

CompTIA

Exam Questions N10-009

CompTIA Network+ Exam



NEW QUESTION 1

- (Topic 3)

A network technician is attempting to harden a commercial switch that was recently purchased. Which of the following hardening techniques best mitigates the use of publicly available information?

- A. Changing the default password
- B. Blocking inbound SSH connections
- C. Removing the gateway from the network configuration
- D. Restricting physical access to the switch

Answer: A

Explanation:

Changing the default password is a hardening technique that best mitigates the use of publicly available information, such as vendor documentation, online forums, or hacking tools, that may reveal the default credentials of a commercial switch. By changing the default password to a strong and unique one, the network technician can prevent unauthorized access to the switch configuration and management. References:

? Network Hardening - N10-008 CompTIA Network+ : 4.3 - YouTube¹

? CompTIA Network+ Certification Exam Objectives, page 151

NEW QUESTION 2

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 3

- (Topic 3)

An organization has a security requirement that all network connections can be traced back to a user. A network administrator needs to identify a solution to implement on the wireless network. Which of the following is the best solution?

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

Answer: A

Explanation:

Enterprise authentication is a method of securing wireless networks that uses an external authentication server, such as RADIUS, to verify the identity of users and devices. Enterprise authentication can provide user traceability by logging the network connections and activities of each authenticated user. This can help the organization meet its security requirement and comply with any regulations or policies that mandate user accountability¹².

References:

? CompTIA Network+ N10-008 Certification Exam Objectives, page 83

? CompTIA Network+ Cert Guide: Wireless Networking, page 13

NEW QUESTION 4

- (Topic 3)

A network administrator needs to create an SVI on a Layer 3-capable device to separate voice and data traffic. Which of the following best explains this use case?

- A. A physical interface used for trunking logical ports
- B. A physical interface used for management access
- C. A logical interface used for the routing of VLANs
- D. A logical interface used when the number of physical ports is insufficient

Answer: C

Explanation:

An SVI, or switched virtual interface, is a logical interface that is created on a Layer 3- capable device, such as a multilayer switch or a router. An SVI is associated with a VLAN and can be used to route traffic between different VLANs on the same device or across multiple devices. An SVI can also provide management access, security features, and quality of service (QoS) for the VLAN. An SVI is different from a physical interface, which is a port that connects to a physical device or network. A physical interface can be used for trunking, which is a method of carrying multiple VLANs over a single link, or for connecting to a single VLAN. An SVI is also different from a subinterface, which is a logical division of a physical interface that can be assigned to different VLANs.

References:

? VLANs and Trunking – N10-008 CompTIA Network+ : 2.11

? Switched Virtual Interfaces – N10-008 CompTIA Network+ : 2.22

NEW QUESTION 5

- (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 6

- (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 7

- (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 8

- (Topic 3)

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

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

Answer: B

NEW QUESTION 9

- (Topic 3)

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

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

Answer: D

Explanation:

Traceroute is a network diagnostic tool that allows you to trace the path that network packets take from one device to another. By running traceroute to the file server, the technician can see the sequence of devices and networks that the packets pass through on their way to the file server. This can help the technician to

determine if there is a problem with the network connection between the user's computer and the file server, or if the issue is with the file server itself.

NEW QUESTION 10

- (Topic 3)

A 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 10

- (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 13

- (Topic 3)

Which of the following documents is MOST likely to be associated with identifying and documenting critical applications?

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

Answer: D

Explanation:

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

References: Network+ Study Guide Objective 5.2: Explain disaster recovery and business continuity concepts.

NEW QUESTION 16

- (Topic 3)

A security engineer is trying to connect cameras to a 12-port PoE switch, but only eight cameras turn on. Which of the following should the engineer check first?

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

Answer: B

Explanation:

The most likely reason why only eight cameras turn on is that the PoE switch does not have enough power budget to supply all 12 cameras. The engineer should check the voltage and wattage ratings of the PoE switch and the cameras, and make sure they are compatible and sufficient. The Ethernet cable type, transceiver compatibility, and DHCP addressing are less likely to cause this problem, as they would affect the data transmission rather than the power delivery.

References:

? CompTIA Network+ N10-008 Certification Study Guide, page 181

? CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 352

? PoE Troubleshooting: The Common PoE Errors and Solutions3

NEW QUESTION 19

- (Topic 3)

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

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

Answer: C

Explanation:

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

References² - VoIP Troubleshooting: 5 Fixes for Common Connection Issues - Nextiva³ - Troubleshooting VoIP — Is it You or the Network? - PingPlotter

NEW QUESTION 24

- (Topic 3)

Which of the following is most likely to be implemented to actively mitigate intrusions on a host device?

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

Answer: A

Explanation:

HIDS (host-based intrusion detection system) is a type of security software that monitors and analyzes the activity on a host device, such as a computer or a server. HIDS can detect and alert on intrusions, such as malware infections, unauthorized access, configuration changes, or policy violations. HIDS can also actively mitigate intrusions by blocking or quarantining malicious processes, files, or network connections¹.

HIPS (host-based intrusion prevention system) is similar to HIDS, but it can also prevent intrusions from happening in the first place by enforcing security policies and rules on the host device². MDS (multilayer switch) is a network device that combines the functions of a switch and a router, and it does not directly protect a host device from intrusions³. NIPS (network-based intrusion prevention system) is a network device that monitors and blocks malicious traffic on the network level, and it does not operate on the host device level⁴.

NEW QUESTION 27

- (Topic 3)

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

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

Answer: CD

Explanation:

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

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

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

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

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

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

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

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

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

NEW QUESTION 30

- (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 32

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 33

- (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 34

- (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 35

- (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 the following terminations should the technician use when running a cable from the ISP's port to 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 38

- (Topic 3)

Users are reporting poor wireless performance in some areas of an industrial plant The wireless controller is measuring a low EIRP value compared to the recommendations noted on the 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 39

- (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 42

- (Topic 3)

Which of the following would be used to adjust resources dynamically for a virtual web server under variable loads?

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

Answer: B

Explanation:

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

NEW QUESTION 43

- (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 46

- (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 49

- (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 50

- (Topic 3)

Which of the following redundant devices creates broadcast storms when connected together on a high-availability network?

- A. Switches
- B. Routers
- C. Access points
- D. Servers

Answer: A

Explanation:

Switches are devices that forward data based on MAC addresses. They create separate collision domains for each port, which reduces the chance of collisions on the network. However, if multiple switches are connected together without proper configuration, they can create broadcast storms, which are situations where broadcast frames are endlessly forwarded between switches, consuming network bandwidth and resources. Broadcast storms can be prevented by using protocols such as Spanning Tree Protocol (STP), which eliminates loops in the network topology. References: CompTIA Network+ N10-008 Certification Study Guide, page 67; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-14.

NEW QUESTION 55

- (Topic 3)

A user calls the IT department to report being unable to log in after locking the computer. The user resets the password, but later in the day the user is again unable to log in after locking the computer. Which of the following attacks against the user is MOST likely taking place?

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

Answer: A

NEW QUESTION 56

- (Topic 3)

Which of the following routing technologies is used to prevent network failure at the gateway by protecting data traffic from a failed router?

- A. BGP
- B. OSPF
- C. EIGRP
- D. FHRP

Answer: D

Explanation:

FHRP stands for First Hop Redundancy Protocol, and it is a group of protocols that allow routers to work together to provide backup or failover for the default gateway in a network. FHRP can prevent network failure at the gateway by protecting data traffic from a failed router and ensuring that there is always an active router to forward packets. Some examples of FHRP protocols are HSRP, VRRP, and GLBP12.

References: 1: CompTIA Network+ N10-008 Cert Guide - Chapter 13: Routing Protocols32: First Hop Redundancy Protocols (FHRP) Explained4

NEW QUESTION 61

- (Topic 3)

A technician installed an 8-port switch in a user's office. The user needs to add a second computer in the office, so the technician connects both PCs to the switch and connects the switch to the wall jack. However, the new PC cannot connect to network resources. The technician then observes the following:

- The new computer does not get an IP address on the client's VLAN.
- Both computers have a link light on their NICs.
- The new PC appears to be operating normally except for the network issue.
- The existing computer operates normally.

Which of the following should the technician do NEXT to address the situation?

- A. Contact the network team to resolve the port security issue.
- B. Contact the server team to have a record created in DNS for the new PC.
- C. Contact the security team to review the logs on the company's SIEM.
- D. Contact the application team to check NetFlow data from the connected switch.

Answer: A

NEW QUESTION 65

- (Topic 3)

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

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

Answer: D

NEW QUESTION 66

- (Topic 3)

An IT administrator is creating an alias to the primary customer's domain. Which of the following DNS record types does this represent?

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

Answer: A

Explanation:

A CNAME record is a type of DNS record that maps an alias name to a canonical name, or the primary domain name. A CNAME record is used to create subdomains or alternative names for the same website, without having to specify the IP address for each alias. For example, a CNAME record can map www.example.com to example.com, or mail.example.com to example.com. References: CompTIA Network+ N10-008 Cert Guide, Chapter 2, Section 2.4

NEW QUESTION 71

- (Topic 3)

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

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

Answer: A

NEW QUESTION 75

- (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 77

- (Topic 3)

A network technician needs to ensure the company's external mail server can pass reverse lookup checks. Which of the following records would the technician MOST likely configure? (Choose Correct option and give explanation directly from CompTIA Network+ Study guide or documents)

- A. PTR
- B. AAAA
- C. SPF
- D. CNAME

Answer: A

Explanation:

A PTR (Pointer) record is used to map an IP address to a domain name, which is necessary for reverse lookup checks. Reverse lookup checks are performed by external mail servers to verify the identity of the sender of the email. By configuring a PTR record, the network technician can ensure that the company's external mail server can pass these checks. According to the CompTIA Network+ Study Guide, "A PTR record is used to map an IP address to a domain name, and it is often used for email authentication."

NEW QUESTION 81

- (Topic 3)

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

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

Answer: C

Explanation:

Baseline configurations are the standard settings and parameters that are applied to network devices, such as switches, routers, firewalls, etc., to ensure consistent performance, security, and functionality across the network. Baseline configurations can include aspects such as IP addresses, VLANs, passwords, protocols, access lists, firmware versions, etc. Baseline configurations are usually documented and updated regularly to reflect any changes or modifications made to the network devices.

The lead network engineer most likely provided baseline configurations to the network administrator to ensure that the new switches are set up properly and in accordance with the network design and policies. Baseline configurations can help to simplify the deployment process, reduce errors and inconsistencies, and facilitate troubleshooting and maintenance.

The other options are not correct because they are not the most likely documentation that the lead network engineer provided to the network administrator. They are:

? Physical network diagram. A physical network diagram is a graphical representation of the physical layout and connections of the network devices and components, such as cables, ports, switches, routers, servers, etc. A physical network diagram can help to visualize the network topology, identify the locations and distances of the devices, and plan for cabling and power requirements. However, a physical network diagram does not provide the specific settings and parameters that need to be configured on the network devices, such as the switches.

? Site survey reports. A site survey report is a document that summarizes the findings and recommendations of a site survey, which is a process of assessing the suitability and readiness of a location for installing and operating network devices and components. A site survey report can include aspects such as environmental conditions, power and cooling availability, security and safety measures, interference and noise sources, signal coverage and quality, etc. A site survey report can help to identify and resolve any potential issues or challenges that may affect the network performance and reliability. However, a site survey report does not provide the specific settings and parameters that need to be configured on the network devices, such as the switches.

? Logical network diagram. A logical network diagram is a graphical representation of the logical structure and functionality of the network devices and components, such as subnets, IP addresses, VLANs, protocols, routing, firewall rules, etc. A logical network diagram can help to understand the network design, architecture, and policies, as well as the data flow and communication paths between the devices. However, a logical network diagram does not provide the specific settings and parameters that need to be configured on the network devices, such as the switches.

References1: Network+ (Plus) Certification | CompTIA IT Certifications2: What is a Baseline Configuration? - Definition from Techopedia3: What is a Physical Network Diagram? - Definition from Techopedia4: What is a Site Survey? - Definition from Techopedia5: [What is a Logical Network Diagram? - Definition from Techopedia]

NEW QUESTION 82

- (Topic 3)

Which of the following is a security flaw in an application or network?

- A. A threat
- B. A vulnerability
- C. An exploit
- D. A risk

Answer: B

Explanation:

A vulnerability is a security flaw in an application or network that can be exploited by an attacker, allowing them to gain access to sensitive data or take control of the system. Vulnerabilities can range from weak authentication methods to unpatched software, allowing attackers to gain access to the system or data they would not otherwise be able to access. Exploits are programs or techniques used to take advantage of vulnerabilities, while threats are potential dangers, and risks are the likelihood of a threat becoming a reality.

NEW QUESTION 83

- (Topic 3)

A wireless technician is working to upgrade the wireless infrastructure for a company. The company currently uses the 802.11g wireless standard on all access points. The company requires backward compatibility and is requesting the least expensive solution. Which of the following should the technician recommend to the company?

- A. 802.11a
- B. 802.11ac
- C. 802Hax
- D. 802.11n

Answer: D

Explanation:

* 802.11n is a wireless standard that supports data rates up to 600 Mbps and operates in both 2.4 GHz and 5 GHz frequency bands. 802.11n is backward compatible with 802.11g, which operates only in 2.4 GHz band. 802.11n is the least expensive solution that can upgrade the wireless infrastructure for the company, as it does not require replacing all the access points or wireless devices

NEW QUESTION 85

- (Topic 3)

Which of the following best describe the functions of Layer 2 of the OSI model? (Select two).

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

Answer: AD

Explanation:

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

References:

? OSI Model | Computer Networking | CompTIA1

NEW QUESTION 90

- (Topic 3)

Which of the following describes traffic going in and out of a data center from the internet?

- A. Demarcation point
- B. North-South
- C. Fibre Channel
- D. Spine and leaf

Answer: B

NEW QUESTION 92

- (Topic 3)

A malicious user is using special software to perform an on-path attack. Which of the following best practices should be configured to mitigate this threat?

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

Answer: A

NEW QUESTION 97

- (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 99

- (Topic 3)

Which of the following ports is a secure protocol?

- A. 20
- B. 23
- C. 443

D. 445

Answer: C

Explanation:

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

NEW QUESTION 102

- (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 106

- (Topic 3)

After installing a new wireless access point, an engineer tests the device and sees that it is not performing at the rated speeds. Which of the following should the engineer do to troubleshoot the issue? (Select two).

- A. Ensure a bottleneck is not coming from other devices on the network.
- B. Install the latest firmware for the device.
- C. Create a new VLAN for the access point.
- D. Make sure the SSID is not longer than 16 characters.
- E. Configure the AP in autonomous mode.
- F. Install a wireless LAN controller.

Answer: AB

Explanation:

One possible cause of poor wireless performance is a bottleneck in the network, which means that other devices or applications are consuming too much bandwidth or resources and limiting the speed of the wireless access point. To troubleshoot this issue, the engineer should ensure that there is no congestion or interference from other devices on the network, such as wired clients, servers, routers, switches, or other wireless access points. The engineer can use tools such as network analyzers, bandwidth monitors, or ping tests to check the network traffic and latency¹².

Another possible cause of poor wireless performance is outdated firmware on the device, which may contain bugs or vulnerabilities that affect the functionality or security of the wireless access point. To troubleshoot this issue, the engineer should install the latest firmware for the device from the manufacturer's website or support portal. The engineer should follow the instructions carefully and backup the configuration before updating the firmware. The engineer can also check the release notes or changelog of the firmware to see if there are any improvements or fixes related to the wireless performance³.

The other options are not relevant to troubleshooting poor wireless performance. Creating a new VLAN for the access point may help with network segmentation or security, but it will not improve the speed of the wireless connection. Making sure the SSID is not longer than 16 characters may help with compatibility or readability, but it will not affect the wireless performance. Configuring the AP in autonomous mode may give more control or flexibility to the engineer, but it will not enhance the wireless speed. Installing a wireless LAN controller may help with managing multiple access points or deploying advanced features, but it will not increase the wireless performance.

NEW QUESTION 111

- (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 112

- (Topic 3)

Which of the following would be BEST suited for a long cable run with a 40Gbps bandwidth?

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

Answer: C

Explanation:

Cat 7 is a type of twisted-pair copper cable that supports up to 40 Gbps bandwidth and up to 100 meters cable length. Cat 7 is suitable for long cable runs that require high-speed data transmission. Cat 7 has better shielding and crosstalk prevention than lower categories of cables.

References: Network+ Study Guide Objective 1.5: Compare and contrast network cabling types, features and their purposes.

NEW QUESTION 113

- (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 118

- (Topic 3)

Which of the following options represents the participating computers in a network?

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

Answer: A

NEW QUESTION 119

- (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 control. 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 123

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 127

- (Topic 3)

A firewall administrator observes log entries of traffic being allowed to a web server on port 80 and port 443. The policy for this server is to only allow traffic on port

443. The firewall administrator needs to investigate how this change occurred to prevent a reoccurrence. Which of the following should the firewall administrator do next?

- A. Consult the firewall audit logs.
- B. Change the policy to allow port 80.
- C. Remove the server object from the firewall policy.
- D. Check the network baseline.

Answer: A

Explanation:

Firewall audit logs are records of the changes made to the firewall configuration, policies, and rules. They can help the firewall administrator to track who, when, and what changes were made to the firewall, and identify any unauthorized or erroneous modifications that could cause security issues or network outages. By consulting the firewall audit logs, the firewall administrator can investigate how the change that allowed traffic on port 80 to the web server occurred, and prevent it from happening again

NEW QUESTION 131

- (Topic 3)

Which of the following layers of the OSI model has new protocols activated when a user moves from a wireless to a wired connection?

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

Answer: A

Explanation:

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

NEW QUESTION 135

- (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 139

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 141

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 143

- (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 145

- (Topic 3)

A network technician is troubleshooting an issue that involves connecting to a server via SSH. The server has one network interface that does not support subinterfaces. The technician

runs a command on the server and receives the following output:

Proto	Local address	Foreign address	State
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING
TCP	10.10.10.15:22	10.10.10.42:21231	ESTABLISHED

On the host, the technician runs another command and receives the following:

Destination	Gateway	Genmask	Flags	Iface
default	31.242.12.9	0.0.0.0	UG	eth0
192.168.1.0	0.0.0.0	255.255.255.0	UG	eth1

Which of the following best explains the issue?

- A. A firewall is blocking access to the server.
- B. The server is plugged into a trunk port.
- C. The host does not have a route to the server.
- D. The server is not running the SSH daemon.

Answer: C

NEW QUESTION 147

- (Topic 3)

An infrastructure company is implementing a cabling solution to connect sites on multiple continents. Which of the following cable types should the company use for this project?

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

Answer: B

Explanation:

Single-mode fiber is a type of optical fiber that has a small core diameter and allows only one mode of light to propagate. This reduces signal attenuation and increases transmission distance, making it suitable for long-distance communication networks.

Single-mode fiber can carry data over thousands of kilometers without requiring repeaters or amplifiers. Single-mode fiber is also immune to electromagnetic interference and has a higher bandwidth than multimode fiber. Therefore, single-mode fiber is the best cable type for connecting sites on multiple continents.

References: [CompTIA Network+ Certification Exam Objectives], [Single-mode optical fiber - Wikipedia]

Single-mode fiber optic cable uses a single ray of light to transmit data. This allows it to achieve very low attenuation and high bandwidth.

Multimode fiber optic cable uses multiple rays of light to transmit data. This results in higher attenuation and lower bandwidth than single-mode cable.

Twisted pair copper cable uses two insulated copper wires to transmit data. It is less expensive than fiber optic cable, but it has higher attenuation and lower bandwidth. When choosing a cable type for a long-distance application, it is important to consider the following factors:

? Attenuation: The amount of signal loss that occurs over the length of the cable.

? Bandwidth: The amount of data that can be transmitted over the cable per second.

? Cost: The cost of the cable and installation.

Single-mode fiber optic cable is the best choice for long-distance applications because it

has the lowest attenuation and highest bandwidth of any cable type. However, it is also the most expensive cable type.

NEW QUESTION 149

- (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 153

- (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 158

- (Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 162

- (Topic 3)

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

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

Answer: D

Explanation:

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

References:

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

NEW QUESTION 164

- (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 167

- (Topic 3)

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

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

Answer: A

NEW QUESTION 171

- (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 173

- (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 175

- (Topic 3)

A technician uses a badge to enter a security checkpoint on a corporate campus. An unknown individual quickly walks in behind the technician without speaking.

Which of the following types of attacks did the technician experience?

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

Answer: A

Explanation:

Tailgating is a type of physical security attack where an unauthorized person follows an authorized person into a restricted area without their consent or

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

NEW QUESTION 177

- (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 181

- (Topic 3)

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

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

Answer: D

NEW QUESTION 185

- (Topic 3)

A network technician receives a report about a performance issue on a client PC that is connected to port 1/3 on a network switch. The technician observes the following configuration output from the switch:

1/1	Client PC	Connected	Full	1000
1/2	Client PC	Connected	Full	1000
1/3	Client PC	Connected	Full	10

Which of the following is a cause of the issue on port 1/3?

- A. Speed
- B. Duplex
- C. Errors
- D. VLAN

Answer: A

NEW QUESTION 187

- (Topic 3)

Which of the following most likely occurs when an attacker is between the target and a legitimate server?

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

Answer: D

Explanation:

An on-path attack (also known as a man-in-the-middle attack) is a type of security attack where the attacker places themselves between two devices (often a web browser and a web server) and intercepts or modifies communications between the two1. The attacker can then collect information as well as impersonate either of the two agents. For example, an on-path attacker could capture login credentials, redirect traffic to malicious sites, or inject malware into legitimate web pages. The other options are not correct because they describe different types of attacks:

•IP spoofing is the practice of forging the source IP address of a packet to make it appear as if it came from a trusted or authorized source2.

•VLAN hopping is a technique that allows an attacker to access a VLAN that they are not authorized to access by sending packets with a modified VLAN tag3.

•Rogue DHCP is a scenario where an unauthorized DHCP server offers IP configuration parameters to clients on a network, potentially causing network disruption or redirection to malicious sites4.

References

- 2: Understanding Targeted Attacks: What is a Targeted Attack? 3: Types of attacks - Security on the web | MDN
1: What is an on-path attacker? | Cloudflare
4: [What is a Rogue DHCP Server? - Definition from Techopedia]

NEW QUESTION 188

- (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 190

- (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 194

- (Topic 3)

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

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

Answer: A

Explanation:

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

- ? High availability and resilience: A mesh network can automatically route around failures or congestion, ensuring that the network remains operational even if some nodes are damaged or disconnected. A mesh network can also self-heal and self-configure, adapting to changes in the network topology or environment.
- ? Extended coverage and scalability: A mesh network can extend the wireless signal beyond the range of a single node, by using other nodes as relays or repeaters. A mesh network can also accommodate more nodes and devices, by adding more links and paths between them.
- ? Low cost and easy deployment: A mesh network can reduce the cost and complexity of installing and maintaining a wireless infrastructure, by eliminating the

need for expensive cabling, towers, or antennas. A mesh network can also be deployed quickly and flexibly, by simply adding or removing nodes as needed. A mesh network is especially suitable for public safety vehicles, because it can provide reliable wireless communication in challenging scenarios, such as 12:

- ? Disaster response: A mesh network can be deployed rapidly in areas where the existing wireless infrastructure is damaged or unavailable, such as after an earthquake, flood, or fire. A mesh network can also support emergency services, such as fire fighting, search and rescue, or medical assistance, by enabling data, voice, and video transmission among the responders and command centers.
- ? Mobile surveillance: A mesh network can enable real-time monitoring and control of public safety vehicles, such as police cars, ambulances, or drones, by providing high-bandwidth and low-latency wireless connectivity. A mesh network can also support video streaming, location tracking, remote sensing, or analytics applications for public safety purposes.
- ? Event management: A mesh network can enhance the security and efficiency of large-scale events, such as concerts, festivals, or parades, by providing wireless coverage and capacity for the event organizers and participants. A mesh network can also support crowd management, traffic control, or public announcement applications for event management.

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

NEW QUESTION 196

- (Topic 3)

A user reports that a crucial fileshare is unreachable following a network upgrade that was completed the night before. A network technician confirms the problem exists. Which of the following troubleshooting Steps should the network technician perform NEXT?

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

Answer: A

Explanation:

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

NEW QUESTION 197

- (Topic 3)

A user wants to avoid using a password to access a third-party website. Which of the following does the user need in order to allow this type of access to the third-party website?

- A. Multifactor
- B. RADIUS
- C. SSO
- D. Local authentication

Answer: C

NEW QUESTION 202

- (Topic 3)

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

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

Answer: D

Explanation:

A tone generator is a device that emits an audible signal on a wire. A tone probe is a device that detects the signal on the wire. By attaching the tone generator to one end of the cable and using the tone probe to scan the other end, the technician can identify which switchport the cable is connected to. This method does not require any knowledge of the computer's IP or MAC address, or access to the switch configuration. It is also faster and more reliable than physically tracing the cable or disconnecting the cable and looking for the link light to go out on the switch.

References
How to find what port im connected to on a switch from my PC? Switch Port Monitoring Guide - Comparitech
Finding Out Which Network Switch Port My Computer is Connected

NEW QUESTION 207

- (Topic 3)

A technician is configuring a wireless access point in a public space for guests to use. Which of the following should the technician configure so that only approved connections are allowed?

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

Answer: B

Explanation:

A captive portal is a web page that requires users to authenticate or accept terms of service before they can access the internet through a wireless access point. A captive portal can be used to control who can use the wireless network, limit the bandwidth or time of usage, or display advertisements or information. A captive portal is a common feature of public wireless networks, such as those in hotels, airports, cafes, or libraries. A captive portal can prevent unauthorized or malicious users from accessing the network or consuming network resources.

ReferencesPublic Wireless Access Points Definition | Law InsiderAre Public Wi-Fi Networks Safe? What You Need To Know

NEW QUESTION 209

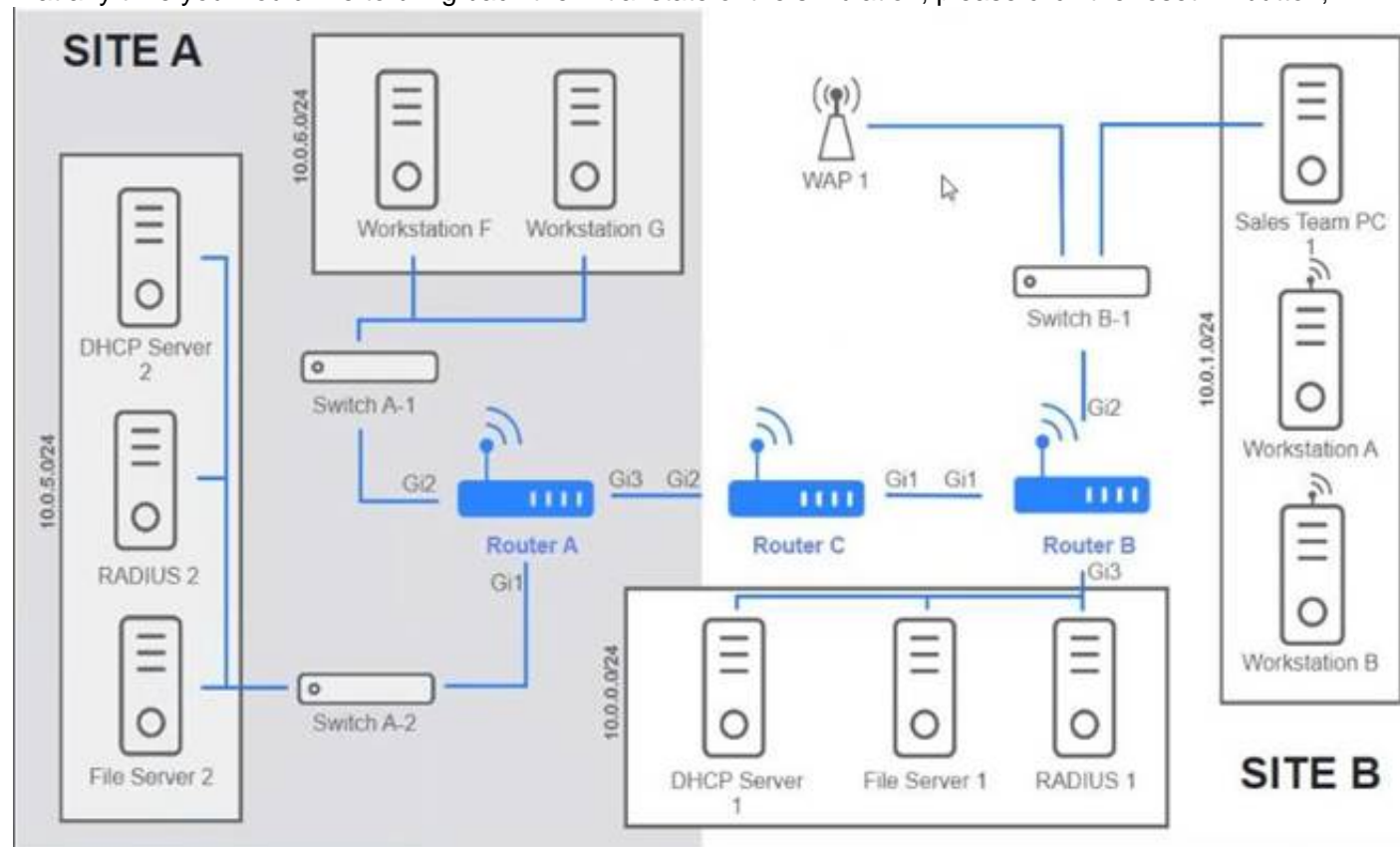
- (Topic 3)

Users are unable to access files on their department share located on file_server 2. The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.

INSTRUCTIONS

Click on each router to review output, identity any Issues, and configure the appropriate solution

If at any time you would like to bring back the initial state of the simulation, please click the reset All button;



Routing Table

Routing Configuration

```

Router-B# show ip route

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

See the solution configuration below in Explanation.

Router A

Routing Table

Routing Configuration

Was a problem found?: ☒ Yes ☐ No

Install Static Route

Destination Prefix: 10.0.5.0

Destination Prefix Mask: 255.255.255.0

Interface: Gi1

Reset to Default

Save

Close

Router B

Routing Table
Routing Configuration

Was a problem found?: ☒ Yes ☐ No

Install Static Route

Destination Prefix: 10.0.5.0

Destination Prefix Mask: 255.255.255.0

Interface: Gi1

Reset to Default
Save
Close

Router C

Routing Table
Routing Configuration

Was a problem found?: ☐ Yes ☒ No

Install Static Route

Destination Prefix:

Destination Prefix Mask:

Interface:

Reset to Default
Save
Close

NEW QUESTION 214

- (Topic 3)

Which of the following ports should a network administrator enable for encrypted log-in to a network switch?

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

Answer: A

Explanation:

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

which is a protocol for web communication. Port 123 is used by NTP, which is a protocol for time synchronization

NEW QUESTION 218

- (Topic 3)

A non-employee was able to enter a server room. Which of the following could have prevented this from happening?

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

Answer: B

Explanation:

A biometric reader is a device that scans a person's physical characteristics, such as fingerprints, iris, or face, and compares them to a database of authorized users. A biometric reader can be used to restrict access to a server room and prevent unauthorized entry. A biometric reader provides a high level of security and cannot be easily bypassed or duplicated.

References: Network+ Study Guide Objective 5.1: Summarize the importance of physical security controls.

NEW QUESTION 221

- (Topic 3)

A network administrator needs to create a way to redirect a network resource that has been on the local network but is now hosted as a SaaS solution. Which of the following records should be used to accomplish the task?

- A. TXT
- B. AAA
- C. PTR
- D. CNAME

Answer: D

Explanation:

CNAME stands for Canonical Name, and it is a type of DNS record that creates an alias for another domain name. A CNAME record can be used to redirect a network resource that has been moved to a different location, such as a SaaS solution. For example, if a web server that was previously hosted on the local network with the domain name `www.example.com` is now hosted by a SaaS provider with the domain name `www.saasprovider.com`, a CNAME record can be created to point `www.example.com` to `www.saasprovider.com`. This way, the users can still access the web server using the original domain name, and the DNS server will resolve it to the new domain name. References

? CNAME is one of the common DNS record types covered in Objective 1.6 of the CompTIA Network+ N10-008 certification exam¹.

? CNAME can be used to redirect a network resource that has been moved to a different location²³.

? CNAME creates an alias for another domain name²³.

1: CompTIA Network+ Certification Exam Objectives, page 4 2: DNS Record Types – N10- 008 CompTIA Network+ : 1.6 3: The Official CompTIA Network+ Student Guide (Exam N10-008), Chapter 1, page 32

NEW QUESTION 222

- (Topic 3)

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

Switch 1:

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

Switch 2:

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

Switch 3:

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

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

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

Answer: AE

NEW QUESTION 226

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 230

- (Topic 3)

Which of the following would be increased by adding encryption to data communication across the network?

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

Answer: D

Explanation:

Confidentiality is the property of preventing unauthorized access or disclosure of data. Encryption is a method of transforming data into an unreadable format that can only be decrypted by authorized parties who have the correct key. Encryption can increase the confidentiality of data communication across the network by

making it harder for attackers to intercept or eavesdrop on the data. References: Network+ Study Guide
Objective 4.1: Summarize the purposes of physical security devices. Subobjective: Encryption.

NEW QUESTION 231

- (Topic 3)

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

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

Answer: E

NEW QUESTION 235

- (Topic 3)

A hacker used a packet sniffer on the network to capture the hardware address of the server. Which of the following types of attacks can the hacker perform now?

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

Answer: B

Explanation:

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

NEW QUESTION 236

- (Topic 3)

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

- ? 110
- ? 66

- A. BiX
- B. Krone

Answer: A

Explanation:

A 110 block is a type of punch-down block that is used to terminate twisted-pair cables in Ethernet networks. It is a non-proprietary standard that is widely used in structured cabling systems for voice and data applications. A 110 block can support up to 100 MHz of bandwidth and can be used with Cat 3, Cat 5, Cat 5e, and Cat 6 cables¹².

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

NEW QUESTION 238

- (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 is set to debugging, which is the most verbose and detailed level of logging. This means that the switch will send a lot of information to the syslog server, which can cause excessive network traffic and storage consumption. To fix the issue, the technician should adjust the logging level to a lower value, such

as informational or warning, which will reduce the amount of data logged

NEW QUESTION 239

- (Topic 3)

An auditor assessing network best practices was able to connect a rogue switch into a network Jack and get network connectivity. Which of the following controls would BEST address this risk?

- A. Activate port security on the switchports providing end user access.
- B. Deactivate Spanning Tree Protocol on network interfaces that are facing public areas.
- C. Disable Neighbor Resolution Protocol in the Layer 2 devices.
- D. Ensure port tagging is in place for network interfaces in guest areas

Answer: A

NEW QUESTION 241

- (Topic 3)

A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User 3 and sees the Ethernet is properly connected. However, the network interface's indicator lights are not blinking on either the computer or the switch. Which of the following is the most likely cause?

- A. The switch failed.
- B. The default gateway is wrong.
- C. The port is shut down.
- D. The VLAN assignment is incorrect.

Answer: C

Explanation:

If the port is shut down, it means that the switch has disabled the port and is not sending or receiving any traffic on it. This would explain why the network interface's indicator lights are not blinking on either the computer or the switch, and why the user cannot access resources on the network. The port could be shut down manually by the network administrator, or automatically by the switch due to security or error conditions.

References

? Port shutdown is one of the common switch configuration options covered in Objective 2.3 of the CompTIA Network+ N10-008 certification exam1.

? Port shutdown can cause the network interface's indicator lights to stop blinking2.

? Port shutdown can prevent the user from accessing resources on the network3.

1: CompTIA Network+ Certification Exam Objectives, page 5 2: CompTIA Network+ N10- 008: Switch not forwarding frames on trunked port3 3: Cable Management – N10-008 CompTIA Network+ : 1.3

NEW QUESTION 245

- (Topic 3)

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

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

Answer: D

Explanation:

Port mirroring is a feature that allows a network switch to copy the traffic from one or more ports to another port for monitoring purposes. Port mirroring can be used to analyze the network traffic from a specific source, destination, or protocol without affecting the normal operation of the network. Port mirroring can also help to detect and troubleshoot network problems, such as performance issues, security breaches, or policy violations.

The other options are not correct because they do not meet the requirements of the question. They are:

? Turn on port security. Port security is a feature that restricts the number and type of devices that can connect to a switch port. Port security can help to prevent unauthorized access, MAC address spoofing, or MAC flooding attacks. However, port security does not allow the network security engineer to view the traffic from the user's PC to the switch.

? Implement dynamic ARP inspection. Dynamic ARP inspection (DAI) is a feature that validates the ARP packets on a network and prevents ARP spoofing attacks. DAI can help to protect the network from man-in-the-middle, denial-of-service, or data interception attacks. However, DAI does not allow the network security engineer to view the traffic from the user's PC to the switch.

? Configure 802.1Q. 802.1Q is a standard that defines how to create and manage virtual LANs (VLANs) on a network. VLANs can help to segment the network into logical groups based on function, security, or performance. However, 802.1Q does not allow the network security engineer to view the traffic from the user's PC to the switch.

References1: Port Mirroring - an overview | ScienceDirect Topics2: Network+ (Plus) Certification | CompTIA IT Certifications3: Port Security - an overview | ScienceDirect Topics4: Dynamic ARP Inspection - an overview | ScienceDirect Topics5: 802.1Q - an overview | ScienceDirect Topics

NEW QUESTION 247

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 249

- (Topic 3)

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

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

Answer: B

Explanation:

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

References

? 1: Port Mirroring - CompTIA Network+ Certification (N10-008): The Total Course [Video]

? 2: CompTIA Network+ Certification Exam Objectives, page 5

? 3: CompTIA Network+ N10-005: 2.1 – Port Mirroring - Professor Messer IT Certification Training Courses

? 4: CompTIA Network+ N10-005: 1.4 – Port Mirroring

NEW QUESTION 254

- (Topic 3)

A newly installed multifunction copier needs to be set up so scanned documents can be emailed to recipients. Which of the following ports from the copier's IP address should be allowed?

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

Answer: B

Explanation:

Port 25 is the port number that is commonly used for Simple Mail Transfer Protocol (SMTP), which is a protocol that allows sending and receiving email messages over a network¹. Port 25 from the copier's IP address should be allowed so that scanned documents can be emailed to recipients.

Port 22 is the port number that is commonly used for Secure Shell (SSH), which is a protocol that allows secure and encrypted remote access and control of a device over a network¹. Port 22 from the copier's IP address is not necessary for emailing scanned documents.

Port 53 is the port number that is commonly used for Domain Name System (DNS), which is a protocol that allows resolving domain names to IP addresses and vice versa on a network¹. Port 53 from the copier's IP address is not necessary for emailing scanned documents.

Port 80 is the port number that is commonly used for Hypertext Transfer Protocol (HTTP), which is a protocol that allows transferring web pages and other resources over a network¹. Port 80 from the copier's IP address is not necessary for emailing scanned documents.

NEW QUESTION 257

- (Topic 3)

A support agent receives a report that a remote user's wired devices are constantly disconnecting and have slow speeds. Upon inspection, the support agent sees that the user's coaxial modem has a signal power of -97dB Which of the following should the support agent recommend to troubleshoot the issue?

- A. Removing any splitters connected to the line
- B. Switching the devices to wireless
- C. Moving the devices closer to the modem
- D. Lowering the network speed

Answer: A

Explanation:

A splitter is a device that divides a coaxial cable into two or more branches, allowing multiple devices to share the same cable connection. However, a splitter also reduces the signal strength and quality of the cable, which can affect the performance and reliability of the devices connected to it. A signal power of -97dB is very low and indicates a weak or poor cable signal, which can cause constant disconnections and slow speeds.

The support agent should recommend removing any splitters connected to the line and connecting the coaxial modem directly to the cable outlet. This can help to improve the signal power and quality of the cable, and thus enhance the performance and reliability of the wired devices. Alternatively, the support agent can also suggest using a signal amplifier or booster, which is a device that increases the signal strength and quality of the cable, to compensate for the signal loss caused by the splitter.

The other options are not correct because they are not the best recommendations to troubleshoot the issue. They are:

? Switching the devices to wireless. Switching the devices to wireless may not solve

the issue, as the wireless connection may also depend on the cable signal and quality. Moreover, switching the devices to wireless may introduce other problems, such as interference, security, or compatibility issues, that can affect the performance and reliability of the devices.

? Moving the devices closer to the modem. Moving the devices closer to the modem

may not solve the issue, as the problem is not related to the distance between the devices and the modem, but to the signal power and quality of the cable.

Moreover, moving the devices closer to the modem may not be feasible or convenient for the user, depending on the layout and setup of the location.

? Lowering the network speed. Lowering the network speed may not solve the issue,

as the problem is not related to the bandwidth or capacity of the network, but to the signal power and quality of the cable. Moreover, lowering the network speed may degrade the user experience and satisfaction, as the user may not be able to access or use the network services or applications as expected.

References1: Network+ (Plus) Certification | CompTIA IT Certifications2: What is a Coaxial Splitter? - Definition from Techopedia3: What is a Signal Amplifier? - Definition from Techopedia

NEW QUESTION 262

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 264

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 269

- (Topic 3)

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

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

Answer: A

Explanation:

A screened subnet is a network segment that is isolated from both the internal LAN and the Internet by firewalls. A screened subnet can be used to host internet-facing hosts such as web servers, email servers, or DNS servers. A screened subnet provides an additional layer of security and prevents direct access to the internal network from the Internet.

References: Network+ Study Guide Objective 3.1: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 271

- (Topic 3)

A network administrator needs to change where the outside DNS records are hosted.

Which of the following records should the administrator change at the registrar to accomplish this task?

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

Answer: A

Explanation:

NS stands for Name Server, and it is a DNS record that specifies which servers are authoritative for a domain. The registrar is the entity that manages the domain registration and delegation, and it maintains the NS records for each domain. To change where the outside DNS records are hosted, the network administrator needs to change the NS records at the registrar to point to the new DNS servers that will host the outside DNS records.

References:

? DNS Record Types – N10-008 CompTIA Network+ : 1.61

? CompTIA Network+ N10-008 Cert Guide, page 1472

NEW QUESTION 276

- (Topic 3)

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

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

Answer: C

Explanation:

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

References¹ - Network access control integration with Microsoft Intune | Microsoft Learn

NEW QUESTION 278

- (Topic 3)

A customer wants to log in to a vendor's server using a web browser on a laptop. Which of the following would require the LEAST configuration to allow encrypted access to the server?

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

Answer: A

Explanation:

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

NEW QUESTION 282

- (Topic 3)

Which of the following describes the ability of a corporate IT department to expand its cloud-hosted VM environment with minimal effort?

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

Answer: A

Explanation:

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

NEW QUESTION 283

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 284

- (Topic 3)

A user reports that a new VoIP phone works properly but the computer that is connected to the phone cannot access any network resources. Which of the following MOST Likely needs to be configured correctly to provide network connectivity to the computer?

- A. Port duplex settings
- B. Port aggregation
- C. ARP settings

- D. VLAN tags
- E. MDIX settings

Answer: D

Explanation:

VLAN (virtual LAN) tags are used to identify packets as belonging to a particular VLAN. VLANs are used to segment a network into logical sub-networks, and each VLAN is assigned a unique VLAN tag. If the VLAN tag is not configured correctly, the computer may not be able to access network resources.

NEW QUESTION 288

- (Topic 3)

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

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

Answer: D

NEW QUESTION 290

- (Topic 3)

Which of the following layers is where TCP/IP port numbers identify which network application is receiving the packet and where it is applied?

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

Answer: B

Explanation:

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

NEW QUESTION 295

- (Topic 3)

Due to concerns around single points of failure, a company decided to add an additional WAN to the network. The company added a second MPLS vendor to the current MPLS WAN and deployed an additional WAN router at each site. Both MPLS providers use OSPF on the WAN network, and EIGRP is run internally. The first site to go live with the new WAN is successful, but when the second site is activated significant network issues occur. Which of the following is the MOST likely cause for the WAN instability?

- A. A routing loop
- B. Asymmetrical routing
- C. A switching loop
- D. An incorrect IP address

Answer: B

Explanation:

Asymmetrical routing is the most likely cause for the WAN instability. When two different routing protocols are used, like OSPF and EIGRP, it can cause asymmetrical routing, which results in traffic being routed differently in each direction. This can lead to instability in the WAN. A CDP neighbor change, a switching loop, or an incorrect IP address are not likely causes for WAN instability.

NEW QUESTION 297

- (Topic 3)

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

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

Answer: B

Explanation:

The maximum duration that a given service can be down before it impacts operations is often referred to as the Recovery Time Objective (RTO). RTO is a key consideration in any backup and disaster recovery plan, as it determines how quickly the organization needs to be able to recover from a disruption or failure. It is typically expressed in terms of time, and it helps to inform the design and implementation of the backup solution. For example, if an organization has a critical service that must be available 24/7, it may have a very low RTO, requiring that the service be restored within a matter of minutes or even seconds. On the other hand, if the service can be down for a longer period of time without significantly impacting operations, the organization may have a higher RTO. When selecting a backup solution, it is important to consider the organization's RTO requirements and ensure that the solution is capable of meeting those needs. A solution that

does not meet the organization's RTO requirements may not be sufficient to ensure the availability of critical services in the event of a disruption or failure.

NEW QUESTION 302

- (Topic 3)

Which of the following refers to a weakness in a mechanism or technical process?

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

Answer: A

Explanation:

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

NEW QUESTION 303

- (Topic 3)

A new student is given credentials to log on to the campus Wi-Fi. The student stores the password in a laptop and is able to connect; however, the student is not able to connect with a phone when only a short distance from the laptop. Given the following information:

Signal strength	90%
Coverage	80%
Interference	15%
Number of connection attempts	10

Which of the following is MOST likely causing this connection failure?

- A. Transmission speed
- B. Incorrect passphrase
- C. Channel overlap
- D. Antenna cable attenuation/signal loss

Answer: B

NEW QUESTION 304

- (Topic 3)

A virtual machine has the following configuration:

- IPv4 address: 169.254.10.10
- Subnet mask: 255.255.0.0

The virtual machine can reach colocated systems but cannot reach external addresses on the internet. Which of the following is most likely the root cause?

- A. The subnet mask is incorrect.
- B. The DHCP server is offline.
- C. The IP address is an RFC1918 private address.
- D. The DNS server is unreachable.

Answer: B

Explanation:

The IP address 169.254.10.10 is an APIPA (Automatic Private IP Addressing) address, which is assigned by the operating system when a DHCP server is not available or reachable. APIPA addresses are in the range of 169.254.0.0/16, and they allow the device to communicate with other devices on the same local network, but not with external networks or the internet. Therefore, the most likely root cause of the virtual machine's connectivity issue is that the DHCP server is offline or malfunctioning, and the virtual machine cannot obtain a valid IP address from it.

References

- ? 1: CompTIA Network+ N10-008 Certification Study Guide, page 86
- ? 2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 9
- ? 3: CompTIA Network+ N10-008 Certification Practice Test, question 4

NEW QUESTION 308

- (Topic 3)

Which of the following routing protocols has routes that are classified with an administrative distance of 110?

- A. BGP
- B. OSPF
- C. EIGRP
- D. RIP

Answer: B

Explanation:

Administrative distance is a measure of the trustworthiness of a routing protocol. The smaller the administrative distance value, the more reliable the protocol.

Each routing protocol has its own default administrative distance value. OSPF has a default administrative distance of 110, which means it is more reliable than RIP (120) but less reliable than EIGRP (90) or BGP (20).

References := Administrative Distance of Routing Protocols - Networks Training, What is Administrative Distance? - Cisco, Adjust Administrative Distance for Route Selection in Cisco IOS Routers ..., Administrative Distance (AD) and Autonomous System (AS)

NEW QUESTION 313

- (Topic 3)

Which of the following routing protocols should be implemented to create a route between a local area network and an ISP?

- A. BGP
- B. EIGRP
- C. RIP
- D. OSPF

Answer: A

Explanation:

BGP stands for Border Gateway Protocol, and it is a routing protocol that is used to exchange routing information between different autonomous systems (AS) on the Internet. An AS is a network or a group of networks that are under the same administrative control and share a common routing policy. BGP is used to create routes between local area networks and Internet service providers (ISPs), as well as between different ISPs. BGP is considered an exterior gateway protocol (EGP), as opposed to an interior gateway protocol (IGP) such as EIGRP, RIP, or OSPF, which are used to create routes within an AS. References: CompTIA Network+ N10-008 Cert Guide, Chapter 3, Section 3.4

NEW QUESTION 318

- (Topic 3)

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

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

Answer: CD

Explanation:

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

NEW QUESTION 321

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 326

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * N10-009 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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