



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)

Which of the following compromises internet-connected devices and makes them vulnerable to becoming part of a botnet? (Select TWO).

- A. Deauthentication attack
- B. Malware infection
- C. IP spoofing
- D. Firmware corruption
- E. Use of default credentials
- F. Dictionary attack

Answer: BE

NEW QUESTION 3

- (Topic 3)

During an incident, an analyst sends reports regularly to the investigation and leadership teams. Which of the following best describes how PII should be safeguarded during an incident?

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

Answer: C

Explanation:

PII stands for Personally Identifiable Information, which is any data that can be used to identify, contact, or locate a specific individual, such as name, address, phone number, email, social security number, and so on. PII should be safeguarded during an incident to protect the privacy and security of the individuals involved, and to comply with the legal and ethical obligations of the organization. One way to safeguard PII during an incident is to implement data encryption, which is a process of transforming data into an unreadable format that can only be accessed by authorized parties who have the decryption key. Data encryption can prevent unauthorized access, modification, or disclosure of PII by malicious actors or third parties. Another way to safeguard PII during an incident is to create a standardized procedure for deleting data that is no longer needed, such as after the incident is resolved or the investigation is completed. Deleting data that is no longer needed can reduce the risk of data breaches, data leaks, or data theft, and can also save storage space and resources. A standardized procedure for deleting data can ensure that the data is erased securely and completely, and that the deletion process is documented and audited.

References

? 1: CompTIA Network+ N10-008 Certification Study Guide, page 304-305

? 2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 13

? 3: CompTIA Network+ N10-008 Certification Practice Test, question 5

? 4: Data Encryption – N10-008 CompTIA Network+ : 3.1

NEW QUESTION 4

- (Topic 3)

A network technician is troubleshooting a port channel issue. When logging in to one of the switches, the technician sees the following information displayed:

Native VLAN mismatch detected on interface g0/1

Which of the following layers of the OSI model is most likely to be where the issue resides?

- A. Layer 2
- B. Layer 3

- C. Layer 5
- D. Layer 6

Answer: A

Explanation:

Layer 2 of the OSI model is the data link layer, which is responsible for transferring data between adjacent nodes on a network. It uses protocols such as Ethernet, PPP, and HDLC to encapsulate data into frames and add MAC addresses for source and destination identification. It also uses protocols such as STP, LACP, and CDP to manage the physical links and prevent loops, aggregate bandwidth, and discover neighboring devices¹²

A native VLAN mismatch is a common Layer 2 issue that occurs when two switches are connected by a trunk port, but have different native VLANs configured on their interfaces. A native VLAN is the VLAN that is assigned to untagged frames on a trunk port. If the native VLANs do not match, the switches will drop the untagged frames and generate an error message. This can cause connectivity problems and security risks on the network³⁴⁵

To resolve a native VLAN mismatch, the network technician should ensure that both switches have the same native VLAN configured on their trunk ports, or use a different port mode such as access or general.

NEW QUESTION 5

- (Topic 3)

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

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

Answer: B

Explanation:

A screened subnet is a network segment that is isolated from both the internal and external networks by firewalls or routers. It is used to host publicly accessible servers that need some protection from external attacks, but also need to be separated from the internal network for security reasons.

References

? 1: Seven-Second Subnetting – N10-008 CompTIA Network+ : 1.4

? 2: CompTIA Network+ Study Guide: Exam N10-008, 5th Edition, page 56

? 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 22

NEW QUESTION 6

- (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 7

- (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 8

- (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 9

- (Topic 3)

A company is moving to a new building designed with a guest waiting area that has existing network ports. Which of the following practices would BEST secure the network?

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

Answer: B

Explanation:

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

NEW QUESTION 10

- (Topic 3)

A user is required to log in to a main web application, which then grants the user access to all other programs needed to complete job-related tasks. Which of the following authentication methods does this setup describe?

- A. SSO
- B. RADIUS
- C. TACACS+
- D. Multifactor authentication
- E. 802.1X

Answer: A

Explanation:

The authentication method that this setup describes is SSO (Single Sign-On). SSO is a technique that allows a user to log in once to a main web application and then access multiple other applications or services without having to re-enter credentials. SSO simplifies the user experience and reduces the number of passwords to remember and manage. References: CompTIA Network+ N10-008 Certification Study Guide, page 371; The Official CompTIA Network+ Student Guide (Exam N10-008), page 14-5.

NEW QUESTION 10

- (Topic 3)

A network administrator is given the network 80.87.78.0/26 for specific device assignments. Which of the following describes this network?

- A. 80.87.78.0 - 80.87.78.14
- B. 80.87.78.0 - 80.87.78.110
- C. 80.87.78.1 - 80.87.78.62
- D. 80.87.78.1 - 80.87.78.158

Answer: C

Explanation:

The network 80.87.78.0/26 is a Class A network with a subnet mask of /26, which means that it contains 26 bits of network information and 6 bits of host information.

The range of valid host addresses for this network is 80.87.78.1 to 80.87.78.62. Any addresses outside of this range are reserved for special purposes or are not used.

NEW QUESTION 14

- (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 16

- (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 18

- (Topic 3)

A technician is monitoring a network interface and notices the device is dropping packets. The cable and interfaces, however, are in working order. Which of the following is MOST likely the cause?

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

Answer: C

NEW QUESTION 23

- (Topic 3)

During the troubleshooting of an E1 line, the point-to-point link on the core router was accidentally unplugged and left unconnected for several hours. However, the network management team was not notified. Which of the following could have been configured to allow early detection and possible resolution of the issue?

- A. Traps
- B. MIB
- C. OID
- D. Baselines

Answer: A

Explanation:

Traps are unsolicited messages sent by network devices to a network management system (NMS) when an event or a change in status occurs. Traps can help notify the network management team of any issues or problems on the network, such as a link failure or a device reboot. Traps can also trigger actions or alerts on the NMS, such as sending an email or logging the event. MIB stands for Management Information Base and is a database of information that can be accessed and managed by an NMS using SNMP (Simple Network Management Protocol). OID stands for Object Identifier and is a unique name that identifies a specific variable in the MIB. Baselines are measurements of normal network performance and behavior that can be used for comparison and analysis. References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5: Given a scenario, use remote access methods.

NEW QUESTION 28

- (Topic 3)

A network administrator is trying to create a subnet, which is the most efficient size possible, for 31 laptops. Which of the following network subnets would be best in this situation?

- A. 10.10.10.0/24
- B. 10.10.10.0/25
- C. 10.10.10.0/26
- D. 10.10.10.0/27

Answer: D

Explanation:

A /27 subnet mask has 32 IP addresses, of which 30 are usable for hosts. This is the smallest subnet that can accommodate 31 laptops, as the other options have either too few or too many IP addresses. A /27 subnet mask is equivalent to 255.255.255.224 in decimal notation, and has a wildcard mask of 0.0.0.31. The network address is 10.10.10.0, and the broadcast address is 10.10.10.31. The usable host range is 10.10.10.1 to 10.10.10.30.

References

- 1: Subnet Cheat Sheet – 24 Subnet Mask, 30, 26, 27, 29, and other IP Address CIDR Network References
- 2: IP Subnet Calculator

NEW QUESTION 29

- (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. Reterminate 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. Reterminating 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 32

- (Topic 3)

A network technician 13 troubleshooting a specific port on a switch. Which of the following commands should the technician use to see the port configuration?

- A. show route
- B. show Interface
- C. show arp
- D. show port

Answer: B

Explanation:

To see the configuration of a specific port on a switch, the network technician should use the "show interface" command. This command provides detailed information about the interface, including the current configuration, status, and statistics for the interface.

NEW QUESTION 36

- (Topic 3)

Which of the following protocols is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links?

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

Answer: A

NEW QUESTION 38

- (Topic 3)

A technician is troubleshooting network connectivity from a wall jack. Readings from a multimeter indicate extremely low ohmic values instead of the rated impedance from the switchport. Which of the following is the MOST likely cause of this issue?

- A. Incorrect transceivers
- B. Faulty LED
- C. Short circuit
- D. Upgraded OS version on switch

Answer: C

Explanation:

A short circuit is a condition where two conductors in a circuit are connected unintentionally, creating a low resistance path for the current. This causes the voltage to drop and the current to increase, which can damage the circuit or cause a fire. A multimeter can measure the resistance or impedance of a circuit, and if it shows extremely low values, it indicates a short circuit.

NEW QUESTION 41

- (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 43

- (Topic 3)

A technician monitors a switch interface and notices it is not forwarding frames on a trunked port. However, the cable and interfaces are in working order. Which of the following is MOST likely the cause of the issue?

- A. STP policy
- B. Flow control
- C. 802.1Q configuration
- D. Frame size

Answer: C

Explanation:

802.1Q configuration is the most likely cause of the issue where a switch interface is not forwarding frames on a trunked port. 802.1Q is a standard that defines how to create and manage virtual LANs (VLANs) on a switched network. VLANs are logical segments of a network that group devices based on criteria such as function, department, or security level. VLANs can improve network performance, security, and manageability by reducing broadcast domains, isolating traffic, and enforcing policies. A trunked port is a switch port that can carry traffic from multiple VLANs over a single physical link by adding a VLAN tag to each frame. A VLAN tag is a 4-byte header that identifies the VLAN ID and priority of each frame. A trunked port requires 802.1Q configuration to specify which VLANs are allowed or disallowed on the port, and which VLAN is the native or untagged VLAN. If the 802.1Q configuration is incorrect or mismatched between switches, frames may be dropped or misrouted on the trunked port. References: [CompTIA Network+ Certification Exam Objectives], VLAN Trunking Protocol (VTP) Explained | NetworkLessons.com

NEW QUESTION 46

- (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 49

- (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 53

- (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 54

- (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 59

- (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 62

- (Topic 3)

Users are reporting performance issues when attempting to access the main fileshare server. Which of the following steps should a network administrator perform next based on the network troubleshooting methodology?

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

Answer: B

Explanation:

According to the network troubleshooting methodology, the first step is to identify the problem and gather information about the current state of the network using the network troubleshooting tools that are available¹. The next step is to determine if anything has changed in the network configuration, environment, or usage that could have caused or contributed to the performance issues¹. This step helps to narrow down the possible causes and eliminate irrelevant factors. For example, the network administrator could check if there were any recent updates, patches, or modifications to the fileshare server or the network devices that connect to it. They could also check if there was an increase in network traffic or demand for the fileshare server resources².

The other options are not correct because they are not the next steps in the network troubleshooting methodology. Implementing a fix to resolve the connectivity issues (A) is premature without determining the root cause of the problem. Establishing a theory of probable cause³ is a later step that requires testing and verification. Documenting all findings, actions, and lessons learned (D) is the final step that should be done after resolving the problem and restoring normal network operations¹.

NEW QUESTION 67

- (Topic 3)

Which of the following, in addition to a password, can be asked of a user for MFA?

- A. PIN
- B. Favorite color
- C. Hard token
- D. Mother's maiden name

Answer: A

Explanation:

MFA stands for Multi-Factor Authentication, which is a method of verifying the identity of a user by requiring two or more pieces of evidence that belong to different categories: something the user knows, something the user has, or something the user is. A password is something the user knows, and it is usually combined with another factor such as a PIN (Personal Identification Number) or a hard token (a physical device that generates a one-time code) that the user has. A favorite color or a mother's maiden name are not suitable for MFA, as they are also something the user knows and can be easily guessed or compromised.

References

? 1: Multi-Factor Authentication – N10-008 CompTIA Network+ : 3.1

? 2: CompTIA Network+ Certification Exam Objectives, page 13

? 3: CompTIA Network+ N10-008 Certification Study Guide, page 250

? 4: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 14

NEW QUESTION 68

- (Topic 3)

A network technician wants to find the shortest path from one node to every other node in the network. Which of the following algorithms will provide the FASTEST convergence time?

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

Answer: B

Explanation:

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

NEW QUESTION 72

- (Topic 3)

An ISP is providing Internet to a retail store and has terminated its point of connection using a standard Cat 6 pin-out Which of me following terminations should the technician use when running a cable from the ISP's port lo the front desk?

- A. F-type connector
- B. TIA/E1A-56S-B
- C. LC
- D. SC

Answer: B

Explanation:

The termination that the technician should use when running a cable from the ISP's port to the front desk is B. TIA/EIA-568-B. This is a standard pin-out for Cat 6 cables that is used for Ethernet and other network physical layers¹. It specifies how to arrange the eight wires in an RJ45 connector, which is a common type of connector for network cables.

NEW QUESTION 77

- (Topic 3)

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

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

Answer: AE

Explanation:

? AP transmit power: You should check if your APs have sufficient power output and adjust them if needed. You should also make sure they are not exceeding regulatory limits for your region.

? Antenna gain: You should check if your antennas have adequate gain for your coverage area and replace them if needed. You should also make sure they are aligned properly and not obstructed by any objects.

In the scenario described, the wireless controller is measuring a low EIRP value compared to the recommendations noted in the most recent site survey. EIRP is the combination of the power transmitted by the access point and the antenna gain. Therefore, to increase the EIRP value to meet the site survey's specifications, the administrator should verify or replace the AP transmit power (option A) and the antenna gain (option E). This can be achieved by adjusting the transmit power settings on the AP or by replacing the AP's antenna with one that has a higher gain

NEW QUESTION 80

- (Topic 3)

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

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

Answer: A

NEW QUESTION 85

- (Topic 3)

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

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

Answer: A

Explanation:

A protocol analyzer is the best way to verify traffic to and from the server. A protocol analyzer, also known as a packet sniffer or network analyzer, is a tool that captures and analyzes the network packets that are sent and received by a device. A protocol analyzer can show the source and destination IP addresses, ports, protocols, and payload of each packet, as well as any errors or anomalies in the network communication. A protocol analyzer can help troubleshoot network connectivity issues by identifying the root cause of the problem, such as misconfigured firewall rules, incorrect routing, or faulty network devices¹².

To use a protocol analyzer to verify traffic to and from the server, the customer can follow these steps:

? Install a protocol analyzer tool on a device that is connected to the same network as the server, such as Wireshark³ or Microsoft Network Monitor⁴.

? Select the network interface that is used to communicate with the server, and start capturing the network traffic.

? Filter the captured traffic by using the IP address or hostname of the server, or by using a specific port or protocol that is used by the database service.

? Analyze the filtered traffic and look for any signs of successful or failed connection attempts, such as TCP SYN, ACK, or RST packets, or ICMP messages.

? If there are no connection attempts to or from the server, then there may be a problem with the network configuration or device settings that prevent the traffic from reaching the server.

? If there are connection attempts but they are rejected or dropped by the server, then there may be a problem with the server configuration or service settings that prevent the traffic from being accepted by the server.

The other options are not the best ways to verify traffic to and from the server. nmap is a tool that can scan a network and discover hosts and services, but it cannot capture and analyze the network packets in detail. ipconfig is a command that can display and configure the IP settings of a device, but it cannot monitor or test the network communication with another device. Speed test is a tool that can measure the bandwidth and latency of a network connection, but it cannot diagnose or troubleshoot specific network problems.

NEW QUESTION 90

- (Topic 3)

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

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

Answer: D

NEW QUESTION 91

- (Topic 3)

A network architect is developing documentation for an upcoming IPv4/IPv6 dual-stack implementation. The architect wants to shorten the following IPv6 address: ef82:0000:0000:0000:0000:1ab1:1234:1bc2. Which of the following is the MOST appropriate shortened version?

- A. ef82:0:1ab1:1234:1bc2
- B. ef82:0::1ab1:1234:1bc2
- C. ef82:0:0:0:0:1ab1:1234:1bc2
- D. ef82::1ab1:1234:1bc2

Answer: D

Explanation:

The most appropriate shortened version of the IPv6 address ef82:0000:0000:0000:0000:1ab1:1234:1bc2 is ef82::1ab1:1234:1bc2. IPv6 addresses are 128-bit hexadecimal values that are divided into eight groups of 16 bits each, separated by colons. IPv6 addresses can be shortened by using two rules: omitting leading zeros within each group, and replacing one or more consecutive groups of zeros with a double colon (::). Only one double colon can be used in an address.

Applying these rules to the given address results in ef82::1ab1:1234:1bc2. References: CompTIA Network+ N10-008 Certification Study Guide, page 114; The Official CompTIA Network+ Student Guide (Exam N10-008), page 5-7.

NEW QUESTION 96

- (Topic 3)

A company is reviewing ways to cut the overall cost of its IT budget. A network technician suggests removing various computer programs from the IT budget and only providing these programs on an as-needed basis. Which of the following models would meet this requirement?

- A. Multitenancy
- B. IaaS
- C. SaaS
- D. VPN

Answer: C

Explanation:

SaaS stands for Software as a Service and is a cloud computing model where software applications are hosted and delivered over the internet by a service provider. SaaS can help the company cut the overall cost of its IT budget by eliminating the need to purchase, install, update, and maintain various computer programs on its own devices. The company can access the programs on an as-needed basis and pay only for what it uses. Multitenancy is a feature of cloud computing where multiple customers share the same physical or virtual resources. IaaS stands for Infrastructure as a Service and is a cloud computing model where computing resources such as servers, storage, and networking are provided over the internet by a service provider. VPN stands for Virtual Private Network.

and is a technology that creates a secure and encrypted connection over a public network.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.9: Compare and contrast common network service types.

NEW QUESTION 97

- (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 102

- (Topic 3)

The Chief Executive Officer of a company wants to ensure business operations are not disrupted in the event of a disaster. The solution must have fully redundant equipment, real-time synchronization, and zero data loss. Which Of the following should be prepared?

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

Answer: C

Explanation:

A hot site is a backup site that is fully equipped and ready to take over the operations of the primary site in the event of a disaster. A hot site has real-time synchronization with the primary site and can provide zero data loss. A hot site is the most expensive and reliable option for disaster recovery.

References: Network+ Study Guide Objective 5.3: Explain common scanning, monitoring and patching processes and summarize their expected outputs.

NEW QUESTION 106

- (Topic 3)

In which of the following components do routing protocols belong in a software-defined network?

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

Answer: B

Explanation:

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

NEW QUESTION 107

- (Topic 3)

A network engineer designed and implemented a new office space with the following characteristics:

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

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

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

D. Change to directional antennas-

Answer: D

Explanation:

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

NEW QUESTION 110

- (Topic 3)

Which of the following is the IEEE link cost for a Fast Ethernet interface in STP calculations?

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

Answer: D

Explanation:

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

NEW QUESTION 112

- (Topic 3)

A network administrator needs to monitor traffic on a specific port on a switch. Which of the following should the administrator configure to accomplish the task?

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

Answer: C

Explanation:

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

NEW QUESTION 113

- (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 117

- (Topic 3)

A network technician has determined the cause of a network disruption. Which of the following is the NEXT step for the technician to perform?

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

Answer: C

NEW QUESTION 121

- (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 122

- (Topic 3)

Which of the following architectures is used for FTP?

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

Answer: A

Explanation:

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

NEW QUESTION 123

- (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 126

- (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 128

- (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 130

- (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 135

- (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 138

- (Topic 3)

A network technician receives a support ticket concerning multiple users who are unable access the company's shared drive. The switch interface that the shared drive is connected to is displaying the following:

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

Which of the following is MOST likely the issue?

- A. The switchport is shut down
- B. The cable is not plugged in.
- C. The loopback is not set
- D. The bandwidth configuration is incorrect.

Answer: A

Explanation:

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

NEW QUESTION 141

- (Topic 3)

A network engineer needs to change an entire subnet of SLAAC-configured workstation addresses. Which of the following methods would be the best for the engineer to use?

- A. Change the address prefix in ARP in order for the workstations to retrieve their new addresses.
- B. Change the address prefix in a router in order for the router to advertise the new prefix with an ND.
- C. Change the address prefix scope in a DHCP server in order for the workstations to retrieve their new addresses.

D. Change the workstations' address prefix manually because an automated method does not exist.

Answer: B

Explanation:

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

References¹ - IPv6 Stateless Address Auto-configuration (SLAAC) | NetworkAcademy.io² - IPv6 SLAAC – Stateless Address Autoconfiguration - Study-CCNA3 - Mastering IPv6

SLAAC Concepts and Configuration - Cisco Press

NEW QUESTION 142

- (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 146

- (Topic 3)

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

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

Answer: A

NEW QUESTION 151

- (Topic 3)

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

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

Answer: AC

Explanation:

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

NEW QUESTION 154

- (Topic 3)

Which of the following should a network administrator configure when adding OT devices to an organization's architecture?

- A. Honeynet
- B. Data-at-rest encryption
- C. Time-based authentication
- D. Network segmentation

Answer: D

Explanation:

Network segmentation is the process of dividing a network into smaller subnets or segments, each with its own security policies and access controls. This can help isolate OT devices from IT devices, guest networks, and other potential threats, as well as improve network performance and efficiency. Network segmentation is a recommended security practice for OT environments, as it can limit the attack surface, contain the damage of a breach, and comply with regulatory standards.

<https://sectrio.com/complete-guide-to-ot-network-segmentation/>

NEW QUESTION 156

- (Topic 3)

Which of the following documents dictates the uptimes that were agreed upon by the involved parties?

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

Answer: C

Explanation:

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

NEW QUESTION 157

- (Topic 3)

During a risk assessment which of the following should be considered when planning to mitigate high CPU utilization of a firewall?

- A. Recovery time objective
- B. Uninterruptible power supply
- C. NIC teaming
- D. Load balancing

Answer: D

Explanation:

The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs. This does nothing to help with CPU utilization. Load balancing does this.

NEW QUESTION 160

- (Topic 3)

A company is designing a SAN and would like to use STP as its medium for communication. Which of the following protocols would BEST suit me company's needs?

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

Answer: B

Explanation:

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

NEW QUESTION 162

- (Topic 3)

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

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

Answer: B

Explanation:

The document used to inform all parties about the scope of the project before it starts is likely a project charter.

A project charter is a document that outlines the key aspects of a project, including the project's objectives, scope, stakeholders, and resources. It serves as a formal agreement between the project team and the stakeholders, and helps to define the project's goals and constraints.

A project charter typically includes information about the project's scope, including the specific deliverables that are expected and any constraints or limitations that may impact the project. It may also include details about the project team and stakeholders, the project schedule and budget, and the roles and responsibilities of each party.

By creating a project charter, the Chief Executive Officer and the network administrator can ensure that all parties involved in the project have a clear understanding of the project's goals and objectives, and can help to prevent misunderstandings or miscommunications during the project.

What is in a project charter?

A project charter is a formal short document that states a project exists and provides project managers with written authority to begin work. A project charter document describes a project to create a shared understanding of its goals, objectives and resource requirements before the project is scoped out in detail.

What are the 5 elements of the project charter?

What Are the Contents of a Project Charter? A project charter should always include an overview, an outline of scope, an approximate schedule, a budget estimate, anticipated risks, and key stakeholders

NEW QUESTION 167

- (Topic 3)

Network connectivity in an extensive forest reserve was achieved using fiber optics. A network fault was detected, and now the repair team needs to check the

integrity of the fiber cable. Which of the following actions can reduce repair time?

- A. Using a tone generator and wire map to determine the fault location
- B. Using a multimeter to locate the fault point
- C. Using an OTDR In one end of the optic cable to get the fiber length information
- D. Using a spectrum analyzer and comparing the current wavelength with a working baseline

Answer: C

NEW QUESTION 171

- (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 175

- (Topic 3)

A network technician is attempting to increase throughput by configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch. Which of the following is the BEST choice concerning speed and duplex for all interfaces that are participating in the link aggregation?

- A. Half duplex and 1GB speed
- B. Full duplex and 1GB speed
- C. Half duplex and 100MB speed
- D. Full duplex and 100MB speed

Answer: B

Explanation:

The best choice for configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch is to use full duplex and 1GB speed for all interfaces that are participating in the link aggregation. This will allow for maximum throughput, as the full duplex connection will enable simultaneous sending and receiving of data, and the 1GB speed will ensure that the data is transferred quickly. According to the CompTIA Network+ Study Guide, "Full-duplex Ethernet allows the network adapter to transmit and receive data simultaneously, which can result in double the bandwidth of half-duplex Ethernet." Additionally, the official text states, "Ethernet and Fast Ethernet use different speeds for data transmission, with Ethernet being 1,000 megabits (1 gigabit) per second and Fast Ethernet being 100 megabits per second."

NEW QUESTION 178

- (Topic 3)

A user took a laptop on a trip and made changes to the network parameters while at the airport. The user can access all internet websites but not corporate intranet websites. Which of the following is the most likely cause of the issue?

- A. Duplicate IP address
- B. Duplicate SSID
- C. Incorrect DNS
- D. Incorrect subnet mask

Answer: C

Explanation:

DNS (Domain Name System) is a service that translates domain names into IP addresses. Corporate intranet websites are usually hosted on private IP addresses that are not accessible from the public internet. Therefore, the user's laptop needs to use the correct DNS server that can resolve the intranet domain names to the private IP addresses. If the user changed the network parameters at the airport and did not revert them back, the laptop might be using a public DNS server that does not have the records for the intranet websites. This would cause the user to access all internet websites but not corporate intranet websites.

References:

? An Overview of DNS - N10-008 CompTIA Network+ : 1.61

? DNS Configuration – CompTIA A+ 220-11012

? CompTIA Network+ Certification Exam Objectives, page 53

NEW QUESTION 180

- (Topic 3)

A network technician recently installed 35 additional workstations. After installation, some users are unable to access network resources. Many of the original workstations that are experiencing the network access issue were offline when the new workstations were turned on. Which of the following is the MOST likely cause of this issue?

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

Answer: B

NEW QUESTION 185

- (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 188

- (Topic 3)

The lack of a formal process to grant network permissions to different profiles of employees and contractors is leading to an increasing number of security incidents. Non-uniform and overly permissive network accesses are being granted. Which of the following would be the MOST appropriate method to improve the security of the environment?

- A. Change the default permissions to implicit deny
- B. Configure uniform ACLs to employees and NAC for contractors.
- C. Deploy an RDP server to centralize the access to the network
- D. Implement role-based access control

Answer: D

Explanation:

The most appropriate method to improve the security of the environment would be to implement role-based access control (RBAC). With RBAC, users are granted access to the network based on their role within the organization. This allows for more granular access control, as different roles may require different levels of access. Additionally, this ensures that users only have access to the resources they need and no more. This helps to reduce the risk of unauthorized access or misuse of the network. References and further information can be found in the CompTIA Network+ Study Manual, Chapter 8, Access Control.

RBAC is a method of restricting network access based on the roles of individual users within the organization. With RBAC, users are granted access only to the resources they need to perform their specific job functions. This approach reduces the risk of unauthorized access, provides greater visibility into user activity, and simplifies network management. Changing the default permissions to implicit deny may improve security, but it could also cause issues for legitimate users who require access to specific resources. Configuring uniform ACLs and NAC for contractors is a step in the right direction, but it may not be enough to address the overall lack of a formal process for granting network permissions. Deploying an RDP server to centralize access to the network is not a viable solution, as it would not address the root cause of the security incidents.

Therefore, the most appropriate option is to implement role-based access control. Reference: CompTIA Network+ Study Guide, Fourth Edition, Chapter 7, section 7.4.

NEW QUESTION 190

- (Topic 3)

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

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

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

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

Answer: D

Explanation:

The users are unable to navigate to websites on the internet but can access local network resources, indicating a possible DNS issue. The ping command result showing "TTL expired in transit" suggests that packets are not reaching their destination due to a DNS misconfiguration that is not resolving website names into IP addresses correctly³. A possible solution is to check and correct the DNS server settings on the network devices⁴.

References: 3: What does "TTL expired in transit" mean?⁵⁴: CompTIA Network+ N10-008 Cert Guide - Chapter 14: Network Monitoring²

NEW QUESTION 192

- (Topic 3)

A network client is trying to connect to the wrong TCP port. Which of the following responses would the client MOST likely receive?

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

Answer: A

NEW QUESTION 196

- (Topic 3)

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

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

Answer: A

Explanation:

Client roaming refers to the ability of a wireless device to seamlessly connect to a different access point (AP) as the user moves around the facility. This can help to improve network stability and reduce interruptions in mobile applications. An extended service deployment is a type of wireless network configuration that uses multiple APs to cover a large area, such as a warehouse facility. By using a wireless controller to manage the APs, the network can be better optimized for client roaming, which can improve network stability.

"Roaming With multiple WAPs in an ESS, clients will connect to whichever WAP has the strongest signal. As clients move through the space covered by the broadcast area, they will change WAP connections seamlessly, a process called roaming."

NEW QUESTION 201

- (Topic 3)

A network engineer is troubleshooting application connectivity issues between a server and a client. The network engineer needs to view the certificate exchange between the two hosts. Which of the following tools should the network engineer use?

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

Answer: B

Explanation:

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

NEW QUESTION 202

- (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 192.168.0.0/16. 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 206

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 211

- (Topic 3)

A technician is setting up DNS records on local servers for the company's cloud DNS to enable access by hostname. Which of the following records should be used?

- A. A
- B. MX
- C. CNAME
- D. NS

Answer: A

Explanation:

An A record, also known as an address record, is a type of DNS record that maps a hostname to an IPv4 address. An A record is used to resolve a domain name to an IP address, so that clients can connect to the server or service by using the domain name instead of the IP address. For example, an A record can map www.example.com to 192.0.2.1.

An A record is the most common type of DNS record for cloud DNS, as it allows the company to use a custom domain name for their cloud services, such as web hosting, email, or storage. An A record can also be used to create subdomains, such as blog.example.com or mail.example.com, that point to different IP addresses or servers. The other options are not correct because they are not the best type of DNS record for cloud DNS. They are:

? MX. MX stands for mail exchange, and it is a type of DNS record that specifies the

mail servers that are responsible for receiving and delivering email messages for a domain name. MX records are used for email services, but they are not sufficient for cloud DNS, as they do not map a hostname to an IP address.

? CNAME. CNAME stands for canonical name, and it is a type of DNS record that specifies an alias name for another domain name. CNAME records are used to create multiple names for the same IP address or server, such as www.example.com and example.com. CNAME records are useful for cloud DNS, but they are not the best type, as they depend on another A record to resolve the IP address.

? NS. NS stands for name server, and it is a type of DNS record that delegates a DNS zone to an authoritative server. NS records are used to specify which DNS servers are responsible for answering queries for a domain name or a subdomain. NS records are essential for cloud DNS, but they are not the best type, as they do not map a hostname to an IP address.

References¹: DNS records overview | Google Cloud²: Network+ (Plus) Certification | CompTIA IT Certifications³: CloudDNS: What is a DNS record?

NEW QUESTION 214

- (Topic 3)

Which of the following cloud components can filter inbound and outbound traffic between cloud resources?

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

Answer: C

Explanation:

Network security groups are cloud components that can filter inbound and outbound traffic between cloud resources based on rules and priorities. Network security groups can be applied to virtual machines, subnets, or network interfaces to control the network access and security. Network security groups can allow or deny traffic based on the source, destination, port, and protocol of the packets. Network security groups are different from NAT gateways, service endpoints, and virtual private clouds, which are other cloud components that have different functions and purposes.

References

? 1: Network Security Groups – N10-008 CompTIA Network+ : 3.2

? 2: CompTIA Network+ N10-008 Certification Study Guide, page 329-330

? 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 17

? 4: CompTIA Network+ N10-008 Certification Practice Test, question 10

NEW QUESTION 219

- (Topic 3)

Which of the following types of data center architectures will MOST likely be used in a large SDN and can be extended beyond the data center?

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

Answer: D

Explanation:

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

NEW QUESTION 221

- (Topic 3)

All packets arriving at an interface need to be fully analyzed. Which of the following features should be used to enable monitoring of the packets?

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

Answer: D

Explanation:

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

NEW QUESTION 224

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 226

- (Topic 3)

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

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

Answer: C

NEW QUESTION 228

- (Topic 3)

Users within a corporate network need to connect to the Internet, but corporate network policy does not allow direct connections. Which of the following is MOST likely to be used?

- A. Proxy server
- B. VPN client
- C. Bridge
- D. VLAN

Answer: A

NEW QUESTION 231

- (Topic 3)

To comply with an industry regulation, all communication destined to a secure server should be logged and archived on a storage device. Which of the following can be configured to fulfill this requirement?

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

Answer: B

NEW QUESTION 236

- (Topic 3)

An engineer is using a tool to run an ICMP sweep of a network to find devices that are online. When reviewing the results, the engineer notices a number of workstations that are currently verified as being online are not listed in the report.

The tool was configured to scan using the following information: Network address: 172.28.16.0

CIDR: /22

The engineer collected the following information from the client workstation: IP address: 172.28.17.206

Subnet mask: 255.255.252.0

Which of the following MOST likely explains why the tool is failing to detect some workstations?

- A. The scanned network range is incorrect.
- B. The subnet mask on the client is misconfigured.
- C. The workstation has a firewall enabled.
- D. The tool is unable to scan remote networks.

Answer: C

Explanation:

A firewall is a device or software that filters and controls the incoming and outgoing network traffic based on predefined rules. A firewall can block ICMP packets, which are used for ping and other diagnostic tools. If the workstation has a firewall enabled, it may not respond to the ICMP sweep and appear as offline. The engineer should check the firewall settings on the workstation and allow ICMP traffic if needed.

References: Network+ Study Guide Objective 4.1: Given a scenario, use the appropriate tool.

NEW QUESTION 240

- (Topic 3)

A security team would like to use a system in an isolated network to record the actions of potential attackers. Which of the following solutions is the security team implementing?

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

Answer: B

Explanation:

The solution that the security team is implementing to record the actions of potential attackers in an isolated network is a honeypot. A honeypot is a decoy system that simulates a real network or service, but has no actual value or function. A honeypot is designed to attract and trap attackers who try to infiltrate or compromise the network, and then monitor and analyze their behavior and techniques. A honeypot can help the security team learn about the attackers' motives, methods, and tools, and improve their defense

strategies accordingly. References: CompTIA Network+ N10-008 Certification Study Guide, page 358; The Official CompTIA Network+ Student Guide (Exam N10-008), page 14-1.

NEW QUESTION 242

- (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 246

- (Topic 3)

A Network engineer is investigating issues on a Layer 2 Switch. The department typically snares a Switchport during meetings for presentations, but after the first user Shares, no Other users can connect. Which Of the following is MOST likely related to this issue?

- A. Spanning Tree Protocol is enabled on the switch.
- B. VLAN trunking is enabled on the switch.
- C. Port security is configured on the switch.
- D. Dynamic ARP inspection is configured on the switch.

Answer: C

NEW QUESTION 249

- (Topic 3)

A network administrator is installing a new server in the data center. The administrator is concerned the amount of traffic generated will exceed 1GB. and higher-throughput NiCs are not available for installation. Which of the following is the BEST solution for this issue?

- A. Install an additional NIC and configure LACP.
- B. Remove some of the applications from the server.
- C. Configure the NIC to use full duplex
- D. Configure port mirroring to send traffic to another server.
- E. Install a SSD to decrease data processing time.

Answer: A

NEW QUESTION 250

- (Topic 3)

A network administrator wants to know which systems on the network are at risk of a known vulnerability. Which of the following should the administrator reference?

- A. SLA
- B. Patch management policy
- C. NDA
- D. Site survey report
- E. CVE

Answer: E

Explanation:

A Common Vulnerabilities and Exposures (CVE) is a publicly available database of known security vulnerabilities and exposures that affect various software and hardware products. A CVE entry provides a standardized identifier, a brief description, and references to related sources of information for each vulnerability or exposure. A network administrator can reference the CVE database to check if any of the systems on the network are affected by a known vulnerability, and if so, what are the potential impacts and mitigations.

A Service Level Agreement (SLA) is a contract between a service provider and a customer that defines the expected level and quality of service, such as availability, performance, and security. An SLA does not provide information on specific vulnerabilities or exposures affecting the systems or services.

A Patch Management Policy is a set of rules and procedures that govern how patches are applied to systems and software to fix bugs, improve functionality, or address security issues. A patch management policy can help prevent or reduce the risk of vulnerabilities or exposures, but it does not provide information on specific vulnerabilities or exposures affecting the systems or software.

A Non-Disclosure Agreement (NDA) is a legal contract between two or more parties that prohibits the disclosure of confidential or proprietary information to unauthorized parties. An NDA does not provide information on specific vulnerabilities or exposures affecting the systems or information.

A Site Survey Report is a document that summarizes the results of a physical inspection and assessment of a network site, such as the layout, infrastructure, equipment, and environmental conditions. A site survey report can help identify and resolve potential network issues, such as interference, signal strength, or coverage, but it does not provide information on specific vulnerabilities or exposures affecting the network devices or software.

References

What is CVE?

What is a Service Level Agreement (SLA)? Guide to Enterprise Patch Management Planning

NDA, MSA, SOW and SLA. Confidentiality agreements when you outsource QA Site Survey Report

NEW QUESTION 255

- (Topic 3)

A network administrator received a report stating a critical vulnerability was detected on an application that is exposed to the internet. Which of the following is the appropriate NEXT step?

- A. Check for the existence of a known exploit in order to assess the risk
- B. Immediately shut down the vulnerable application server.
- C. Install a network access control agent on the server.
- D. Deploy a new server to host the application.

Answer: A

Explanation:

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

NEW QUESTION 258

- (Topic 3)

A security vendor needs to add a note to the DNS to validate the ownership of a company domain before services begin. Which of the following records did the security company MOST likely ask the company to configure?

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

Answer: A

Explanation:

TXT stands for Text and is a type of DNS record that can store arbitrary text data associated with a domain name. TXT records can be used for various purposes, such as verifying the ownership of a domain, providing information about a domain, or implementing security mechanisms such as SPF (Sender Policy Framework) or DKIM (DomainKeys Identified Mail). In this scenario, the security company most likely asked the company to configure a TXT record with a specific value that can prove the ownership of the domain. AAAA stands for IPv6 Address and is a type of DNS record that maps a domain name to an IPv6 address. CNAME stands for Canonical Name and is a type of DNS record that maps an alias name to another name. SRV stands for Service and is a type of DNS record that specifies the location of a service on a network.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.8: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 261

- (Topic 3)

After installing a series of Cat 8 keystone, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect

take to troubleshoot the issue?

- A. Check to see if the end connections were wrapped in copper tape before terminating.
- B. Use passthrough modular crimping plugs instead of traditional crimping plugs.
- C. Connect the RX/TX wires to different pins.
- D. Run a speed test on a device that can only achieve 100Mbps speeds.

Answer: A

Explanation:

Cat 8 keystones are shielded to prevent interference from external sources, but they also require proper grounding to avoid interference from within the cable. Wrapping the end connections with copper tape before terminating them is one way to ensure a good ground connection and reduce interference. Using passthrough modular crimping plugs, connecting the RX/TX wires to different pins, or running a speed test on a slow device are not relevant or effective steps to troubleshoot the issue.

References:

- ? CompTIA Network+ N10-008 Certification Study Guide, page 191
- ? CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 362
- ? CAT8 RJ45 Keystone Problem : r/HomeNetworking2
- ? How to Terminate Cat8 Shielded Keystone Jacks3

NEW QUESTION 265

- (Topic 3)

A technician is configuring a static IP address on a new device in a newly created subnet. The work order specifies the following requirements:

- The IP address should use the highest address available in the subnet.
- The default gateway needs to be set to 172.28.85.94.
- The subnet mask needs to be 255.255.255.224.

Which of the following addresses should the engineer apply to the device?

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

Answer: A

Explanation:

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

NEW QUESTION 267

- (Topic 3)

Which of the following is a benefit of the spine-and-leaf network topology?

- A. Increased network security
- B. Stable network latency
- C. Simplified network management
- D. Eliminated need for inter-VLAN routing

Answer: A

NEW QUESTION 269

- (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 273

- (Topic 3)

Which of the following can be used to aggregate logs from different devices and would make analysis less difficult?

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

Answer: B

Explanation:

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

NEW QUESTION 276

- (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 278

- (Topic 3)

Which of the following can be used to identify users after an action has occurred?

- A. Access control vestibule
- B. Cameras
- C. Asset tag
- D. Motion detectors

Answer: B

Explanation:

Cameras can be used to identify users after an action has occurred by recording their faces, clothing, or other distinctive features. Cameras are often used as a deterrent and a forensic tool for security purposes. Access control vestibules, asset tags, and motion detectors are not effective in identifying users, but rather in controlling access, tracking assets, and detecting movement.

References:

CompTIA Network+ N10-008 Certification Exam Objectives, Domain 5.0: Network Security, Subobjective 5.1: Summarize the importance of physical security controls, page 231 CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008), Chapter 18: Network Security, Section: Physical Security, page 7372

NEW QUESTION 280

- (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 281

- (Topic 3)

Which of the following would be used to forward requests and replies between a DHCP server and client?

- A. Relay

- B. Lease
- C. Scope
- D. Range

Answer: B

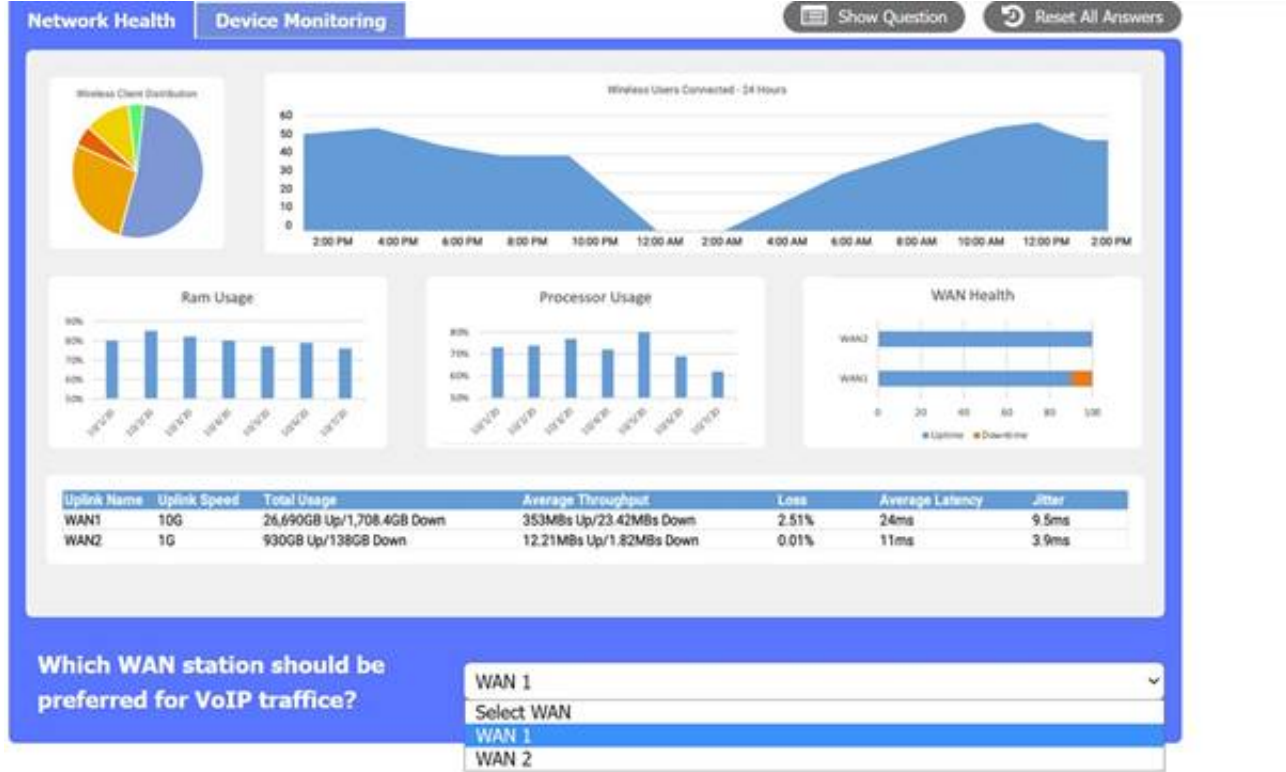
NEW QUESTION 283

SIMULATION - (Topic 3)

After a recent power outage, users are reporting performance issues accessing the application servers. Wireless users are also reporting intermittent Internet issues.

INSTRUCTIONS

Click on each tab at the top of the screen. Select a widget to view information, then use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Network Health

Device Monitoring

Show Question

Reset All Answers

Device Status

Alert (3)

Up (8)

Warning (2)

Down (1)

8

3

2

1

Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

Which device is experiencing connectivity issues?

Select Answer

Router A

Router B

WAP1

WAP2

WirelessController

Switch A

Switch B

DHCP Server

Web Server

APP Server

Router A

Which workstation IP is generating the MOST traffic?

Select Answer

10.1.99.28

10.1.99.14

10.1.99.10

10.1.99.22

10.1.99.24

206.208.133.10

206.208.133.9

10.1.50.14

10.1.50.13

10.1.59.81

10.1.90.53

10.1.90.55

206.208.133.9

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Network Health:
WAN 2 appears to have a lower average latency and loss percentage, which would make it the preferred WAN station for VoIP traffic. VoIP traffic requires low latency and packet loss to ensure good voice quality and reliability. WAN 1 seems to have higher RAM and processor usage, which could also affect the performance of VoIP traffic.
Here's the summary of the key metrics for WAN 1 and WAN 2 from the image provided:
? WAN 1:
? WAN 2:
For VoIP traffic, low latency and jitter are particularly important to ensure voice quality. While WAN 1 has higher bandwidth and throughput, it also has higher latency and jitter compared to WAN 2. However, WAN 2 has much lower loss, lower latency, and lower jitter, which are more favorable for VoIP traffic that is sensitive to delays and variation in packet arrival times.
Given this information, WAN 2 would generally be preferred for VoIP traffic due to its lower latency, lower jitter, and significantly lower loss percentage, despite its lower bandwidth compared to WAN 1. The high bandwidth of WAN 1 may be more suitable for other types of traffic that are less sensitive to latency and jitter, such as bulk data transfers.



Device Monitoring:
the device that is experiencing connectivity issues is the APP Server or Router 1, which has a status of Down. This means that the server is not responding to network requests or sending any data. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.



A screenshot of a computer
Description automatically generated

NEW QUESTION 287

- (Topic 3)
Which of the following security controls indicates unauthorized hardware modifications?

- A. Biometric authentication
- B. Media device sanitization
- C. Change management policy
- D. Tamper-evident seals

Answer: A

NEW QUESTION 290

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

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

Answer: A

Explanation:

One possible process that the administrator used to identify the root cause of the spam issue is traffic analysis. Traffic analysis is a technique that monitors and analyzes the network traffic that flows between devices or applications. Traffic analysis can help troubleshoot network problems by identifying the source, destination, volume, frequency, and content of the network packets¹².

To use traffic analysis to identify the root cause of the spam issue, the administrator could follow these steps:

? Install a traffic analysis tool on the server or a device that is connected to the same network as the server, such as Wireshark³, tcpdump⁴, or Microsoft Network Monitor⁵.

? Start capturing the network traffic and filter it by using the IP address or hostname

of the server, or by using a specific port or protocol that is used by the email service, such as SMTP (port 25), POP3 (port 110), or IMAP (port 143).

? Analyze the filtered traffic and look for any signs of abnormal or malicious activity, such as high volume of outgoing emails, unknown recipients, suspicious attachments, or spam keywords.

? Trace back the source of the spam emails to the infected workstation by using its IP address or MAC address.

? Isolate and clean up the infected workstation by using an antivirus or malware removal tool.

The other options are not processes that the administrator used to identify the root cause of the spam issue. Availability monitoring is a technique that measures and reports the uptime and downtime of a network device or service. Availability monitoring can help troubleshoot network problems by detecting any failures or outages that affect the network performance. Baseline metrics are a set of standard measurements that establish the normal behavior or performance of a network device or service. Baseline metrics can help troubleshoot network problems by comparing the current state of the network with the expected state and identifying any deviations or anomalies. Network discovery is a technique that scans and maps the network devices and services that are connected to a network. Network discovery can help troubleshoot network problems by providing a comprehensive and updated view of the network topology and configuration.

NEW QUESTION 291

- (Topic 3)

An ISP is unable to provide services to a user in a remote area through cable and DSL. Which of the following is the NEXT best solution to provide services without adding external infrastructure?

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

Answer: C

Explanation:

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

NEW QUESTION 293

- (Topic 3)

Which of the following describes a network in which users and devices need to mutually authenticate before any network resource can be accessed?

- A. Least privilege
- B. Local authentication
- C. Zero trust
- D. Need to know

Answer: C

Explanation:

A zero trust network is a network in which users and devices need to mutually authenticate before any network resource can be accessed. A zero trust network assumes that no one and nothing can be trusted by default, even if they were previously verified or are within the network perimeter. A zero trust network uses various technologies and practices, such as data and log aggregation, cybersecurity analytics, continuous diagnostics and mitigation, user behavior analytics, microsegmentation, and identity and access management, to enforce granular and dynamic policies based on the context and behavior of the users and devices¹²³.

References:

? What is Zero Trust? | Internet of Things | CompTIA³

? The Death of the Perimeter: Zero Trust is (Almost) Here to Stay | Cybersecurity | CompTIA²

? CompTIA Network+ Certification Exam N10-008 Practice Test 17 -

ExamCompass¹

NEW QUESTION 298

- (Topic 3)

An attacker sends more connection requests than a server can handle, causing the server to crash- Which of the following types of attacks is this an example of?

- A. ARP poisoning
- B. Denial-of-service
- C. MAC flooding
- D. On-path

Answer: B

Explanation:

A denial-of-service (DoS) attack is an example of an attack where an attacker sends more connection requests than a server can handle, causing the server to crash. A DoS attack is a type of cyberattack that aims to disrupt the normal functioning of a network service or resource by overwhelming it with excessive or malformed traffic. A DoS attack can prevent legitimate users from accessing the service or resource, resulting in degraded performance, unavailability, or data loss. A DoS attack can target various network layers, protocols, or components, such as servers, routers, firewalls, or applications. References: [CompTIA Network+ Certification Exam Objectives], What Is a Denial-of-Service (DoS) Attack? | Cisco

NEW QUESTION 299

- (Topic 3)

Which of the following steps of the troubleshooting methodology would most likely include checking through each level of the OSI model after the problem has been identified?

- A. Establish a theory.
- B. Implement the solution.
- C. Create a plan of action.
- D. Verify functionality.

Answer: C

Explanation:

Creating a plan of action is the step of the troubleshooting methodology that would most likely include checking through each level of the OSI model after the problem has been identified. According to the web search results, the troubleshooting methodology consists of the following steps: 12

? Define the problem: Identify the symptoms and scope of the problem, and gather relevant information from users, devices, and logs.

? Establish a theory: Based on the information collected, hypothesize one or more possible causes of the problem, and rank them in order of probability.

? Test the theory: Test the most probable cause first, and if it is not confirmed, eliminate it and test the next one. Repeat this process until the root cause is found or a new theory is needed.

? Create a plan of action: Based on the confirmed cause, devise a solution that can resolve the problem with minimal impact and risk. The solution may involve checking through each level of the OSI model to ensure that all layers are functioning properly and that there are no configuration errors, physical damages, or logical inconsistencies³⁴

? Implement the solution: Execute the plan of action, and monitor the results. If the problem is not solved, revert to the previous state and create a new plan of action.

? Verify functionality: Confirm that the problem is fully resolved and that the network is restored to normal operation. Perform preventive measures if possible to avoid recurrence of the problem.

? Document the findings: Record the problem description, the solution, and the outcome. Update any relevant documentation, such as network diagrams, policies, or procedures.

References1: Troubleshooting Methods for Cisco IP Networks 2: Troubleshooting Methodologies - CBT IT Certification Training 3: How to use the OSI Model to Troubleshoot Networks 4: How is the OSI model used in troubleshooting? – Sage-Answer

NEW QUESTION 302

- (Topic 3)

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

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

Answer: D

Explanation:

Wireless drivers can affect the performance and compatibility of your wireless connection⁵. If only a new line of laptops using the organization's standard image has experienced slow wireless speeds, it could be that their wireless drivers are outdated or incompatible with the network. Updating the device wireless drivers could resolve this issue.

Wireless drivers play an important role in the performance of a wireless connection, as they control how the device interacts with the wireless network. If the laptops in question are using an outdated version of the wireless driver, it could be causing the slow speeds. The network administrator should recommend updating the device wireless drivers first to see if this resolves the issue.

NEW QUESTION 304

- (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 308

- (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 313

- (Topic 3)

A network technician is troubleshooting a network issue for employees who have reported issues with speed when accessing a server in another subnet. The server is in another building that is 410ft (125m) away from the employees' building. The 10GBASE-T connection between the two buildings uses Cat 5e. Which of the following BEST explains the speed issue?

- A. The connection type is not rated for that distance
- B. A broadcast storm is occurring on the subnet.
- C. The cable run has interference on it
- D. The connection should be made using a Cat 6 cable

Answer: D

Explanation:

The 10GBASE-T connection between the two buildings uses Cat 5e, which is not rated for a distance of 410ft (125m). According to the CompTIA Network+ Study Manual, for 10GBASE-T connections, "Cat 5e is rated for up to 55m, Cat 6a is rated for 100m, and Cat 7 is rated for 150m." Therefore, the speed issue is likely due to the fact that the connection type is not rated for the distance between the two buildings. To resolve the issue, the technician should consider using a Cat 6a or Cat 7 cable to increase the distance the connection is rated for.

NEW QUESTION 318

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 321

- (Topic 3)

A network administrator is troubleshooting a connection to a remote site. The administrator runs a command and sees the following output:

```
Tracing route to 10.10.0.22 over a maximum of 30 hops:
 0  14ms  20ms  15ms  192.168.1.253
 1  10ms  15ms  12ms  172.16.0.21
 2   5ms   10ms  10ms  10.10.5.3
 3  10ms  15ms  12ms  10.12.2.1
 4   5ms   10ms  10ms  10.10.5.3
 5  10ms  15ms  12ms  10.12.2.1
 6   5ms   10ms  10ms  10.10.5.3
 7  10ms  15ms  12ms  10.12.2.1
```

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

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

Answer: A

Explanation:

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

NEW QUESTION 326

- (Topic 3)

A customer has an attached USB printer that needs to be shared with other users. The desktop team set up printer sharing. Now, the network technician needs to obtain the necessary information about the PC and share it with other users so they can connect to the printer. Which of the following commands should the technician use to get the required information? (Select TWO).

- A. arp
- B. route
- C. netstat
- D. tcpdump
- E. hostname
- F. ipconfig

Answer: EF

Explanation:

The hostname and ipconfig commands should be used to get the required information about the PC and share it with other users so they can connect to the printer. The hostname command displays the name of the computer on a network. The ipconfig command displays the IP configuration of the computer, including its IP address, subnet mask, default gateway, and DNS servers. These information are necessary for other users to locate and connect to the shared printer on the network. For example, other users can use the UNC path \\hostname\printername or \\ipaddress\printername to access the shared printer. References: [CompTIA Network+ Certification Exam Objectives], How to Share a Printer in Windows 10

NEW QUESTION 329

- (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 332

.....

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](#)