Exam Questions N10-009

CompTIA Network+ Exam

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

NEW QUESTION 1
- (Topic 3)
Which of the following can have multiple VLAN interfaces?

A. Hub
B. Layer 3 switch
C. Bridge
D. Load balancer

Answer: B

NEW QUESTION 2
- (Topic 3)
Which of the following would most likely affect design considerations when building out an IDF?

A. The source panel amperage
B. The fire suppression system
C. The humidity levels
D. The cable transmission speeds

Answer: B

Explanation:
The fire suppression system is a design consideration when building out an IDF because it can affect the safety and reliability of the network equipment and cabling. A fire suppression system is a system that detects and extinguishes fires in a building, using water, gas, or chemicals. Depending on the type of fire suppression system, it can have different impacts on the IDF design, such as:
? Water-based systems, such as sprinklers, can damage the network equipment and cabling if they are activated by a fire or a false alarm. Therefore, the IDF should be designed to protect the equipment and cabling from water exposure, such as using waterproof cabinets, drip pans, and conduits.
? Gas-based systems, such as clean agent systems, can displace the oxygen in the IDF and cause suffocation for anyone inside. Therefore, the IDF should be designed to allow for ventilation and air circulation, as well as warning signs and alarms to alert anyone in the IDF before the gas is released.
? Chemical-based systems, such as dry chemical systems, can leave a residue on the network equipment and cabling that can affect their performance and lifespan. Therefore, the IDF should be designed to minimize the contact between the chemical and the equipment and cabling, as well as provide a means for cleaning and restoring them after a fire.
The other options are not correct because:
? The source panel amperage is not a design consideration when building out an IDF, as it is determined by the electrical circuit and the power needs of the network equipment and cabling. The source panel amperage does not affect the layout, location, or protection of the IDF.
? The humidity levels are not a design consideration when building out an IDF, as they are controlled by the HVAC system and the ventilation of the IDF. The humidity levels do not affect the layout, location, or protection of the IDF.
? The cable transmission speeds are not a design consideration when building out an IDF, as they are determined by the type and quality of the network cabling and the network equipment. The cable transmission speeds do not affect the layout, location, or protection of the IDF.

NEW QUESTION 3
- (Topic 3)
Which of the following is the MOST appropriate use case for the deployment of a clientless VPN?

A. Secure web access to internal corporate resources.
B. Upgrade security via the use of an NFV technology
C. Connect two data centers across the internet.
D. Increase VPN availability by using a SDWAN technology.

Answer: A

NEW QUESTION 4
- (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 5
- (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 6
- (Topic 3)
A technician removes an old PC from the network and replaces it with a new PC that is unable to connect to the LAN. Which of the Mowing is MOST likely the cause of the issue?

A. Port security
B. Port tagging
C. Port aggregation
D. Port mirroring

Answer: A

Explanation:
It is most likely that the issue is caused by port security, as this is a feature that can prevent new devices from connecting to the LAN. Port tagging, port aggregation, and port mirroring are all features that are used to manage traffic on the network, but they are not related to the connectivity of new devices. If the technician has configured port security on the network and the new PC does not meet the security requirements, it will not be able to connect to the LAN.

NEW QUESTION 7
- (Topic 3)
A technician is expanding a wireless network and adding new access points. The company requires that each access point broadcast the same SSID. Which of the following should the technician implement for this requirement?

A. MIMO
B. Roaming
C. Channel bonding
D. Extended service set

Answer: D

Explanation:
An extended service set (ESS) is a wireless network that consists of two or more access points (APs) that share the same SSID and are connected by a distribution system, such as a switch or a router. An ESS allows wireless clients to roam seamlessly between different APs without losing connectivity or changing network settings. An ESS can also increase the coverage area and capacity of a wireless network

NEW QUESTION 8
- (Topic 3)
The following DHCP scope was configured for a new VLAN dedicated to a large deployment of 325 loT sensors:

DHCP network scope:	10.10.0.0/24
Exclusion range:	10.10.10.1-10.10.10.10
Gateway:	10.10.0.1
DNS:	10.10.0.2
DHCP option 66(TFTP):	10.10.10.4
DHCP option 4(NTP):	10.10.10.5

The first 244 loT sensors were able to connect to the TFTP server, download the configuration file, and register to an loT management system. The other sensors are being shown as offline. Which of the following should be performed to determine the MOST likely cause of the partial deployment of the sensors?

A. Check the gateway connectivity to the TFTP server.
B. Check the DHCP network scope.
C. Check whether the NTP server is online.
D. Check the loT devices for a hardware failure.

Answer: B

NEW QUESTION 9
- (Topic 3)
A user calls the help desk to report being unable to reach a file server. The technician logs in to the user's computer and verifies that pings fall to respond back when trying to reach the file server. Which of the following would BEST help the technician verify whether the file server is reachable?

A. netstat
B. ipconfig
C. nslookup
D. traceroute

Answer: D

Explanation:
Traceroute is a network diagnostic tool that allows you to trace the path that network packets take from one device to another. By running traceroute to the file server, the technician can see the sequence of devices and networks that the packets pass through on their way to the file server. This can help the technician to determine if there is a problem with the network connection between the user's computer and the file server, or if the issue is with the file server itself.

NEW QUESTION 10
- (Topic 3)
A company receives a cease-and-desist order from its ISP regarding prohibited torrent activity. Which of the following should be implemented to comply with the cease-and-desist order?

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

Answer: B

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

NEW QUESTION 10
- (Topic 3)
A technician discovered that some information on the local database server was changed during a tile transfer to a remote server. Which of the following should concern the technician the MOST?

A. Confidentiality
B. Integrity
C. DDoS
D. On-path attack

Answer: B

Explanation:
The technician should be most concerned about data integrity and security. If information on the local database server was changed during a file transfer to a remote server, it could indicate that unauthorized access or modifications were made to the data. It could also indicate a failure in the file transfer process, which could result in data loss or corruption. The technician should investigate the cause of the changes and take steps to prevent it from happening again in the future. Additionally, they should verify the integrity of the data and restore it from a backup if necessary to ensure that the correct and complete data is available. The technician should also take appropriate actions such as notifying the system administrator and management of the incident, and following the incident management process to minimize the damage caused by the incident.

NEW QUESTION 15
- (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 19
- (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 21
- (Topic 3)
Which of the following technologies would MOST likely De used to prevent the loss of connection between a virtual server and network storage devices?

A. Multipathing
B. VRRP

C. Port aggregation
D. NIC teaming

Answer: D

Explanation:
NIC teaming is a technology that allows multiple network interface cards (NICs) to work together as a single logical interface, providing redundancy and load balancing. This can prevent the loss of connection between a virtual server and network storage devices if one of the NICs fails or becomes disconnected.
References: [CompTIA Network+ Certification Exam Objectives], Domain 2.0 Networking Concepts, Objective 2.5: Explain the purposes and use cases for advanced networking devices, Subobjective: NIC bonding/teaming

NEW QUESTION 24
- (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 28
- (Topic 3)
Which of the following records can be used to track the number of changes on a DNS zone?

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

Answer: A

Explanation:
The DNS 'start of authority' (SOA) record stores important information about a domain or zone such as the email address of the administrator, when the domain was last updated, and how long the server should wait between refreshes. All DNS zones need an SOA record in order to conform to IETF standards. SOA records are also important for zone transfers.

NEW QUESTION 31
- (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 35
- (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 38
- (Topic 3)
Which of the following is most likely to be implemented to actively mitigate intrusions on a host device?

A. HIDS
B. MDS
C. HIPS
D. NIPS

Answer: A

Explanation:
HIDS (host-based intrusion detection system) is a type of security software that monitors and analyzes the activity on a host device, such as a computer or a server. HIDS can detect and alert on intrusions, such as malware infections, unauthorized access, configuration changes, or policy violations. HIDS can also actively mitigate intrusions by blocking or quarantining malicious processes, files, or network connections1.
HIPS (host-based intrusion prevention system) is similar to HIDS, but it can also prevent intrusions from happening in the first place by enforcing security policies and rules on the host device2. MDS (multilayer switch) is a network device that combines the functions of a switch and a router, and it does not directly protect a host device from intrusions3. NIPS (network-based intrusion prevention system) is a network device that monitors and blocks malicious traffic on the network level, and it does not operate on the host device level4.

NEW QUESTION 42
- (Topic 3)
A bank installed a new smart TV to stream online video services, but the smart TV was not able to connect to the branch Wi-Fi. The next day. a technician was able to connect the TV to the Wi-Fi, but a bank laptop lost network access at the same time. Which of the following is the MOST likely cause?

A. DHCP scope exhaustion
B. AP configuration reset
C. Hidden SSID
D. Channel overlap

Answer: A

Explanation:
DHCP scope exhaustion is the situation when a DHCP server runs out of available IP addresses to assign to clients. DHCP stands for Dynamic Host Configuration Protocol, which is a network protocol that automatically assigns IP addresses and other configuration parameters to clients on a network. A DHCP scope is a range of IP addresses that a DHCP server can distribute to clients. If the DHCP scope is exhausted, new clients will not be able to obtain an IP address and connect to the network. This can explain why the smart TV was not able to connect to the branch Wi-Fi on the first day, and why the bank laptop lost network access on the next day when the TV was connected. The technician should either increase the size of the DHCP scope or reduce the lease time of the IP addresses to avoid DHCP scope exhaustion. References: [CompTIA Network+ Certification Exam Objectives], DHCP Scope Exhaustion - What Is It? How Do You Fix It?

NEW QUESTION 44
- (Topic 3)
Which of the following focuses on application delivery?

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

Answer: C

Explanation:
SaaS is the cloud computing model that focuses on application delivery. SaaS stands for Software as a Service, which is a cloud computing model that provides software applications over the internet. SaaS allows customers to access and use software applications without installing or maintaining them on their own devices or servers. SaaS offers advantages such as scalability, accessibility, compatibility, and cost-effectiveness.
Customers can use SaaS applications on demand and pay only for what they use. References: [CompTIA Network+ Certification Exam Objectives], What Is Software as a Service (SaaS)? | IBM

NEW QUESTION 49
- (Topic 3)
A network administrator is reviewing the network device logs on a syslog server. The messages are normal but the stamps on the messages are incorrect. Which of the following actions should the administrator take to ensure the log message time stamps are correct?

A. Change the NTP settings on the network device
B. Change the time on the syslog server
C. Update the network device firmware
D. Adjust the timeout settings on the syslog server
E. Adjust the SSH settings on the network device.

Answer: A

NEW QUESTION 51
- (Topic 3)
A customer reports there is no access to resources following the replacement of switches. A technician goes to the site to examine the configuration and discovers redundant links between two switches. Which of the following is the reason the network is not functional?

A. The ARP cache has become corrupt.
B. CSMA/CD protocols have failed.
C. STP is not configured.
D. The switches are incompatible models

Answer: C

Explanation:
The reason the network is not functional is that STP (Spanning Tree Protocol) is not configured on the switches. STP is a protocol that prevents loops in a network topology by blocking redundant links between switches. If STP is not enabled, the switches will forward broadcast frames endlessly, creating a broadcast storm that consumes network resources and disrupts communication. References: CompTIA Network+ N10-008 Certification Study Guide, page 67; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-14.

NEW QUESTION 54
- (Topic 3)
Users are reporting performance issues when attempting to access the main fileshare server. Which of the following steps should a network administrator perform next based on the network troubleshooting methodology?

A. Implement a fix to resolve the connectivity issues.
B. Determine if anything has changed.
C. Establish a theory of probable cause.
D. Document all findings, actions, and lessons learned.

Answer: B

Explanation:
According to the network troubleshooting methodology, the first step is to identify the problem and gather information about the current state of the network using the network troubleshooting tools that are available1. The next step is to determine if anything has changed in the network configuration, environment, or usage that could have caused or contributed to the performance issues1. This step helps to narrow down the possible causes and eliminate irrelevant factors. For example, the network administrator could check if there were any recent updates, patches, or modifications to the fileshare server or the network devices that connect to it. They could also check if there was an increase in network traffic or demand for the fileshare server resources2.
The other options are not correct because they are not the next steps in the network troubleshooting methodology. Implementing a fix to resolve the connectivity issues (A) is premature without determining the root cause of the problem. Establishing a theory of probable cause © is a later step that requires testing and verification. Documenting all findings, actions, and lessons learned (D) is the final step that should be done after resolving the problem and restoring normal network operations1.

NEW QUESTION 58
- (Topic 3)
A network technician wants to find the shortest path from one node to every other node in the network. Which of the following algorithms will provide the FASTEST convergence time?

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

Answer: B

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

NEW QUESTION 61
- (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 65
- (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 67
- (Topic 3)
A company has multiple offices around the world. The computer rooms in some office locations are too warm Dedicated sensors are in each room, but the process of checking each sensor takes a long time. Which of the following options can the company put In place to automate temperature readings with internal resources?

A. Implement NetFlow.
B. Hire a programmer to write a script to perform the checks
C. Utilize ping to measure the response.
D. Use SNMP with an existing collector server

Answer: D

Explanation:
SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a management server. By using SNMP, the company can set up an SNMP agent on each sensor, which will report its temperature readings to an existing collector server. This will enable the company to monitor the temperatures of all their sensors in real-time without the need for manual checks. Additionally, SNMP's scalability means that even if the company adds more rooms or sensors, the existing system can be easily expanded to accommodate them.

NEW QUESTION 68
- (Topic 3)
A network technician needs to ensure that all files on a company's network can be moved in a safe and protected manner without interception from someone who is not the intended recipient. Which of the following would allow the network technician to meet these requirements?

A. FTP
B. TFTP
C. SMTP
D. SFTP

Answer: D

NEW QUESTION 71
- (Topic 3)
The power company notifies a network administrator that it will be turning off the power to the building over the weekend. Which of the following is the BEST solution to prevent the servers from going down?

A. Redundant power supplies
B. Uninterruptible power supply
C. Generator
D. Power distribution unit

Answer: A

NEW QUESTION 75
- (Topic 3)
In which of the following components do routing protocols belong in a software-defined network?

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

Answer: B

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

NEW QUESTION 80
- (Topic 3)
Due to space constraints in an IDF, a network administrator can only a do a single switch to

accommodate three data networks. The administrator needs a configuration that will allow each device to access its expected network without additional connections. The configuration must also allow each device to access the rest of the network. Which of the following should the administrator do to meet these requirements? (Select TWO).

A. Untag the three VLANs across the uplink
B. Tag an individual VLAN across the uplink
C. Untag an individual VLAN per device port
D. Tag an individual VLAN per device port
E. Tag the three VLANs across the uplink.
F. Tag the three VLANs per device port.

Answer: AC

Explanation:
To achieve this, you should do two things:
? Tag the three VLANs across the uplink port that connects to another switch or router. This will allow data packets from different VLANs to cross over into other networks.
? Untag an individual VLAN per device port that connects to an end device. This will assign each device to its expected network without additional connections.

NEW QUESTION 81
- (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 84
- (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 86
- (Topic 3)
Which of the following devices would be used to extend the range of a wireless network?

A. A repeater
B. A media converter
C. A router
D. A switch

Answer: A

Explanation:
A repeater is a device used to extend the range of a wireless network by receiving, amplifying, and retransmitting wireless signals. It is typically used to extend the range of a wireless network in a large area, such as an office building or a campus. Repeaters can also be used to connect multiple wireless networks together, allowing users to move seamlessly between networks. As stated in the CompTIA Network+ Study Manual, "a wireless repeater is used to extend the range of a wireless network by repeating the signal from one access point to another."

NEW QUESTION 90
- (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 95
- (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 96
- (Topic 3)
Which of the following is the most secure connection used to inspect and provide controlled internet access when remote employees are connected to the corporate network?

A. Site-to-site VPN
B. Full-tunnel VPN
C. Split-tunnel VPN
D. SSH

Answer: B

Explanation:
A full-tunnel VPN is a type of virtual private network (VPN) that encrypts and routes all the traffic from the remote device to the corporate network, regardless of the destination or protocol. This provides a secure connection for the remote employees to access the corporate resources, as well as inspect and control the internet access through the corporate firewall and proxy servers. A full-tunnel VPN also prevents any leakage of sensitive data or exposure to malicious attacks from the public internet. A full-tunnel VPN is more secure than a split-tunnel VPN, which only encrypts and routes the traffic destined for the corporate network, while allowing the traffic for other destinations to bypass the VPN and use the local internet connection. A site-to-site VPN is a type of VPN that connects two or more networks, such as branch offices or data centers, over the internet. It is not suitable for connecting individual remote employees to the corporate network. SSH stands for Secure Shell, and it is a protocol that allows secure remote login and command execution over an encrypted channel. It is not a type of VPN, and it does not provide
controlled internet access. References: CompTIA Network+ N10-008 Cert Guide, Chapter 5, Section 5.3

NEW QUESTION 98
- (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 101
- (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 104
- (Topic 3)
A security engineer is trying to determine whether an internal server was accessed by hosts on the internet. The internal server was shut down during the investigation Which of the following will the engineer review to determine whether the internal server had an unauthorized access attempt?

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

Answer: A

NEW QUESTION 109
- (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 111
- (Topic 3)
A user reports that a new VoIP phone works properly, but the computer that is connected to the phone cannot access any network resources. Which of the following MOST likely needs to be configured correctly to provide network connectivity to the computer?

A. Port duplex settings
B. Port aggregation
C. ARP settings
D. VLAN tags
E. MDIX settings

Answer: A

NEW QUESTION 112
- (Topic 3)
Which of the following should be used to manage outside cables that need to be routed to various multimode uplinks?

A. Fiber distribution panel
B. 110 punchdown block
C. PDU
D. TIA/EIA-568A patch bay

E. Cat 6 patch panel

Answer: A

Explanation:
A fiber distribution panel is a device that provides a central location for connecting and managing fiber optic cables and optical modules. It can support various types and speeds of fiber optic links, including multimode uplinks. Therefore, a fiber distribution panel should be used to manage outside cables that need to be routed to various multimode uplinks.

NEW QUESTION 114
- (Topic 3)
Which of the following would be BEST suited for a long cable run with a 40Gbps bandwidth?

A. Cat 5e
B. Cat 6a
C. Cat 7
D. Cat 8

Answer: C

Explanation:
Cat 7 is a type of twisted-pair copper cable that supports up to 40 Gbps bandwidth and up to 100 meters cable length. Cat 7 is suitable for long cable runs that require high-speed data transmission. Cat 7 has better shielding and crosstalk prevention than lower categories of cables.
References: Network+ Study Guide Objective 1.5: Compare and contrast network cabling types, features and their purposes.

NEW QUESTION 119
- (Topic 3)
A Chief Executive Officer and a network administrator came to an agreement With a vendor to purchase new equipment for the data center A document was drafted so all parties would be Informed about the scope of the project before It started. Which of the following terms BEST describes the document used?

A. Contract
B. Project charter
C. Memorandum of understanding
D. Non-disclosure agreement

Answer: B

Explanation:
The document used to inform all parties about the scope of the project before it starts is likely a project charter.
A project charter is a document that outlines the key aspects of a project, including the project's objectives, scope, stakeholders, and resources. It serves as a formal agreement between the project team and the stakeholders, and helps to define the project's goals and constraints.
A project charter typically includes information about the project's scope, including the specific deliverables that are expected and any constraints or limitations that may impact the project. It may also include details about the project team and stakeholders, the project schedule and budget, and the roles and responsibilities of each party.
By creating a project charter, the Chief Executive Officer and the network administrator can ensure that all parties involved in the project have a clear understanding of the project's goals and objectives, and can help to prevent misunderstandings or miscommunications during the project.
What is in a project charter?
A project charter is a formal short document that states a project exists and provides project managers with written authority to begin work. A project charter document describes a project to create a shared understanding of its goals, objectives and resource requirements before the project is scoped out in detail.
What are the 5 elements of the project charter?
What Are the Contents of a Project Charter? A project charter should always include an overview, an outline of scope, an approximate schedule, a budget estimate, anticipated risks, and key stakeholders

NEW QUESTION 120
- (Topic 3)
Which of the following issues are present with RIPv2? (Select TWO).

A. Route poisoning
B. Time to converge
C. Scalability
D. Unicast
E. Adjacent neighbors
F. Maximum transmission unit

Answer: BC

Explanation:
The disadvantages of RIP (Routing Information Protocol) include the following.
---Outdated, insecure, and slow. This is your parents' protocol. It was a thing before the Web was born.
---The more well-known problem of the 15 hop limitation in which data must travel
---Convergence time is terrible for information propagation in a network
---Metrics. It determines the number of hops from source to destination, and gives no regard to other factors when determining the best path for data to travel
---Overhead. A good example would be routing tables. These are broadcast at half-minute intervals to other routers regardless of whether the data has changed or not. It's essentially like those old cartoons where the town guard in the walled city cries out, '10 o' the clock and all is well!'.
RIPv2 introduced more security and reduced broadcast traffic, which is relevant for some available answers here.

NEW QUESTION 123
- (Topic 3)
A network technician recently installed 35 additional workstations. After installation, some users are unable to access network resources. Many of the original

workstations that are experiencing the network access issue were offline when the new workstations were turned on. Which of the following is the MOST likely cause of this issue?

A. Incorrect VLAN setting
B. Insufficient DHCP scope
C. Improper NIC setting
D. Duplicate IP address

Answer: B

NEW QUESTION 126
- (Topic 3)
A network technician is troubleshooting a connectivity issue. All users within the network report that they are unable to navigate to websites on the internet; however, they can still access local network resources. The technician issues a command and receives the following results:

```
Pinging comptia.com [172.67.217.56] with 32 bytes of data:
Reply from 172.67.217.56: TTL expired in transit.
Reply from 172.67.217.56: TTL expired in transit.
Reply from 172.67.217.56: TTL expired in transit.
Reply from 172.67.217.56: TTL expired in transit.
```

Which of the following best explains the result of this command?

A. Incorrect VLAN settings
B. Upstream routing loop
C. Network collisions
D. DNS misconfiguration

Answer: D

Explanation:
The users are unable to navigate to websites on the internet but can access local network resources, indicating a possible DNS issue. The ping command result showing “TTL expired in transit” suggests that packets are not reaching their destination due to a DNS misconfiguration that is not resolving website names into IP addresses correctly3. A possible solution is to check and correct the DNS server settings on the network devices4.
References: 3: What does “TTL expired in transit” mean?54: CompTIA Network+ N10-008 Cert Guide - Chapter 14: Network Monitoring2

NEW QUESTION 129
- (Topic 3)
A network client is trying to connect to the wrong TCP port. Which of the following responses would the client MOST likely receive?

A. RST
B. FIN
C. ICMP Time Exceeded
D. Redirect

Answer: A

NEW QUESTION 130
- (Topic 3)
An employee working in a warehouse facility is experiencing interruptions in mobile applications while walking around the facility. According to a recent site survey, the WLAN comprises autonomous APs that are directly connected to the internet, providing adequate signal coverage. Which of the following is the BEST solution to improve network stability?

A. Implement client roaming using an extended service deployment employing a wireless controller.
B. Remove omnidirectional antennas and adopt a directional bridge.
C. Ensure all APs of the warehouse support MIMO and Wi-Fi 4.
D. Verify that the level of EIRP power settings is set to the maximum permitted by regulations.

Answer: A

Explanation:
Client roaming refers to the ability of a wireless device to seamlessly connect to a different access point (AP) as the user moves around the facility. This can help to improve network stability and reduce interruptions in mobile applications. An extended service deployment is a type of wireless network configuration that uses multiple APs to cover a large area, such as a warehouse facility. By using a wireless controller to manage the APs, the network can be better optimized for client roaming, which can improve network stability.
"Roaming With multiple WAPs in an ESS, clients will connect to whichever WAP has the strongest signal. As clients move through the space covered by the broadcast area, they will change WAP connections seamlessly, a process called roaming."

NEW QUESTION 134
- (Topic 3)
A technician was cleaning a storage closet and found a box of transceivers labeled 8Gbps. Which of the following protocols uses those transceivers?

A. Coaxial over Ethernet
B. Internet Small Computer Systems Interface
C. Fibre Channel
D. Gigabit interface converter

Answer: C

Explanation:
The transceivers labeled 8Gbps are likely to be used with the Fibre Channel protocol. Fibre Channel is a high-speed networking technology that is primarily used to connect storage devices to servers in storage area networks (SANs). It is capable of transmitting data at speeds of up to 8 Gbps (gigabits per second), and uses specialized transceivers to transmit and receive data over fiber optic cables.
Coaxial over Ethernet (CoE) is a networking technology that uses coaxial cables to transmit data, and is not related to the transceivers in question. Internet Small Computer Systems Interface (iSCSI) is a protocol that allows devices to communicate over a network using the SCSI protocol, and does not typically use specialized transceivers. Gigabit interface converter (GBIC) is a type of transceiver used to transmit and receive data over fiber optic cables, but it is not capable of transmitting data at 8 Gbps.

NEW QUESTION 136
- (Topic 3)
A company wants to invest in new hardware for the core network infrastructure. The management team requires that the infrastructure be capable of being repaired in less than 60 minutes if any major part fails. Which of the following metrics is MOST likely associated with this requirement?

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

Answer: B

Explanation:
MTTR is directly related to how quickly a system can be repaired if any major part fails3. The management team requires that the infrastructure be capable of being repaired in less than 60 minutes, which means they have a low MTTR requirement.
MTTR stands for Mean Time To Repair and is a metric used to measure the average amount of time it takes to repair a failed component or system. In this case, the requirement is for the infrastructure to be capable of being repaired in less than 60 minutes if any major part fails, which means the MTTR should be less than 60 minutes.

NEW QUESTION 140
- (Topic 3)
Which of the following layers of the OSI model has new protocols activated when a user moves from a wireless to a wired connection?

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

Answer: A

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

NEW QUESTION 145
- (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 149
- (Topic 3)
Which of the following types of data center architectures will MOST likely be used in a large SDN and can be extended beyond the data center?

A. iSCSI
B. FCoE
C. Three-tiered network
D. Spine and leaf
E. Top-of-rack switching

Answer: D

Explanation:
The type of data center architecture that will most likely be used in a large SDN and can be extended beyond the data center is spine and leaf. Spine and leaf is a network topology that consists of two layers of switches: spine switches and leaf switches. Spine switches are interconnected to each other and form the core of the network, while leaf switches are connected to each spine switch and form the access layer of the network. Spine and leaf topology provides high scalability, performance, and flexibility for data center networks, especially for SDN (Software Defined Networking) environments that require dynamic traffic flows and virtualization. References: CompTIA Network+ N10-008 Certification Study Guide, page 16; The Official CompTIA Network+ Student Guide (Exam N10-008), page 1-9.

NEW QUESTION 153
- (Topic 3)
All packets arriving at an interface need to be fully analyzed. Which of me following features should be used to enable monitoring of the packets?

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

Answer: D

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

NEW QUESTION 157
- (Topic 3)
A company has wireless APS that were deployed with 802.11g. A network engineer has noticed more frequent reports of wireless performance issues during the lunch hour in comparison to the rest of the day. The engineer thinks bandwidth consumption will increase while users are on their breaks, but network utilization logs do not show increased bandwidth numbers. Which Of the following would MOST likely resolve this issue?

A. Adding more wireless APS
B. Increasing power settings to expand coverage
C. Configuring the APS to be compatible with 802.1la
D. Changing the wireless channel used

Answer: C

Explanation:
* 802.11g is an older wireless standard that operates in the 2.4 GHz frequency band and has a maximum data rate of 54 Mbps. 802.11a is a newer wireless standard that operates in the 5 GHz frequency band and has a maximum data rate of 54 Mbps. By configuring the APS to be compatible with 802.11a, the network engineer can reduce interference and congestion in the 2.4 GHz band and improve wireless performance.
References: Network+ Study Guide Objective 2.5: Implement network troubleshooting methodologies

NEW QUESTION 160
- (Topic 3)
Which of the following would be used to enforce and schedule critical updates with supervisory approval and include backup plans in case of failure?

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

Answer: A

NEW QUESTION 163
- (Topic 3)
To comply with an industry regulation, all communication destined to a secure server should be logged and archived on a storage device. Which of the Mowing can be configured to fulfill this requirement?

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

Answer: B

NEW QUESTION 167
- (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 171
- (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 173
- (Topic 3)
A security team would like to use a system in an isolated network to record the actions of potential attackers. Which of the following solutions is the security team implementing?

A. Perimeter network
B. Honeypot
C. Zero trust infrastructure
D. Network segmentation

Answer: B

Explanation:
The solution that the security team is implementing to record the actions of potential attackers in an isolated network is a honeypot. A honeypot is a decoy system that simulates a real network or service, but has no actual value or function. A honeypot is designed to attract and trap attackers who try to infiltrate or compromise the network, and then monitor and analyze their behavior and techniques. A honeypot can help the security team learn about the attackers’ motives, methods, and tools, and improve their defense
strategies accordingly. References: CompTIA Network+ N10-008 Certification Study Guide, page 358; The Official CompTIA Network+ Student Guide (Exam N10-008), page 14-1.

NEW QUESTION 174
- (Topic 3)
After upgrading to a SOHO router that supports Wi-Fi 6, the user determines throughput has not increased. Which of the following is the MOST likely cause of the issue?

A. The wireless router is using an incorrect antenna type.
B. The user's workstation does not support 802.11 ax.
C. The encryption protocol is mismatched
D. The network is experiencing interference.

Answer: B

Explanation:
The user’s workstation does not support 802.11 ax, which is the technical name for Wi-Fi 6. Wi-Fi 6 is a new wireless standard that offers faster speeds, higher capacity, and lower latency than previous standards. However, to take advantage of these
benefits, both the router and the workstation need to support Wi-Fi 6. If the workstation only supports an older standard, such as 802.11 ac or Wi-Fi 5, then the throughput will not increase even if the router supports Wi-Fi 6. References: [CompTIA Network+ Certification Exam Objectives], What is Wi-Fi 6? Here’s what you need to know | PCWorld

NEW QUESTION 179
- (Topic 3)

A network administrator requires redundant routers on the network, but only one default gateway is configurable on a workstation. Which of the following will allow for redundant routers with a single IP address?

A. EIGRP
B. VRRP
C. MPLS
D. STP

Answer: B

Explanation:
Virtual Router Redundancy Protocol (VRRP) is a protocol that allows for redundant routers on the network with a single IP address. VRRP works by creating a virtual router that consists of one master router and one or more backup routers. The virtual router has its own IP address and MAC address that are shared among the routers in the group. The master router responds to traffic sent to the virtual router's IP address, while the backup routers monitor the master router's status. If the master router fails, one of the backup routers takes over as the new master router and continues to respond to traffic. This way, VRRP provides high availability and fault tolerance for the network. References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 230)

NEW QUESTION 183
- (Topic 3)
A network administrator is setting up a web-based application for a company. The application needs to be continually accessible to all end users.
Which of the following would best ensure this need is fulfilled?

A. NIC teaming
B. Cold site
C. Snapshots
D. High availability

Answer: D

Explanation:
High availability is a quality of a system or component that assures a high level of operational performance for a given period of time. High availability means that an IT system, component, or application can operate at a high level, continuously, without intervention, for a given time period. High-availability infrastructure is configured to deliver quality performance and handle different loads and failures with minimal or zero downtime. High availability is important for web-based applications, as it ensures that the application is always accessible to the end users, even in the event of a server or component failure. High availability can be achieved by eliminating single points of failure, implementing redundancy, load balancing, and failover mechanisms.

NEW QUESTION 186
- (Topic 3)
A technician is investigating packet loss to a device that has varying data bursts throughout the day. Which of the following will the technician MOST likely configure to resolve the issue?

A. Flow control
B. Jumbo frames
C. Duplex
D. Port mirroring

Answer: A

Explanation:
Ethernet flow control is a mechanism for temporarily stopping the transmission of data on Ethernet family computer networks. The goal of this mechanism is to avoid packet loss in the presence of network congestion.
Flow control is a mechanism that allows a device to regulate the amount of data it receives from another device, ensuring that the receiving device is not overwhelmed with data. If the device experiencing packet loss is receiving large bursts of data at times when it is not able to process it quickly enough, configuring flow control could help prevent packets from being lost.
"In theory, flow control can help with situations like a host that can't keep up with the flow of traffic. It enables the host to send an Ethernet PAUSE frame, which asks the switch to hold up for some amount of time so the host can catch its breath. If the switch can, it'll buffer transmissions until the pause expires, and then start sending again. If the host catches up early, it can send another PAUSE frame with a delay of zero to ask the switch to resume. In practice, flow control can cause latency trouble for modern real-time applications such as VoIP, and the same needs are usually met by QoS"

NEW QUESTION 191
- (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 195
- (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 196
- (Topic 3)
A network engineer is installing hardware in a newly renovated data center. Major concerns that were addressed during the renovation induded air circulation, building power redundancy, and the need for continuous monitoring. The network engineer IS creating alerts based on the following operation specifications:

AC input voltage	100 to 240VAC
AC maximum input current	<2.7A at 100V
Redundant power supply	Yes
Operating temperature	32–104°F (0–40°C)
Storage temperature	-4–149°F (-20–65°C)
Operating humidity	10–85%
Storage humidity	5–95%

Which of the following should the network engineer configure?

A. Environmental monitoring alerts for humidity greater than 95%
B. SIEM to parse syslog events for a failed power supply
C. SNMP traps to report when the chassis temperature exceeds 950F (3500)
D. UPS monitoring to report when input voltage drops below 220VAC

Answer: C

Explanation:
The alert that the network engineer should configure based on the operation specifications is SNMP traps to report when the chassis temperature exceeds 95°F (35°C). SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate their status and performance information to a central management system, called an SNMP manager. SNMP traps are messages that are sent by network devices to notify the SNMP manager of an event or condition that requires attention, such as an error, a failure, or a threshold violation. In this case, the network engineer should configure SNMP traps on the network devices to send an alert when their chassis temperature exceeds 95°F (35°C), which is the maximum operating temperature specified in the table. This alert would help the network engineer monitor and troubleshoot any overheating issues that could affect the network performance or availability. References: CompTIA Network+ N10-008 Certification Study Guide, page 228; The Official CompTIA Network+ Student Guide (Exam N10-008), page 8-11.

NEW QUESTION 198
- (Topic 3)
An engineer needs to verity the external record tor SMTP traffic. The engineer logged in to the server and entered the nslookup command. Which of the following commands should the engineer send before entering the DNS name?

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

Answer: D

NEW QUESTION 202
- (Topic 3)
A network technician is troubleshooting a connection to a web server. The Technician Is unable to ping the server but is able to verify connectivity to the web service using Tenet. Which of the following protocols is being blocked by me firewall?

A. UDP
B. ARP
C. ICMP
D. TCP

Answer: C

Explanation:
ICMP (Internet Control Message Protocol) is a protocol that is used to send error and control messages between network devices, such as ping requests and replies. ICMP is being blocked by the firewall, which prevents the network technician from pinging the web server. TCP (Transmission Control Protocol) is a protocol that provides reliable and ordered delivery of data between network devices, such as web service requests and responses using HTTP (Hypertext Transfer Protocol). TCP is not being blocked by the firewall, which allows the network technician to verify connectivity to the web service using Telnet. UDP (User Datagram Protocol) is a protocol that provides fast and efficient delivery of data between network devices, but does not guarantee reliability or order. UDP is used

for applications such as streaming media or online gaming. ARP (Address Resolution Protocol) is a protocol that resolves IP addresses to MAC addresses on a local network. References: [CompTIA Network+ Certification Exam Objectives], Domain 2.0 Networking Concepts, Objective 2.1: Compare and contrast OSI and TCP/IP models, Subobjective: TCP/IP model layers (Application/Transport/Internet/Network Interface)

NEW QUESTION 203
- (Topic 3)
A security vendor needs to add a note to the DNS to validate the ownership of a company domain before services begin. Which of the following records did the security company MOST likely ask the company to configure?

A. TXT
B. AAAA
C. CNAME
D. SRV

Answer: A

Explanation:
TXT stands for Text and is a type of DNS record that can store arbitrary text data associated with a domain name. TXT records can be used for various purposes, such as verifying the ownership of a domain, providing information about a domain, or implementing security mechanisms such as SPF (Sender Policy Framework) or DKIM (DomainKeys Identified Mail). In this scenario, the security company most likely asked the company to configure a TXT record with a specific value that can prove the ownership of the domain. AAAA stands for IPv6 Address and is a type of DNS record that maps a domain name to an IPv6 address. CNAME stands for Canonical Name and is a type of DNS record that maps an alias name to another name. SRV stands for Service and is a type of DNS record that specifies the location of a service on a network.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.8: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 205
- (Topic 3)
Which of the following is a valid alternative to maintain a deployed proxy technology while saving physical space in the data center by moving the network service to the virtualization infrastructure?

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

Answer: A

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

NEW QUESTION 208
- (Topic 3)
A device is connected to a managed Layer 3 network switch. The MAC address of the device is known, but the static IP address assigned to the device is not. Which of the following features of a Layer 3 network switch should be used to determine the IPv4 address of the device?

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

Answer: C

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

NEW QUESTION 209
- (Topic 3)
A technician is consolidating a topology with multiple SSIDs into one unique SSiD deployment. Which of the following features will be possible after this new configuration?

A. Seamless roaming
B. Basic service set
C. WPA

D. MU-MIMO

Answer: A

NEW QUESTION 212
- (Topic 3)
A technician is configuring a static IP address on a new device in a newly created subnet. The work order specifies the following requirements:
• The IP address should use the highest address available in the subnet.
• The default gateway needs to be set to 172.28.85.94.
• The subnet mask needs to be 255.255.255.224.
Which of the following addresses should the engineer apply to the device?

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

Answer: A

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

NEW QUESTION 216
- (Topic 3)
Which of the following can be used to aggregate logs from different devices and would make analysis less difficult?

A. Syslog
B. SIEM
C. Event logs
D. NetFlow

Answer: B

Explanation:
SIEM stands for Security Information and Event Management, and it is a system that collects, normalizes, and analyzes log data from different sources in a centralized platform. SIEM can help identify security incidents, monitor network performance, and generate reports and alerts. SIEM can make log analysis less difficult by providing a unified view of the log data, correlating events across different devices, and applying rules and filters to detect anomalies and patterns12.
References: 1: CompTIA Network+ N10-008 Cert Guide - Chapter 14: Network Monitoring32: Log Aggregation: What It Is & How It Works | Datadog4

NEW QUESTION 219
- (Topic 3)
A user stores large graphic files. The lime required to transfer the files to the server is excessive due to network congestion. The user's budget does not allow for the current switches to be replaced. Which of the following can be used to provide FASTER transfer times?

A. Half duplex
B. Jumbo frames
C. LACP
D. 802.1Q

Answer: B

Explanation:
Jumbo frames are Ethernet frames that can carry more than 1500 bytes of payload data. Jumbo frames can reduce the overhead and improve the throughput of large file transfers, as fewer frames are needed to send the same amount of data. Jumbo frames can be used to provide faster transfer times, as long as the network devices support them

NEW QUESTION 222
- (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 227
- (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 229
- (Topic 3)
Which of the following protocols should be used when Layer 3 availability is of the highest concern?

A. LACP
B. LDAP
C. FHRP
D. DHCP

Answer: C

Explanation:
FHRP stands for First Hop Redundancy Protocol, which is a group of protocols that allow routers or switches to provide backup or failover for the default gateway in a network. FHRP ensures that the network traffic can reach its destination even if the primary gateway fails or becomes unavailable. Some examples of FHRP protocols are HSRP, VRRP, and GLBP.
References
? 1: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 18
? 2: CompTIA Network+ N10-008 Certification Practice Test, question 9
? 3: CompTIA Network+ Study Guide: Exam N10-008, 5th Edition, page 263
? 4: CompTIA Network+ (N10-008) Practice Exam w/PBQ & Solution, question 5
? 5: What's on the CompTIA Network+ 008 certification? | CompTIA, section 3.1

NEW QUESTION 233
- (Topic 3)
A network administrator is configuring a firewall to allow for a new cloud-based email server. The company standard is to use SMTP to route email traffic. Which of the following ports, by default, should be reserved for this purpose?

A. 23
B. 25
C. 53
D. 110

Answer: B

Explanation:

Port 25, by default, should be reserved for SMTP traffic to allow for a new cloud-based email server. SMTP stands for Simple Mail Transfer Protocol, which is a network protocol that enables email communication between mail servers and clients. SMTP uses port 25 as its default port for sending and receiving email messages over TCP/IP networks. A cloud-based email server is an email server that is hosted on a cloud service provider's infrastructure, rather than on-premise or in-house. A cloud-based email server can offer advantages such as scalability, reliability, security, and cost-effectiveness. To allow for a new cloud-based email server, a firewall should be configured to open port 25 for SMTP traffic. References: [CompTIA Network+ Certification Exam Objectives], What Is SMTP? | Mailtrap Blog, Cloud Email Server: What Is It & How Does It Work? | Zoho Mail

NEW QUESTION 235
- (Topic 3)
A technician uses a badge to enter a security checkpoint on a corporate campus. An unknown individual quickly walks in behind the technician without speaking. Which of the following types of attacks did the technician experience?

A. Tailgating
B. Evil twin
C. On-path
D. Piggybacking

Answer: A

Explanation:
Tailgating is a type of physical security attack where an unauthorized person follows an authorized person into a restricted area without their consent or knowledge. Tailgating can allow an attacker to bypass security measures and gain access to sensitive information or resources. In this scenario, the technician experienced tailgating when the unknown individual walked in behind the technician without speaking. Piggybacking is similar to tailgating, but it involves the consent or cooperation of the authorized person. Evil twin is a type of wireless network attack where an attacker sets up a rogue access point that mimics a legitimate one. On-path is a type of network attack where an attacker intercepts and modifies traffic between two parties.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.2: Given a scenario, use appropriate network hardening techniques.

NEW QUESTION 238
- (Topic 3)
A desktop support department has observed slow wireless speeds for a new line of laptops using the organization's standard image. No other devices have experienced the same issue. Which of the following should the network administrator recommend troubleshooting FIRST to resolve this issue?

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

Answer: D

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

NEW QUESTION 243
- (Topic 3)
An IT technician needs to increase bandwidth to a server. The server has multiple gigabit ports. Which of the following can be used to accomplish this without replacing hardware?

A. STP
B. 802. IQ
C. Duplex
D. LACP

Answer: D

Explanation:
LACP stands for Link Aggregation Control Protocol and is a protocol that allows multiple physical ports to be combined into a single logical port. This can increase bandwidth, redundancy, and load balancing for a server. LACP is part of the IEEE 802.3ad standard for link aggregation. STP stands for Spanning Tree Protocol and is a protocol that prevents loops in a network by blocking redundant links. 802.1Q is a standard for VLAN (Virtual Local Area Network) tagging, which allows multiple logical networks to share the same physical infrastructure. Duplex is a mode of communication that determines how data is transmitted and received on a link. Full duplex allows simultaneous transmission and reception, while half duplex allows only one direction at a time.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5: Compare and contrast network cabling types, standards and speeds.

NEW QUESTION 245
- (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 246
- (Topic 3)
A PC user who is on a local network reports very slow speeds when accessing files on the network server The user's PC Is connecting, but file downloads are very slow when compared to other users' download speeds The PC's NIC should be capable of Gigabit Ethernet. Which of the following will MOST likely fix the issue?

A. Releasing and renewing the PC's IP address
B. Replacing the patch cable
C. Reseating the NIC inside the PC
D. Flushing the DNS cache

Answer: B

Explanation:
A slow download speed can be caused by a faulty patch cable, which is the cable used to connect the user's PC to the network server. If the patch cable is damaged, the connection will be slower than expected, resulting in slow download speeds. Replacing the patch cable is the most likely solution to this issue, as it will provide a new, reliable connection that should allow for faster download speeds.

NEW QUESTION 248
- (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 253
- (Topic 3)
A user reports that a crucial fileshare is unreachable following a network upgrade that was completed the night before. A network technician confirms the problem exists. Which of the following
troubleshooting Steps should the network technician perform NEXT?

A. Establish a theory of probable cause.
B. Implement a solution to fix the problem.
C. Create a plan of action to resolve the problem.
D. Document the problem and the solution.

Answer: A

Explanation:
Establishing a theory of probable cause is the third step in the general troubleshooting process, after identifying the problem and gathering information. Establishing a theory of probable cause involves using the information gathered to formulate one or more possible explanations for the problem and testing them to verify or eliminate them. In this scenario, the network technician has confirmed the problem exists
and should proceed to establish a theory of probable cause based on the information available, such as the network upgrade that was completed the night before.
Implementing a solution to fix the problem is the fifth step in the general troubleshooting process, after establishing a plan of action. Implementing a solution involves applying the chosen method or technique to resolve the problem and verifying its effectiveness. In this scenario, the network technician has not established a plan of action yet and should not implement a solution without knowing the cause of the problem.
Creating a plan of action to resolve the problem is the fourth step in the general troubleshooting process, after establishing a theory of probable cause. Creating a plan of action involves selecting the best method or technique to address the problem based on the available resources, constraints, and risks. In this scenario, the network technician has not established a theory of probable cause yet and should not create a plan of action without knowing the cause of the problem.
Documenting the problem and the solution is the seventh and final step in the general troubleshooting process, after implementing preventive measures. Documenting the problem and the solution involves recording the details of the problem, its symptoms, its cause, its solution, and its preventive measures for future reference and improvement. In this scenario, the network technician has not implemented preventive measures yet and should not document the problem and the solution without resolving and preventing it.

NEW QUESTION 258
- (Topic 3)
Which of the following use cases would justify the deployment of an mGRE hub-and-spoke topology?

A. An increase in network security using encryption and packet encapsulation
B. A network expansion caused by an increase in the number of branch locations to the headquarters
C. A mandatory requirement to increase the deployment of an SDWAN network
D. An improvement in network efficiency by increasing the useful packet payload

Answer: B

Explanation:

mGRE (Multipoint GRE) is a type of GRE (Generic Routing Encapsulation) tunnel that allows a single interface to support multiple tunnel endpoints, instead of having to configure a separate point-to-point tunnel for each destination. mGRE simplifies the configuration and management of large-scale VPN networks, such

as DMVPN (Dynamic Multipoint VPN), which is a Cisco technology that uses mGRE, NHRP (Next Hop Resolution Protocol), and IPsec to create secure and dynamic VPN connections between a hub and multiple spokes1.
A network expansion caused by an increase in the number of branch locations to the headquarters would justify the deployment of an mGRE hub-and-spoke topology, because it would reduce the complexity and overhead of configuring and maintaining multiple point- to-point tunnels between the hub and each spoke. mGRE would also enable spoke-to- spoke communication without having to go through the hub, which would improve the network performance and efficiency23.
The other options are not directly related to the use case of mGRE hub-and-spoke topology. An increase in network security using encryption and packet encapsulation can be achieved by using IPsec, which is a separate protocol that can be applied to any type of GRE tunnel, not just mGRE. A mandatory requirement to increase the deployment of an SDWAN network can be met by using various technologies and vendors, not necessarily mGRE or DMVPN. An improvement in network efficiency by increasing the useful packet payload can be achieved by using various techniques, such as compression, fragmentation, or QoS, not specifically mGRE.
ReferencesUnderstanding Cisco Dynamic Multipoint VPN - DMVPN, mGRE, NHRPMGRE Easy Steps - Cisco CommunityWhat is DMVPN (Dynamic Multipoint VPN), NHRP, mGRE and How to configu - Cisco Community

NEW QUESTION 259
- (Topic 3)
Clients have reported slowness between a branch and a hub location. The senior engineer suspects asymmetrical routing is causing the issue. Which of the following should the engineer run on both the source and the destination network devices to validate this theory?

A. traceroute
B. ping
C. route
D. nslookup

Answer: A

Explanation:

Asymmetric routing occurs when traffic does not traverse the same path in both directions of a conversation. This can cause problems when there are stateful devices, such as firewalls or NAT devices, in the path that expect the traffic to be symmetrical. Asymmetric routing can also result in suboptimal TCP performance, as TCP assumes that the SYN and ACK packets take the same path1.
To validate the theory of asymmetric routing, the engineer should run the traceroute command on both the source and the destination network devices. The traceroute command shows the route that packets take to reach a destination, by displaying the IP addresses and hostnames of the routers along the path, as well as the time taken for each hop. By comparing the output of the traceroute command from both ends, the engineer can determine if the traffic is taking different paths in each direction, and identify where the asymmetry occurs2.
The ping command is not sufficient to validate the theory of asymmetric routing, as it only tests the connectivity and latency between two devices, but does not show the intermediate hops or the path taken by the packets. The route command shows the routing table of a device, but does not show the actual path taken by the packets. The nslookup command resolves a hostname to an IP address, or vice versa, but does not show the route or the connectivity between two devices.
ReferencesHow to Find & Fix Asymmetric Routing Issues | AuvikIdentifying and Troubleshooting Asymmetric Routing in WAAS - Cisco Community

NEW QUESTION 261
- (Topic 3)
An administrator needs to ensure an access switch is sending the appropriate logs to the network monitoring server. Which of the following logging levels is most appropriate for the access layer switch?

A. Level 0
B. Level 2
C. Level 5
D. Level 7

Answer: C

Explanation:

Logging levels are used to categorize the severity and importance of log messages generated by network devices. The lower the level, the higher the priority. Level 0 is the most critical, while level 7 is the most verbose and least important. Level 5 is the default logging level for most Cisco devices, and it corresponds to notifications. Notifications are messages that indicate normal but significant events, such as interface status changes, configuration changes, or system restarts. These messages are useful for monitoring the health and performance of the network, and they do not generate excessive traffic or consume too much memory or CPU resources. Therefore, level 5 is the most appropriate logging level for an access layer switch, which connects end devices to the network and does not need to log debug or informational messages.
ReferencesHow to configure logging in Cisco IOSCisco Guide to Harden Cisco IOS DevicesCisco Privilege Levels – Explanation and Configuration

NEW QUESTION 266
- (Topic 3)
A network administrator walks into a data center and notices an unknown person is following closely. The administrator stops and directs the person to the security desk.
Which of the following attacks did the network administrator prevent?

A. Evil twin
B. Tailgating
C. Piggybacking
D. Shoulder surfing

Answer: B

Explanation:

Tailgating is a type of physical security attack in which an unauthorized person follows an authorized person into a restricted area, such as a data center, without proper identification or authentication. Tailgating can allow attackers to access sensitive data, equipment, or network resources, or to plant malicious devices or software. The network administrator prevented tailgating by stopping and directing the unknown person to the security desk, where they would have to verify their identity and purpose.

ReferencesDigital Threats and Cyberattacks at the Network LevelNetwork attacks and how to prevent them

NEW QUESTION 267
- (Topic 3)
A user cannot connect to the network, although others in the office are unaffected. The network technician sees that the link lights on the NIC are not on. The technician needs to check which switchport the user is connected to, but the cabling is not labeled. Which of the following is the best way for the technician to find where the computer is connected?

A. Look up the computer's IP address in the switch ARP table.
B. Use a cable tester to trace the cable.
C. Look up the computer's MAC address in the switch CAM table.
D. Use a tone generator to trace the cable.

Answer: D

Explanation:

A tone generator is a device that emits an audible signal on a wire. A tone probe is a device that detects the signal on the wire. By attaching the tone generator to one end of the cable and using the tone probe to scan the other end, the technician can identify which switchport the cable is connected to. This method does not require any knowledge of the computer's IP or MAC address, or access to the switch configuration. It is also faster and more reliable than physically tracing the cable or disconnecting the cable and looking for the link light to go out on the switch.
ReferencesHow to find what port im connected to on a switch from my PC?Switch Port Monitoring Guide - ComparitechFinding Out Which Network Switch Port My Computer is Connected

NEW QUESTION 271
- (Topic 3)
A network engineer has added a new route on a border router and is trying to determine if traffic is using the new route. Which of the following commands should the engineer use?

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

Answer: C

Explanation:

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

NEW QUESTION 272
- (Topic 3)
Which of the following passwords would provide the best defense against a brute-force attack?

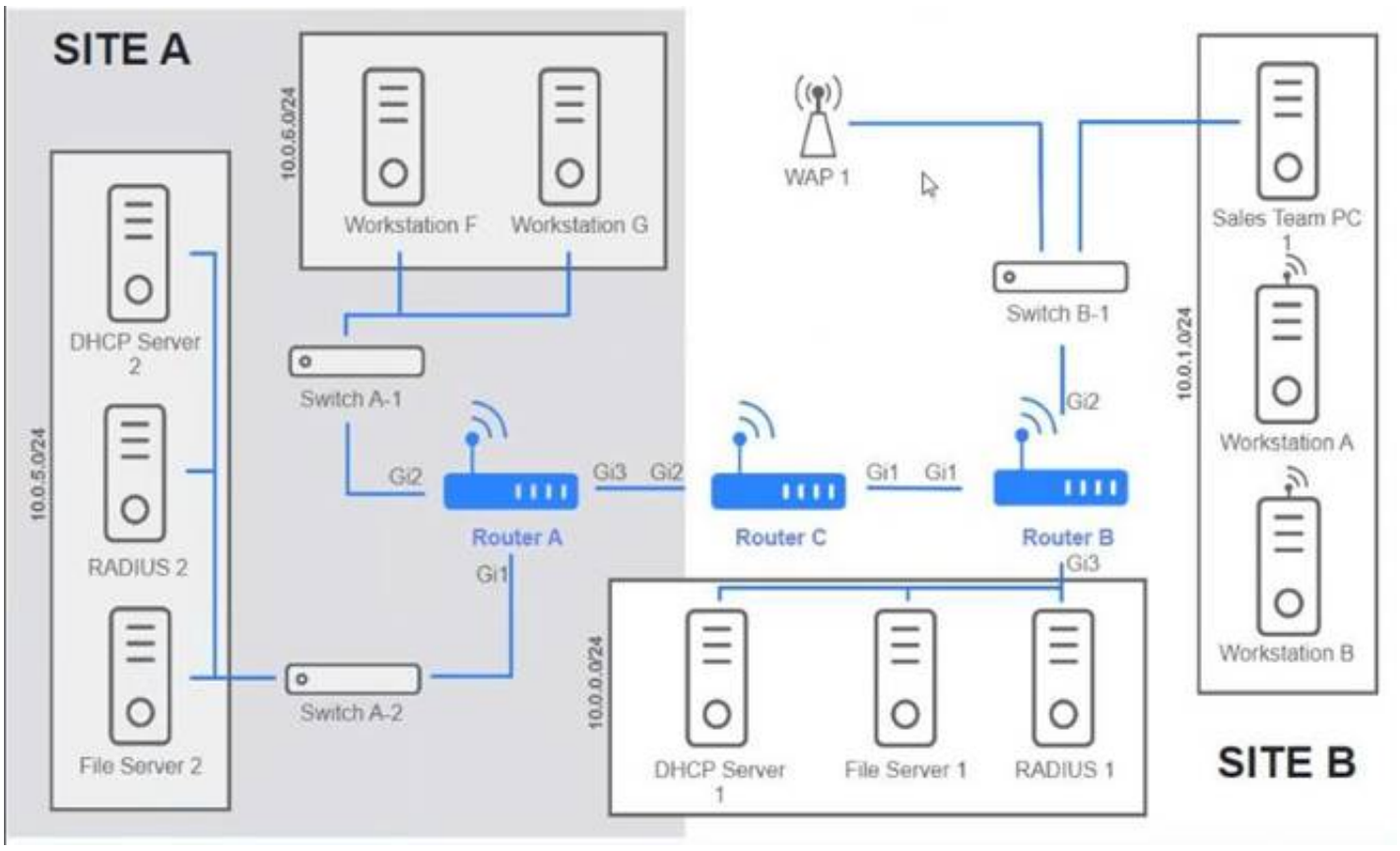
A. ThislsMyPasswordForWork
B. Qwerty!@#$
C. Password! 1
D. T5!8j5

Answer: D

Explanation:

A brute-force attack is a method of guessing passwords by trying every possible combination of characters until the correct one is found. The longer and more complex the password, the harder it is to crack by brute-force. A password that provides the best defense against a brute-force attack should have a combination of uppercase and lowercase letters, numbers, and special characters, and should be as long as possible. The password T5!8j5 meets these criteria, while the other options are either too short, too simple, or too common.
References:
? Password Attacks – N10-008 CompTIA Network+ : 4.21
? CompTIA Network+ Cert Guide: Security Concepts and Tools, page 25 https://www.pearsonitcertification.com/articles/article.aspx?p=3021579&seqNum=2

NEW QUESTION 275
- (Topic 3)
Users are unable to access files on their department share located on flle_server 2. The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.
INSTRUCTIONS
Click on each router to review output, identity any Issues, and configure the appropriate solution
If at any time you would like to bring back the initial state of trie simulation, please click the reset All button;



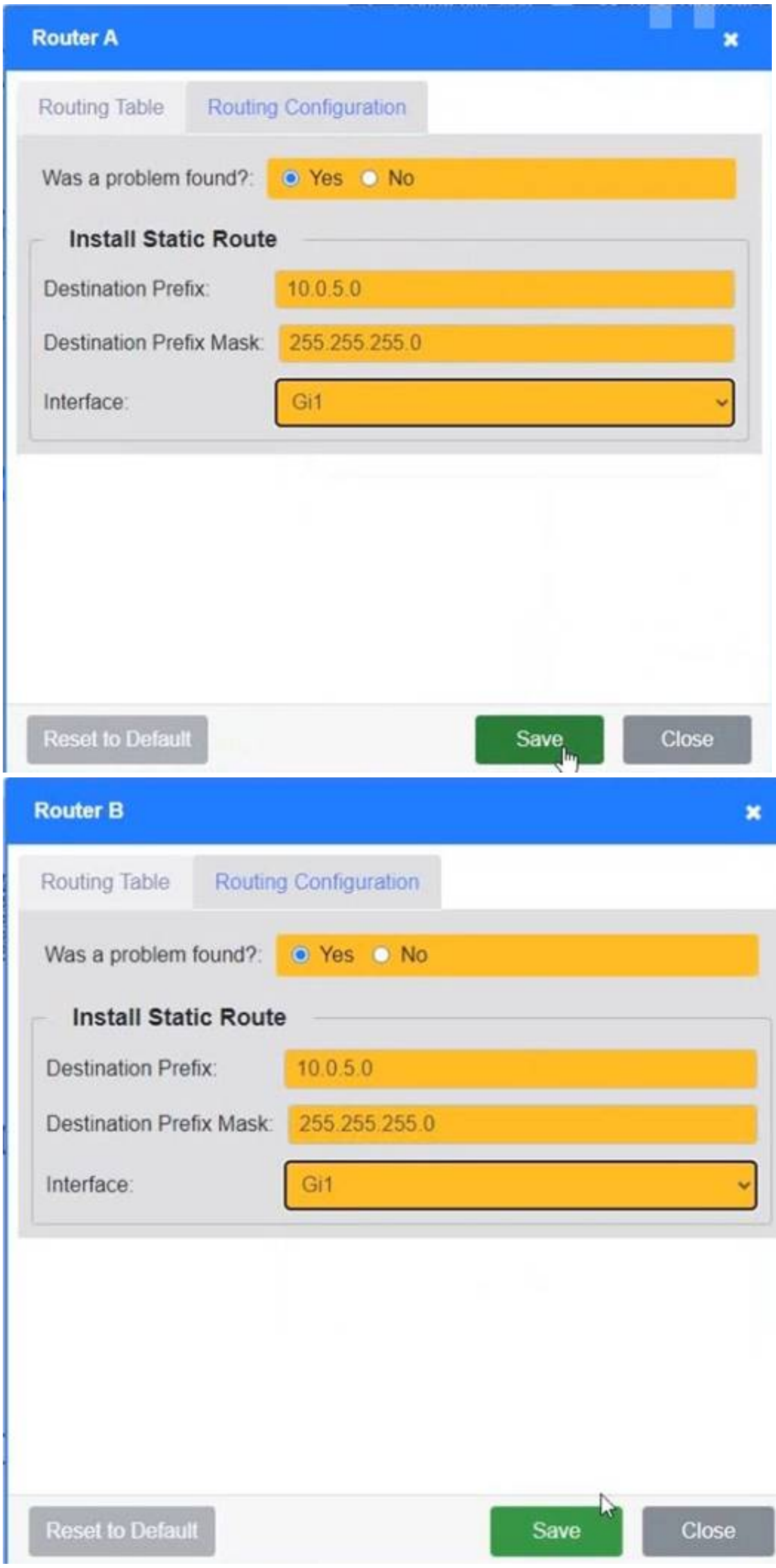
Routing Table | Routing Configuration

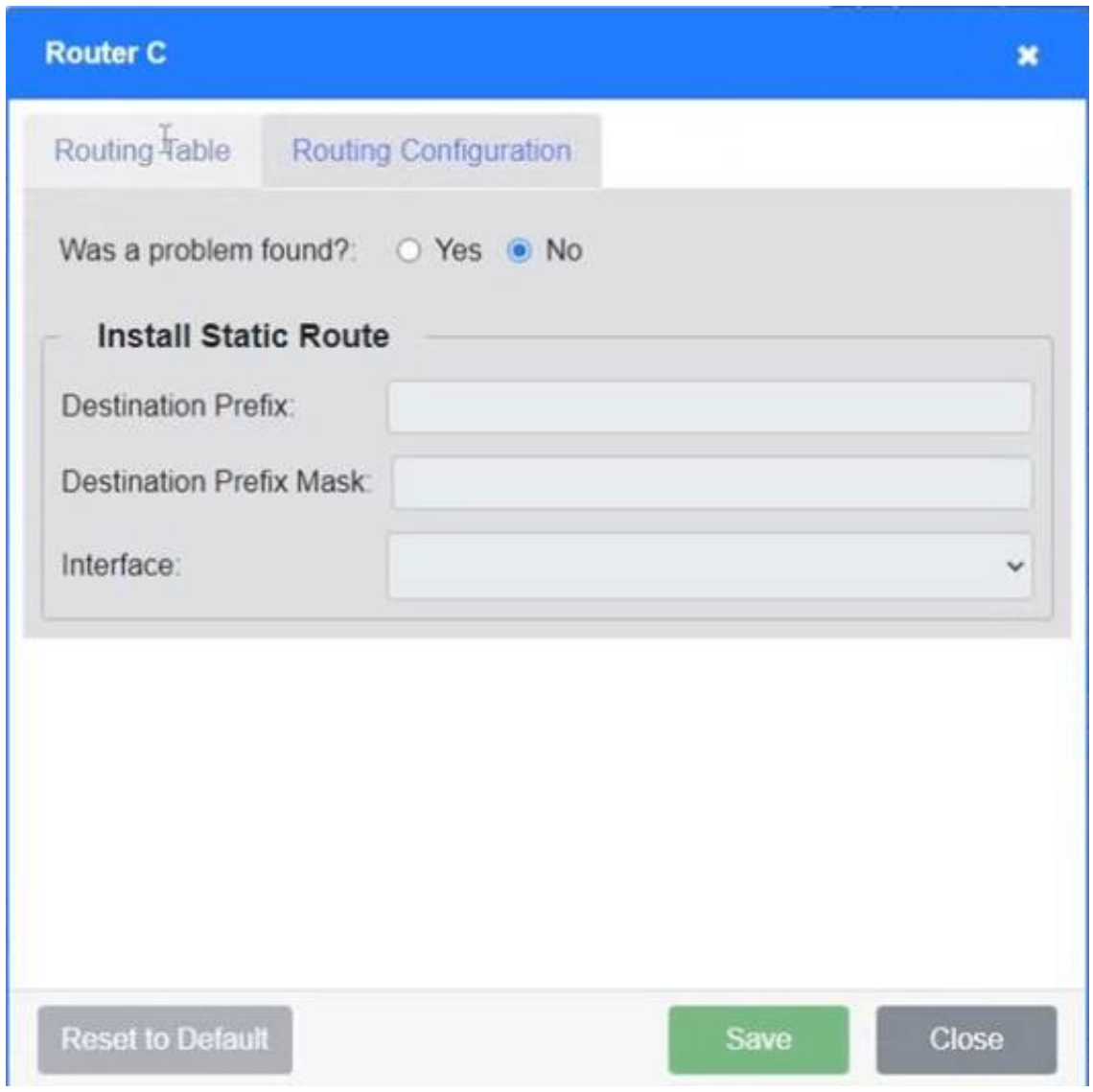
```
Router-B# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, GigabitEthernet1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/22 is directly connected, GigabitEthernet3
L        10.0.0.1/32 is directly connected, GigabitEthernet3
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.4/30 is directly connected, GigabitEthernet1
L        172.16.27.5/32 is directly connected, GigabitEthernet1
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
See the solution configuration below in Explanation.


Router A
Routing Table
Routing Configuration
Was a problem found?: Yes No
Install Static Route
Destination Prefix: 10.0.5.0
Destination Prefix Mask: 255.255.255.0
Interface: Gi1
Reset to Default
Save
Close
Router B
Routing Table
Routing Configuration
Was a problem found?: Yes No
Install Static Route
Destination Prefix: 10.0.5.0
Destination Prefix Mask: 255.255.255.0
Interface: Gi1
Reset to Default
Save
Close



NEW QUESTION 278
- (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 280
- (Topic 3)
A medical building offers patients Wi-Fi in the waiting room. Which of the following security features would be the BEST solution to provide secure connections and keep the medical data protected?

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

Answer: A

NEW QUESTION 281
- (Topic 3)
A computer engineer needs to ensure that only a specific workstation can connect to port 1 on a switch. Which of the following features should the engineer configure on the switch interface?

A. Port tagging
B. Port security
C. Port mirroring
D. Port aggregation

Answer: B

Explanation:
Port security is a feature that can be configured on a switch interface to limit and identify the MAC addresses of workstations that are allowed to connect to that specific port. This can help ensure that only a specific workstation (or workstations) can connect to the interface. According to the CompTIA Network+ Study Manual, “Port security can be used to specify which MAC addresses are allowed to connect to a particular switch port. If a port security violation is detected, the

switch can take a number of different actions, such as shutting down the port, sending an SNMP trap, or sending an email alert."

NEW QUESTION 286
- (Topic 3)
A network administrator needs to add access points to the network because coverage in some areas is improper. Which of the following should the administrator do first?

A. Interference analysis
B. Wireless survey
C. Traffic analysis
D. Packet capture

Answer: B

Explanation:
A wireless survey is the first step that a network administrator should do before adding access points to the network. A wireless survey is a process of collecting data about the wireless environment, such as signal strength, channel usage, interference, and coverage. A wireless survey can help the network administrator to determine the optimal locations and configurations for the access points to provide the best possible coverage and performance for the wireless network. A wireless survey can also help to identify and troubleshoot any issues that may cause improper coverage in some areas.
https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html

NEW QUESTION 290
- (Topic 3)
Which of the following would be increased by adding encryption to data communication across the network?

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

Answer: D

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

NEW QUESTION 291
- (Topic 3)
A network administrator has received calls every day for the past few weeks from three users who cannot access the network. The administrator asks all the users to reboot their PCs, but the same users still cannot access the system. The following day, three different users report the same issue, and the administrator asks them all to reboot their PCs; however, this does not fix the issue. Which of the following is MOST likely occurring?

A. Incorrect firewall settings
B. Inappropriate VLAN assignment
C. Hardware failure
D. Overloaded CAM table in switch
E. DHCP scope exhaustion

Answer: E

NEW QUESTION 296
- (Topic 3)
A hacker used a packet sniffer on the network to capture the hardware address of the server. Which of the following types of attacks can the hacker perform now?

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

Answer: B

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

NEW QUESTION 300
- (Topic 3)
A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds hundreds of CRC errors on an interface. Which of the following is the MOST likely cause of these errors?

A. A bad wire on the Cat 5e cable
B. The wrong VLAN assignment to the switchport
C. A misconfigured QoS setting on the router
D. Both sides of the switch trunk set to full duplex

Answer: A

NEW QUESTION 301
- (Topic 3)
A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks does the technician need to install?
? 110
? 66

A. BiX
B. Krone

Answer: A

Explanation:
A 110 block is a type of punch-down block that is used to terminate twisted-pair cables in Ethernet networks. It is a non-proprietary standard that is widely used in structured cabling systems for voice and data applications. A 110 block can support up to 100 MHz of bandwidth and can be used with Cat 3, Cat 5, Cat 5e, and Cat 6 cables12.
A 66 block is another type of punch-down block that is mainly used for telephone wiring. It is an older and less reliable standard than the 110 block and does not support high-speed data transmission3. A BiX block is a proprietary punch-down block that is developed by NORDX/CDT and is mostly used in Canada. It can support up to 250 MHz of bandwidth and can be used with Cat 5e and Cat 6 cables4. A Krone block is another proprietary punch-down block that is developed by ADC Krone and is mostly used in Europe. It can support up to 100 MHz of bandwidth and can be used with Cat 5 and Cat 5e cables. Therefore, the best option for the customer who wants to use non-proprietary standards is the 110 block.

NEW QUESTION 303
- (Topic 3)
Which of the following would be the MOST cost-effective recovery solution for a company's lower-priority applications?

A. Warm site
B. Cloud site
C. Hot site
D. Cold site

Answer: C

NEW QUESTION 304
- (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 308
- (Topic 3)
A network administrator is testing performance improvements by configuring channel bonding on an 802.Hac AP. Although a site survey detected the majority of the 5GHz frequency spectrum was idle, being used only by the company's WLAN and a nearby government radio system, the AP is not allowing the administrator to manually configure a large portion of the 5GHz frequency range. Which of the following would be BEST to configure for the WLAN being tested?

A. Upgrade the equipment to an AP that supports manual configuration of the ElRP power settings.
B. Switch to 802.11
C. disable channel auto-selection, and enforce channel bonding on the configuration.
D. Set up the AP to perform a dynamic selection of the frequency according to regulatory requirements.
E. Deactivate the band 5GHz to avoid Interference with the government radio

Answer: C

NEW QUESTION 312
- (Topic 3)
A network technician needs to install patch cords from the UTP patch panel to the access switch for a newly occupied set of offices. The patch panel is not labeled for easy jack identification. Which of the following tools provides the easiest way to identify the appropriate patch panel port?

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

Answer: A

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

NEW QUESTION 315
- (Topic 3)
Which of the following describes the BEST device to configure as a DHCP relay?

A. Bridge
B. Router
C. Layer 2 switch
D. Hub

Answer: B

Explanation:
Normally, routers do not forward broadcast traffic. This means that each broadcast domain must be served by its own DHCP server. On a large network with multiple subnets, this would mean provisioning and configuring many DHCP servers. To avoid this scenario, a DHCP relay agent can be configured to provide forwarding of DHCP traffic between subnets. Routers that can provide this type of forwarding are described as RFC 1542 compliant. The DHCP relay intercepts broadcast DHCP frames, applies a unicast address for the appropriate DHCP server, and forwards them over the interface for the subnet containing the server. The DHCP server can identify the original IP subnet from the packet and offer a lease from the appropriate scope. The DHCP relay also performs the reverse process of directing responses from the server to the appropriate client subnet.

NEW QUESTION 318
- (Topic 3)
A network security engineer is investigating a potentially malicious Insider on the network. The network security engineer would like to view all traffic coming from the user's PC to the switch without interrupting any traffic or having any downtime. Which of the following should the network security engineer do?

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

Answer: D

Explanation:
Port mirroring is a feature that allows a network switch to copy the traffic from one or more ports to another port for monitoring purposes. Port mirroring can be used to analyze the network traffic from a specific source, destination, or protocol without affecting the normal operation of the network. Port mirroring can also help to detect and troubleshoot network problems, such as performance issues, security breaches, or policy violations.
The other options are not correct because they do not meet the requirements of the question. They are:
? Turn on port security. Port security is a feature that restricts the number and type
of devices that can connect to a switch port. Port security can help to prevent unauthorized access, MAC address spoofing, or MAC flooding attacks. However, port security does not allow the network security engineer to view the traffic from the user’s PC to the switch.
? Implement dynamic ARP inspection. Dynamic ARP inspection (DAI) is a feature
that validates the ARP packets on a network and prevents ARP spoofing attacks. DAI can help to protect the network from man-in-the-middle, denial-of-service, or data interception attacks. However, DAI does not allow the network security engineer to view the traffic from the user’s PC to the switch.
? Configure 802.1Q. 802.1Q is a standard that defines how to create and manage
virtual LANs (VLANs) on a network. VLANs can help to segment the network into logical groups based on function, security, or performance. However, 802.1Q does not allow the network security engineer to view the traffic from the user’s PC to the switch.
References1: Port Mirroring - an overview | ScienceDirect Topics2: Network+ (Plus) Certification | CompTIA IT Certifications3: Port Security - an overview | ScienceDirect Topics4: Dynamic ARP Inspection - an overview | ScienceDirect Topics5: 802.1Q - an overview | ScienceDirect Topics

NEW QUESTION 320
- (Topic 3)
Which of the following is a document that states what the minimum performance expectations are within a network?

A. Memorandum of understanding
B. Service-level agreement
C. Non-disclosure agreement
D. Baseline metrics

Answer: B

Explanation:
A service-level agreement (SLA) is a document that states what the minimum performance expectations are within a network, such as uptime, throughput, latency, and security. An SLA is usually signed between a service provider and a customer, and it specifies the penalties or remedies if the service level is not met

NEW QUESTION 323
- (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 326
- (Topic 3)
Which of the following would enable a network technician to implement dynamic routing?

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

Answer: C

NEW QUESTION 330
- (Topic 3)
A newly installed multifunction copier needs to be set up so scanned documents can be emailed to recipients. Which of the following ports from the copier's IP address should be allowed?

A. 22
B. 25
C. 53
D. 80

Answer: B

Explanation:
Port 25 is the port number that is commonly used for Simple Mail Transfer Protocol (SMTP), which is a protocol that allows sending and receiving email messages over a network1. Port 25 from the copier's IP address should be allowed so that scanned documents can be emailed to recipients.
Port 22 is the port number that is commonly used for Secure Shell (SSH), which is a protocol that allows secure and encrypted remote access and control of a device over a network1. Port 22 from the copier's IP address is not necessary for emailing scanned documents.
Port 53 is the port number that is commonly used for Domain Name System (DNS), which is a protocol that allows resolving domain names to IP addresses and vice versa on a network1. Port 53 from the copier's IP address is not necessary for emailing scanned documents.
Port 80 is the port number that is commonly used for Hypertext Transfer Protocol (HTTP), which is a protocol that allows transferring web pages and other resources over a network1. Port 80 from the copier's IP address is not necessary for emailing scanned documents.

NEW QUESTION 335
- (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 340
- (Topic 3)
A systems administrator wants to use the least amount of equipment to segment two departments that nave cables terminating in the same room. Which of the following would allow this to occur?

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

Answer: D

NEW QUESTION 345
.....

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