



CompTIA

Exam Questions N10-009

CompTIA Network+ Exam

NEW QUESTION 1

- (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 2

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 3

- (Topic 3)

Which of the following protocols can be routed?

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

Answer: C

Explanation:

iSCSI (Internet Small Computer System Interface) is a protocol that allows SCSI commands to be transported over IP networks¹. iSCSI can be routed because it contains a network address and a device address, as required by a routable protocol². iSCSI can be used to access block-level storage devices over a network, such as SAN (Storage Area Network).

FCoE (Fibre Channel over Ethernet) is a protocol that allows Fibre Channel frames to be encapsulated and transported over Ethernet networks¹. FCoE cannot be routed because it does not contain a network address, only a device address. FCoE operates at the data link layer and requires special switches and adapters to support it. FCoE can also be used to access block-level storage devices over a network, such as SAN.

Fibre Channel is a protocol that provides high-speed and low-latency communication between servers and storage devices¹. Fibre Channel cannot be routed because it does not use IP networks, but rather its own dedicated network infrastructure. Fibre Channel operates at the physical layer and the data link layer and requires special cables, switches, and adapters to support it. Fibre Channel can also be used to access block-level storage devices over a network, such as SAN.

NetBEUI (NetBIOS Extended User Interface) is an old protocol that provides session-level communication between devices on a local network¹. NetBEUI cannot be routed because it does not contain a network address, only a device address. NetBEUI operates at the transport layer and relies on NetBIOS for name resolution. NetBEUI is obsolete and has been replaced by other protocols, such as TCP/IP.

NEW QUESTION 4

- (Topic 3)

A Chief Information Officer wants to monitor network breaching in a passive, controlled manner. Which of the following would be best to implement?

- A. Honeypot
- B. Perimeter network
- C. Intrusion prevention system

D. Port security

Answer: A

Explanation:

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

NEW QUESTION 5

- (Topic 3)

A network is experiencing extreme latency when accessing a particular website. Which of the following commands will BEST help identify the issue?

- A. ipconfig
- B. netstat
- C. tracert
- D. ping

Answer: C

NEW QUESTION 6

- (Topic 3)

A company streams video to multiple devices across a campus. When this happens, several users report a degradation of network performance. Which of the following would MOST likely address this issue?

- A. Enable IGMP snooping on the switches.
- B. Implement another DHCP server.
- C. Reconfigure port tagging for the video traffic.
- D. Change the SSID of the APs

Answer: A

NEW QUESTION 7

- (Topic 3)

Which of the following IP packet header fields is the mechanism for ending loops at Layer 3?

- A. Checksum
- B. Type
- C. Time-to-live
- D. Protocol

Answer: C

Explanation:

The time-to-live (TTL) field is the mechanism for ending loops at Layer 3, which is the network layer of the OSI model. The TTL field is an 8-bit field that indicates the maximum time or number of hops that an IP packet can travel before it is discarded. Every time an IP packet passes through a router, the router decrements the TTL value by one. If the TTL value reaches zero, the router drops the packet and sends an ICMP message back to the source, informing that the packet has expired. This way, the TTL field prevents an IP packet from looping endlessly in a network with routing errors or cycles¹²³.

The other options are not mechanisms for ending loops at Layer 3. The checksum field is a 16-bit field that is used to verify the integrity of the IP header. The checksum field is calculated by adding all the 16-bit words in the header and taking the one's complement of the result. If the checksum field does not match the calculated value, the IP packet is considered corrupted and discarded¹². The type field, also known as the type of service (TOS) or differentiated services code point (DSCP) field, is an 8-bit field that is used to specify the quality of service (QoS) or priority of the IP packet. The type field can indicate how the packet should be handled in terms of delay, throughput, reliability, or cost¹². The protocol field is an 8-bit field that is used to identify the transport layer protocol that is encapsulated in the IP packet. The protocol field can indicate whether the payload is a TCP segment, a UDP datagram, an ICMP message, or another protocol¹².

NEW QUESTION 8

- (Topic 3)

A network technician is investigating a trouble ticket for a user who does not have network connectivity. All patch cables between the wall jacks and computers in the building were upgraded over the weekend from Cat 5 to Cat 6. The newly installed cable is crimped with a TIA/EIA 568A on one end and a TIA/EIA 568B on the other end.

Which of the following should the technician do to MOST likely fix the issue?

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

Answer: B

Explanation:

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

NEW QUESTION 9

- (Topic 3)

A user notifies a network administrator about losing access to a remote file server. The network administrator is able to ping the server and verifies the current firewall rules do not block access to the network fileshare. Which of the following tools would help identify which ports are open on the remote file server?

- A. dig
- B. nmap
- C. tracert
- D. nslookup

Answer: B

Explanation:

nmap is the tool that would help identify which ports are open on the remote file server. nmap stands for Network Mapper, which is a free and open-source tool that can perform various network scanning and discovery tasks. nmap can help identify which ports are open on a remote device by sending probes or packets to different ports and analyzing the responses. nmap can also provide information about the operating system, services, versions, firewalls, or vulnerabilities of the remote device. nmap can be useful for network administrators, security professionals, or hackers to monitor, audit, or attack network devices. References: [CompTIA Network+ Certification Exam Objectives], Nmap - Free Security Scanner For Network Exploration & Security Audits

NEW QUESTION 10

- (Topic 3)

Which of the following types of attacks can be used to gain credentials by setting up rogue APs with identical corporate SSIDs?

- A. VLAN hopping
- B. Evil twin
- C. DNS poisoning
- D. Social engineering

Answer: B

NEW QUESTION 10

- (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 13

- (Topic 3)

A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light does not come on. Which of the following should a technician try first to troubleshoot this issue?

- A. Reverse the fibers.
- B. Rereminate the fibers.
- C. Verify the fiber size.
- D. Examine the cable runs for visual faults.

Answer: A

Explanation:

One of the most common causes of fiber connectivity issues is the reversal of the fibers. This means that the transmit (TX) and receive (RX) ports on one end of the fiber link are not matched with the corresponding ports on the other end. For example, if the TX port on one device is connected to the TX port on another device, and the same for the RX ports, then the devices will not be able to communicate with each other. This can result in no indicator light, no link, or no data transmission¹².

To troubleshoot this issue, the technician should first try to reverse the fibers. This can be done by swapping the connectors at one end of the fiber patch cable, or by using a crossover adapter or cable that reverses the polarity of the fibers. The technician should then check if the indicator light comes on and if the devices can communicate properly¹². The other options are not the first steps to troubleshoot this issue. Rereminating the fibers is a time-consuming and costly process that should be done only if there is evidence of physical damage or poor quality of the termination. Verifying the fiber size is not relevant in this scenario, as multimode fiber is compatible with multimode fiber, and any mismatch in core diameter or bandwidth would result in high attenuation, not complete loss of signal. Examining the cable runs for visual faults is a useful technique, but it requires a special tool called a visual fault locator (VFL) that emits a visible red light through the fiber and shows any breaks or bends along the cable. However, a VFL cannot detect polarity issues or connector problems, so it is not sufficient to troubleshoot this issue

NEW QUESTION 14

- (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 18

- (Topic 3)

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

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

Answer: A

NEW QUESTION 23

- (Topic 3)

Which of the following technologies would MOST likely be 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)

A large number of PCs are obtaining an APIPA IP address, and a number of new computers were added to the network. Which of the following is MOST likely causing the PCs to obtain an APIPA address?

- A. Rogue DHCP server
- B. Network collision
- C. Incorrect DNS settings
- D. DHCP scope exhaustion

Answer: D

Explanation:

DHCP scope exhaustion means that there are no more available IP addresses in the DHCP server's pool of addresses to assign to new devices on the network. When this happens, the devices will use APIPA (Automatic Private IP Addressing) to self-configure an IP address in the range of 169.254.0.1 to 169.254.255.254. These addresses are not routable and can only communicate with other devices on the same local network. A rogue DHCP server (A) is an unauthorized DHCP server that can cause IP address conflicts or security issues by assigning IP addresses to devices on the network. A network collision (B) is a situation where two or more devices try to send data on the same network segment at the same time, causing interference and data loss. Incorrect DNS settings © can prevent devices from resolving domain names to IP addresses, but they do not affect the DHCP process.

NEW QUESTION 28

- (Topic 3)

Which of the following is an advantage of using the cloud as a redundant data center?

- A. The process of changing cloud providers is easy.
- B. Better security for company data is provided.
- C. The initial capital expenses are lower.
- D. The need for backups is eliminated.

Answer: C

Explanation:

Using the cloud as a redundant data center means that the company does not need to invest in building and maintaining a physical backup site, which can be costly and time-consuming. Instead, the company can pay for the cloud services as needed, which can reduce the initial capital expenses and operational costs. However, this does not mean that the other options are true. Changing cloud providers may not be easy due to compatibility, contractual, or regulatory issues. Security for company data may not be better in the cloud, depending on the cloud provider's policies and practices. The need for backups is not eliminated, as the cloud data still needs to be protected from loss, corruption, or unauthorized access.

References:

? Part 1 of current page talks about how Bing is your AI-powered copilot for the web and provides various examples of how it can help you with different tasks, such as writing a joke, creating a table, or summarizing research. However, it does not mention anything about using the cloud as a redundant data center.

? Part 2 of current page shows the search results for “ai powered search bing chat”, which include web, image, and news results. However, none of these results seem to be relevant to the question, as they are mostly about Bing’s features, products, or announcements, not about cloud computing or data centers.
? Therefore, I cannot find the answer or the explanation from the current page. I have to use my own knowledge and information from other sources to verify the answer and provide a short but comprehensive explanation. I will cite these sources using numerical references.
? : CompTIA Network+ Certification Exam Objectives, Version 8.0, Domain 3.0: Network Operations, Objective 3.4: Given a scenario, use appropriate resources to support configuration management, Subobjective 3.4.2: Cloud-based configuration management, <https://www.comptia.jp/pdf/comptia-network-n10-008-exam-objectives.pdf>
? : Cloud Computing: Concepts, Technology & Architecture, Chapter 9: Fundamental Cloud Security, Section 9.1: Cloud Security Threats, <https://ptgmedia.pearsoncmg.com/images/9780133387520/samplepages/9780133387520.pdf>
? : Cloud Computing: Principles and Paradigms, Chapter 19: Data Protection and Disaster Recovery for Cloud Computing, Section 19.1: Introduction, <https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470940105.ch19>

NEW QUESTION 29

- (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 32

- (Topic 3)

Which of the following is used to elect an STP root?

- A. A bridge ID
- B. A bridge protocol data unit
- C. Interface port priority
- D. A switch's root port

Answer: B

Explanation:

"Using special STP frames known as bridge protocol data units (BPDUs), switches communicate with other switches to prevent loops from happening in the first place. Configuration BPDUs establish the topology, where one switch is elected root bridge and acts as the center of the STP universe. Each switch then uses the root bridge as a reference point to maintain a loop-free topology."

NEW QUESTION 35

- (Topic 3)

An engineer recently decided to upgrade the firmware on a router. During the upgrade, the help desk received calls about a network outage, and a critical ticket was opened. The network manager would like to create a policy to prevent this from happening in the future. Which of the following documents should the manager create?

- A. Change management
- B. incident response
- C. Standard operating procedure
- D. System life cycle

Answer: A

NEW QUESTION 40

- (Topic 3)

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

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

Answer: CD

Explanation:

QSFP+ is a type of transceiver that supports 40 gigabit Ethernet (40GbE) over four lanes of 10 gigabit Ethernet (10GbE) each. QSFP+ stands for quad small form-factor pluggable plus, and it is a compact and hot-swappable module that plugs into a QSFP+ port on a network device. QSFP+ transceivers can support various types of cables and connectors, such as direct attach copper (DAC), active optical cable (AOC), or fiber optic cable. Multimode is a type of fiber optic cable that supports multiple modes of light propagation within the core. Multimode fiber optic cable can carry higher bandwidth and data rates than single-mode fiber optic cable, but over shorter distances. Multimode fiber optic cable is commonly used for short-reach applications, such as within a data center or a campus network. Multimode fiber optic cable can be paired with QSFP+ transceivers to achieve 40GbE connectivity.

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

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

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

? Cat 6a. Cat 6a is a type of twisted-pair copper cable that supports 10 gigabit

Ethernet (10GbE) over distances up to 100 meters. Cat 6a stands for category 6 augmented, and it is an enhanced version of Cat 6 cable that offers better performance and reduced crosstalk. Cat 6a cable can be paired with 10Gbase-T transceivers to achieve 10GbE connectivity. However, Cat 6a cable cannot support 40GbE by itself, unless it is used in a breakout configuration with a QSFP+ transceiver.

? Cat 5e. Cat 5e is a type of twisted-pair copper cable that supports 1 gigabit

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

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

NEW QUESTION 41

- (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 42

- (Topic 3)

Users in a branch can access an In-house database server, but it is taking too long to fetch records. The analyst does not know whether the issue is being caused by network latency. Which of the following will the analyst MOST likely use to retrieve the metrics that are needed to resolve this issue?

- A. SNMP
- B. Link state
- C. Syslog
- D. QoS
- E. Traffic shaping

Answer: A

NEW QUESTION 47

- (Topic 3)

Which of the following DNS records maps an alias to a true name?

- A. AAAA
- B. NS
- C. TXT
- D. CNAME

Answer: D

Explanation:

A CNAME (Canonical Name) record is a type of DNS (Domain Name System) record that maps an alias name to a canonical or true domain name. For example, a CNAME record can map blog.example.com to example.com, which means that blog.example.com is an alias of example.com. A CNAME record is useful when you want to point multiple subdomains to the same IP address, or when you want to change the IP address of a domain without affecting the subdomains1.

NEW QUESTION 52

- (Topic 3)

Which of the following fiber connector types is the most likely to be used on a network interface card?

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

Answer: A

Explanation:

LC (local connector) is the most likely fiber connector type to be used on a network interface card, because it is a small form factor connector that can fit more interfaces on a single card. LC connectors use square connectors that have a locking mechanism on the top, similar to an RJ45 copper connector. LC connectors are also compatible with SFP (small form-factor pluggable) modules that are often used to link a gigabit Ethernet port with a fiber network¹².

References:

? Optical Fiber Connectors – CompTIA Network+ N10-007 – 2.11

? CompTIA Network+ Certification Exam Objectives²

NEW QUESTION 55

- (Topic 3)

A network administrator would like to purchase a device that provides access ports to endpoints and has the ability to route between networks. Which of the following would be BEST for the administrator to purchase?

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

Answer: B

NEW QUESTION 56

- (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 60

- (Topic 3)

Which of the following attacks utilizes a network packet that contains multiple network tags?

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

Answer: B

NEW QUESTION 63

- (Topic 3)

A network technician wants to deploy a new wireless access point to reduce user latency. Currently, the organization has the following deployed:

Which of the following channels should the new device broadcast on?

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

Answer: D

Explanation:

The best channel for a new wireless access point is one that does not overlap with the existing channels used by other devices. Overlapping channels can cause interference and degrade the performance of the wireless network. According to the web search results, the 2.4 GHz band has 11 channels in the U.S., but only channels 1, 6, and 11 are non-overlapping. Since the existing devices are using channels 1 and 6, the new device should use channel 11 to avoid adjacent-channel interference¹²

References¹: Why Channels 1, 6 and 11? | MetaGeek ²: How to Choose the Best Wi-Fi Channels for Your Network - Lifewire

NEW QUESTION 68

- (Topic 3)

A company is opening a new building on the other side of its campus. The distance from the closest building to the new building is 1,804ft (550m). The company needs to connect the networking equipment in the new building to the Other buildings on the campus without using a repeater. Which Of the following transceivers should the company use?

- A. 10GBASE-SW
- B. 10GBASE-LR

- C. 10GBASE-LX4 over multimode fiber
- D. 10GBASE-SR

Answer: B

Explanation:

10GBASE-LR is a standard for 10 Gbps Ethernet over single-mode fiber optic cable. It can support a maximum distance of 6.2 miles (10 km), which is much longer than the distance between the buildings. 10GBASE-SW, 10GBASE-LX4, and 10GBASE-SR are all standards for 10 Gbps Ethernet over multimode fiber optic cable, which have shorter maximum distances ranging from 984ft (300m) to 1,312ft (400m).

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 71

- (Topic 3)

A technician is troubleshooting reports that a networked printer is unavailable. The printer's IP address is configured with a DHCP reservation, but the address cannot be pinged from the print server in the same subnet. Which of the following is MOST likely the cause of the connectivity failure?

- A. Incorrect VLAN
- B. DNS failure
- C. DHCP scope exhaustion
- D. Incorrect gateway

Answer: D

NEW QUESTION 76

- (Topic 3)

A VOIP phone is plugged in to a port but cannot receive calls. Which Of the following needs to be done on the port to address the issue?

- A. Trunk all VLANs on the port.
- B. Configure the native VLAN.
- C. Tag the traffic to voice VLAN.
- D. Disable VLANs.

Answer: C

Explanation:

To enable a VOIP phone to receive calls on a port, the traffic needs to be tagged to the voice VLAN that is configured on the switch. This allows the phone to communicate with the voice network and the PBX server. Tagging the traffic also separates the voice traffic from the data traffic that may be coming from a computer connected to the phone. The port should be configured to tag the traffic for the voice VLAN and untag the traffic for the data VLAN. Trunking all VLANs on the port is unnecessary and may cause security issues. Configuring the native VLAN is not relevant for this issue. Disabling VLANs would prevent the phone from working at all.

References:

Optical Fiber Connectors – CompTIA Network+ N10-007 – 2.13

? VoIP and computer on separate VLANs through one cable

NEW QUESTION 77

- (Topic 3)

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

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

Answer: AF

NEW QUESTION 79

- (Topic 3)

Which of the following topologies is designed to fully support applications hosted in on-premises data centers, public or private clouds, and SaaS services?

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

Answer: A

NEW QUESTION 81

- (Topic 3)

A technician is investigating why a PC cannot reach a file server with the IP address 192.168.8.129. Given the following TCP/IP network configuration:

Link-local IPv6 address	fe80::28e4:a7cc:a55e:4bea
IPv4 address	192.168.8.105
Subnet mask	255.255.255.128
Default gateway	192.168.8.1

Which of the following configurations on the PC is incorrect?

- A. Subnet mask
- B. IPv4 address
- C. Default gateway
- D. IPv6 address

Answer: C

Explanation:

The default gateway is the IP address of the router that connects the PC to other networks. The default gateway should be on the same subnet as the PC's IPv4 address. However, in this case, the default gateway is 192.168.9.1, which is on a different subnet than the PC's IPv4 address of 192.168.8.15. Therefore, the default gateway configuration on the PC is incorrect and prevents the PC from reaching the file server on another subnet.

NEW QUESTION 86

- (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 91

- (Topic 3)

A network administrator is concerned about a rainbow table being used to help access network resources. Which of the following must be addressed to reduce the likelihood of a rainbow table being effective?

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

Answer: A

Explanation:

A password policy must be addressed to reduce the likelihood of a rainbow table being effective. A rainbow table is a precomputed table of hashed passwords and their corresponding plaintext values. A rainbow table can be used to crack hashed passwords by performing a reverse lookup of the hash value in the table. A password policy is a set of rules and guidelines that define how passwords should be created, used, and managed in an organization. A password policy can help prevent rainbow table attacks by enforcing strong password requirements, such as length, complexity, expiration, and history. A strong password is one that is hard to guess or crack by using common methods such as brute force or dictionary attacks. References: [CompTIA Network+ Certification Exam Objectives], What Is Rainbow Table Attack? | Kaspersky, Password Policy Best Practices | Thycotic

NEW QUESTION 96

- (Topic 3)

A technician completed troubleshooting and was able to fix an issue. Which of the following is the BEST method the technician can use to pass along the exact steps other technicians should follow in case the issue arises again?

- A. Use change management to build a database
- B. Send an email stating that the issue is resolved.
- C. Document the lessons learned
- D. Close the ticket and inform the users.

Answer: C

Explanation:

Documenting the lessons learned is the best method for passing along the exact steps other technicians should follow in case the issue arises again. Lessons learned are the knowledge and experience gained from completing a project or solving a problem. Documenting the lessons learned helps to capture the best practices, challenges, solutions, and recommendations for future reference and improvement. Documenting the lessons learned can also help to update the

knowledge base, standard operating procedures, or policies related to the issue. References: [CompTIA Network+ Certification Exam Objectives], Lessons Learned: Definition & Examples for Project Managers

NEW QUESTION 101

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 104

- (Topic 3)

A network resource was accessed by an outsider as a result of a successful phishing campaign. Which of the following strategies should be employed to mitigate the effects of phishing?

- A. Multifactor authentication
- B. Single sign-on
- C. RADIUS
- D. VPN

Answer: A

Explanation:

Multifactor authentication is a security measure that requires users to provide multiple pieces of evidence before they can access a network resource. This could include requiring users to enter a username, password, and a code sent to the user's mobile phone before they are allowed access. This ensures that the user is who they say they are, reducing the risk of malicious actors gaining access to network resources as a result of a successful phishing campaign.

NEW QUESTION 108

- (Topic 3)

A company's web server is hosted at a local ISP. This is an example of:

- A. allocation.
- B. an on-premises data center.
- C. a branch office.
- D. a cloud provider.

Answer: D

NEW QUESTION 113

- (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 114

- (Topic 3)

To access production applications and data, developers must first connect remotely to a different server. From there, the developers are able to access production data. Which of the following does this BEST represent?

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

Answer: E

NEW QUESTION 115

- (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 traceroute 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 117

- (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 120

- (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 125

- (Topic 3)

Which of the following network cables involves bouncing light off of protective cladding?

- A. Twinaxial
- B. Coaxial
- C. Single-mode
- D. Multimode

Answer: D

Explanation:

Multimode fiber optic cables use multiple paths of light that bounce off the cladding, which is a layer of glass or plastic that surrounds the core of the cable.

<https://www.explainthatstuff.com/fiberoptics.html>

NEW QUESTION 128

- (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 131

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 133

- (Topic 3)

Which of the following commands can be used to display the IP address, subnet address, gateway address, and DNS address on a Windows computer?

- A. netstat -a
- B. ifconfig
- C. ip addr
- D. ipconfig /all

Answer: D

Explanation:

The ipconfig command is a utility that allows you to view and modify the network configuration of a Windows computer. By running the command "ipconfig /all", you can view detailed information about the network configuration of your computer, including the IP address, subnet mask, default gateway, and DNS server addresses.

Option A (netstat -a) is a command that displays active network connections and their status, but it does not display IP address or other network configuration information. Option B (ifconfig) is a command used on Linux and Unix systems to view and modify network configuration, but it is not available on Windows. Option C (ip addr) is a command used on Linux and Unix systems to view and modify network configuration, but it is not available on Windows.

NEW QUESTION 136

- (Topic 3)

A network technician needs to use an RFC1918 IP space for a new office that only has a single public IP address. Which of the following subnets should the technician use for the LAN?

- A. 10.10.10.0/24
- B. 127.16.10.0/24
- C. 174.16.10.0/24
- D. 198.18.10.0/24

Answer: A

Explanation:

The RFC1918 IP space is a set of private IP addresses that are not routable on the public Internet and can be used for internal networks. The RFC1918 IP space consists of three ranges: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16¹. Out of the four options, only A. 10.10.10.0/24 belongs to one of these ranges, specifically the 10.0.0.0/8 range. Therefore, the technician should use this subnet for the LAN.

References¹: https://en.wikipedia.org/wiki/Private_network

NEW QUESTION 138

- (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 142

- (Topic 3)

Which of the following would be the BEST choice to connect branch sites to a main office securely?

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

Answer: A

Explanation:

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

NEW QUESTION 143

- (Topic 3)

Which of the following connectors and terminations are required to make a Cat 6 cable that connects from a PC to a non-capable MDIX switch? (Select TWO).

- A. T1A-568-A - TIA-568-B
- B. TIA-568-B - TIA-568-B
- C. RJ11
- D. RJ45
- E. F-type

Answer: AD

NEW QUESTION 146

- (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 HTTPS.

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 allowed.

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 148

- (Topic 3)

Which of the following allows for an devices within a network to share a highly reliable time source?

- A. NTP
- B. SNMP
- C. SIP
- D. DNS

Answer: A

Explanation:

Network Time Protocol (NTP) is a protocol used to maintain a highly accurate and reliable clock time on all devices within a network. NTP works by synchronizing the time of all the devices within a network to a single, highly accurate time source. This allows for the time of all the devices to be kept in sync with each other, ensuring a consistent and reliable time source for all devices within the network.

NEW QUESTION 152

- (Topic 3)

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

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

Which of the following should the analyst recommend?

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

Answer: A**Explanation:**

This answer will help the organization to avoid expending resources on identifying non-relevant events, as the 404 errors on image files are not indicative of any security threat or issue, but rather a misconfiguration or a broken link on the web server. The 404 errors on image files are also very frequent and repetitive, as shown by the web server log, which can clutter the log and make it harder to spot any relevant events. By filtering out these errors, the analyst can focus on more important events and reduce the noise in the log. The other answers are not as good as A, because they either do not address the problem of identifying non-relevant events, or they are based on incorrect assumptions or information. For example:

? B. Updating firewall rules to block 202.180.155.1 is not a good answer, because the IP address 202.180.155.1 is not doing anything malicious or suspicious, but rather requesting image files that do not exist on the web server. Blocking this IP address will not improve the security of the web server, but rather create unnecessary firewall rules and possibly deny legitimate access to the web server.

? C. Resyncing the network time server and monitoring logs for future anomalous behavior is not a good answer, because there is no evidence that the network time server is out of sync or causing any problems. The web server log shows that the entries are all within a few minutes of each other, which is normal and expected. Resyncing the network time server will not help the analyst to identify non-relevant events, but rather waste time and resources on an unrelated task.

? D. Checking with the penetration testing team to see if the team ran any scans on January 14, 2021 is not a good answer, because the web server log does not show any signs of a penetration test or a scan. The log shows only 404 errors on image files, which are not typical of a penetration test or a scan, which would usually target different types of files, ports, or vulnerabilities. Checking with the penetration testing team will not help the analyst to identify non-relevant events, but rather distract the analyst from the actual events and possibly create false alarms.

<https://www.professormesser.com/network-plus/n10-008/n10-008-video/general-network-troubleshooting-n10-008/>

NEW QUESTION 153

- (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 154

- (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 158

- (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 162

- (Topic 3)

During a recent security audit, a contracted penetration tester discovered the organization uses a number of insecure protocols. Which of the following ports should be disallowed so only encrypted protocols are allowed? (Select TWO).

- A. 22
- B. 23
- C. 69
- D. 443
- E. 587
- F. 8080

Answer: BC

NEW QUESTION 166

- (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 170

- (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 173

- (Topic 3)

A technician is concerned about unauthorized personnel moving assets that are installed in a data center server rack. The technician installs a networked sensor that sends an alert when the server rack door is opened. Which of the following did the technician install?

- A. Cipher lock
- B. Asset tags
- C. Access control vestibule
- D. Tamper detection

Answer: D

Explanation:

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

References:

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

NEW QUESTION 174

- (Topic 3)

A network engineer is concerned about VLAN hopping happening on the network. Which of the following should the engineer do to address this concern?

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

Answer: B

Explanation:

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

NEW QUESTION 179

- (Topic 3)

A network administrator installed a new data and VoIP network. Users are now experiencing poor call quality when making calls. Which of the following should the administrator do to increase VoIP performance?

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

Answer: A

Explanation:

"Benefits of Voice VLAN

It ensures that your VoIP (Voice over Internet Phone) devices do not have to contend directly with all the broadcasts and other traffic from the data VLAN. A voice VLAN can simplify network configuration in some circumstances."

<https://community.fs.com/blog/auto-voip-vs-voice-vlan-what-s-the-difference.html> Jumbo Frames

"When jumbo frames on a VoIP/UC network are enabled, it can cause the same kind of delay to your network transmissions."

"VoIP uses will always not benefit from jumbo frame, as VoIP like gaming, is latency and time sensitive. Jumbo Frame for Internet Purpose: You will not see any performance boost as the files that came across the internet does not support jumbo frame."

<https://www.ankmax.com/newsinfo/1358641.html#:~:text=VoIP%20uses%20will%20always>

%20not,does%20not%20support%20jumbo%20frame.

"To summarize this general best practice guide, you should NOT enable jumbo frame feature as a general home user."

NEW QUESTION 183

- (Topic 3)

A user stores large graphic files. The time 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 185

- (Topic 3)

Which of the following network types is composed of computers that can all communicate with one another with equal permissions and allows users to directly share what is on or attached to their computers?

- A. Local area network
- B. Peer-to-peer network
- C. Client-server network
- D. Personal area network

Answer: B

Explanation:

A peer-to-peer network is a type of network in which each computer (or node) can communicate directly with any other node, without requiring a central server or authority. Each node can act as both a client and a server, and can share its own resources, such as files, printers, or internet connection, with other nodes. A peer-to-peer network allows users to directly access and exchange what is on or attached to their computers, with equal permissions and responsibilities

NEW QUESTION 189

- (Topic 3)

Which of the following is most likely to have the HIGHEST latency while being the most accessible?

- A. Satellite
- B. DSL
- C. Cable
- D. 4G

Answer: A

NEW QUESTION 191

- (Topic 3)

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

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

Answer: C

Explanation:

A captive portal is a web page that is displayed to newly connected users of a Wi-Fi network before they are granted broader access to network resources. Captive portals are commonly used to present a landing or log-in page which may require authentication, payment, acceptance of an end-user license agreement, acceptable use policy, survey completion, or other valid credentials that both the host and user agree to adhere by¹²³

A possible cause of the issue is that the user has not completed the captive portal authentication process, which prevents the VPN from establishing a secure connection over the Wi-Fi network. The user may need to open a web browser and follow the instructions on the captive portal page to gain full access to the internet.

NEW QUESTION 195

- (Topic 3)

A network technician is investigating why a core switch is logging excessive amounts of data to the syslog server. The running configuration of the switch showed the following logging information:

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

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

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

Answer: D

Explanation:

The logging level debugging is the highest level of logging, which means that the switch will log every possible event, including low-priority and verbose messages. This can result in excessive amounts of data being sent to the syslog server, which can affect the performance and storage of the server. To fix the issue, the technician should adjust the logging level to a lower value, such as informational, warning, or error, depending on the desired level of detail and severity. This will reduce the amount of log data generated by the switch and only send the relevant and necessary messages to the syslog server.

<https://betterstack.com/community/guides/logging/log-levels-explained/>

NEW QUESTION 199

- (Topic 3)

A network administrator received complaints of intermittent network connectivity issues. The administrator investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?

- A. Enable spanning tree.
- B. Configure port security.
- C. Change switch port speed limits.
- D. Enforce 802.1Q tagging.

Answer: A

Explanation:

Spanning tree is a protocol that prevents network loops by dynamically disabling or enabling switch ports based on the network topology. Network loops can cause intermittent connectivity issues, such as broadcast storms, MAC address table instability, and multiple frame transmission. By enabling spanning tree, the network administrator can ensure that there is only one active path between any two network devices at any given time. References:

? CompTIA Network+ N10-008 Certification Exam Objectives, page 91

? CompTIA Network+ Cert Guide: Switching and Virtual LANs, page 172

NEW QUESTION 204

- (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 206

- (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 210

- (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 215

- (Topic 3)

Which of the following is MOST appropriate for enforcing bandwidth limits when the performance of an application is not affected by the use of buffering but is heavily impacted by packet drops?

- A. Traffic shaping
- B. Traffic policing
- C. Traffic marking
- D. Traffic classification

Answer: B

Explanation:

Traffic policing is a mechanism that monitors the traffic in any network and enforces a bandwidth limit by discarding packets that exceed a certain rate¹. This can reduce congestion and ensure fair allocation of bandwidth among different applications or users. However, discarding packets can also affect the performance and quality of some applications, especially those that are sensitive to packet loss, such as voice or video. Traffic shaping is a congestion control mechanism that delays packets that exceed a certain rate instead of discarding them¹. This can smooth out traffic bursts and avoid packet loss, but it also introduces latency and jitter. Traffic shaping can be beneficial for applications that can tolerate some delay but not packet loss, such as file transfers or streaming.

Traffic marking is a mechanism that assigns different priority levels to packets based on their type, source, destination, or other criteria². This can help to differentiate between different classes of service and apply different policies or treatments to them. However, traffic marking does not enforce bandwidth limits by itself; it only provides information for other mechanisms to act upon.

Traffic classification is a process that identifies and categorizes packets based on their characteristics, such as protocol, port number, payload, or behavior. This can help to distinguish between different types of traffic and apply appropriate policies or actions to them. However, traffic classification does not enforce bandwidth limits by itself; it only provides input for other mechanisms to use.

NEW QUESTION 219

- (Topic 3)

A network security engineer is responding to a security incident. The engineer suspects that an attacker used an authorized administrator account to make configuration changes to the boundary firewall. Which of the following should the network security engineer review?

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

Answer: B

Explanation:

Audit logs are records of the actions performed by users or processes on a system or network device. They can provide information about who made what changes, when, and why. Audit logs are essential for detecting and investigating security incidents, as well as for ensuring compliance with policies and regulations. Audit logs can help the network security engineer to identify the source of the unauthorized configuration changes to the boundary firewall, as well as the scope and impact of the changes.

References¹ - Changes to Cyber Essentials requirements – April 2021 update² - 8 Firewall Best Practices for Securing the Network³ - How to secure your network boundaries with a firewall

NEW QUESTION 223

- (Topic 3)

A network security administrator needs to monitor the contents of data sent between a secure network and the rest of the company. Which of the following monitoring methods will accomplish this task?

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

Answer: A

Explanation:

Port mirroring is a method of monitoring network traffic by copying the data packets from one port to another port on the same switch or router. This allows the network security administrator to analyze the contents of the data sent between different networks without affecting the performance or security of the original traffic. Port mirroring can be configured to capture all traffic or only specific types of traffic, such as VLANs, protocols, or IP addresses.

References:

? Port Mirroring - CompTIA Network+ N10-008 Domain 3.1 - YouTube¹

? CompTIA Network+ Certification Exam Objectives, page 142

NEW QUESTION 224

- (Topic 3)

Which of the following types of connections would need to be set up to provide access from the internal network to an external network so multiple satellite offices can communicate securely using various ports and protocols?

- A. Client-to-site VPN
- B. Clientless VPN
- C. RDP
- D. Site-to-site VPN
- E. SSH

Answer: D

NEW QUESTION 228

- (Topic 3)

After a company installed a new IPS, the network is experiencing speed degradation. A network administrator is troubleshooting the issue and runs a speed test. The results from the different network locations are as follows:
Which of the following is the most likely issue?

- A. Packet loss
- B. Bottlenecking
- C. Channel overlap
- D. Network congestion

Answer: B

Explanation:

The most likely issue is bottlenecking. Bottlenecking occurs when a component or device limits the performance or capacity of the network. In this case, the IPS (intrusion prevention system) may be causing a bottleneck by inspecting and filtering the incoming and outgoing traffic, which reduces the speed and bandwidth available for the network devices¹²

To confirm this issue, the network administrator can compare the speed test results before and after installing the IPS, and check the IPS configuration and logs for any errors or warnings. The network administrator can also try to bypass the IPS temporarily and run the speed test again to see if there is any improvement³

If the IPS is indeed the cause of the bottleneck, the network administrator can try to optimize the IPS settings, such as adjusting the inspection rules, thresholds, and priorities, to reduce the processing overhead and latency. Alternatively, the network administrator can upgrade the IPS hardware or software, or add more IPS devices to balance the load and increase the throughput⁴⁵

1: What is Network Congestion? Common Causes and How to Fix Them? -

GeeksforGeeks 2: Network congestion - Wikipedia 3: How to Fix Packet Loss - Lifewire 4: How to Optimize Your IPS Performance - Cisco 5: How to Avoid Network Bottlenecks - TechRepublic

NEW QUESTION 232

- (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 234

- (Topic 3)

A network administrator is looking for a solution to extend Layer 2 capabilities and replicate backups between sites. Which of the following is the best solution?

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

Answer: B

Explanation:

Data center interconnect (DCI) is a solution that allows Layer 2 connectivity and data replication between geographically dispersed data centers. DCI can be implemented using various technologies, such as optical networks, MPLS, VPNs, or Ethernet. DCI can provide benefits such as improved disaster recovery, load balancing, resource pooling, and cloud services.

References:

? Data Center Interconnect - CompTIA Network+ N10-008 Domain 1.4 - YouTube¹

? CompTIA Network+ Certification Exam Objectives, page 92

NEW QUESTION 238

- (Topic 3)

A network architect needs to create a wireless field network to provide reliable service to public safety vehicles. Which of the following types of networks is the best solution?

- A. Mesh
- B. Ad hoc
- C. Point-to-point
- D. Infrastructure

Answer: A

Explanation:

A mesh network is the best solution for creating a wireless field network to provide reliable service to public safety vehicles. A mesh network is a type of wireless network that consists of multiple nodes that communicate with each other directly or through intermediate nodes, forming a web-like topology. A mesh network does not rely on a central access point or router, but rather on the cooperation and coordination of the nodes themselves. A mesh network has several advantages for public safety applications, such as¹²:

? High availability and resilience: A mesh network can automatically route around failures or congestion, ensuring that the network remains operational even if some nodes are damaged or disconnected. A mesh network can also self-heal and self-configure, adapting to changes in the network topology or environment.

? Extended coverage and scalability: A mesh network can extend the wireless signal beyond the range of a single node, by using other nodes as relays or repeaters. A mesh network can also accommodate more nodes and devices, by adding more links and paths between them.

? Low cost and easy deployment: A mesh network can reduce the cost and complexity of installing and maintaining a wireless infrastructure, by eliminating the need for expensive cabling, towers, or antennas. A mesh network can also be deployed quickly and flexibly, by simply adding or removing nodes as needed. A mesh network is especially suitable for public safety vehicles, because it can provide reliable wireless communication in challenging scenarios, such as 12:

? Disaster response: A mesh network can be deployed rapidly in areas where the existing wireless infrastructure is damaged or unavailable, such as after an earthquake, flood, or fire. A mesh network can also support emergency services, such as fire fighting, search and rescue, or medical assistance, by enabling data, voice, and video transmission among the responders and command centers.

? Mobile surveillance: A mesh network can enable real-time monitoring and control of public safety vehicles, such as police cars, ambulances, or drones, by providing high-bandwidth and low-latency wireless connectivity. A mesh network can also support video streaming, location tracking, remote sensing, or analytics applications for public safety purposes.

? Event management: A mesh network can enhance the security and efficiency of large-scale events, such as concerts, festivals, or parades, by providing wireless coverage and capacity for the event organizers and participants. A mesh network can also support crowd management, traffic control, or public announcement applications for event management.

The other options are not the best solutions for creating a wireless field network to provide reliable service to public safety vehicles. An ad hoc network is a type of wireless network that consists of devices that communicate with each other directly without any central coordination or infrastructure. An ad hoc network is simple and flexible, but it has limited scalability and performance³. A point-to-point network is a type of wireless network that consists of two devices that communicate with each other over a single link. A point-to-point network is fast and secure, but it has limited coverage and functionality. An infrastructure network is a type of wireless network that consists of devices that communicate with each other through an access point or router. An infrastructure network is stable and robust, but it has high cost and complexity.

NEW QUESTION 243

- (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 245

- (Topic 3)

A technician is contracted to install a redundant cluster of devices from the ISP In case of a hardware failure within the network. Which of the following would provide the BEST redundant solution in Layer 2 devices?

- A. Multiple routers
- B. Multiple switches
- C. Multiple firewalls
- D. Multiple budes

Answer: B

NEW QUESTION 249

- (Topic 3)

A company realizes that only half of its employees work in the office, and the employees who work from home no longer need a computer at the office. Which of the following security measures should the network administrator implement when removing a computer from a cubicle?

- A. Disable DHCP on the computer being removed.
- B. Place the switch port in a private VLAN.
- C. Apply a firewall rule to block the computer's IP address.
- D. Remove the employee's network access.

Answer: D

Explanation:

The best security measure to implement when removing a computer from a cubicle is to remove the employee's network access. This will prevent the employee from accessing any network resources or data from the computer, as well as prevent any unauthorized users from using the computer to access the network. Removing the employee's network access can be done by deleting or disabling the user account, revoking the credentials, or changing the permissions. The other options are not as effective or necessary as removing the employee's network access. They are:

- Disabling DHCP on the computer being removed will prevent the computer from obtaining an IP address from the network, but it will not prevent the computer from using a static IP address or accessing the network through another device.
- Placing the switch port in a private VLAN will isolate the computer from other devices on the network, but it will not prevent the computer from accessing the

network through another port or device.

•Applying a firewall rule to block the computer's IP address will prevent the computer from communicating with the network, but it will not prevent the computer from changing its IP address or accessing the network through another device.

References

1: CompTIA Network+ N10-008 Cert Guide - O'Reilly Media 2: Network+ (Plus) Certification | CompTIA IT Certifications

3: 10 Ways to Secure Office Workstations - Computer Security

NEW QUESTION 250

- (Topic 3)

A divide-and-conquer approach is a troubleshooting method that involves breaking a complex problem into smaller and more manageable parts, and then testing each part to isolate the cause of the problem. In this scenario, the technician is using a divide-and-conquer approach by pinging the default gateway and DNS server of the workstation, which are two possible sources of connectivity issues. By pinging these devices, the technician can determine if the problem is related to the local network or the external network.

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

- A. A router with only one available LAN port
- B. A firewall performing deep packet inspection
- C. A hub utilizing jumbo frames
- D. A switch using Spanning Tree Protocol

Answer: A

Explanation:

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

References:

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

? CompTIA Network+ Certification Exam Objectives, page 92

NEW QUESTION 254

- (Topic 3)

A junior network engineer is trying to change the native network ID to a non-default value that can then be applied consistently throughout the network environment. Which of the following issues is the engineer attempting to prevent?

- A. DDoS
- B. ARP spoofing
- C. VLAN hopping
- D. Rogue DHCP

Answer: C

Explanation:

VLAN hopping is a type of network attack where an attacker can send or receive traffic from a VLAN that they are not supposed to access. VLAN hopping can allow an attacker to bypass security policies, access sensitive data, or launch other attacks on the network. VLAN hopping can be performed using two methods: double tagging and switch spoofing1.

Double tagging is where the attacker sends a frame with two VLAN tags, one for the native VLAN and one for the target VLAN. The native VLAN is the VLAN that is used for untagged traffic on a trunk port. If the attacker's access port is in the same VLAN as the native VLAN, the switch will accept the frame and forward it on the trunk port. The switch will remove the first tag, which is the native VLAN, and send the frame with the second tag, which is the target VLAN. The frame will then reach the target VLAN and be processed by the devices in that VLAN.

Switch spoofing is where the attacker sends Dynamic Trunking Protocol (DTP) packets and tries to negotiate a trunk with the switch. DTP is a Cisco protocol that allows switches to automatically form trunks between them. If the switch's port is configured with the default dynamic auto or dynamic desirable mode, it will accept the DTP packets and form a trunk with the attacker. The attacker will then have access to all VLANs on the trunk.

To prevent VLAN hopping, the junior network engineer is trying to change the native network ID to a non-default value that can then be applied consistently throughout the network environment. This means that the engineer is changing the VLAN that is used for untagged traffic on the trunk ports to a different VLAN than the default VLAN 1. This will prevent double tagging attacks, as the attacker's access port will not be in the same VLAN as the native VLAN, and the switch will not accept the frames with two tags. The engineer should also disable DTP on the trunk ports and use the switchport nonegotiate command to prevent switch spoofing attacks2.

ReferencesVLAN Hopping - NetworkLessons.comVLAN Hopping on Native VLAN - Cisco Community

NEW QUESTION 255

- (Topic 3)

Users report they cannot reach any websites on the internet. An on-site network engineer is able to duplicate the issue on a different PC. The network engineer then tries to ping a website and receives the following message:

Ping request could not find host www.google.com. Please check the name and try again. Which of the following is the next step the engineer should take?

- A. Ping 127. 0. 0. 1 to test local hardware.
- B. Test the website from outside the company.
- C. Ping internal name server functionality.
- D. Check internet firewall logs for blocked DNS traffi

Answer: C

Explanation:

The error message "Ping request could not find host www.google.com" indicates that the network engineer's PC cannot resolve the hostname www.google.com to its corresponding IP address. This means that there is a problem with the DNS (Domain Name System) service, which is responsible for translating hostnames

to IP addresses and vice versa. The DNS service can be provided by internal or external name servers, depending on the network configuration. The next step the engineer should take is to ping the internal name server functionality, which means to test if the PC can communicate with the name server that is configured in its network settings, and if the name server can resolve internal hostnames, such as those of the company's servers or devices. To do this, the engineer can use the following commands:

- ? To find out the IP address of the name server, use `ipconfig /all` and look for the DNS Servers entry.
- ? To ping the name server, use `ping <name server IP address>` and check if the packets are sent and received successfully.
- ? To test the name resolution, use `nslookup <internal hostname>` and check if the name server returns the correct IP address.

If the ping or the nslookup commands fail, it means that the internal name server is not working properly, and the engineer should troubleshoot the name server configuration or connectivity. If the ping and the nslookup commands succeed, it means that the internal name server is working properly, but there is a problem with the external name resolution, and the engineer should check the internet firewall logs for blocked DNS traffic, or test the website from outside the company.

References Windows 10 can't resolve hostnames - ping with IP works but not with hostname Ping request could not find host xyz.local. Please check the name and try again DNS problem, nslookup works, ping doesn't Users are connected to a switch on an Ethernet interface of a campus router. The service provider is connected to the serial 1 interface on the router. The output of the interfaces is:

E1/0: 192.168.8.1/24 S1: 192.168.7.252/30

NEW QUESTION 258

- (Topic 3)

A network consultant is installing a new wireless network with the following specifications:

5GHz

1,300Mbps 20/40/80MHz

Which of the following standards should the network consultant use?

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

Answer: B

NEW QUESTION 259

- (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 264

- (Topic 3)

Which of the following would be used to indicate when unauthorized access to physical internal hardware has occurred?

- A. Motion detectors
- B. Radio frequency identification tags
- C. Tamper evident seal
- D. Locking racks

Answer: C

Explanation:

A tamper evident seal is a device or material that provides a visible indication of unauthorized access to physical internal hardware. Tamper evident seals can be stickers, labels, tapes, locks, or seals that are designed to break, tear, or change color when someone tries to open, remove, or tamper with them. Tamper evident seals can help deter and detect physical security breaches, such as theft, vandalism, or sabotage of hardware devices¹². Tamper evident seals can also provide evidence for forensic analysis and legal action³.

References

1 - What Is Hardware Security? Definition, Threats, and Best Practices 2 - Device Physical Security Guideline | Information Security Office

3 - What is unauthorized physical access? – Heimduo

NEW QUESTION 267

- (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 272

- (Topic 3)

Which of the following OSI model layers is where a technician would view UDP information?

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

Answer: D

NEW QUESTION 274

- (Topic 3)

A technician is troubleshooting a user's connectivity issues and finds that the computer's IP address was changed to 169.254.0.1.

Which of the following is the most likely reason?

- A. Two or more computers have the same IP address in the ARP table.
- B. The computer automatically set this address because the DHCP was not available.
- C. The computer was set up to perform as an NTP server.
- D. The computer is on a VPN and is the first to obtain a different IP address in that network.

Answer: B

Explanation:

IP addresses beginning with 169.254. are called link-local addresses or APIPA (Automatic Private IP Addressing)1. They are assigned by the computer itself when it cannot reach a DHCP server to obtain a valid IP address from the network2. This can happen for several reasons, such as a faulty router, a misconfigured network, or a disconnected cable3.

To troubleshoot this issue, the technician should check the network settings, the router configuration, and the physical connection of the computer. The technician should also try to renew the IP address by using the command `ipconfig /renew` in Windows or `dhclient` in Linux. If the problem persists, the technician may need to contact the network administrator or the ISP for further assistance.

NEW QUESTION 277

- (Topic 3)

A newly installed VoIP phone is not getting the DHCP IP address it needs to connect to the phone system. Which of the following tasks needs to be completed to allow the phone to operate correctly?

- A. Assign the phone's switchport to the correct VLAN
- B. Statically assign the phone's gateway address.
- C. Configure a route on the VoIP network router.
- D. Implement a VoIP gateway

Answer: A

NEW QUESTION 279

- (Topic 3)

Many IP security cameras use RTSP to control media playback. Which of the following default transport layer port numbers does RTSP use?

- A. 445
- B. 554
- C. 587
- D. 5060

Answer: B

Explanation:

RTSP stands for Real Time Streaming Protocol and is an application-level network protocol designed for controlling media playback on streaming media servers. RTSP uses the default transport layer port number 554 for both TCP and UDP1. Port 445 is used for SMB (Server Message Block), a protocol for file and printer sharing. Port 587 is used for SMTP (Simple Mail Transfer Protocol), a protocol for sending email messages. Port 5060 is used for SIP (Session Initiation Protocol), a protocol for initiating and managing multimedia sessions.

References: 1 Real Time Streaming Protocol - Wikipedia (https://en.wikipedia.org/wiki/Real_Time_Streaming_Protocol)

NEW QUESTION 284

- (Topic 3)

A network technician is selecting new network hardware, and availability is the main concern. Which of the following availability concepts should the technician consider?

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

Answer: A

Explanation:

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

NEW QUESTION 288

- (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 EIRP 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 289

- (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 293

- (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 297

- (Topic 3)

Which of the following ports should be used to securely receive mail that is synchronized across multiple devices?

- A. 25
- B. 110
- C. 443
- D. 993

Answer: D

NEW QUESTION 298

- (Topic 3)

A network manager wants to view network traffic for devices connected to a switch. A network engineer connects an appliance to a free port on the switch and needs to configure the switch port connected to the appliance. Which of the following is the best option for the engineer to enable?

- A. Trunking
- B. Port mirroring
- C. Full duplex
- D. SNMP

Answer: B

Explanation:

Port mirroring is a feature that allows a switch to copy the traffic from one or more ports to another port, where a network analyzer or a monitoring device can capture and analyze the traffic. Port mirroring is useful for troubleshooting and security purposes, as it allows the network engineer to see the traffic that is passing through the switch without affecting the normal operation of the network.

References

- ? 1: Port Mirroring - CompTIA Network+ Certification (N10-008): The Total Course [Video]
- ? 2: CompTIA Network+ Certification Exam Objectives, page 5
- ? 3: CompTIA Network+ N10-005: 2.1 – Port Mirroring - Professor Messer IT Certification Training Courses
- ? 4: CompTIA Network+ N10-005: 1.4 – Port Mirroring

NEW QUESTION 300

- (Topic 3)

Which of the following can be used to decrease latency during periods of high utilization of a firewall?

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

Answer: B

Explanation:

NIC Teaming, also known as load balancing and failover (LBFO), allows multiple network adapters on a computer to be placed into a team for the following purposes:

(<https://www.bing.com/search?q=what+is+nic+teaming+used+for%3F&form=QBLH&sp=-1&pq=what+is+nic+teaming+used+for&sc=10-28&q=n&sk=&cvid=13882A9A9B584D8099F4ABCAD034E821&ghsh=0&ghacc=0&ghpl=>)

NEW QUESTION 303

- (Topic 3)

Which of the following can be used to validate domain ownership by verifying the presence of pre-agreed content contained in a DNS record?

- A. SOA
- B. SRV
- C. AAA
- D. TXT

Answer: D

Explanation:

"One final usage of the TXT resource record is how some cloud service providers, such as Azure, validate ownership of custom domains. You are provided with data to include in your TXT record, and once that is created, the domain is verified and able to be used. The thought is that if you control the DNS, then you own the domain name."

NEW QUESTION 307

- (Topic 3)

A network technician is planning a network scope. The web server needs to be within 12.31.69.1 to 12.31.69.29. Which of the following would meet this requirement?

- A. Lease time
- B. Range reservation
- C. DNS
- D. Superscope

Answer: A

NEW QUESTION 308

- (Topic 3)

A network administrator replaced a faulty NIC in a printer, but the printer is still not reachable. The printer is configured with the correct IP address, mask, and gateway, and a link light is lit on the switch port that the printer is attached to.

Which of the following is the best command for the administrator to run first on the switch?

- A. show vlan
- B. show route
- C. show arp
- D. show config

Answer: A

Explanation:

The best command for the administrator to run first on the switch is show vlan, which displays the VLAN configuration information on the switch, such as the VLAN IDs, names, and ports. The show vlan command can help the administrator to verify if the printer is assigned to the correct VLAN, and if there is any mismatch or misconfiguration that prevents the printer from being reachable. The show route command displays the routing table on the switch, which is not relevant for the printer connectivity, as the printer is configured with the correct gateway. The show arp command displays the ARP cache on the switch, which maps the IP addresses to the MAC addresses of the devices. The show arp command can help the administrator to check if the switch has learned the MAC address of the printer, but it is not the best command to run first, as the ARP cache can be cleared or updated frequently. The show config command displays the running configuration on the switch, which includes the VLAN configuration, but it also includes other information that is not related to the printer issue, such as the hostname, the interface settings, the security settings, and so on. The show config command can be overwhelming and time-consuming to analyze, so it is not the best command to run first.

References

- ? 1: VLANs and Trunking – N10-008 CompTIA Network+ : 2.3
- ? 2: N10-008 CompTIA Network+ : 5.5
- ? 3: Interface Configurations – N10-008 CompTIA Network+ : 2.3
- ? 4: Configuring VLANs – CompTIA Network+ N10-006 – 2.6

NEW QUESTION 310

- (Topic 3)

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

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

Answer: C

Explanation:

According to the CompTIA Network+ troubleshooting model 123, this is the first step in troubleshooting a network problem. The technician should gather information about the current state of the network, such as error messages, device status, network topology, and user feedback. This can help narrow down the scope of the problem and eliminate possible causes.

NEW QUESTION 312

- (Topic 3)

An engineer needs to restrict the database servers that are in the same subnet from communicating with each other. The database servers will still need to communicate with the application servers in a different subnet. In some cases, the database servers will be clustered, and the servers will need to communicate with other cluster members. Which of the following technologies will be BEST to use to implement this filtering without creating rules?

- A. Private VLANs
- B. Access control lists
- C. Firewalls
- D. Control plane policing

Answer: A

Explanation:

"Use private VLANs: Also known as port isolation, creating a private VLAN is a method of restricting switch ports (now called private ports) so that they can communicate only with a particular uplink. The private VLAN usually has numerous private ports and only one uplink, which is usually connected to a router, or firewall."

NEW QUESTION 317

- (Topic 3)

An engineer is gathering data to determine the effectiveness of UPSs in use at remote retail locations. Which of the following statistics can the engineer use to determine the availability of the remote network equipment?

- A. Uptime
- B. NetFlow baseline
- C. SNMP traps
- D. Interface statistics

Answer: A

Explanation:

Uptime is a statistic that can be used to determine the availability of the remote network equipment. Uptime is the amount of time that a device or system has been running without experiencing any failures or disruptions. It is commonly expressed as a percentage of total time, such as 99.99% uptime. By measuring the uptime of the network equipment at the remote retail locations, the engineer can determine how reliable and available the equipment is.

NEW QUESTION 319

- (Topic 3)

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

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

Answer: B

Explanation:

A duplicate IP address occurs when two devices on the same network have the same IP address assigned to them. This can cause intermittent connection issues, as the network devices may not be able to distinguish between the two conflicting devices. A duplicate IP address can be caused by a visitor manually configuring a static IP address that is already in use by another device on the guest network. The network IP range of 192.168.1.0/28 has only 14 usable host addresses, so the chances of a duplicate IP address are higher than a larger network.

References

? 1: Troubleshooting IP Configurations – CompTIA Network+ N10-006 – 4.6

? 2: Troubleshooting Duplicate IP Addresses - CompTIA Network+ N10-005: 2.5

? 3: Network Address Translation – N10-008 CompTIA Network+ : 1.4

NEW QUESTION 323

- (Topic 3)

Which of the following will reduce routing table lookups by performing packet forwarding decisions independently of the network layer header?

- A. MPLS
- B. mGRE
- C. EIGRP
- D. VRRP

Answer: A

Explanation:

Multiprotocol Label Switching, or MPLS, is a networking technology that routes traffic using the shortest path based on "labels," rather than network addresses, to handle forwarding over private wide area networks. As a scalable and protocol- independent solution, MPLS assigns labels to each data packet, controlling the path the packet follows. MPLS greatly improves the speed of traffic, so users don't experience downtime when connected to the network.

NEW QUESTION 326

- (Topic 3)

A technician needs to set up a wireless connection that utilizes MIMO on non-overlapping channels. Which of the following would be the best choice?

- A. 802.11a
- B. 802.11b
- C. 802.11g
- D. 802.11n

Answer: D

Explanation:

802.11n is the best choice for setting up a wireless connection that utilizes MIMO on non-overlapping channels. 802.11n is a wireless standard that offers faster speeds and longer range than previous standards. 802.11n uses multiple-input multiple- output (MIMO) technology, which allows multiple antennas to transmit and receive multiple spatial streams of data simultaneously. MIMO can improve wireless performance, reliability, and capacity by exploiting multipath propagation and spatial diversity. 802.11n also uses non-overlapping channels in both the 2.4 GHz and 5 GHz frequency bands to avoid interference and increase bandwidth. Non-overlapping channels are channels that do not share any part of their frequency spectrum with other channels. References: [CompTIA Network+ Certification Exam Objectives], 802.11n - Wikipedia

NEW QUESTION 328

- (Topic 3)

A user is unable to reach any resources on the internet. A technician goes to the site and obtains the following output from the workstation:

Network Destination	Netmask	Gateway	Interface	Metric
10.10.51.0	255.255.255.0	On-Link	10.10.51.147	291
10.10.51.147	255.255.255.255	On-Link	10.10.51.147	291
10.10.51.255	255.255.255.255	On-Link	10.10.51.147	297
127.0.0.0	255.0.0.0	On-Link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-Link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-Link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-Link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-Link	10.10.51.147	291
255.255.255.255	255.255.255.255	On-Link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-Link	10.10.51.147	291

Which of the following commands should the technician use to correct the issue?

- A. route ADD 0.0.0.0 MASK 0.0.0.0 10.10.51.10 metric 35
- B. route CHANGE 10.10.51.0 MASK 255.255.255.255 10.10.52.1 metric 5
- C. route CHANGE 10.10.51.255 MASK 255.0.0.0 On-Link metric 1
- D. route DELETE 127.255.255.255

Answer: A

Explanation:

The route command is used to view and manipulate the IP routing table in Windows operating systems⁴⁵⁶ The routing table contains information about how to reach different network destinations. The output from the workstation shows that the routing table does not have a default gateway, which is a router that forwards packets to other networks that are not directly connected to the local network. A default gateway is usually specified by a route with a destination of 0.0.0.0 and a netmask of 0.0.0.0, which matches any IP address. To correct the issue, the technician can use the route ADD command to add a default gateway to the routing table. The syntax of the command is:

route ADD <destination> MASK <netmask> <gateway> metric <metric>

The destination and netmask parameters should be 0.0.0.0 to indicate a default route. The gateway parameter should be the IP address of the router that can reach the internet, which is 10.10.51.10 in this case. The metric parameter is an optional value that indicates the cost or preference of the route, which can be used to choose between multiple routes to the same destination. A lower metric means a higher preference. The metric parameter can be any integer between 1 and 9999. In this case, the metric parameter can be 35 or any other value.

Therefore, the correct command is:

route ADD 0.0.0.0 MASK 0.0.0.0 10.10.51.10 metric 35

NEW QUESTION 331

- (Topic 3)

Which of the following bandwidth management techniques uses buffers at the client side to prevent TCP retransmissions from occurring when the ISP starts to drop packets of specific types that exceed the agreed traffic rate?

- A. Traffic shaping
- B. Traffic policing
- C. Traffic marking
- D. Traffic prioritization

Answer: D

NEW QUESTION 333

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The N10-009 Practice Test Here](#)