

Exam Questions N10-009

CompTIA Network+ Exam

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



NEW QUESTION 1

- (Topic 3)

Which of the following would most likely affect design considerations when building out an IDF?

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

Answer: B

Explanation:

The fire suppression system is a design consideration when building out an IDF because it can affect the safety and reliability of the network equipment and cabling. A fire suppression system is a system that detects and extinguishes fires in a building, using water, gas, or chemicals. Depending on the type of fire suppression system, it can have different impacts on the IDF design, such as:

? Water-based systems, such as sprinklers, can damage the network equipment and cabling if they are activated by a fire or a false alarm. Therefore, the IDF should be designed to protect the equipment and cabling from water exposure, such as using waterproof cabinets, drip pans, and conduits.

? Gas-based systems, such as clean agent systems, can displace the oxygen in the IDF and cause suffocation for anyone inside. Therefore, the IDF should be designed to allow for ventilation and air circulation, as well as warning signs and alarms to alert anyone in the IDF before the gas is released.

? Chemical-based systems, such as dry chemical systems, can leave a residue on the network equipment and cabling that can affect their performance and lifespan. Therefore, the IDF should be designed to minimize the contact between the chemical and the equipment and cabling, as well as provide a means for cleaning and restoring them after a fire.

The other options are not correct because:

? The source panel amperage is not a design consideration when building out an IDF, as it is determined by the electrical circuit and the power needs of the network equipment and cabling. The source panel amperage does not affect the layout, location, or protection of the IDF.

? The humidity levels are not a design consideration when building out an IDF, as they are controlled by the HVAC system and the ventilation of the IDF. The humidity levels do not affect the layout, location, or protection of the IDF.

? The cable transmission speeds are not a design consideration when building out an IDF, as they are determined by the type and quality of the network cabling and the network equipment. The cable transmission speeds do not affect the layout, location, or protection of the IDF.

NEW QUESTION 2

- (Topic 3)

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

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

Answer: BE

NEW QUESTION 3

- (Topic 3)

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 4

- (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 accountability.

References:

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

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

NEW QUESTION 5

- (Topic 3)

Which of the following is the MOST appropriate use case for the deployment of a clientless VPN?

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

Answer: A

NEW QUESTION 6

- (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 7

- (Topic 3)

Which of the following is required for hosts to receive DHCP addresses from a server that is located on a different subnet?

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

Answer: D

Explanation:

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

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

NEW QUESTION 8

- (Topic 3)

A technician is trying to install a VoIP phone, but the phone is not turning on. The technician checks the cable going from the phone to the switch, and the cable is good. Which of the following actions IS needed for this phone to work?

- A. Add a POE injector
- B. Enable MDIX.
- C. Use a crossover cable.
- D. Reconfigure the port.

Answer: A

NEW QUESTION 9

- (Topic 3)

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

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

Answer: B

Explanation:

One of the best practices to secure the network would be to disable unneeded switchports in the guest waiting area. This will prevent unauthorized users from connecting to the network through these ports. It's important to identify which switchports are not in use and disable them, as this will prevent unauthorized access

to the network. Other practices such as ensuring all guests sign an NDA, lowering the radio strength to reduce Wi-Fi coverage in the waiting area and enabling MAC filtering to block unknown hardware addresses are not as effective in securing the network as disabling unneeded switchports. Enforcing an NDA with guests may not stop a malicious user from attempting to access the network, reducing the radio strength only limits the Wi-Fi coverage, and MAC filtering can be easily bypassed by hackers.

NEW QUESTION 10

- (Topic 3)

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

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

Answer: C

NEW QUESTION 10

- (Topic 3)

A 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 15

- (Topic 3)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 16

- (Topic 3)

Which of the following is the best action to take before sending a network router to be recycled as electronic waste?

- A. Turn on port security.
- B. Shred the switch hard drive.
- C. Back up and erase the configuration.
- D. Remove the company asset ID tag.

Answer: C

Explanation:

Before disposing of a network router, it is important to back up and erase the configuration to prevent unauthorized access to sensitive data and network settings. A network router may contain information such as passwords, IP addresses, firewall rules, VPN settings, and other network parameters that could be exploited by hackers or malicious users. By backing up the configuration, you can preserve the network settings for future reference or reuse. By erasing the configuration, you can wipe out the data and restore the router to its factory default state.

NEW QUESTION 19

- (Topic 3)

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 21

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 26

- (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 31

- (Topic 3)

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

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

Answer: A

Explanation:

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

References:

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

? CompTIA Network+ Certification Exam Objectives²

NEW QUESTION 32

- (Topic 3)

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

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

Answer: A

NEW QUESTION 35

- (Topic 3)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 39

- (Topic 3)

Which of the following protocols can be used to change device configurations via encrypted and authenticated sessions? (Select TWO).

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

Answer: BD

NEW QUESTION 40

- (Topic 3)

A company is considering shifting its business to the cloud. The management team is concerned at the availability of the third-party cloud service. Which of the following should the management team consult to determine the promised availability of the cloud provider?

- A. Memorandum of understanding
- B. Business continuity plan
- C. Disaster recovery plan
- D. Service-level agreement

Answer: D

Explanation:

A Service-level agreement (SLA) is a document that outlines the responsibilities of a cloud service provider and the customer. It typically includes the agreed-upon availability of the cloud service provider, the expected uptime for the service, and the cost of any downtime or other service interruptions. Consulting the SLA is the best way for the management team to determine the promised availability of the cloud provider. Reference: CompTIA Cloud+ Study Guide, 6th Edition, page 28.

NEW QUESTION 43

- (Topic 3)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 47

- (Topic 3)

The power company notifies a network administrator that it will be turning off the power to the building over the weekend. Which of the following is the BEST solution to prevent the servers from going down?

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

Answer: A

NEW QUESTION 49

- (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 54

- (Topic 3)

Due to space constraints in an IDF, a network administrator can only add a single switch to accommodate three data networks. The administrator needs a configuration that will allow each device to access its expected network without additional connections. The configuration must also allow each device to access the rest of the network. Which of the following should the administrator do to meet these requirements? (Select TWO).

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

Answer: AC

Explanation:

To achieve this, you should do two things:

? Tag the three VLANs across the uplink port that connects to another switch or router. This will allow data packets from different VLANs to cross over into other networks.

? Untag an individual VLAN per device port that connects to an end device. This will assign each device to its expected network without additional connections.

NEW QUESTION 55

- (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 57

- (Topic 3)

Which of the following devices would be used to extend the range of a wireless network?

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

Answer: A

Explanation:

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

wireless network by repeating the signal from one access point to another."

NEW QUESTION 61

- (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 62

- (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 67

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 70

- (Topic 3)

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

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

Answer: C

Explanation:

Documenting the lessons learned is the best method for passing along the exact steps other technicians should follow in case the issue arises again. Lessons learned are the knowledge and experience gained from completing a project or solving a problem. Documenting the lessons learned helps to capture the best practices, challenges, solutions, and recommendations for future reference and improvement. Documenting the lessons learned can also help to update the knowledge base, standard operating procedures, or policies related to the issue. References: [CompTIA Network+ Certification Exam Objectives], Lessons Learned: Definition & Examples for Project Managers

NEW QUESTION 71

- (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?

- A. 110
- B. 66
- C. Bix
- D. Krone

Answer: A

Explanation:

A 110 block is a type of punch-down block that is used to distribute Ethernet to multiple computers in an office. A punch-down block is a device that connects one group of wires to another group of wires by using a special tool that pushes the wires into slots on the block. A 110 block is a non-proprietary standard that supports up to Category 6 cabling and can be used for voice or data applications. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 64)

NEW QUESTION 73

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 78

- (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 80

- (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 81

- (Topic 3)

A help desk technician is concerned that a client's network cable issues may be causing intermittent connectivity. Which of the following would help the technician determine if this is the issue?

- A. Run the show interface command on the switch
- B. Run the traceroute command on the server
- C. Run iperf on the technician's desktop
- D. Ping the client's computer from the router
- E. Run a port scanner on the client's IP address

Answer: A

Explanation:

To determine if a client's network cable issues may be causing intermittent connectivity, the help desk technician can run the show interface command on the switch.

This command allows the technician to view the status and statistics of the various interfaces on the switch, including the physical link status and the number of transmitted and received packets. If the interface is experiencing a large number of errors or dropped packets, this could indicate a problem with the network cable

or with the connection between the client's device and the switch.

"Cisco routers and switches have a show interfaces IOS command that provides interface statistics/status information, including link state (up/down), speed/duplex, send/receive traffic, cyclic redundancy checks (CRCs), and protocol packet and byte counts."

NEW QUESTION 86

- (Topic 3)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 87

- (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 90

- (Topic 3)

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

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

Answer: A

NEW QUESTION 94

- (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 98

- (Topic 3)

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

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

Answer: B

Explanation:

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

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

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

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

What is in a project charter?

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

What are the 5 elements of the project charter?

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

NEW QUESTION 101

- (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 106

- (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 111

- (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 115

- (Topic 3)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 118

- (Topic 3)

A technician was cleaning a storage closet and found a box of transceivers labeled 8Gbps. Which of the following protocols uses those transceivers?

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

Answer: C

Explanation:

The transceivers labeled 8Gbps are likely to be used with the Fibre Channel protocol. Fibre Channel is a high-speed networking technology that is primarily used to connect storage devices to servers in storage area networks (SANs). It is capable of transmitting data at speeds of up to 8 Gbps (gigabits per second), and uses specialized transceivers to transmit and receive data over fiber optic cables.

Coaxial over Ethernet (CoE) is a networking technology that uses coaxial cables to transmit data, and is not related to the transceivers in question. Internet Small Computer Systems Interface (iSCSI) is a protocol that allows devices to communicate over a network using the SCSI protocol, and does not typically use specialized transceivers. Gigabit interface converter (GBIC) is a type of transceiver used to transmit and receive data over fiber optic cables, but it is not capable of transmitting data at 8 Gbps.

NEW QUESTION 123

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 126

- (Topic 3)

A user from a remote office is reporting slow file transfers. Which of the following tools will an engineer MOST likely use to get detailed measurement data?

- A. Packet capture
- B. IPerf
- C. SIEM log review
- D. Internet speed test

Answer: B

Explanation:

An engineer will most likely use IPerf to get detailed measurement data about the user's slow file transfers. IPerf is a tool used for measuring network performance and bandwidth, and it can be used to measure the speed and throughput of file transfers from the remote office. It can also provide detailed information about the latency and jitter of the connection, which can be used to troubleshoot the slow file transfers. Reference: CompTIA Network+ Study Manual (Chapter 10, Page 214).

NEW QUESTION 129

- (Topic 3)

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

- A. VPN headend
- B. Proxy server

- C. Bridge
- D. Load balancer

Answer: A

Explanation:

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

NEW QUESTION 130

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 134

- (Topic 3)

An online gaming company needs a cloud solution that will allow for more virtual resources to be deployed when tournaments are held. The number of users who access the service increases during tournaments. The company also needs the resources to return to baseline levels once the resources are not needed in order to reduce cost. Which of the following cloud concepts would provide the best solution?

- A. Scalability
- B. Hybrid
- C. Multitenancy
- D. Elasticity

Answer: D

Explanation:

Elasticity is the ability of a cloud service to automatically adjust the amount of resources allocated to meet the changing demand of the users. Elasticity enables a cloud service to scale up or down resources quickly and efficiently, without requiring manual intervention or planning. Elasticity is ideal for scenarios where the demand is unpredictable, dynamic, or seasonal, such as online gaming tournaments. By using elasticity, the online gaming company can ensure optimal performance and user experience during peak times, while also saving costs and avoiding overprovisioning during off-peak times.

The other options are not correct because they do not address the specific needs of the online gaming company. They are:

- Scalability is the ability of a cloud service to handle an increase or decrease in the demand of the users by adding or removing resources. Scalability is similar to elasticity, but it is more manual, planned, and predictive, while elasticity is automatic, prompt, and reactive. Scalability is suitable for scenarios where the demand is steady, predictable, or gradual, such as a growing business or a long-term project.
- Hybrid is a type of cloud model that combines two or more clouds, such as on-premises private, hosted private, or public, that can be centrally managed to enable interoperability for various use cases. Hybrid cloud can offer benefits such as flexibility, security, and cost- efficiency, but it does not directly address the need for dynamic resource allocation for the online gaming company.
- Multitenancy is a feature of cloud services that allows multiple users or customers to share the same physical or virtual resources, such as servers, databases, or applications, while maintaining isolation and privacy. Multitenancy can offer benefits such as efficiency, scalability, and cost-effectiveness, but it does not directly address the need for dynamic resource allocation for the online gaming company.

References

1: Understand cloud concepts | Microsoft Press Store 2: What Is Hybrid Cloud? - Cisco

3: Difference between Elasticity and Scalability in Cloud Computing 4: Scalability and Elasticity in Cloud Computing - GeeksforGeeks

NEW QUESTION 139

- (Topic 3)

A network team is getting reports that air conditioning is out in an IDF. The team would like to determine whether additional network issues are occurring. Which of the following should the network team do?

- A. Confirm that memory usage on the network devices in the IDF is normal.
- B. Access network baseline data for references to an air conditioning issue.
- C. Verify severity levels on the corporate syslog server.
- D. Check for SNMP traps from a network device in the IDF.
- E. Review interface statistics looking for cyclic redundancy errors.

Answer: D

Explanation:

"Baselines play an integral part in network documentation because they let you monitor the network's overall performance. In simple terms, a baseline is a measure of performance that indicates how hard the network is working and where network resources are spent. The purpose of a baseline is to provide a basis of comparison. For example, you can compare the network's performance results taken in March to results taken in June, or from one year to the next. More commonly, you would compare the baseline information at a time when the network is having a problem to information recorded when the network was operating with greater efficiency. Such comparisons help you determine whether there has been a problem with the network, how significant that problem is, and even where

the problem lies."

NEW QUESTION 141

- (Topic 3)

During an annual review of policy documents, a company decided to adjust its recovery time frames. The company agreed that critical applications can be down for no more than six hours, and the acceptable amount of data loss is no more than two hours. Which of the following should be documented as the RPO?

- A. Two hours
- B. Four hours
- C. Six hours
- D. Eight hours

Answer: A

Explanation:

“ RPO designates the variable amount of data that will be lost or will have to be re-entered during network downtime. RTO designates the amount of “real time” that can pass before the disruption begins to seriously and unacceptably impede the flow of normal business operations.”

NEW QUESTION 142

- (Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 143

- (Topic 3)

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

- A. Adding more wireless APS
- B. Increasing power settings to expand coverage
- C. Configuring the APS to be compatible with 802.11a
- D. Changing the wireless channel used

Answer: C

Explanation:

* 802.11g is an older wireless standard that operates in the 2.4 GHz frequency band and has a maximum data rate of 54 Mbps. 802.11a is a newer wireless standard that operates in the 5 GHz frequency band and has a maximum data rate of 54 Mbps. By configuring the APS to be compatible with 802.11a, the network engineer can reduce interference and congestion in the 2.4 GHz band and improve wireless performance.

References: Network+ Study Guide Objective 2.5: Implement network troubleshooting methodologies

NEW QUESTION 148

- (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 disaster. 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 151

- (Topic 3)

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

- A. QoS traffic classification
- B. Port mirroring
- C. Flow control

D. Link Aggregation Control Protocol

Answer: B

NEW QUESTION 152

- (Topic 3)

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

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

Which of the following should the analyst recommend?

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

Answer: A

Explanation:

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

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

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

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

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

NEW QUESTION 157

- (Topic 3)

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

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

Answer: C

Explanation:

ICMP (Internet Control Message Protocol) is a protocol that is used to send error and control messages between network devices, such as ping requests and replies. ICMP is being blocked by the firewall, which prevents the network technician from pinging the web server. TCP (Transmission Control Protocol) is a protocol that provides reliable and ordered delivery of data between network devices, such as web service requests and responses using HTTP (Hypertext Transfer Protocol). TCP is not being blocked by the firewall, which allows the network technician to verify connectivity to the web service using Telnet. UDP (User Datagram Protocol) is a protocol that provides fast and efficient delivery of data between network devices, but does not guarantee reliability or order. UDP is used for applications such as streaming media or online gaming. ARP (Address Resolution Protocol) is a protocol that resolves IP addresses to MAC addresses on a local network. References: [CompTIA Network+ Certification Exam Objectives], Domain 2.0 Networking Concepts, Objective 2.1: Compare and contrast OSI and TCP/IP models, Subobjective: TCP/IP model layers (Application/Transport/Internet/Network Interface)

NEW QUESTION 162

- (Topic 3)

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

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

Answer: E

Explanation:

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

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

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

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

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

References

What is CVE?

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

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

NEW QUESTION 165

- (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 166

- (Topic 3)

After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect take to troubleshoot the issue?

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

Answer: A

Explanation:

Cat 8 keystones are shielded to prevent interference from external sources, but they also require proper grounding to avoid interference from within the cable.

Wrapping the end connections with copper tape before terminating them is one way to ensure a good ground connection and reduce interference. Using passthrough modular crimping plugs, connecting the RX/TX wires to different pins, or running a speed test on a slow device are not relevant or effective steps to troubleshoot the issue.

References:

? CompTIA Network+ N10-008 Certification Study Guide, page 191

? CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 362

? CAT8 RJ45 Keystone Problem : r/HomeNetworking2

? How to Terminate Cat8 Shielded Keystone Jacks3

NEW QUESTION 167

- (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 169

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 173

- (Topic 3)

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

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

Answer: A

Explanation:

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

? CompTIA Network+ N10-008 Certification Exam Objectives, page 91
? CompTIA Network+ Cert Guide: Switching and Virtual LANs, page 172

NEW QUESTION 177

- (Topic 3)

A technician is equipped with a tablet, a smartphone, and a laptop to troubleshoot a switch with the help of support over the phone. However, the technician is having issues interconnecting all these tools in troubleshooting the switch. Which Of the following should the technician use to gain connectivity?

- A. PAN
- B. WAN
- C. LAN
- D. MAN

Answer: A

Explanation:

A PAN stands for Personal Area Network and it is a type of network that connects devices within a small range, such as a few meters. A PAN can use wireless technologies such as Bluetooth or Wi-Fi to interconnect devices such as tablets, smartphones, and laptops. A technician can use a PAN to gain connectivity among these tools and troubleshoot the switch.

References: Network+ Study Guide Objective 1.2: Explain devices, applications, protocols and services at their appropriate OSI layers.

NEW QUESTION 182

SIMULATION - (Topic 3)

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

INSTRUCTIONS

Click on each tab at the top of the screen. Select a widget to view information, then

use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Health Device Monitoring Show Question Reset All Answers

Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms

Which WAN station should be preferred for VoIP traffic?

WAN 1
Select WAN
WAN 1
WAN 2

Network Health Device Monitoring Show Question Reset All Answers

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

Which device is experiencing connectivity issues?

Select Answer
Router A
Router B
WAP1
WAP2
WirelessController
Switch A
Switch B
DHCP Server
Web Server
APP Server
Router A

Which workstation IP is generating the MOST traffic?

Select Answer
10.1.99.28
10.1.99.14
10.1.99.10
10.1.99.22
10.1.99.24
206.208.133.10
206.208.133.9
10.1.50.14
10.1.50.13
10.1.59.81
10.1.90.53
10.1.90.55
206.208.133.9

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Network Health:

WAN 2 appears to have a lower average latency and loss percentage, which would make it the preferred WAN station for VoIP traffic. VoIP traffic requires low latency and packet loss to ensure good voice quality and reliability. WAN 1 seems to have higher RAM and processor usage, which could also affect the performance of VoIP traffic.

Here's the summary of the key metrics for WAN 1 and WAN 2 from the image provided:

? WAN 1:
? WAN 2:

For VoIP traffic, low latency and jitter are particularly important to ensure voice quality. While WAN 1 has higher bandwidth and throughput, it also has higher latency and jitter compared to WAN 2. However, WAN 2 has much lower loss, lower latency, and lower jitter, which are more favorable for VoIP traffic that is sensitive to delays and variation in packet arrival times. Given this information, WAN 2 would generally be preferred for VoIP traffic due to its lower latency, lower jitter, and significantly lower loss percentage, despite its lower bandwidth compared to WAN 1. The high bandwidth of WAN 1 may be more suitable for other types of traffic that are less sensitive to latency and jitter, such as bulk data transfers.



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



A screenshot of a computer
Description automatically generated

NEW QUESTION 185

- (Topic 3)
An attacker sends more connection requests than a server can handle, causing the server to crash- Which of the following types of attacks is this an example of?

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

Answer: B

Explanation:

A denial-of-service (DoS) attack is an example of an attack where an attacker sends more connection requests than a server can handle, causing the server to crash. A DoS attack is a type of cyberattack that aims to disrupt the normal functioning of a network service or resource by overwhelming it with excessive or

malformed traffic. A DoS attack can prevent legitimate users from accessing the service or resource, resulting in degraded performance, unavailability, or data loss. A DoS attack can target various network layers, protocols, or components, such as servers, routers, firewalls, or applications. References: [CompTIA Network+ Certification Exam Objectives], What Is a Denial-of-Service (DoS) Attack? | Cisco

NEW QUESTION 189

- (Topic 3)

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

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

Answer: C

Explanation:

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

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

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

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

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

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

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

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

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

NEW QUESTION 190

SIMULATION - (Topic 3)

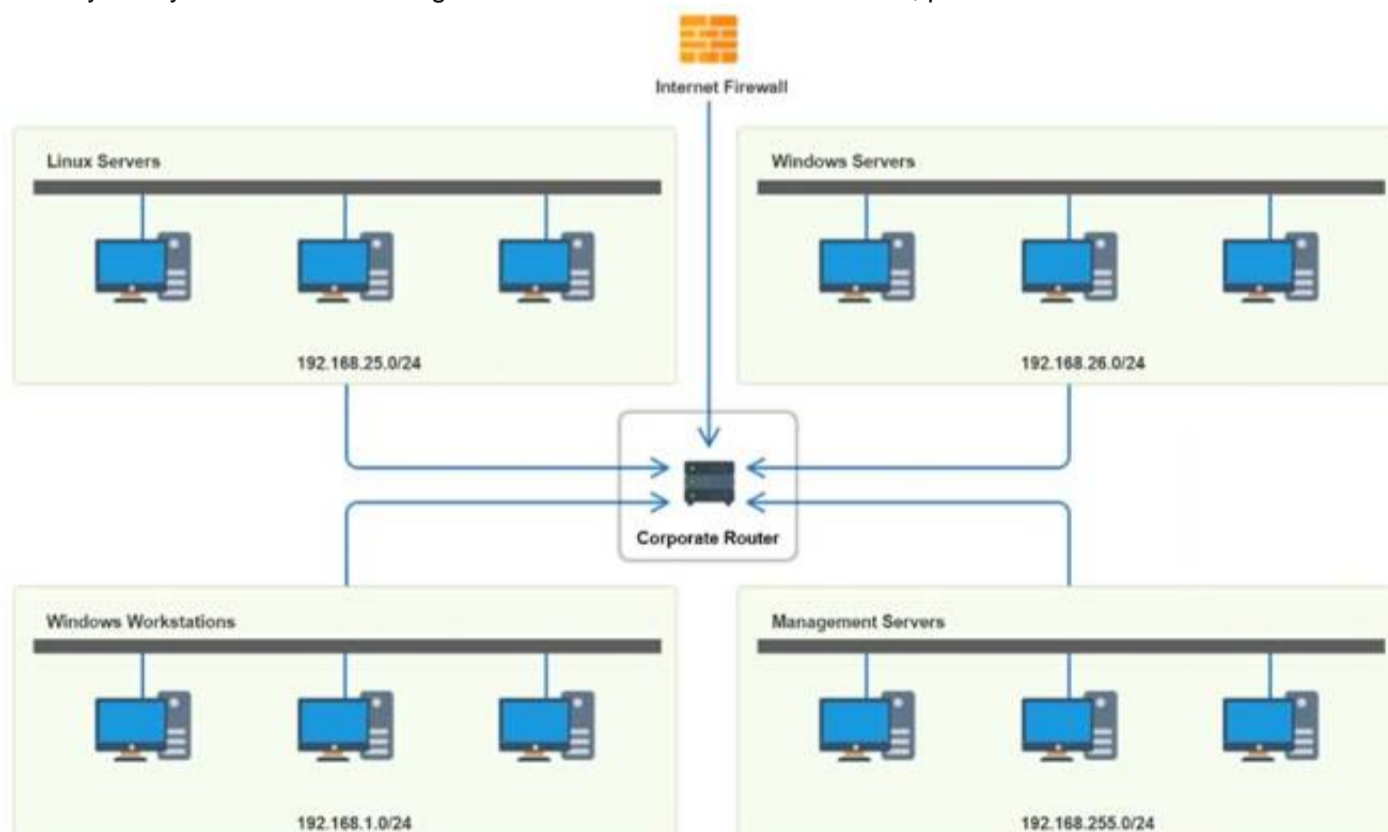
You have been tasked with implementing an ACL on the router that will:

- * 1. Permit the most commonly used secure remote access technologies from the management network to all other local network segments
- * 2. Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.
- * 3. Prohibit any traffic that has not been specifically allowed.

INSTRUCTIONS

Use the drop-downs to complete the ACL

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



Router Access Control List ✕					
Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	Any	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Router Access Control List					
Rule	Source	Destination	Protocol	Service	Action
1	192.168.255.0	192.168.26.0	TCP	SSH	Allow
2	192.168.255.0	192.168.25.0	TCP	SSH	Allow
3	192.168.255.0	192.168.1.0	TCP	SSH	Allow
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0	Any	TCP	RDP	Deny
7	192.168.1.0	Any	TCP	VNC	Deny
8	192.168.1.0	Any	Any	Any	Allow
9	Any	Any	Any	Any	Deny

NEW QUESTION 193

- (Topic 3)

A coffee shop owner hired a network consultant to provide recommendations for installing a new wireless network. The coffee shop customers expect high speeds even when the network is congested. Which of the following standards should the consultant recommend?

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

Answer: B

Explanation:

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

NEW QUESTION 196

- (Topic 3)

An IT technician needs to increase bandwidth to a server. The server has multiple gigabit ports. Which of the following can be used to accomplish this without replacing hardware?

- A. STP
- B. 802.1Q
- C. Duplex
- D. LACP

Answer: D

Explanation:

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

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5: Compare and contrast network cabling types, standards and speeds.

NEW QUESTION 200

- (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 201

- (Topic 3)

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

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

Answer: B

Explanation:

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

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

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

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

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

NEW QUESTION 206

- (Topic 3)

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

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

Answer: A

Explanation:

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

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

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

? Low cost and easy deployment: A mesh network can reduce the cost and complexity of installing and maintaining a wireless infrastructure, by eliminating the need for expensive cabling, towers, or antennas. A mesh network can also be deployed quickly and flexibly, by simply adding or removing nodes as needed.

A mesh network is especially suitable for public safety vehicles, because it can provide reliable wireless communication in challenging scenarios, such as¹²:

? 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 207

- (Topic 3)

An AP uses a 98ft (30m) Cat 6 cable to connect to an access switch. The cable is wired through a duct close to a three-phase motor installation. Anytime the three-phase is turned on, all users connected to the switch experience high latency on the network. Which Of the following is MOST likely the cause Of the issue?

- A. Interference
- B. Attenuation
- C. Open circuit
- D. Short circuit

Answer: A

Explanation:

Interference is a phenomenon that occurs when unwanted signals or noise affect the transmission or reception of data signals on a network. Interference can cause network issues such as high latency, low throughput, packet loss, or errors. Interference can be caused by various sources, such as electromagnetic fields, radio waves, power lines, or electrical devices. In this scenario, the three-phase motor installation is a source of interference that affects the Cat 6 cable that

connects the AP to the access switch. The cable is wired through a duct close to the motor installation, which exposes it to the electromagnetic fields generated by the motor. Anytime the motor is turned on, the interference causes high latency for all users connected to the switch.

NEW QUESTION 210

- (Topic 3)

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

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

Answer: B

NEW QUESTION 215

- (Topic 3)

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

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

Answer: D

Explanation:

The best security measure to implement when removing a computer from a cubicle is to remove the employee's network access. This will prevent the employee from accessing any network resources or data from the computer, as well as prevent any unauthorized users from using the computer to access the network. Removing the employee's network access can be done by deleting or disabling the user account, revoking the credentials, or changing the permissions.

The other options are not as effective or necessary as removing the employee's network access. They are:

- Disabling DHCP on the computer being removed will prevent the computer from obtaining an IP address from the network, but it will not prevent the computer from using a static IP address or accessing the network through another device.
- Placing the switch port in a private VLAN will isolate the computer from other devices on the network, but it will not prevent the computer from accessing the network through another port or device.
- Applying a firewall rule to block the computer's IP address will prevent the computer from communicating with the network, but it will not prevent the computer from changing its IP address or accessing the network through another device.

References

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

3: 10 Ways to Secure Office Workstations - Computer Security

NEW QUESTION 220

- (Topic 3)

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

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

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

Answer: A

Explanation:

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

References:

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

? CompTIA Network+ Certification Exam Objectives, page 92

NEW QUESTION 221

- (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 224

- (Topic 3)

A technician reviews a network performance report and finds a high level of collisions happening on the network. At which of the following layers of the OSI model would these collisions be found?

- A. Layer 1
- B. Layer 3
- C. Layer 4
- D. Layer 7

Answer: A

Explanation:

Collisions occur when two or more devices try to transmit signals on the same physical medium at the same time. This causes interference and data loss. Collisions can only happen at the physical layer of the OSI model, which is responsible for transmitting and receiving raw bits over a physical medium such as a cable or a wireless channel. The physical layer does not have any mechanism to prevent or resolve collisions. Therefore, higher layers of the OSI model, such as the data link layer, need to implement protocols to detect and recover from collisions, such as CSMA/CD for Ethernet networks. References Collision in computer networking Data Link Layer | Layer 2 | The OSI-Model

NEW QUESTION 229

- (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 231

- (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 235

- (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 237

- (Topic 3)

A computer engineer needs to ensure that only a specific workstation can connect to port 1 on a switch. Which of the following features should the engineer configure on the switch interface?

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

Answer: B

Explanation:

Port security is a feature that can be configured on a switch interface to limit and identify the MAC addresses of workstations that are allowed to connect to that specific port. This can help ensure that only a specific workstation (or workstations) can connect to the interface. According to the CompTIA Network+ Study Manual, "Port security can be used to specify which MAC addresses are allowed to connect to a particular switch port. If a port security violation is detected, the switch can take a number of different actions, such as shutting down the port, sending an SNMP trap, or sending an email alert."

NEW QUESTION 240

- (Topic 3)

Which of the following is used when a workstation sends a DHCP broadcast to a server on another LAN?

- A. Reservation
- B. Dynamic assignment
- C. Helper address
- D. DHCP offer

Answer: C

Explanation:

A helper address is an IP address that is configured on a router interface to forward DHCP broadcast messages to a DHCP server on another LAN. A DHCP broadcast message is a message that a workstation sends when it needs to obtain an IP address from a DHCP server. Since broadcast messages are not routed across different networks, a helper address is needed to relay the DHCP broadcast message to the DHCP server on another network. References:
<https://www.comptia.org/training/books/network-n10-008-study-guide> (page 199)

NEW QUESTION 245

- (Topic 3)

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

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

Answer: C

Explanation:

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

References

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

3 - What is unauthorized physical access? – Heimduo

NEW QUESTION 249

- (Topic 3)

A technician needs to configure a routing protocol for an internet-facing edge router. Which of the following routing protocols will the technician MOST likely use?

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

Answer: A

NEW QUESTION 251

- (Topic 3)

An international company is transferring its IT assets including a number of WAPs from the United States to an office in Europe for deployment. Which of the following considerations should the company research before implementing the wireless hardware?

- A. WPA2 cipher
- B. Regulatory Impacts
- C. CDMA configuration
- D. 802.11 standards

Answer: B

Explanation:

When transferring IT assets, including wireless access points (WAPs), from one country to another, it's important to research the regulatory impacts of the move. Different countries have different regulations and compliance requirements for wireless devices, such as frequency bands, power levels, and encryption standards. Failing to comply with these regulations can result in fines or other penalties.

NEW QUESTION 252

- (Topic 3)

A network administrator needs to set up a file server to allow user access. The organization uses DHCP to assign IP addresses. Which of the following is the best solution for the administrator to set up?

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

Answer: B

Explanation:

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

NEW QUESTION 256

- (Topic 3)

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

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

Answer: D

NEW QUESTION 257

- (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 260

- (Topic 3)

Which of the following is a document that states what the minimum performance expectations are within a network?

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

Answer: B

Explanation:

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

NEW QUESTION 262

- (Topic 3)

Which of the following would be used when connecting devices that have different physical characteristics?

- A. A proxy server
- B. An industrial control system
- C. A load balancer
- D. A media converter

Answer: D

NEW QUESTION 263

- (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 267

- (Topic 3)

Which of the following is a major difference between a router and a Layer 3 switch?

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

Answer: A

Explanation:

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

NEW QUESTION 272

- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 273

- (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 277

- (Topic 3)

Which of the following should be used to associate an IPv6 address with a domain name?

- A. AAAA
- B. A
- C. SOA
- D. TXT

Answer: A

Explanation:

An AAAA record is a type of DNS record that maps a domain name to an IPv6 address. It is similar to an A record, which maps a domain name to an IPv4 address, but it uses a 128-bit address instead of a 32-bit one. An AAAA record allows a domain name to be resolved by both IPv4 and IPv6 clients, and it is necessary for accessing websites and services that use IPv6.

NEW QUESTION 280

- (Topic 3)

Classification using labels according to information sensitivity and impact in case of unauthorized access or leakage is a mandatory component of:

- A. an acceptable use policy.
- B. a memorandum of understanding.
- C. data loss prevention,
- D. a non-disclosure agreement.

Answer: C

Explanation:

Data loss prevention (DLP) is a set of tools and processes that aim to prevent unauthorized access or leakage of sensitive information. One of the components of DLP is data classification, which involves labeling data according to its information sensitivity and impact in case of unauthorized disclosure. Data classification helps to identify and protect the most critical and confidential data and apply appropriate security controls and policies. References: Network+ Study Guide Objective 5.1: Explain the importance of policies, processes and procedures for IT governance. Subobjective: Data loss prevention.

NEW QUESTION 285

- (Topic 3)

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

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

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

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

Answer: A

Explanation:

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

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

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

Therefore, the correct command is:

route ADD 0.0.0.0 MASK 0.0.0.0 10.10.51.10 metric 35

NEW QUESTION 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 294

- (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 299

- (Topic 3)

A network technician is hired to review all the devices within a network and make recommendations to improve network efficiency. Which of the following should the technician do FIRST before reviewing and making any recommendations?

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

Answer: A

Explanation:

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

NEW QUESTION 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 307

- (Topic 3)

Which of the following network devices can perform routing between VLANs?

- A. Layer 2 switch
- B. Layer 3 switch
- C. Load balancer
- D. Bridge

Answer: B

Explanation:

<https://www.practicalnetworking.net/stand-alone/routing-between-vlans/#:~:text=A%20router%20will%20perform%20the,to%20communicate%20with%20on,e%20another.>

NEW QUESTION 308

- (Topic 3)

A network technician is selecting a replacement for a damaged fiber cable that goes directly to an SFP transceiver on a network switch. Which of the following cable connectors should be used?

- A. RJ45
- B. LC
- C. MT
- D. F-type

Answer: C

NEW QUESTION 310

- (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 311

- (Topic 3)

Which of the following routing protocols is BEST suited for use on a perimeter router?

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

Answer: D

Explanation:

BGP stands for Border Gateway Protocol and it is used to exchange routing information between autonomous systems (AS) on the Internet. A perimeter router is a router that connects an AS to another AS or to the Internet. Therefore, BGP is the best suited routing protocol for a perimeter router. References: Network+ Study Guide Objective 2.4: Compare and contrast the characteristics of network topologies, types and technologies.

NEW QUESTION 313

- (Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 314

- (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 318

- (Topic 3)

Which of the following is the DNS feature that controls how long a lookup is stored in cache on a server?

- A. CNAME
- B. TTL
- C. SOA
- D. SRV

Answer: B

Explanation:

TTL stands for Time to Live, and it is a field on DNS records that controls how long each record is valid and cached by the DNS resolver before it expires and requests a new one. The TTL value is measured in seconds, and it affects how quickly DNS changes propagate across the Internet. A lower TTL means that the DNS resolver will refresh the record more frequently, but it also increases the load on the DNS servers. A higher TTL means that the DNS resolver will cache the record longer, but it also delays the update of the record.

NEW QUESTION 320

- (Topic 3)

While working in a coffee shop, an attacker watches a user log in to a corporate system and writes down the user's log-in credentials. Which of the following social engineering attacks is this an example of?

- A. Shoulder surfing
- B. Dumpster diving
- C. Phishing
- D. Tailgating

Answer: A

Explanation:

Shoulder surfing is the social engineering attack where an attacker watches a user log in to a corporate system and writes down the user's log-in credentials. Social engineering is a type of attack that exploits human psychology and behavior to manipulate or trick people into revealing sensitive information or performing malicious actions. Shoulder surfing is a form of social engineering that involves observing or eavesdropping on someone's screen, keyboard, or paper documents to obtain confidential information such as passwords, PINs, or credit card numbers. Shoulder surfing can be done in person or remotely using cameras or other devices. Shoulder surfing can be prevented by using privacy filters, locking screens, shielding keyboards, or being aware of one's surroundings. References: [CompTIA Network+ Certification Exam Objectives], What Is Shoulder Surfing? | Definition & Examples | Forcepoint

NEW QUESTION 321

- (Topic 3)

A technician is assisting a user who cannot connect to a website. The technician attempts to ping the default gateway and DNS server of the workstation. According to troubleshooting methodology, this is an example of:

- A. a divide-and-conquer approach.
- B. a bottom-up approach.
- C. a top-to-bottom approach.
- D. implementing a solution.

Answer: A

NEW QUESTION 325

- (Topic 3)

An employee reports to a network administrator that internet access is not working. Which of the following should the administrator do FIRST?

- A. Establish a theory of probable cause.
- B. Identify symptoms.
- C. Determine if anything has changed.
- D. Ask the user to restart the computer.

Answer: C

Explanation:

When a user reports that internet access is not working, it is important to first determine if there have been any recent changes to the network or the user's computer that could have caused the issue. This could include changes to the network configuration, the installation of new software or hardware, or other events that could have impacted the user's ability to access the internet. By determining if anything has changed, the administrator can narrow down the possible causes of the issue and focus on addressing the most likely cause.

NEW QUESTION 326

- (Topic 3)

A network administrator is planning to implement device monitoring to enhance network visibility. The security team requires that the solution provides authentication and encryption.

Which of the following meets these requirements?

- A. SIEM

- B. Syslog
- C. NetFlow
- D. SNMPv3

Answer: D

Explanation:

SNMPv3 is a protocol that allows network administrators to monitor and manage network devices such as routers, switches, servers, printers, and more. SNMPv3 provides authentication and encryption features that ensure the security and integrity of the data exchanged between the management station and the network devices. SNMPv3 uses a user-based security model (USM) that supports three levels of security: noAuthNoPriv, authNoPriv, and authPriv. The noAuthNoPriv level provides no authentication or encryption, the authNoPriv level provides authentication but no encryption, and the authPriv level provides both authentication and encryption¹².

References

? SNMP is one of the common network monitoring protocols covered in Objective 3.1 of the CompTIA Network+ N10-008 certification exam³.

? SNMPv3 provides authentication and encryption features for network monitoring¹².

? SNMPv3 uses a user-based security model with three levels of security¹².

1: SNMP - N10-008 CompTIA Network+ : 3.1 - Professor Messer IT Certification Training Courses 2: CompTIA Network+ N10-008 Cert Guide, Chapter 13, page 413 3: CompTIA Network+ Certification Exam Objectives, page 7

NEW QUESTION 328

- (Topic 3)

A network administrator needs to provide evidence to confirm that recent network outages were caused by increased traffic generated by a recently released application. Which of the following actions will BEST support the administrator's response?

- A. Generate a network baseline report for comparison.
- B. Export the firewall traffic logs.
- C. Collect the router's NetFlow data.
- D. Plot interface statistics for dropped packets.

Answer: C

NEW QUESTION 332

- (Topic 3)

A customer called the help desk to report a network issue. The customer recently added a hub between the switch and the router in order to duplicate the traffic flow to a logging device. After adding the hub, all the Other network components that were connected to the switch slowed more than expected. Which Of the following is the MOST likely cause Of the issue?

- A. Duplex mismatch
- B. Flow control failure
- C. STP malfunction
- D. 802.1Q disabled

Answer: A

Explanation:

A duplex mismatch is a situation where two devices on a network have different duplex settings, such as full-duplex or half-duplex. Full-duplex means that a device can send and receive data simultaneously, while half-duplex means that a device can only send or receive data at a time. A duplex mismatch can cause performance issues, such as collisions, errors, or slow throughput. In this scenario, the customer added a hub between the switch and the router. A hub is a device that operates at half-duplex and broadcasts all traffic to all ports. A switch and a router are devices that operate at full-duplex and forward traffic to specific ports. Therefore, adding a hub between the switch and the router can cause a duplex mismatch and slow down all the other network components that were connected to the switch.

References: <https://www.comparitech.com/net-admin/hub-vs-switch-vs-router/> <https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/10561-3.html>

NEW QUESTION 336

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

N10-009 Practice Exam Features:

- * N10-009 Questions and Answers Updated Frequently
- * N10-009 Practice Questions Verified by Expert Senior Certified Staff
- * N10-009 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * N10-009 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year