an example of on-demand scalable hardware that is typically housed in the vendor's data center?

A. DaaS
B. laaS
C. PaaS
D. SaaS

Answer: B

Explanation:
IaaS is an example of on-demand scalable hardware that is typically housed in the vendor's data center. IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources over the internet. IaaS allows customers to rent servers, storage, network devices, and other hardware components from a cloud service provider, rather than purchasing and maintaining them on-premise. IaaS offers advantages such as scalability, flexibility, cost-effectiveness, and reliability. Customers can adjust their hardware resources according to their needs and pay
only for what they use. Customers can also access their hardware resources from anywhere via a web browser or an API. References: [CompTIA Network+ Certification Exam Objectives], What Is Infrastructure as a Service (IaaS)? | IBM

NEW QUESTION 299
- (Topic 3)
Which of the following requires network devices to be managed ustng a different set of IP addresses?

A. Console
B. Split tunnel
C. Jump box
D. Out of band

Answer: D

Explanation:
Out of band management is a process for accessing and managing network devices and infrastructure at remote locations through a separate management plane from the production network. Out of band management requires network devices to be managed using a different set of IP addresses than the ones used for in-band management or data traffic. This provides a secure and dedicated alternate access method to administer connected devices and IT assets without using the corporate LAN.

NEW QUESTION 304
- (Topic 3)
An employee reports to a network administrator that internet access is not working. Which of the following should the administrator do FIRST?

A. Establish a theory of probable cause.
B. Identify symptoms.
C. Determine if anything has changed.
D. Ask the user to restart the computer.

Answer: C

Explanation:
When a user reports that internet access is not working, it is important to first determine if there have been any recent changes to the network or the user's computer that could have caused the issue. This could include changes to the network configuration, the installation of new software or hardware, or other events that could have impacted the user's ability to access the internet. By determining if anything has changed, the administrator can narrow down the possible causes of the issue and focus on addressing the most likely cause.

NEW QUESTION 305
- (Topic 3)
Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

A. SSO
B. TACACS+
C. Zero Trust
D. Separation of duties
E. Multifactor authentication

Answer: B

Explanation:
TACACS+ is used to authenticate users and authorize access to network resources. This protocol provides greater network security by encrypting the authentication credentials and reducing the risk of unauthorized access. According to the CompTIA Network+ Study Manual, “TACACS+ is an authentication protocol used to centralize authentication and authorization for network devices. It is a more secure alternative to Telnet for handling logins and for granting privileges to users.”

NEW QUESTION 308
- (Topic 3)
A network administrator needs to connect two routers in a point-to-point configuration and conserve IP space. Which of the following subnets should the administrator use?

A. /24
B. /26
C. /28
D. /30

Answer: D

Explanation:
A /30 subnet is the smallest possible subnet that can be used for a point-to-point configuration between two routers. A /30 subnet has only two usable host addresses, one for each router, and a network address and a broadcast address. A /30 subnet conserves IP space by minimizing the number of wasted addresses. A /24, /26, or /28 subnet would have more usable host addresses than needed for a point-to-point configuration and would waste IP space.
References:
? Routing Technologies – N10-008 CompTIA Network+ : 2.21
? CompTIA Network+ Certification Exam Objectives, page 10

NEW QUESTION 309
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your N10-009 Exam with Our Prep Materials Via below:

https://www.certleader.com/N10-009-dumps.html