Exam Questions N10-009

CompTIA Network+ Exam

https://www.2passeasy.com/dumps/N10-009/

NEW QUESTION 1
- (Topic 3)
A network administrator is configuring logging on an edge switch. The requirements are to log each time a switch port goes up or down. Which of the following logging levels will provide this information?

A. Warnings
B. Notifications
C. Alert
D. Errors

Answer: B

Explanation:
 Notifications are the lowest logging level and will provide the desired information regarding switch port up/down activity. According to the CompTIA Network+ Study Manual, notifications "are used for logging normal activities, such as port up/down events, link changes, and link flaps."

NEW QUESTION 2
- (Topic 3)
During an incident, an analyst sends reports regularly to the investigation and leadership teams. Which of the following best describes how PII 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 3
- (Topic 3)
An organization has a security requirement that all network connections can be traced back to a user. A network administrator needs to identify a solution to implement on the wireless network. Which of the following is the best solution?

A. Implementing enterprise authentication
B. Requiring the use of PSKs
C. Configuring a captive portal for users
D. Enforcing wired equivalent protection

Answer: A

Explanation:
Enterprise authentication is a method of securing wireless networks that uses an external authentication server, such as RADIUS, to verify the identity of users and devices. Enterprise authentication can provide user traceability by logging the network connections and activities of each authenticated user. This can help the organization meet its security requirement and comply with any regulations or policies that mandate user accountability12.
References:
? CompTIA Network+ N10-008 Certification Exam Objectives, page 83
? CompTIA Network+ Cert Guide: Wireless Networking, page 13

NEW QUESTION 4
- (Topic 3)
Which of the following is required for hosts to receive DHCP addresses from a server that is located on a different subnet?

A. DHCP scope
B. DHCP snooping
C. DHCP reservations
D. DHCP relay

Answer: D

Explanation:
 A DHCP relay is a network device that forwards DHCP requests from clients on one subnet to a DHCP server on another subnet. This allows the DHCP server to assign IP addresses and other network configuration parameters to clients across different subnets. A DHCP scope is a range of IP addresses that a DHCP server can assign to clients. A DHCP snooping is a security feature that filters and validates DHCP messages on a switch. A DHCP reservation is a way to assign a

specific IP address to a specific client
based on its MAC address. References: Part 2 of the current page talks about DHCP relay and its functions. You can also find more information about DHCP relay on [this page].

NEW QUESTION 5
- (Topic 3)
Which of the following protocols can be routed?

A. FCoE
B. Fibre Channel
C. iSCSI
D. NetBEUI

Answer: C

Explanation:
iSCSI (Internet Small Computer System Interface) is a protocol that allows SCSI commands to be transported over IP networks1. iSCSI can be routed because it contains a network address and a device address, as required by a routable protocol2. iSCSI can be used to access block-level storage devices over a network, such as SAN (Storage Area Network).
FCoE (Fibre Channel over Ethernet) is a protocol that allows Fibre Channel frames to be encapsulated and transported over Ethernet networks1. FCoE cannot be routed because it does not contain a network address, only a device address. FCoE operates at the data link layer and requires special switches and adapters to support it. FCoE can also be used to access block-level storage devices over a network, such as SAN.
Fibre Channel is a protocol that provides high-speed and low-latency communication between servers and storage devices1. Fibre Channel cannot be routed because it does not use IP networks, but rather its own dedicated network infrastructure. Fibre Channel operates at the physical layer and the data link layer and requires special cables, switches, and adapters to support it. Fibre Channel can also be used to access block-level storage devices over a network, such as SAN.
NetBEUI (NetBIOS Extended User Interface) is an old protocol that provides session-level communication between devices on a local network1. NetBEUI cannot be routed because it does not contain a network address, only a device address. NetBEUI operates at the transport layer and relies on NetBIOS for name resolution. NetBEUI is obsolete and has been replaced by other protocols, such as TCP/IP.

NEW QUESTION 6
- (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 7
- (Topic 3)
A network administrator is given the network 80.87.78.0/26 for specific device assignments. Which of the following describes this network?

A. 80.87.78 0 - 80.87.78.14
B. 80.87.78 0 - 80.87.78.110
C. 80.87.78 1 - 80.87.78.62
D. 80.87.78.1 - 80.87.78.158

Answer: C

Explanation:
The network 80.87.78.0/26 is a Class A network with a subnet mask of /26, which means that it contains 26 bits of network information and 6 bits of host information.
The range of valid host addresses for this network is 80.87.78.1 to 80.87.78.62. Any addresses outside of this range are reserved for special purposes or are not used.

NEW QUESTION 8
- (Topic 3)
A network technician is investigating a trouble ticket for a user who does not have network connectivity. All patch cables between the wall jacks and computers in the building were upgraded over the weekend from Cat 5 to Cat 6. The newly installed cable is crimped with a TIA/EIA 568A on one end and a TIA/EIA 568B on the other end.
Which of the following should the technician do to MOST likely fix the issue?

A. Ensure the switchport has PoE enabled.
B. Crimp the cable as a straight-through cable.
C. Ensure the switchport has STP enabled.
D. Crimp the cable as a rollover cable.

Answer: B

Explanation:
A straight-through cable is a type of twisted pair cable that has the same wiring standard (TIA/EIA 568A or 568B) on both ends. This is the most common type of

cable used for connecting devices of different types, such as a computer and a switch. A cable that has different wiring standards on each end (TIA/EIA 568A on one end and 568B on the other) is called a crossover cable, which is used for connecting devices of the same type, such as two computers or two switches. Therefore, the technician should crimp the cable as a straight-through cable to fix the issue.

NEW QUESTION 9
- (Topic 3)
A customer needs six usable IP addresses. Which of the following best meets this requirement?

A. 255.255.255.128
B. 255.255.255.192
C. 255.255.255.224
D. 255.255.255.240

Answer: C

NEW QUESTION 10
- (Topic 3)
A technician is monitoring a network interface and notices the device is dropping packets. The cable and interfaces, however, are in working order. Which of the following is MOST likely the cause?

A. OID duplication
B. MIB mismatch
C. CPU usage
D. Encapsulation errors

Answer: C

NEW QUESTION 10
- (Topic 3)
A network engineer needs to create a subnet that has the capacity for five VLANs. with the following number of clients lo be allowed on each:

VLAN 10	50 users
VLAN 20	35 users
VLAN 30	20 users
VLAN 40	75 users
VLAN 50	130 users

Which of the following is the SMALLEST subnet capable of this setup that also has the capacity to double the number of clients in the future?

A. 10.0.0.0/21
B. 10.0.0.0/22
C. 10.0.0.0/23
D. 10.0.0.0/24

Answer: B

NEW QUESTION 13
- (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 17
- (Topic 3)
Which of the following protocols is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links?

A. OSPF
B. RIPv2
C. QoS
D. STP

Answer: A

NEW QUESTION 20
- (Topic 3)
A Wi-Fi network was recently deployed in a new, multilevel budding. Several issues are now being reported related to latency and drops in coverage. Which of the following is the FIRST step to troubleshoot the issues?

A. Perform a site survey.
B. Review the AP placement
C. Monitor channel utilization.
D. Test cable attenuation.

Answer: A

NEW QUESTION 23
- (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 27
- (Topic 3)
A security engineer is trying to connect cameras to a 12-port PoE switch, but only eight cameras turn on. Which of the following should the engineer check first?

A. Ethernet cable type
B. Voltage
C. Transceiver compatibility
D. DHCP addressing

Answer: B

Explanation:
The most likely reason why only eight cameras turn on is that the PoE switch does not
have enough power budget to supply all 12 cameras. The engineer should check the voltage and wattage ratings of the PoE switch and the cameras, and make sure they are compatible and sufficient. The Ethernet cable type, transceiver compatibility, and DHCP addressing are less likely to cause this problem, as they would affect the data transmission rather than the power delivery.
References:
? CompTIA Network+ N10-008 Certification Study Guide, page 181
? CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 352
? PoE Troubleshooting: The Common PoE Errors and Solutions3

NEW QUESTION 32
- (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 36
- (Topic 3)
Which of the following devices Is used to configure and centrally manage access points Installed at different locations?

A. Wireless controller
B. Load balancer

C. Proxy server
D. VPN concentrator

Answer: A

Explanation:
Access points (APs) can be configured and centrally managed using a wireless LAN controller (WLC). A WLC is a device that connects to multiple APs and provides centralized management and control of those APs. The WLC can be used to configure settings such as wireless network parameters, security settings, and quality of service (QoS) policies. Additionally, the WLC can be used to monitor the status of connected APs, track client connections, and gather statistics on network usage. Some vendors such as Cisco, Aruba, Ruckus, etc. provide wireless LAN controllers as part of their wireless networking solutions.

NEW QUESTION 40
- (Topic 3)
Which of the following fiber connector types is the most likely to be used on a network interface card?

A. LC
B. SC
C. ST
D. MPO

Answer: A

Explanation:
LC (local connector) is the most likely fiber connector type to be used on a network interface card, because it is a small form factor connector that can fit more interfaces on a single card. LC connectors use square connectors that have a locking mechanism on the top, similar to an RJ45 copper connector. LC connectors are also compatible with SFP (small form-factor pluggable) modules that are often used to link a gigabit Ethernet port with a fiber network12.
References:
? Optical Fiber Connectors – CompTIA Network+ N10-007 – 2.11
? CompTIA Network+ Certification Exam Objectives2

NEW QUESTION 44
- (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 48
- (Topic 3)
Which of the following protocols can be used to change device configurations via encrypted and authenticated sessions? (Select TWO).

A. SNMPv3
B. SSh
C. Telnet
D. IPSec
E. ESP
F. Syslog

Answer: BD

NEW QUESTION 53
- (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 54
- (Topic 3)
Users are reporting poor wireless performance in some areas of an industrial plant The wireless controller is measuring a tow EIRP value compared to me recommendations noted on me most recent site survey. Which of the following should be verified or replaced for the EIRP value to meet the site survey's specifications? (Select TWO).

A. AP transmit power
B. Channel utilization
C. Signal loss
D. Update ARP tables
E. Antenna gain
F. AP association time

Answer: AE

Explanation:
? AP transmit power: You should check if your APs have sufficient power output and adjust them if needed. You should also make sure they are not exceeding regulatory limits for your region.
? Antenna gain: You should check if your antennas have adequate gain for your coverage area and replace them if needed. You should also make sure they are aligned properly and not obstructed by any objects.
In the scenario described, the wireless controller is measuring a low EIRP value compared to the recommendations noted in the most recent site survey. EIRP is the combination of the power transmitted by the access point and the antenna gain. Therefore, to increase the EIRP value to meet the site survey's specifications, the administrator should verify or replace the AP transmit power (option A) and the antenna gain (option E). This can be achieved by adjusting the transmit power settings on the AP or by replacing the AP's antenna with one that has a higher gain

NEW QUESTION 56
- (Topic 3)
Network traffic is being compromised by DNS poisoning every time a company's router is connected to the internet. The network team detects a non-authorized DNS server being assigned to the network clients and remediates the incident by setting a trusted DNS server, but the issue occurs again after internet exposure. Which of the following best practices should be implemented on the router?

A. Change the device's default password.
B. Disable router advertisement guard.
C. Activate control plane policing.
D. Disable unneeded network services.

Answer: A

NEW QUESTION 59
- (Topic 3)
Which of the following would be used to adjust resources dynamically for a virtual web server under variable loads?

A. Elastic computing
B. Scalable networking
C. Hybrid deployment
D. Multitenant hosting

Answer: B

Explanation:
A technique used to adjust resources dynamically for a virtual web server under variable loads is called auto-scaling. Auto-scaling automatically increases or decreases the number of instances of a virtual web server in response to changes in demand, ensuring that the right amount of resources are available to handle incoming traffic. This can help to improve the availability and performance of a web application, as well as reduce costs by avoiding the need to provision and maintain excess capacity.

NEW QUESTION 62
- (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 67
- (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 68
- (Topic 3)
A user calls the IT department to report being unable to log in after locking the computer The user resets the password, but later in the day the user is again unable to log in after locking the computer Which of the following attacks against the user IS MOST likely taking place?

A. Brute-force
B. On-path
C. Deauthentication
D. Phishing

Answer: A

NEW QUESTION 71
- (Topic 3)
A network administrator is investigating a performance issue on a dual-link connection—VPN and MPLS—to a partner network. The MPLS is the primary path, and the VPN is used as a backup. While communicating, the delay is measured at 18ms, which is higher than the 6ms expected when the MPLS link is operational but lower than the 30ms expected tor the VPN connection. Which of the following will MOST likely point to the root cause of the Issue?

A. Checking the routing tables on both sides to ensure there is no asymmetric routing
B. Checking on the partner network for a missing route pointing to the VPN connection
C. Running iPerf on both sides to confirm the delay that Is measured is accurate
D. Checking for an incorrect VLAN assignment affecting the MPLS traffic

Answer: A

Explanation:
Asymmetric routing can occur when two routers have different paths for the same two hosts, resulting in increased latency and possible packet loss. According to the CompTIA Network+ Study Manual, "If the path from the source to the destination is not the same in both directions, the packets will take different routes and the latency can increase significantly." To confirm this, the network administrator should check the routing tables on both sides of the connection and ensure that the same path is used in both directions.

NEW QUESTION 72
- (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 77
- (Topic 3)
A network administrator installed an additional IDF during a building expansion project. Which of the following documents need to be updated to reflect the change? (Select TWO).

A. Data loss prevention policy
B. BYOD policy
C. Acceptable use policy
D. Non-disclosure agreement
E. Disaster recovery plan
F. Physical network diagram

Answer: AF

NEW QUESTION 82
- (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 87
- (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 89
- (Topic 3)
Which of the following is the IEEE link cost for a Fast Ethernet interface in STP calculations?

A. 2
B. 4
C. 19
D. 100

Answer: D

Explanation:
The IEEE standard for link cost for a Fast Ethernet interface is 100, and for a Gigabit Ethernet interface is 19. These values are based on the bandwidth of the interface, with lower values indicating a higher-bandwidth interface.

NEW QUESTION 90
- (Topic 3)
A network administrator needs to monitor traffic on a specific port on a switch. Which of the following should the administrator configure to accomplish the task?

A. Port security
B. Port tagging
C. Port mirroring
D. Media access control

Answer: C

Explanation:
Port mirroring is a technique that allows a network administrator to monitor the traffic on a specific port on a switch by sending a copy of the packets seen on that port to another port where a monitoring device is connected1. Port mirroring can be used to analyze and debug data, diagnose errors, or perform security audits on the network without affecting the normal operation of the switch

NEW QUESTION 95
- (Topic 3)
Which of the following best describe the functions of Layer 2 of the OSI model? (Select two).

A. Local addressing
B. Error preventing
C. Logical addressing
D. Error detecting
E. Port addressing
F. Error correcting

Answer: AD

Explanation:

Layer 2 of the OSI model, also known as the data link layer, is responsible for physical addressing and error detecting. Physical addressing refers to the use of MAC addresses to identify and locate devices on a network segment. Error detecting refers to the use of techniques such as checksums and CRCs to identify and correct errors in the data frames.
References:
? OSI Model | Computer Networking | CompTIA1

NEW QUESTION 100
- (Topic 3)
A network technician has determined the cause of a network disruption. Which of the following is the NEXT step for the technician to perform?

A. Validate the findings in a top-to-bottom approach
B. Duplicate the issue, if possible
C. Establish a plan of action to resolve the issue
D. Document the findings and actions

Answer: C

NEW QUESTION 103
- (Topic 3)
A malicious user is using special software 10 perform an on-path attack. Which of the following best practices should be configured to mitigate this threat?

A. Dynamic ARP inspection
B. Role-based access
C. Control plane policing
D. MAC filtering

Answer: A

NEW QUESTION 106
- (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 108
- (Topic 3)
A network administrator is working to configure a new device to provide Layer 2 connectivity to various endpoints including several WAPs. Which of the following devices will the administrator MOST likely configure?

A. WLAN controller
B. Cable modem
C. Load balancer
D. Switch
E. Hub

Answer: D

Explanation:
A switch is a device that provides Layer 2 connectivity to various endpoints by forwarding frames based on MAC addresses. A switch can also connect to several WAPs (wireless access points) to provide wireless connectivity to wireless devices.

NEW QUESTION 109
- (Topic 3)
A network administrator is concerned about a rainbow table being used to help access network resources. Which of the following must be addressed to reduce the likelihood of a rainbow table being effective?

A. Password policy
B. Remote access policy
C. Acceptable use policy
D. Data loss prevention policy

Answer: A

Explanation:
A password policy must be addressed to reduce the likelihood of a rainbow table being effective. A rainbow table is a precomputed table of hashed passwords and their corresponding plaintext values. A rainbow table can be used to crack hashed passwords by performing a reverse lookup of the hash value in the table. A password policy is a set of rules and guidelines that define how passwords should be created, used, and managed in an organization. A password policy can help prevent rainbow table attacks by enforcing strong password requirements, such as length, complexity, expiration, and history. A strong password is one that is

hard to guess or crack by using common methods such as brute force or dictionary attacks. References: [CompTIA Network+ Certification Exam Objectives], What Is Rainbow Table Attack? | Kaspersky, Password Policy Best Practices | Thycotic

NEW QUESTION 111
- (Topic 3)
A technician is working on a ticket for a user in the human resources department who received a new PC that does not connect to the internet. All users in human resources can access the
internet. The technician can ping the PC from the human resources router but not from the IT network. Which of the following is the most likely cause of the issue?

A. Duplicate IP address
B. Misconfigured RIP
C. Improper VLAN assignment
D. Incorrect default gateway

Answer: D

Explanation:
An incorrect default gateway can cause a PC to not connect to the internet, because the default gateway is the device that routes traffic from the local network to other networks. If the PC has a wrong default gateway configured, it may not be able to reach the internet router or the IT network router. The technician can ping the PC from the human resources router because they are on the same local network, but not from the IT network router because they are on different networks.
A duplicate IP address can cause a PC to not communicate with other devices on the same network, because the IP address is the unique identifier of a device on a network. If two devices have the same IP address, they may cause IP conflicts and packet loss. However, a duplicate IP address would not prevent the technician from pinging the PC from the human resources router, because they are on the same network.
A misconfigured RIP can cause a router to not learn or advertise routes to other networks, because RIP is a routing protocol that dynamically exchanges routing information between routers. If a router has a wrong RIP configuration, it may not be able to reach or share routes with other routers. However, a misconfigured RIP would not affect the PC's connectivity to the internet, because the PC does not use RIP.
An improper VLAN assignment can cause a PC to not communicate with other devices on the same or different networks, because a VLAN is a logical segmentation of a network that isolates traffic based on criteria such as function, security, or performance. If a PC is assigned to a wrong VLAN, it may not be able to access the resources or services that it needs. However, an improper VLAN assignment would not prevent the technician from pinging the PC from the human resources router, because they are on the same physical network.
References
What is a Default Gateway?
What's an IP Conflict and How Do You Resolve It? What is RIP (Routing Information Protocol)?
What is a VLAN? How to Set Up a VLAN Network
CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION 115
- (Topic 3)
A WAN technician reviews activity and identifies newly installed hardware that is causing outages over an eight-hour period. Which of the following should be considered FIRST?

A. Network performance baselines
B. VLAN assignments
C. Routing table
D. Device configuration review

Answer: D

Explanation:
The most likely cause of outages due to newly installed hardware is a misconfiguration of the device settings. Therefore, the first step should be to review the device configuration and check for any errors or inconsistencies that might affect the WAN connectivity. References: Network+ Study Guide Objective 2.1: Explain the importance of network documentation.

NEW QUESTION 118
- (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 121
- (Topic 3)
A network technician receives a support ticket concerning multiple users who are unable access the company's shared drive. The switch interface that the shared drive Is connected to is displaying die following:

```
GigabitEthernet0/9 is down, line protocol is down (notconnect)
        Hardware is Gigabit Ethernet, address is C800.84bf.9847 (via c800.84bf.9847)
        MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
        reliability 255/255, txload 1/255, rxload 1/255
        Encapsulation ARPA, loopback not set
```

Which of the following is MOST likely the Issue?

A. The switchport Is shut down
B. The cable Is not plugged In.
C. The loopoack Is not set
D. The bandwidth configuration is incorrect.

Answer: A

Explanation:
The switchport is shut down, which means it is administratively disabled and cannot forward traffic. The image shows that the switchport status is "down" and the protocol status is "down", indicating that there is no physical or logical connection. The cable is plugged in, as shown by the "connected" message under the interface name. The loopback is not set, as shown by the "loopback not set" message under the encapsulation type. The bandwidth configuration is correct, as shown by the "BW 10000 Kbit/sec" message under the MTU size. References: [CompTIA Network+ Certification Exam Objectives], Domain 3.0 Infrastructure, Objective 3.1: Given a scenario, use appropriate networking tools, Subobjective: Command line tools (ping, netstat, tracert, etc.)

NEW QUESTION 126
- (Topic 3)
A network engineer needs to change an entire subnet of SLAAC-configured workstation addresses. Which of the following methods would be the best for the engineer to use?

A. Change the address prefix in ARP in order for the workstations to retrieve their new addresses.
B. Change the address prefix in a router in order for the router to advertise the new prefix with an ND.
C. Change the address prefix scope in a DHCP server in order for the workstations to retrieve their new addresses.
D. Change the workstations' address prefix manually because an automated method does not exist.

Answer: B

Explanation:
SLAAC (Stateless Address Autoconfiguration) is a mechanism that enables each host on the network to auto-configure a unique IPv6 address without any device keeping track of which address is assigned to which node12. SLAAC uses link-local addresses and the interface's MAC address or a random number to generate the host portion of the IPv6 address2. SLAAC also relies on Router Solicitation (RS) and Router Advertisement (RA) messages to obtain the network prefix and other information from a router12. Therefore, to change an entire subnet of SLAAC-configured workstation addresses, the network engineer needs to change the address prefix in a router and let the router advertise the new prefix with an ND (Neighbor Discovery) message. This way, the workstations will receive the new prefix and update their IPv6 addresses accordingly3.
References1 - IPv6 Stateless Address Auto-configuration (SLAAC) | NetworkAcademy.io2 - IPv6 SLAAC – Stateless Address Autoconfiguration - Study-CCNA3 - Mastering IPv6
SLAAC Concepts and Configuration - Cisco Press

NEW QUESTION 130
- (Topic 3)
To access production applications and data, developers must first connect remotely to a different server From there, the developers are able to access production data Which of the following does this BEST represent?

A. A management plane
B. A proxy server
C. An out-of-band management device
D. A site-to-site VPN
E. A jump box

Answer: E

NEW QUESTION 135
- (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 139
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.

Core Switch 1

Access Switch 1　　　　　　　　　　　　　　**Access Switch 2**

PC1　　　　　　**PC2**　　　　　　**PC3**　　　　　　**PC4**

| PC1	PC2	PC3	PC4
0200.0000.0003	Select MAC Address	0200.0000.0004	Select MAC Address
Select IP Address	10.10.30.51	Select IP Address	10.10.30.53
Select VLAN	Select VLAN	Select VLAN	Select VLAN
Select Interface	Select Interface	Select Interface	Select Interface
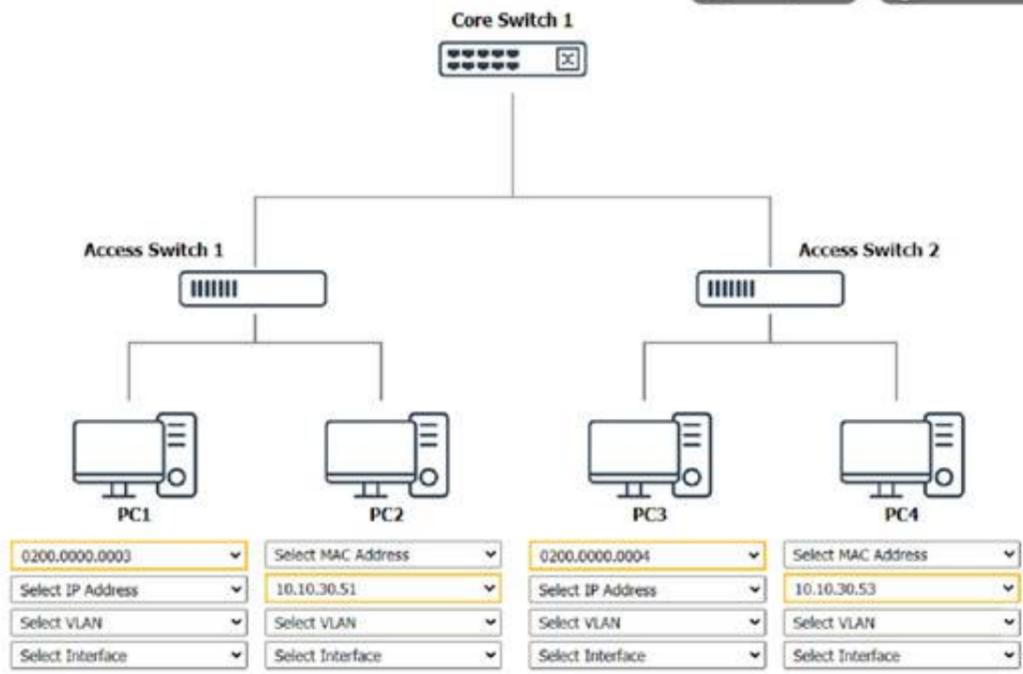
Core Switch 1 Prompt ☒

```
C:\> nmap
   % Invalid input detected.
C:\> netdiscover
   % Invalid input detected.
C:\> |
```

Access Switch 1 Prompt ☒

```
C:\> nmap
   % Invalid input detected.
C:\>
```

Access Switch 2 Prompt ☒

```
C:\>
```
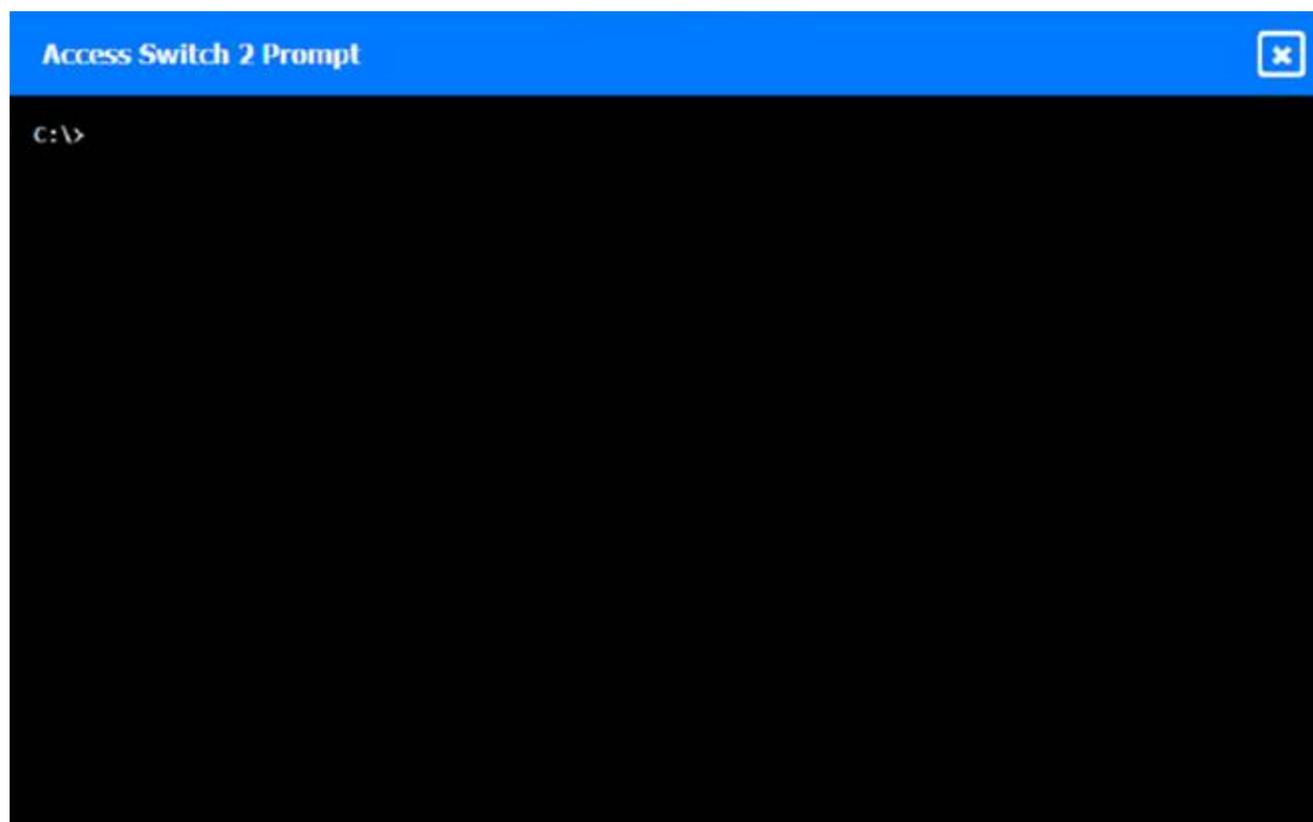
A. Mastered
B. Not Mastered

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 143
- (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 145
- (Topic 3)
A network administrator is reviewing the following metrics from a network management system regarding a switchport. The administrator suspects an issue because users are calling in regards to the switchport's performance:

Metric	Value
Uptime	201 days, 3 hours, 18 minutes
MDIX	On
CRCs	0
Giants	2508
Output queue maximum	40
Packets input	136208849
Packets output	64458087024

Based on the information in the chart above, which of the following fs the cause of these performance issues?

A. The connected device is exceeding the configured MTU.
B. The connected device is sending too many packets
C. The switchport has been up for too long
D. The connected device is receiving too many packets.
E. The switchport does not have enough CRCs

Answer: A

NEW QUESTION 149
- (Topic 3)
Which of the following options represents the participating computers in a network?

A. Nodes
B. CPUs
C. Servers
D. Clients

Answer: A

NEW QUESTION 153
- (Topic 3)
To reduce costs and increase mobility, a Chief Technology Officer (CTO) wants to adopt cloud services for the organization and its affiliates. To reduce the impact for users, the CTO wants key services to run from the on-site data center and enterprise services to run in the cloud. Which of the following deployment models is the best choice for the organization?

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

Answer: B

Explanation:
A hybrid cloud deployment model is a combination of on-premise and cloud solutions, where some resources are hosted in-house and some are hosted by a cloud provider. A hybrid cloud model can offer the benefits of both public and private clouds, such as scalability, cost-efficiency, security, and control12. A hybrid cloud model can also reduce the impact for users, as they can access the key services from the on-site data center and the enterprise services from the cloud

NEW QUESTION 155
- (Topic 3)
A network technician is having issues connecting an loT 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 160
- (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 162
- (Topic 3)
A network engineer is troubleshooting application connectivity issues between a server and a client. The network engineer needs to view the certificate exchange between the two hosts. Which of the following tools should the network engineer use?

A. dig
B. tcpdump
C. nmap
D. traceroute

Answer: B

Explanation:
tcpdump is a tool that can capture and analyze network traffic, including the certificate exchange between two hosts. It can display the contents of packets, such as the SSL/TLS handshake, which involves the exchange of certificates. dig is a tool that can query DNS servers for domain name information. nmap is a tool that can scan ports and services on a network. traceroute is a tool that can show the path and hops between a source and a destination.

NEW QUESTION 165
- (Topic 3)
A network administrator is decommissioning a server. Which of the following will the network administrator MOST likely consult?

A. Onboarding and off boarding policies
B. Business continuity plan
C. Password requirements
D. Change management documentation

Answer: D

NEW QUESTION 170
- (Topic 3)
Which of the following would be the BEST choice to connect branch sites to a main office securely?

A. VPN headend
B. Proxy server
C. Bridge
D. Load balancer

Answer: A

Explanation:
Host-to-Site, or Client-to-Site, VPN allows for remote servers, clients, and other hosts to establish tunnels through a VPN gateway (or VPN headend) via a private network. The tunnel between the headend and the client host encapsulates and encrypts data.

NEW QUESTION 171
- (Topic 3)
Which of the following cloud components can filter inbound and outbound traffic between cloud resources?

A. NAT gateways
B. Service endpoints
C. Network security groups
D. Virtual private cloud

Answer: C

Explanation:
Network security groups are cloud components that can filter inbound and outbound traffic between cloud resources based on rules and priorities. Network security groups can be applied to virtual machines, subnets, or network interfaces to control the network access and security. Network security groups can allow or deny traffic based on the source, destination, port, and protocol of the packets. Network security groups are different from NAT gateways, service endpoints, and virtual private clouds, which are other cloud components that have different functions and purposes.
References
? 1: Network Security Groups – N10-008 CompTIA Network+ : 3.2
? 2: CompTIA Network+ N10-008 Certification Study Guide, page 329-330
? 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 17
? 4: CompTIA Network+ N10-008 Certification Practice Test, question 10

NEW QUESTION 173
- (Topic 3)
An organization would like to implement a disaster recovery strategy that does not require a facility agreement or idle hardware. Which of the following strategies MOST likely meets the organization's requirements?

A. Cloud site
B. Cold site

C. Warm site
D. Hot site

Answer: A

Explanation:
A cloud site is a type of disaster recovery site that uses cloud computing services to provide backup and recovery of data and applications in the event of a disaster1. A cloud site does not require a facility agreement or idle hardware, as the cloud provider manages the infrastructure and resources on demand. A cloud site can also offer scalability, flexibility, and cost-effectiveness compared to other types of disaster recovery sites.

NEW QUESTION 174
- (Topic 3)
A security team updated a web server to require https:// in the URL. Although the IP address did not change, users report being unable to reach the site. Which of the following should the security team do to allow users to reach the server again?

A. Configure the switch port with the correct VLAN.
B. Configure inbound firewall rules to allow traffic to port 443.
C. Configure the router to include the subnet of the server.
D. Configure the server with a default route.

Answer: B

Explanation:
One possible reason why users are unable to reach the site after the security team updated the web server to require https:// in the URL is that the firewall rules are blocking the traffic to port 443. Port 443 is the default port for HTTPS, which is the protocol that encrypts and secures the web communication. If the firewall rules do not allow inbound traffic to port 443, then users will not be able to access the web server using HTTPS12.
To troubleshoot this issue, the security team should configure inbound firewall rules to allow traffic to port 443. This can be done by using the firewall-cmd command on RHEL 8.2, which is a tool that manages firewalld, the default firewall service on RHEL. The command to add a rule to allow traffic to port 443 is:
firewall-cmd --permanent --add-port=443/tcp
The --permanent option makes the rule persistent across reboots, and the --add-port option specifies the port number and protocol (TCP) to allow. After adding the rule, the security
team should reload the firewalld service to apply the changes: firewall-cmd --reload
The security team can verify that the rule is active by using this command:
firewall-cmd --list-ports
The output should show 443/tcp among the ports that are allowed34.
The other options are not relevant to troubleshooting this issue. Configuring the switch port with the correct VLAN may help with network segmentation or isolation, but it will not affect the HTTPS protocol or port. Configuring the router to include the subnet of the server may help with network routing or connectivity, but it will not enable HTTPS communication. Configuring the server with a default route may help with network access or reachability, but it will not allow HTTPS traffic.

NEW QUESTION 177
- (Topic 3)
A network administrator is in the process of installing 35 PoE security cameras. After the administrator installed and tested the new cables, the administrator installed the cameras. However, a small number of the cameras do not work. Which of the following is the most likely reason?

A. Incorrect wiring standard
B. Power budget exceeded
C. Signal attenuation
D. Wrong voltage

Answer: B

Explanation:
The power budget is the total amount of power that a PoE switch or injector can provide to the connected PoE devices. If the power budget is exceeded, some of the PoE devices may not receive enough power to function properly. To troubleshoot this issue, the network administrator should check the power consumption of each PoE device and the power capacity of the PoE switch or injector.
References:
? PoE Troubleshooting: The Common PoE Errors and Solutions1
? Security Camera Won't Work - Top 10 Solutions to Fix2
? CompTIA Network+ N10-008 Exam Objectives https://www.comptia.org/certifications/network#examdetails

NEW QUESTION 180
- (Topic 3)
Which of the following can be used to limit the ability of devices to perform only HTTPS connections to an internet update server without exposing the devices to the public internet?

A. Allow connections only to an internal proxy server.
B. Deploy an IDS system and place it in line with the traffic.
C. Create a screened network and move the devices to it.
D. Use a host-based network firewall on each device.

Answer: A

Explanation:
An internal proxy server is a server that acts as an intermediary between internal devices and external servers on the internet. An internal proxy server can be used to limit the ability of devices to perform only HTTPS connections to an internet update server by filtering and forwarding the requests and responses based on predefined rules or policies. An internal proxy server can also prevent the devices from being exposed to the public internet by hiding their IP addresses and providing a layer of security and privacy.

NEW QUESTION 181

- (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 186
- (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 187
- (Topic 3)
A network deployment engineer is deploying a new single-channel 10G optical connection. Which of the following optics should the engineer MOST likely use to satisfy this requirement?

A. QSFP
B. QSFP+
C. SFP
D. SFP+

Answer: D

Explanation:
SFP+ is a type of optical transceiver that supports 10G single-channel transmission over fiber optic cables. SFP+ stands for small form-factor pluggable plus, and it is compatible with SFP slots on switches and routers.

NEW QUESTION 192
- (Topic 3)
A network engineer is concerned about VLAN hopping happening on the network. Which of the following should the engineer do to address this concern?

A. Configure private VLANS.
B. Change the default VLAN.
C. Implement ACLs on the VLAN.
D. Enable dynamic ARP inspection.

Answer: B

Explanation:
VLAN hopping is a type of attack that allows an attacker to access or manipulate traffic on a different VLAN than the one they are connected to. One way to prevent VLAN hopping is to change the default VLAN on a switch. The default VLAN is the VLAN that is assigned to all ports on a switch by default, usually VLAN 1. If an attacker connects to an unused port on a switch that has not been configured with a specific VLAN, they can access or spoof traffic on the default VLAN. By changing the default VLAN to an unused or isolated VLAN, the network administrator can prevent unauthorized access or interference with legitimate traffic on other VLANs. References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 308)

NEW QUESTION 194
- (Topic 3)

While using a secure conference call connection over a corporate VPN, a user moves from a cellular connection to a hotel wireless network. Although the wireless connection and the VPN show a connected status, no network connectivity is present. Which of the following is the most likely cause of this issue?

A. MAC filtering is configured on the wireless connection.
B. The VPN and the WLAN connection have an encryption protocol mismatch.
C. The WLAN is using a captive portal that requires further authentication.
D. Wireless client isolation is enforced on the WLAN settings.

Answer: C

Explanation:
A captive portal is a web page that is displayed to newly connected users of a Wi-Fi network before they are granted broader access to network resources. Captive portals are commonly used to present a landing or log-in page which may require authentication, payment, acceptance of an end-user license agreement, acceptable use policy, survey completion, or other valid credentials that both the host and user agree to adhere by123
A possible cause of the issue is that the user has not completed the captive portal authentication process, which prevents the VPN from establishing a secure connection over the Wi-Fi network. The user may need to open a web browser and follow the instructions on the captive portal page to gain full access to the internet.

NEW QUESTION 195
- (Topic 3)
A network administrator received complaints of intermittent network connectivity issues. The administrator investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?

A. Enable spanning tree.
B. Configure port security.
C. Change switch port speed limits.
D. Enforce 802. IQ tagging.

Answer: A

Explanation:
Spanning tree is a protocol that prevents network loops by dynamically disabling or enabling switch ports based on the network topology. Network loops can cause intermittent connectivity issues, such as broadcast storms, MAC address table instability, and multiple frame transmission. By enabling spanning tree, the network administrator can ensure that there is only one active path between any two network devices at any given time. References:
? CompTIA Network+ N10-008 Certification Exam Objectives, page 91
? CompTIA Network+ Cert Guide: Switching and Virtual LANs, page 172

NEW QUESTION 199
- (Topic 3)
A company has been added to an unapproved list because of spam. The network administrator confirmed that a workstation was infected by malware. Which of the following processes did the administrator use to identify the root cause?

A. Traffic analysis
B. Availability monitoring
C. Baseline metrics
D. Network discovery

Answer: A

Explanation:
One possible process that the administrator used to identify the root cause of the spam issue is traffic analysis. Traffic analysis is a technique that monitors and analyzes the network traffic that flows between devices or applications. Traffic analysis can help troubleshoot network problems by identifying the source, destination, volume, frequency, and content of the network packets12.
To use traffic analysis to identify the root cause of the spam issue, the administrator could follow these steps:
? Install a traffic analysis tool on the server or a device that is connected to the same
network as the server, such as Wireshark3, tcpdump4, or Microsoft Network Monitor5.
? Start capturing the network traffic and filter it by using the IP address or hostname
of the server, or by using a specific port or protocol that is used by the email service, such as SMTP (port 25), POP3 (port 110), or IMAP (port 143).
? Analyze the filtered traffic and look for any signs of abnormal or malicious activity, such as high volume of outgoing emails, unknown recipients, suspicious attachments, or spam keywords.
? Trace back the source of the spam emails to the infected workstation by using its IP address or MAC address.
? Isolate and clean up the infected workstation by using an antivirus or malware removal tool.
The other options are not processes that the administrator used to identify the root cause of the spam issue. Availability monitoring is a technique that measures and reports the uptime and downtime of a network device or service. Availability monitoring can help troubleshoot network problems by detecting any failures or outages that affect the network performance. Baseline metrics are a set of standard measurements that establish the normal behavior or performance of a network device or service. Baseline metrics can help troubleshoot network problems by comparing the current state of the network with the expected state and identifying any deviations or anomalies. Network discovery is a technique that scans and maps the network devices and services that are connected to a network. Network discovery can help troubleshoot network problems by providing a comprehensive and updated view of the network topology and configuration.

NEW QUESTION 202
- (Topic 3)
An on-call network technician receives an automated email alert stating that a power supply on a firewall has just powered down. Which of the following protocols would best allow for this level of detailed device monitoring?

A. TFTP
B. TLS
C. SSL
D. SNMP

Answer: D

Explanation:
SNMP stands for Simple Network Management Protocol, and it is a protocol that allows network devices to communicate their status, performance, and configuration information to a central management system. SNMP can be used to monitor and manage various aspects of network devices, such as CPU usage, memory utilization, interface statistics, temperature, voltage, power supply, etc. SNMP can also generate alerts or notifications when certain events or thresholds are reached, such as a power supply failure, a link down, or a high traffic volume. SNMP is widely used for network monitoring and troubleshooting purposes, as it provides a comprehensive and detailed view of the network health and performance.
The other options are not correct because they are not protocols that allow for detailed device monitoring. They are:
? TFTP. TFTP stands for Trivial File Transfer Protocol, and it is a protocol that allows for simple and fast file transfer between network devices. TFTP is often used to transfer configuration files, firmware updates, or boot images to network devices, such as routers, switches, or firewalls. TFTP does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.
? TLS. TLS stands for Transport Layer Security, and it is a protocol that provides encryption and authentication for data transmission over a network. TLS is often used to secure web traffic, email, or other applications that use TCP as the transport protocol. TLS does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.
? SSL. SSL stands for Secure Sockets Layer, and it is a protocol that provides encryption and authentication for data transmission over a network. SSL is the predecessor of TLS, and it is still used to secure some web traffic, email, or other applications that use TCP as the transport protocol. SSL does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.
References1: What is SNMP? - Definition from WhatIs.com2: Network+ (Plus) Certification
| CompTIA IT Certifications3: What is TFTP? - Definition from WhatIs.com4: What is TLS? - Definition from WhatIs.com5: What is SSL? - Definition from WhatIs.com

NEW QUESTION 205
- (Topic 3)
An ISP is unable to provide services to a user in a remote area through cable and DSL. Which of the following is the NEXT best solution to provide services without adding external infrastructure?

A. Fiber
B. Leased line
C. Satellite
D. Metro optical

Answer: C

Explanation:
 If an ISP is unable to provide services to a user in a remote area through cable and DSL, the next best solution to provide services without adding external infrastructure would likely be satellite. Satellite is a wireless communication technology that uses a network of satellites orbiting the Earth to transmit and receive data. It is well-suited for providing connectivity to remote or rural areas where other types of infrastructure may not be available or may be cost-prohibitive to install.

NEW QUESTION 206
- (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 209
- (Topic 3)
A coffee shop owner hired a network consultant to provide recommendations for installing a new wireless network. The coffee shop customers expect high speeds even when the network is congested. Which of the following standards should the consultant recommend?

A. 802.11ac
B. 802.11ax
C. 802.11g
D. 802.11n

Answer: B

Explanation:
 802.11ax is the latest and most advanced wireless standard, providing higher speeds, lower latency, and more capacity than previous standards. It also supports OFDMA, which allows multiple devices to share a channel and reduce congestion. The other options are older standards that have lower bandwidth, range, and efficiency than 802.11ax. Therefore, 802.11ax is the best option for the coffee shop owner who wants to provide high speeds even when the network is congested.

NEW QUESTION 211
- (Topic 3)
Which of the following fouling protocols is generally used by major ISPs for handing large- scale internet traffic?

A. RIP

B. EIGRP
C. OSPF
D. BGP

Answer: D

NEW QUESTION 212
- (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 216
- (Topic 3)
A business purchased redundant internet connectivity from two separate ISPs. Which of the following is the business MOST likely implementing?

A. NIC teaming
B. Hot site
C. Multipathing
D. Load balancing

Answer: C

Explanation:
Multipathing is a technique that allows a device to use more than one path to communicate with another device. This provides redundancy, load balancing, and fault tolerance for network connections. A business that purchased redundant internet connectivity from two separate ISPs is most likely implementing multipathing to ensure continuous access to the internet in case one ISP fails or becomes
congested. References: CompTIA Network+ N10-008 Certification Study Guide, page 437; The Official CompTIA Network+ Student Guide (Exam N10-008), page 16-8.

NEW QUESTION 221
- (Topic 3)
A network administrator is troubleshooting a connection to a remote site. The administrator runs a command and sees the following output:

```
Tracing route to 10.10.0.22 over a maximum of 30 hops:
1    14ms    20ms    15ms    192.168.1.253
2    10ms    15ms    12ms    172.16.0.21
3    5ms     10ms    10ms    10.10.5.3
4    10ms    15ms    12ms    10.12.2.1
5    5ms     10ms    10ms    10.10.5.3
6    10ms    15ms    12ms    10.12.2.1
7    5ms     10ms    10ms    10.10.5.3
8    10ms    15ms    12ms    10.12.2.1
```

Which of the following is the cause of the connection issue?

A. Routing loop
B. Asymmetrical routing
C. Broadcast storm
D. Switching loop

Answer: A

Explanation:
The cause of the connection issue is a routing loop. A routing loop is a situation where a packet is forwarded in circles between routers, never reaching its destination. A routing loop can be caused by misconfigured or inconsistent routing tables, or by routing protocols that do not update their information properly. A routing loop can be detected by using the traceroute command, which shows the path taken by a packet from the source to the destination. The traceroute output in the image shows that the packet is bouncing back and forth between two routers, 10.12.2.1 and 10.12.2.2, indicating a routing loop. References: CompTIA Network+ N10-008 Certification Study Guide, page 181; The Official CompTIA Network+ Student Guide (Exam N10-008), page 7-9.

NEW QUESTION 222
- (Topic 3)
Which of the following can be used to store various types of devices and provide
contactless delivery to users?

A. Asset tags
B. Biometrics
C. Access control vestibules
D. Smart lockers

Answer: D

NEW QUESTION 227
- (Topic 3)
A network administrator is looking for a solution to extend Layer 2 capabilities and replicate backups between sites. Which of the following is the best solution?

A. Security Service Edge
B. Data center interconnect
C. Infrastructure as code
D. Zero trust architecture

Answer: B

Explanation:
Data center interconnect (DCI) is a solution that allows Layer 2 connectivity and data replication between geographically dispersed data centers. DCI can be implemented using various technologies, such as optical networks, MPLS, VPNs, or Ethernet. DCI can provide benefits such as improved disaster recovery, load balancing, resource pooling, and cloud services.
References:
? Data Center Interconnect - CompTIA Network+ N10-008 Domain 1.4 - YouTube1
? CompTIA Network+ Certification Exam Objectives, page 92

NEW QUESTION 231
- (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 233
- (Topic 3)
A network administrator is creating a VLAN that will only allow executives to connect to a data source. Which of the following is this scenario an example of?

A. Availability
B. Confidentiality
C. Internal threat
D. External threat
E. Integrity

Answer: B

Explanation:

Confidentiality is the principle of preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information1. By creating a VLAN that will only allow executives to connect to a data source, the network administrator is implementing a form of network segmentation that enhances the confidentiality of the data. This prevents unauthorized users or processes from accessing or modifying the data, which could compromise its integrity or availability. Confidentiality is one of the components of the CIA triad, a widely used information security model that guides the efforts and policies aimed at keeping data secure234.
ReferencesDefending Your Network: A Comprehensive Guide to VLAN Hopping AttacksThe CIA triad: Definition, components and examples | CSO OnlineExecutive Summary — NIST SP 1800-25 documentationThe CIA Triad — Confidentiality, Integrity, and Availability ExplainedConfidentiality, Integrity and Availability - DevQA.io

NEW QUESTION 235
- (Topic 3)
A network technician is configuring a wireless network that consists of multiple APS for better coverage and allows roaming between the APS. Which of the following types of SSIDs should the technician configure?

A. Basic Service Set
B. Independent Basic Service Set
C. Extended Service Set
D. Distribution System Service

Answer: C

Explanation:

An extended service set (ESS) is a type of SSID that allows multiple access points (APs) to share the same SSID and provide seamless roaming for wireless clients. An ESS consists of two or more basic service sets (BSSs), which are individual APs with their own SSIDs. A distribution system (DS), such as a wired Ethernet LAN, connects the BSSs and enables data transfer between them. A wireless client can associate with any AP in the ESS and move from one BSS to another without losing connectivity or reauthenticating.

References:
? CompTIA Network+ N10-008 Certification Exam Objectives, page 51
? CompTIA Network+ Cert Guide: Wireless Networking, page 12

NEW QUESTION 240
- (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 241
- (Topic 3)
A non-employee was able to enter a server room. Which of the following could have prevented this from happening?

A. A security camera
B. A biometric reader
C. OTP key fob
D. Employee training

Answer: B

Explanation:
A biometric reader is a device that scans a person's physical characteristics, such as fingerprints, iris, or face, and compares them to a database of authorized users. A biometric reader can be used to restrict access to a server room and prevent unauthorized entry. A biometric reader provides a high level of security and cannot be easily bypassed or duplicated.
References: Network+ Study Guide Objective 5.1: Summarize the importance of physical security controls.

NEW QUESTION 243
- (Topic 3)
Switch 3 was recently added lo an existing stack to extend connectivity to various parts of the network. After the update, new employees were not able to print to the main networked copiers from then workstations. Following are the port configurations for the switch stack in question:

Switch 1:

	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	60	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Active	Active	Active	Active

Switch 2:

	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	60	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Active	Shut down	Active	Active

Switch 3:

	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	80	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Shut down	Shut down	Shut down	Active

Which of the following should be configured to resolve the issue? (Select TWO).

A. Enable the printer ports on Switch 3.
B. Reconfigure the duplex settings on the printer ports on Switch 3.
C. Reconfigure the VLAN on an printer ports to VLAN 20.
D. Enable all ports that are shut down on me stack.
E. Reconfigure the VLAN on the printer ports on Switch 3.
F. Enable wireless APs on Switch 3.

Answer: AE

NEW QUESTION 248
- (Topic 3)
A technician needs to configure a routing protocol for an internet-facing edge router. Which of the following routing protocols will the technician MOST likely use?

A. BGP
B. RIPv2
C. OSPF
D. EIGRP

Answer: A

NEW QUESTION 251
- (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 253
- (Topic 3)
A network administrator needs to set up a file server to allow user access. The organization uses DHCP to assign IP addresses. Which of the following is the best solution for the administrator to set up?

A. A separate scope for the file server using a 132 subnet
B. A reservation for the server based on the MAC address
C. A static IP address within the DHCP IP range
D. A SLAAC for the server

Answer: B

Explanation:
A reservation for the server based on the MAC address means that the DHCP server will assign a specific IP address to the file server every time it requests one, based on its MAC address. This way, the file server will have a consistent IP address that users can access, without the need to manually configure it or use a separate scope. A reservation also ensures that the IP address of the file server will not be given to any other device by the DHCP server

NEW QUESTION 256
- (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 260
- (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 264
- (Topic 3)
Which of the following is the first step a network administrator should take in the troubleshooting methodology?

A. Establish a plan of action.
B. Document findings and outcomes.
C. Test the theory to determine cause.
D. Identify the problem.

Answer: D

Explanation:
According to the network troubleshooting methodology, the first step a network administrator should take is to identify the problem. This involves gathering information from the users, the network devices, and the symptoms of the issue. Identifying the problem helps to narrow down the scope and the possible causes of the network issue. References
? 1: Network troubleshooting methodology | CompTIA Network+ N10-008 …
? 2: Chapter 21. A Network Troubleshooting Methodology - CompTIA Network+ …
? 3: Network Troubleshooting Methodology – N10-008 CompTIA Network+ : 5.1

NEW QUESTION 266
- (Topic 3)
Which of the following devices and encapsulations are found at the data link layer? (Select two).

A. Session
B. Frame
C. Firewall
D. Switch

E. Packet
F. Router

Answer: BD

Explanation:
A frame is a unit of data that is transmitted at the data link layer of the OSI model. A frame consists of a header, a payload, and a trailer. The header contains information such as the source and destination MAC addresses, the frame type, and the error detection code. The payload contains the data from the upper layer protocols, such as IP packets. The trailer contains the frame check sequence, which is used to verify the integrity of the frame. A switch is a device that operates at the data link layer of the OSI model. A switch forwards frames based on the MAC addresses of the devices connected to its ports. A switch can create separate collision domains and reduce network congestion. A switch can also implement VLANs, which are logical groups of devices that share the same broadcast domain, regardless of their physical location. A session is a logical connection between two or more devices that allows the exchange of data at the transport layer of the OSI model. A session is not a device or an encapsulation at the data link layer. A firewall is a device that operates at the network layer or the application layer of the OSI model. A firewall filters packets based on the IP addresses, ports, protocols, or application rules. A firewall is not a device or an encapsulation at the data link layer. A packet is a unit of data that is transmitted at the network layer of the OSI model. A packet consists of a header and a payload. The header contains information such as the source and destination IP addresses, the protocol type, and the hop count. The payload contains the data from the upper layer protocols, such as TCP segments. A packet is not an encapsulation at the data link layer. A router is a device that operates at the network layer of the OSI model. A router forwards packets based on the IP addresses and the routing table. A router can create separate broadcast domains and connect different networks. A router is not a device or an
encapsulation at the data link layer. References: CompTIA Network+ N10-008 Cert Guide, Chapter 2, Section 2.2 and CompTIA Network+ N10-008 Cert Guide, Chapter 3, Section 3.1

NEW QUESTION 267
- (Topic 3)
A store owner would like to have secure wireless access available for both business equipment and patron use. Which of the following features should be configured to allow different wireless access through the same equipment?

A. MIMO
B. TKIP
C. LTE
D. SSID

Answer: D

Explanation:
SSID stands for Service Set Identifier and is the name of a wireless network. A wireless access point (WAP) can support multiple SSIDs, which allows different wireless access through the same equipment. For example, the store owner can create one SSID for business equipment and another SSID for patron use, and assign different security settings and bandwidth limits for each SSID. MIMO stands for Multiple Input Multiple Output and is a technology that uses multiple antennas to improve wireless performance. TKIP stands for Temporal Key Integrity Protocol and is an encryption method for wireless networks. LTE stands for Long Term Evolution and is a cellular network technology. References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.1: Given a scenario, install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

NEW QUESTION 271
- (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 273
- (Topic 3)
A network administrator is investigating reports about network performance and finds high utilization on a switch uplink. The administrator is unsure whether this is an anomaly or normal behavior that will require an upgrade to resolve. Which Of the following should the administrator reference to gain historical perspective?

A. Device configuration review

B. ARP table export
C. Service-level agreement
D. Network performance baseline

Answer: D

Explanation:
 A network performance baseline is a set of metrics that represents the normal or expected behavior of a network under various conditions and scenarios. A network performance baseline can help a network administrator to investigate reports about network performance by comparing the current metrics with the historical metrics and identifying any deviations or anomalies. A network performance baseline can also help to plan and justify network upgrades by showing the trends and patterns of network utilization and performance over time.
A device configuration review is a process that involves checking and verifying the settings and parameters of a network device, such as a switch, router, firewall, or server. A device
configuration review can help a network administrator to troubleshoot network issues by finding and fixing any errors, inconsistencies, or vulnerabilities in the device configuration. A device configuration review can also help to ensure compliance with security policies and best practices by applying the latest updates and patches to the device.
An ARP table export is a file that contains the contents of the ARP (Address Resolution Protocol) table of a network device. The ARP table is a data structure that maps IP addresses to MAC addresses on a local network. An ARP table export can help a network administrator to monitor and manage the network devices on a local network by showing their IP addresses and MAC addresses. An ARP table export can also help to detect and prevent ARP spoofing attacks by identifying any duplicate or malicious entries in the ARP table.
A service-level agreement (SLA) is a contract that defines the expectations and responsibilities of both parties in terms of service quality, availability, performance, and response time. An SLA can help a network administrator to provide and maintain a satisfactory level of service to the customers or users of the network by setting and measuring specific goals and metrics. An SLA can also help to resolve any disputes or issues that may arise between the service provider and the service consumer by establishing clear terms and conditions for the service delivery.

NEW QUESTION 274
- (Topic 3)
A Wi-Fi network was originally configured to be able to handle interference from a microwave oven. The microwave oven was recently removed from the office. Now the network administrator wants to optimize the system to maximize the range of the signal. The main sources of signal degradation are the numerous cubicles and wooden walls between the WAP and the intended destination. Which of the following actions should the administrator take?

A. Implement CDMA.
B. Change from omni to directional.
C. Change the SSID.
D. Change the frequency.

Answer: D

Explanation:
 - the microwave was already removed from the office
- the signal is OK now
- Notice that the question mentions "numerous cubicles and wooden walls" - meaning the signal now won't have the interference as before
- KEY POINT: the admin wants to "maximize the range of the signal:"
Manually change the frequency to 2.4 GHz for more reliable speeds and range. While 5 GHz gives you a stronger signal, it doesn't travel through walls or ceilings as well, so it doesn't give you the best range.
"Microwave ovens: Older microwave ovens, which might not have sufficient shielding, can emit relatively high-powered signals in the 2.4GHz band, resulting in significant interference with WLAN devices operating in the 2.4GHz band."

NEW QUESTION 276
- (Topic 3)
A SQL server connects over port:

A. 445.
B. 995
C. 1433.
D. 1521.

Answer: C

Explanation:
 A SQL server connects over port 1433. Port numbers are used to identify specific applications or services on a network device. Port 1433 is the default port for Microsoft SQL Server, which is a relational database management system that uses SQL (Structured Query Language) to store and manipulate data. References: CompTIA Network+ N10-008 Certification Study Guide, page 147; The Official CompTIA Network+ Student Guide (Exam N10-008), page 6-4.

NEW QUESTION 278
- (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 282

- (Topic 3)
A network engineer is configuring new switches. Some of the trunk ports are in a blocking state. Which of the following should the network engineer reconfigure?

A. STP
B. Port mirroring
C. Flow control
D. LACP

Answer: A

Explanation:
STP (Spanning Tree Protocol) is a protocol that prevents loops in a network by placing some of the switch ports in different states, such as blocking, listening, learning, forwarding, or disabled. A port in the blocking state does not forward frames or participate in frame forwarding. A network engineer can reconfigure STP to change the port states and avoid blocking ports that are needed for trunking.

NEW QUESTION 284
- (Topic 3)
A new office space is being designed. The network switches are up. but no services are running yet A network engineer plugs in a laptop configured as a DHCP client to a switch Which ol the following IP addresses should be assigned to the laptop?

A. 10.1.1.1
B. 169.254.1.128
C. 172 16 128 128
D. 192 168.0.1

Answer: B

Explanation:
 When a DHCP client is connected to a network and no DHCP server is available, the client can automatically configure a link-local address in the 169.254.0.0/16 range using the Automatic Private IP Addressing (APIPA) feature. So, the correct answer is option B, 169.254.1.128. This is also known as an APIPA address.
Reference: CompTIA Network+ Study Guide, Exam N10-007, Fourth Edition, by Todd
Lammle (Chapter 4: IP Addressing)

NEW QUESTION 289
- (Topic 3)
Which of the following is a major difference between a router and a Layer 3 switch?

A. A router can perform PAT, but a Layer 3 switch cannot.
B. A Layer 3 switch is more efficient than a router.
C. A router uses higher speed interfaces than a Layer 3 switch.
D. A Layer 3 switch can run more routing protocols than a router.

Answer: A

Explanation:
PAT (Port Address Translation) is a type of Network Address Translation (NAT) that allows multiple devices to share a single public IP address by using different port numbers. PAT enables devices to access the internet without exposing their private IP addresses. A router is a device that can perform PAT by translating the source IP address and port number of outgoing packets and the destination IP address and port number of incoming packets. A Layer 3 switch is a device that can perform basic routing functions by using IP addresses, but it cannot perform PAT or other advanced routing features that a router can.

NEW QUESTION 294
- (Topic 3)
An IT technician is working on a support ticket regarding an unreachable web-site. The technician has utilized the ping command to the website, but the site is still unreachable. Which of the following tools should the technician use NEXT?

A. ipconfig
B. tracert
C. arp
D. netstat

Answer: B

Explanation:
tracert is a command-line tool that can trace the route of a packet from the source to the destination. It can show the number of hops, the IP address and hostname of each router, and the round-trip time for each hop. tracert can help the technician troubleshoot the unreachable website by identifying where the packet is dropped or delayed along the path. ipconfig is a command-line tool that can display and configure the IP settings of a network interface. arp is a command-line tool that can display and manipulate the Address Resolution Protocol (ARP) cache, which maps IP addresses to MAC addresses. netstat is a command-line tool that can display network connections, routing tables, and statistics. References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.4: Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

NEW QUESTION 298
- (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 segment that is isolated from both the internal LAN and the Internet by firewalls. A screened subnet can be used to host internet-facing hosts such as web servers, email servers, or DNS servers. A screened subnet provides an additional layer of security and prevents direct access to the internal network from the Internet.
References: Network+ Study Guide Objective 3.1: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 299
- (Topic 3)
A company is deploying a SAN at headquarters and a branch office 1, 000ml (1,609km) away that w« access small amounts of data. Which of the following types of connections would be MOST cost effective to implement?

A. ISCSI
B. FCoE
C. Ethernet
D. FC

Answer: A

Explanation:
 Mike Meyers
"Internet Small Computer Systems Interface (iSCSI) is built on top of TCP/IP, enabling devices that use the SCSI protocol to communicate across existing networks using cheap, readily available hardware."
Jason Dion
"iSCSI (IP Small Computer System Interface)
- Lower cost, built using Ethernet switches (<10 Gbps)
- Relies on configuration allowing jumbo frames over the network"

NEW QUESTION 301
- (Topic 3)
Due to a surge in business, a company is onboarding an unusually high number of salespeople. The salespeople are assigned desktops that are wired to the network. The last few salespeople to be onboarded are able to access corporate materials on the network but not sales-specific resources. Which of the following is MOST likely the cause?

A. The switch was configured with port security.
B. Newly added machines are running into DHCP conflicts.
C. The IPS was not configured to recognize the new users.
D. Recently added users were assigned to the wrong VLAN

Answer: D

NEW QUESTION 304
- (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 306
- (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 310
- (Topic 3)
A customer wants to log in t o a vendor's server using a web browser on a laptop. Which of the following would require the LEAST configuration to allow encrypted access to the server?

A. Secure Sockets Layer
B. Site-to-site VPN
C. Remote desktop gateway
D. Client-to-site VPN

Answer: A

Explanation:
SSL is a widely used protocol for establishing secure, encrypted connections between devices over the Internet. It is typically used to secure communication between web browsers and servers, and can be easily enabled on a server by installing an SSL certificate.

NEW QUESTION 315
- (Topic 3)
A company wants to mitigate unauthorized physical connectivity after implementing a hybrid work schedule. Which of the following will the company most likely configure?

A. Intrusion prevention system
B. DHCP snooping
C. ARP inspection
D. Port security

Answer: D

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

NEW QUESTION 318
- (Topic 3)
Which of the following layers is where TCP/IP port numbers identify which network application is receiving the packet and where it is applied?

A. 3
B. 4
C. 5
D. 6
E. 7

Answer: B

Explanation:
Layer 4 is where TCP/IP port numbers identify which network application is receiving the packet and where it is applied. Layer 4 is also known as the transport layer in the TCP/IP model or the OSI model. The transport layer is responsible for providing reliable or unreliable end-to-end data transmission between hosts on a network. The transport layer uses port numbers to identify and multiplex different applications or processes that communicate over the network. Port numbers are 16-bit numbers that range from 0 to 65535 and are divided into three categories: well-known ports (0-1023), registered ports (1024-49151), and dynamic ports (49152-65535). Some examples of well-known port numbers are 80 for HTTP, 443 for HTTPS, and 25 for SMTP. References: [CompTIA Network+ Certification Exam Objectives], Transport Layer - an overview | ScienceDirect Topics

NEW QUESTION 319
- (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 323
- (Topic 3)
Which of the following refers to a weakness in a mechanism or technical process?

A. Vulnerability
B. Risk
C. Exploit
D. Threat

Answer: A

Explanation:
The term that refers to a weakness in a mechanism or technical process is vulnerability. A vulnerability is a flaw or gap in a system's security that can be exploited by an attacker to gain unauthorized access, compromise data, or cause damage. A vulnerability can be caused by design errors, configuration errors, software bugs, human errors, or environmental factors. For example, an outdated software version that has known security holes is a vulnerability that can be exploited by malware or hackers. References: CompTIA Network+ N10-008 Certification Study Guide, page 342; The Official CompTIA Network+ Student Guide (Exam N10-008), page 13-7.

NEW QUESTION 326
- (Topic 3)
An IT technician installs five old switches in a network. In addition to the low port rates on these switches, they also have improper network configurations. After three hours, the network becomes overwhelmed by continuous traffic and eventually shuts down. Which Of the following is causing the issue?

A. Broadcast storm
B. Collisions
C. IP settings
D. Routing loops

Answer: A

Explanation:
A broadcast storm is a situation where a network is flooded with broadcast packets, which are sent to all devices on the network. This can consume bandwidth, cause congestion, and degrade performance. A broadcast storm can be caused by improper network configurations, such as loops or misconfigured switches. In this scenario, the old switches may have created loops or failed to filter broadcast packets, resulting in a broadcast storm that overwhelmed the network. References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.4: Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

NEW QUESTION 331
- (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 332
- (Topic 3)
A network technician is hired to review all the devices within a network and make recommendations to improve network efficiency. Which of the following should the technician do FIRST before reviewing and making any recommendations?

A. Capture a network baseline
B. Perform an environmental review.
C. Read the network logs
D. Run a bandwidth test

Answer: A

Explanation:
Before making any recommendations, a network technician should first capture a network baseline, which is a snapshot of the current performance of the network. This will give the technician a baseline to compare against after any changes are made. According to the CompTIA Network+ Study Manual, the technician should "capture the state of the network before making any changes and then compare the performance after the changes have been made. This will provide an accurate baseline to compare the performance of the network before and after the changes have been made."

NEW QUESTION 335
- (Topic 3)
A consultant is working with two international companies. The companies will be sharing cloud resources for a project. Which of the following documents would provide an agreement on how to utilize the resources?

A. MOU

B. NDA
C. AUP
D. SLA

Answer: A

Explanation:
A memorandum of understanding (MOU) is a document that describes an agreement between two or more parties on how to utilize shared resources for a project. An MOU is not legally binding, but it outlines the expectations and responsibilities of each party involved in the collaboration. An MOU can be used when two international companies want to share cloud resources for a project without creating a formal contract. References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 405)

NEW QUESTION 338
- (Topic 3)
A global company has acquired a local company. The companies are geographically separate. The IP address ranges for the two companies are as follows:
· Global company: 10.0.0.0/16
· Local company: 10.0.0.0/24
Which of the following can the network engineer do to quickly connect the two companies?

A. Assign static routing to advertise the local company's network.
B. Assign an overlapping IP address range to both companies.
C. Assign a new IP address range to the local company.
D. Assign a NAT range to the local company.

Answer: C

Explanation:
Assigning a new IP address range to the local company is the best option to quickly connect the two companies without causing any IP address conflicts or overlaps. This option requires reconfiguring the local company's network devices and updating the routing tables on both sides, but it avoids the need for any NAT or static routing solutions that may introduce additional complexity, cost, or performance issues12 References1: Connecting Networks with Overlapping IP Ranges 2: What Is Network Address Translation (NAT)?

NEW QUESTION 339
- (Topic 3)
A security engineer is installing a new IOS on the network. The engineer has asked a network administrator to ensure all traffic entering and leaving the router interface is available for the IDS. Which of the following should the network administrator do?

A. Install a network tap for the IDS
B. Configure ACLs to route traffic to the IDS.
C. Install an additional NIC into the IDS
D. Install a loopback adapter for the IDS.
E. Add an additional route on the router for the IDS.

Answer: A

Explanation:
a network tap is a way of connecting an IDS out of band, which means it does not interfere with the normal network traffic. A network tap allows you to view a copy of the network traffic transmitted over the media being tapped.

NEW QUESTION 343
- (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 348
- (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 350
- (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. IaaS
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 354
- (Topic 3)
A technician is tasked with setting up a mail server and a DNS server. The mail port should be secured and have the ability to transfer large files. Which of the following ports should be opened? (Select TWO).

A. 22
B. 53
C. 110
D. 389
E. 995
F. 3389

Answer: BE

Explanation:
 Port 53 is used for DNS, which is a service that translates domain names into IP addresses. Port 995 is used for POP3S, which is a protocol for receiving email messages securely. POP3S supports large file transfers and encryption. Therefore, these two ports should be opened for the mail server and the DNS server project

NEW QUESTION 356
- (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 358
- (Topic 3)
A network manager wants to set up a remote access system for the engineering staff. Access to this system will be over a public IP and secured with an ACL. Which of the following best describes this system?

A. VPN
B. Secure Shell
C. Jump server
D. API

Answer: C

Explanation:
A jump server is a system that allows remote access to internal devices through a single, secure device on the public network. A jump server can be configured with an access control list (ACL) to limit who can access the system and what devices they can connect to. A jump server can also use secure protocols such as

SSH or VPN to encrypt the communication between the remote user and the internal device. A jump server is different from a VPN, which creates a virtual private network between the remote user and the internal network. A jump server is also different from a secure shell, which is a protocol that allows remote command execution and file transfer. An API is an application programming interface that allows software components to interact with each other.
References:
? Other Network Appliances – SY0-601 CompTIA Security+ : 3.31

NEW QUESTION 362
- (Topic 3)
Which of the Mowing architectures reduces network latency by enforcing a limit on the number of switching devices on the frame's path between any internal hosts?

A. Spine and leaf
B. Software-defined network
C. Three-tiered
D. Collapsed core

Answer: A

Explanation:
It does this by using a two-level hierarchy of switches, where the spine switches connect to the leaf switches, which in turn connect to the end hosts. This reduces the number of hops a packet must take from one host to another, thus reducing latency. According to the CompTIA Network+ N10-008 Exam Guide, the Spine and Leaf topology is a modern architecture that is used to reduce latency in large networks.

NEW QUESTION 366
- (Topic 3)
A homeowner frequently has guests visit and would like to install a wireless router for their personal devices. The homeowner wants to ensure that the wireless router is compatible with the widest range of devices possible. Which of the following standards should a technician suggest?

A. 802 11ac
B. 802.11b
C. 802 11g
D. 802.11n

Answer: A

Explanation:
* 802.11ac is the latest wireless standard that supports the highest data rates and the most devices. It is backward compatible with previous standards such as 802.11b/g/n, so it can work with older devices as well. 802.11b is the oldest and slowest standard, 802.11g is faster but still outdated, and 802.11n is newer but not as fast or widespread as 802.11ac

NEW QUESTION 367
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual N10-009 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the N10-009 Product From:

https://www.2passeasy.com/dumps/N10-009/

Money Back Guarantee

N10-009 Practice Exam Features:

* N10-009 Questions and Answers Updated Frequently

* N10-009 Practice Questions Verified by Expert Senior Certified Staff

* N10-009 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* N10-009 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year