

CompTIA

Exam Questions N10-009

CompTIA Network+ Exam



NEW QUESTION 1

- (Exam Topic 1)

A company built a new building at its headquarters location. The new building is connected to the company's LAN via fiber-optic cable. Multiple users in the new building are unable to access the company's intranet site via their web browser, but they are able to access internet sites. Which of the following describes how the network administrator can resolve this issue?

- A. Correct the DNS server entries in the DHCP scope
- B. Correct the external firewall gateway address
- C. Correct the NTP server settings on the clients
- D. Correct a TFTP Issue on the company's server

Answer: A

Explanation:

If multiple users in a new building are unable to access the company's intranet site via their web browser but are able to access internet sites, the network administrator can resolve this issue by correcting the DNS server entries in the DHCP scope. The DHCP scope is responsible for assigning IP addresses and DNS server addresses to clients. If the DNS server entries are incorrect, clients will not be able to access intranet sites.

References:

➤ CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 4: Network Implementations, Objective 4.4: Explain the purpose and properties of DHCP.

NEW QUESTION 2

- (Exam Topic 1)

A technician is installing a high-density wireless network and wants to use an available frequency that supports the maximum number of channels to reduce interference. Which of the following standard 802.11 frequency ranges should the technician look for while reviewing WAP specifications?

- A. 2.4GHz
- B. 5GHz
- C. 6GHz
- D. 900MHz

Answer: B

Explanation:

* 802.11 a/b/g/n/ac wireless networks operate in two frequency ranges: 2.4 GHz and 5 GHz. The 5 GHz frequency range supports more channels than the 2.4 GHz frequency range, making it a better choice for high-density wireless networks.

References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 3

- (Exam Topic 1)

An engineer notices some late collisions on a half-duplex link. The engineer verifies that the devices on both ends of the connection are configured for half duplex. Which of the following is the MOST likely cause of this issue?

- A. The link is improperly terminated
- B. One of the devices is misconfigured
- C. The cable length is excessive
- D. One of the devices has a hardware issue

Answer: C

Explanation:

In a half-duplex link, devices can only send or receive data at one time, not simultaneously. Late collisions occur when devices transmit data at the same time after waiting for a clear channel. One of the causes of late collisions is excessive cable length, which increases the propagation delay and makes it harder for devices to detect collisions. The link termination, device configuration, and device hardware are not likely to cause late collisions on a half-duplex link.

NEW QUESTION 4

- (Exam Topic 1)

Which of the following DNS records works as an alias to another record?

- A. AAAA
- B. CNAME
- C. MX
- D. SOA

Answer: B

Explanation:

The DNS record that works as an alias to another record is called CNAME (Canonical Name). CNAME records are used to create an alias for a domain name that points to another domain name.

References:

➤ CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a scenario, implement and configure the appropriate addressing schema.

NEW QUESTION 5

- (Exam Topic 1)

The management team needs to ensure unnecessary modifications to the corporate network are not permitted and version control is maintained. Which of the following documents would BEST support this?

- A. An incident response plan
- B. A business continuity plan
- C. A change management policy
- D. An acceptable use policy

Answer: C

Explanation:

A change management policy is a document that outlines the procedures and guidelines for making changes to a network or system, including how changes are approved, tested, and implemented. By following a change management policy, organizations can ensure that unnecessary modifications to the network are not permitted and version control is maintained. References:

➤ Network+ N10-008 Objectives: 1.6 Given a scenario, implement network configuration and change management best practices.

NEW QUESTION 6

- (Exam Topic 1)

A technician is writing documentation regarding a company's server farm. The technician needs to confirm the server name for all Linux servers. Which of the following commands should the technician run?

- A. ipconfig
- B. nslookup
- C. arp
- D. route

Answer: B

Explanation:

The nslookup command should be run to confirm the server name for all Linux servers. Nslookup is a tool that queries DNS servers to resolve hostnames to IP addresses or vice versa. It can also provide other information about DNS records, such as MX, NS, SOA, etc. By running nslookup with the IP address of a Linux server, the technician can obtain its hostname. References:

<https://www.howtogeek.com/663056/how-to-use-the-nslookup-command-on-linux/>

NEW QUESTION 7

- (Exam Topic 1)

A technician is troubleshooting a wireless connectivity issue in a small office located in a high-rise building. Several APs are mounted in this office. The users report that the network connections frequently disconnect and reconnect throughout the day. Which of the following is the MOST likely cause of this issue?

- A. The AP association time is set too low
- B. EIRP needs to be boosted
- C. Channel overlap is occurring
- D. The RSSI is misreported

Answer: C

Explanation:

Channel overlap is a common cause of wireless connectivity issues, especially in high-density environments where multiple APs are operating on the same or adjacent frequencies. Channel overlap can cause interference, signal degradation, and performance loss for wireless devices. The AP association time, EIRP, and RSSI are not likely to cause frequent disconnects and reconnects for wireless users.

NEW QUESTION 8

- (Exam Topic 1)

Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

- A. Layer 3 switch
- B. VPN headend
- C. Next-generation firewall
- D. Proxy server
- E. Intrusion prevention

Answer: C

Explanation:

Next-generation firewalls can provide content filtering and threat protection, and can manage multiple IPSec site-to-site connections. References: CompTIA Network+ Certification Study Guide, Chapter 5: Network Security.

NEW QUESTION 9

- (Exam Topic 1)

A user tries to ping 192.168.1.100 from the command prompt on the 192.168.2.101 network but gets the following response: U.U.U.U. Which of the following needs to be configured for these networks to reach each other?

- A. Network address translation
- B. Default gateway
- C. Loopback
- D. Routing protocol

Answer: B

Explanation:

A default gateway is a device that routes traffic from one network to another network, such as the Internet. A default gateway is usually configured on each host device to specify the IP address of the router that connects the host's network to other networks. In this case, the user's device and the destination device are on different networks (192.168.1.0/24 and 192.168.2.0/24), so the user needs to configure a default gateway on their device to reach the destination device.

References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.techopedia.com/definition/25761/default-gateway>

NEW QUESTION 10

- (Exam Topic 1)

Which of the following is used to track and document various types of known vulnerabilities?

- A. CVE
- B. Penetration testing
- C. Zero-day
- D. SIEM
- E. Least privilege

Answer: A

Explanation:

CVE stands for Common Vulnerabilities and Exposures, which is a list of publicly disclosed cybersecurity vulnerabilities that is free to search, use, and incorporate into products and services. CVE provides a standardized identifier and description for each vulnerability, as well as references to related sources of information.

CVE helps to track and document various types of known vulnerabilities and facilitates communication and coordination among security professionals. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://cve.mitre.org/cve/>

NEW QUESTION 10

- (Exam Topic 1)

A network administrator is implementing OSPF on all of a company's network devices. Which of the following will MOST likely replace all the company's hubs?

- A. A Layer 3 switch
- B. A proxy server
- C. A NGFW
- D. A WLAN controller

Answer: A

Explanation:

A Layer 3 switch will likely replace all the company's hubs when implementing OSPF on all of its network devices. A Layer 3 switch combines the functionality of a traditional Layer 2 switch with the routing capabilities of a router. By implementing OSPF on a Layer 3 switch, an organization can improve network performance and reduce the risk of network congestion. References: Network+ Certification Study Guide, Chapter 5: Network Security

NEW QUESTION 12

- (Exam Topic 1)

According to troubleshooting methodology, which of the following should the technician do NEXT after determining the most likely probable cause of an issue?

- A. Establish a plan of action to resolve the issue and identify potential effects
- B. Verify full system functionality and, if applicable, implement preventive measures
- C. Implement the solution or escalate as necessary
- D. Test the theory to determine the cause

Answer: A

Explanation:

According to troubleshooting methodology, after determining the most likely probable cause of an issue, the next step is to establish a plan of action to resolve the issue and identify potential effects. This step involves defining the steps needed to implement a solution, considering the possible consequences of each step, and obtaining approval from relevant stakeholders if necessary. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.comptia.org/blog/the-comptia-guide-to-it-troubleshooting>

NEW QUESTION 13

- (Exam Topic 1)

A network is experiencing a number of CRC errors during normal network communication. At which of the following layers of the OSI model will the administrator MOST likely start to troubleshoot?

- A. Layer 1
- B. Layer 2
- C. Layer 3
- D. Layer 4
- E. Layer 5
- F. Layer 6
- G. Layer 7

Answer: A

Explanation:

CRC errors are cyclic redundancy check errors that occur when data is corrupted during transmission. CRC errors are usually caused by physical layer issues such as faulty cables, connectors, ports, or interference. The network administrator will most likely start to troubleshoot at layer 1 of the OSI model, which is the physical layer that deals with the transmission of bits over a medium. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 4.0 Network Troubleshooting and Tools, Objective 4.1 Given a scenario, implement network troubleshooting methodology.

NEW QUESTION 14

- (Exam Topic 1)

Which of the following is the physical topology for an Ethernet LAN?

- A. Bus
- B. Ring
- C. Mesh
- D. Star

Answer: D

Explanation:

In a star topology, all devices on a network connect to a central hub or switch, which acts as a common connection point. Ethernet LANs typically use a star topology, with each device connected to a central switch. References:

➤ Network+ N10-008 Objectives: 2.2 Explain common logical network topologies and their characteristics.

NEW QUESTION 16

- (Exam Topic 1)

A network administrator walks into a datacenter and notices an unknown person is following closely. The administrator stops and directs the person to the security desk. Which of the following attacks did the network administrator prevent?

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

Answer: B

Explanation:

:

Tailgating is a physical security attack where an unauthorized person follows an authorized person into a restricted area without proper identification or authorization. The network administrator prevented this attack by stopping and directing the person to the security desk. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 3.0 Network Security, Objective 3.1 Compare and contrast risk-related concepts.

NEW QUESTION 21

- (Exam Topic 1)

A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

- A. OTDR
- B. Tone generator
- C. Fusion splicer
- D. Cable tester
- E. PoE injector

Answer: A

Explanation:

To detect the exact break point of a fiber link, an engineer should use an OTDR (Optical Time Domain Reflectometer). This device sends a series of pulses into the fiber, measuring the time it takes for the pulses to reflect back, and can pinpoint the exact location of the break.

References:

➤ Network+ N10-007 Certification Exam Objectives, Objective 2.5: Given a scenario, troubleshoot copper cable issues.

➤ FS: OTDR (Optical Time Domain Reflectometer) Testing Principle and Applications

NEW QUESTION 26

- (Exam Topic 1)

Which of the following BEST describes a network appliance that warns of unapproved devices that are accessing the network?

- A. Firewall
- B. AP
- C. Proxy server
- D. IDS

Answer: D

Explanation:

IDS stands for intrusion detection system, which is a network appliance that monitors network traffic and alerts administrators of any suspicious or malicious activity. An IDS can warn of unapproved devices that are accessing the network by detecting anomalies, signatures, or behaviors that indicate unauthorized access attempts or attacks. References:

[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.cisco.com/c/en/us/products/security/what-is-an-intrusion-detection-system-ids.html>

NEW QUESTION 27

- (Exam Topic 1)

A network engineer configured new firewalls with the correct configuration to be deployed to each remote branch. Unneeded services were disabled, and all firewall rules were applied successfully. Which of the following should the network engineer perform NEXT to ensure all the firewalls are hardened successfully?

- A. Ensure an implicit permit rule is enabled

- B. Configure the log settings on the firewalls to the central syslog server
- C. Update the firewalls with current firmware and software
- D. Use the same complex passwords on all firewalls

Answer: C

Explanation:

Updating the firewalls with current firmware and software is an important step to ensure all the firewalls are hardened successfully, as it can fix any known vulnerabilities or bugs and provide new features or enhancements. Enabling an implicit permit rule is not a good practice for firewall hardening, as it can allow unwanted traffic to pass through the firewall. Configuring the log settings on the firewalls to the central syslog server is a good practice for monitoring and auditing purposes, but it does not harden the firewalls themselves. Using the same complex passwords on all firewalls is not a good practice for password security, as it can increase the risk of compromise if one firewall is breached. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 3.0 Network Security, Objective 3.3 Given a scenario, implement network hardening techniques.

NEW QUESTION 29

- (Exam Topic 1)

A network administrator redesigned the positioning of the APs to create adjacent areas of wireless coverage. After project validation, some users still report poor connectivity when their devices maintain an association to a distanced AP. Which of the following should the network administrator check FIRST?

- A. Validate the roaming settings on the APs and WLAN clients
- B. Verify that the AP antenna type is correct for the new layout
- C. Check to see if MU-MIMO was properly activated on the APs
- D. Deactivate the 2.4GHz band on the APS

Answer: A

Explanation:

The network administrator should check the roaming settings on the APs and WLAN clients first. Roaming is the process of switching from one AP to another without losing connectivity. If the roaming settings are not configured properly, some users may experience poor connectivity when their devices stay connected to a distant AP instead of switching to a closer one. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-roam-faq.html>

NEW QUESTION 30

- (Exam Topic 1)

Which of the following would MOST likely be used to review previous upgrades to a system?

- A. Business continuity plan
- B. Change management
- C. System life cycle
- D. Standard operating procedures

Answer: B

Explanation:

Change management is the process of reviewing previous upgrades to a system. It is a systematic approach to managing changes to an organization's IT systems and infrastructure. Change management involves the assessment of potential risks associated with a change, as well as the identification of any necessary resources required to implement the change. References: Network+ Certification Study Guide, Chapter 8: Network Troubleshooting

NEW QUESTION 35

- (Exam Topic 1)

The following configuration is applied to a DHCP server connected to a VPN concentrator:

```
IP address:      10.0.0.1
Subnet mask:     255.255.255.0
Gateway:        10.0.0.254
```

There are 300 non-concurrent sales representatives who log in for one hour a day to upload reports, and 252 of these representatives are able to connect to the VPN without any issues. The remaining sales representatives cannot connect to the VPN over the course of the day. Which of the following can be done to resolve the issue without utilizing additional resources?

- A. Decrease the lease duration
- B. Reboot the DHCP server
- C. Install a new VPN concentrator
- D. Configure a new router

Answer: A

Explanation:

Decreasing the lease duration on the DHCP server will cause clients to renew their IP address leases more frequently, freeing up IP addresses for other clients to use. References: CompTIA Network+ Certification Study Guide, Chapter 3: IP Addressing.

NEW QUESTION 39

- (Exam Topic 2)

A network engineer is designing a new secure wireless network. The engineer has been given the following requirements:

- * 1 Must not use plaintext passwords
- * 2 Must be certificate based
- * 3. Must be vendor neutral

Which of the following methods should the engineer select?

- A. TWP-RC4

- B. CCMP-AES
- C. EAP-TLS
- D. WPA2

Answer: C

Explanation:

EAP-TLS is the method that should be selected to meet the requirements for designing a new secure wireless network. EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) is an authentication protocol that uses X.509 digital certificates for both clients and servers. It provides strong security and mutual authentication by using TLS encryption and public key cryptography. It does not use plaintext passwords or shared secrets that can be compromised or guessed. It is also an open standard that is vendor neutral and supported by most wireless devices¹. References: <https://www.securew2.com/blog/what-is-eap-tls>
1

NEW QUESTION 41

- (Exam Topic 2)

A network technician is observing the behavior of an unmanaged switch when a new device is added to the network and transmits data. Which of the following BEST describes how the switch processes this information?

- A. The data is flooded out of every port
- B. including the one on which it came in.
- C. The data is flooded out of every port but only in the VLAN where it is located.
- D. The data is flooded out of every port, except the one on which it came in
- E. The data is flooded out of every port, excluding the VLAN where it is located

Answer: C

Explanation:

The switch processes the data by flooding it out of every port, except the one on which it came in. Flooding is a process where a switch sends a data frame to all ports except the source port when it does not have an entry for the destination MAC address in its MAC address table. Flooding allows the switch to learn the MAC addresses of the devices connected to its ports and update its MAC address table accordingly. Flooding also ensures that the data frame reaches its intended destination, even if the switch does not know its location. References: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10556-16.html>

NEW QUESTION 42

- (Exam Topic 2)

A network administrator is downloading a large patch that will be uploaded to several enterprise switches simultaneously during the day's upgrade cycle. Which of the following should the administrator do to help ensure the upgrade process will be less likely to cause problems with the switches?

- A. Confirm the patch's MD5 hash prior to the upgrade
- B. Schedule the switches to reboot after an appropriate amount of time.
- C. Download each switch's current configuration before the upgrade
- D. Utilize FTP rather than TFTP to upload the patch

Answer: A

Explanation:

The network administrator should confirm the patch's MD5 hash prior to the upgrade to help ensure the upgrade process will be less likely to cause problems with the switches. MD5 (Message Digest 5) is a cryptographic hash function that produces a 128-bit hash value for any given input. It can be used to verify the integrity and authenticity of a file by comparing its hash value with a known or expected value. If the hash values match, it means that the file has not been corrupted or tampered with during transmission or storage. If the hash values do not match, it means that the file may be damaged or malicious and should not be used for the upgrade. References: <https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/15292-scp.html>

NEW QUESTION 44

- (Exam Topic 2)

A lab environment hosts Internet-facing web servers and other experimental machines, which technicians use for various tasks A technician installs software on one of the web servers to allow communication to the company's file server, but it is unable to connect to it Other machines in the building are able to retrieve files from the file server. Which of the following is the MOST likely reason the web server cannot retrieve the files, and what should be done to resolve the problem?

- A. The lab environment's IDS is blocking the network traffic 1 he technician can whitelist the new application in the IDS
- B. The lab environment is located in the DMZ, and traffic to the LAN zone is denied by default
- C. The technician can move the computer to another zone or request an exception from the administrator.
- D. The lab environment has lost connectivity to the company router, and the switch needs to be rebooted.The technician can get the key to the wiring closet and manually restart the switch
- E. The lab environment is currently set up with hubs instead of switches, and the requests are getting bounced back The technician can submit a request for upgraded equipment to management.

Answer: B

Explanation:

The lab environment is located in the DMZ, and traffic to the LAN zone is denied by default. This is the most likely reason why the web server cannot retrieve files from the file server, and the technician can either move the computer to another zone or request an exception from the administrator to resolve the problem. A DMZ (Demilitarized Zone) is a network segment that separates the internal network (LAN) from the external network (Internet). It usually hosts public-facing servers such as web servers, email servers, or FTP servers that need to be accessed by both internal and external users. A firewall is used to control the traffic between the DMZ and the LAN zones, and usually denies traffic from the DMZ to the LAN by default for security reasons. Therefore, if a web server in the DMZ needs to communicate with a file server in the LAN, it would need a special rule or permission from the firewall administrator. References: <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

NEW QUESTION 46

- (Exam Topic 2)

A network technician is investigating an IP phone that does not register in the VoIP system. Although it received an IP address, it did not receive the necessary DHCP options. The information that is needed for the registration is distributed by the DHCP scope. All other IP phones are working properly. Which of the following does the technician need to verify?

- A. VLAN mismatch
- B. Transceiver mismatch
- C. Latency
- D. DHCP exhaustion

Answer: A

Explanation:

A VLAN mismatch is the most likely reason why an IP phone does not receive the necessary DHCP options for registration. A VLAN mismatch occurs when a device is connected to a switch port that belongs to a different VLAN than the device's intended VLAN. This can cause communication problems or prevent access to network resources. For example, if an IP phone is connected to a switch port that belongs to the data VLAN instead of the voice VLAN, it may not receive the DHCP options that contain information such as the TFTP server address, the NTP server address, or the default gateway address for the voice VLAN. These DHCP options are essential for the IP phone to register with the VoIP system and function properly. References: <https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-c>

NEW QUESTION 47

- (Exam Topic 2)

Which of the following policies is MOST commonly used for guest captive portals?

- A. AUP
- B. DLP
- C. BYOD
- D. NDA

Answer: A

Explanation:

AUP stands for Acceptable Use Policy, which is a policy that defines the rules and guidelines for using a network or service. A guest captive portal is a web page that requires users to agree to the AUP before accessing the Internet or other network resources. This is a common way to enforce security and legal compliance for guest users. References:

https://www.arubanetworks.com/techdocs/Instant_87_WebHelp/Content/instant-ug/captive-portal/captive-portal

NEW QUESTION 51

- (Exam Topic 2)

Which of the following is MOST commonly used to address CVEs on network equipment and/or operating systems?

- A. Vulnerability assessment
- B. Factory reset
- C. Firmware update
- D. Screened subnet

Answer: C

Explanation:

Firmware is a type of software that controls the low-level functions of a hardware device, such as a router, switch, printer, or camera. Firmware updates are patches or upgrades that fix bugs, improve performance, add features, or address security vulnerabilities in firmware. Firmware updates are commonly used to address CVEs (Common Vulnerabilities and Exposures) on network equipment and operating systems, as CVEs are publicly known flaws that can be exploited by attackers. References:

<https://www.comptia.org/blog/what-is-firmware>

NEW QUESTION 54

- (Exam Topic 2)

A city has hired a new employee who needs to be able to work when traveling at home and at the municipal sourcing of a neighboring city that snares services. The employee is issued a laptop, and a technician needs to train the employee on the appropriate solutions for secure access to the network from all the possible locations. On which of the following solutions would the technician MOST likely train the employee?

- A. Site-to-site VPNs between the two city locations and client-to-site software on the employee's laptop for all other remote access
- B. Client-to-site VPNs between the travel locations and site-to-site software on the employee's laptop for all other remote access
- C. Client-to-site VPNs between the two city locations and site-to-site software on the employee's laptop for all other remote access
- D. Site-to-site VPNs between the home and city locations and site-to-site software on the employee's laptop for all other remote access

Answer: A

Explanation:

The technician would most likely train the employee on using site-to-site VPNs between the two city locations and client-to-site software on the employee's laptop for all other remote access. A VPN (Virtual Private Network) is a technology that creates a secure and encrypted tunnel over a public network such as the Internet. It allows remote users or sites to access a private network as if they were directly connected to it. A site-to-site VPN connects two or more networks, such as branch offices or data centers, using a VPN gateway device at each site. A client-to-site VPN connects individual users, such as mobile workers or telecommuters, using a VPN client software on their devices. In this scenario, the employee needs to access the network from different locations, such as home, travel, or another city. Therefore, the technician would train the employee on how to use site-to-site VPNs to connect to the network from another city location that shares services, and how to use client-to-site software to connect to the network from home or travel locations. References: <https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-work>

NEW QUESTION 58

- (Exam Topic 2)

Which of the following would be used to expedite MX record updates to authoritative NSs?

- A. UDP forwarding
- B. DNS caching
- C. Recursive lookup
- D. Time to live

Answer: D

Explanation:

Time to live (TTL) is a value that indicates how long a DNS record can be cached by authoritative NSs (name servers) or other DNS servers before it expires and needs to be updated. A lower TTL value would expedite MX record updates to authoritative NSs, as they would refresh the record more frequently. UDP forwarding is not a DNS term, but a technique of sending UDP packets from one host to another. DNS caching is the process of storing DNS records locally for faster resolution, which does not expedite MX record updates. Recursive lookup is a type of DNS query where a DNS server queries other DNS servers on behalf of a client until it finds the answer, which does not expedite MX record updates.

NEW QUESTION 63

- (Exam Topic 3)

A technician is consolidating a topology with multiple SSIDs into one unique SSID deployment. Which of the following features will be possible after this new configuration?

- A. Seamless roaming
- B. Basic service set
- C. WPA
- D. MU-MIMO

Answer: A

NEW QUESTION 67

- (Exam Topic 3)

A company needs a redundant link to provide a channel to the management network in an incident response scenario. Which of the following remote access methods provides the BEST solution?

- A. Out-of-band access
- B. Split-tunnel connections
- C. Virtual network computing
- D. Remote desktop gateways

Answer: A

Explanation:

Out-of-band access is a remote access method that provides a separate, independent channel for accessing network devices and systems. Out-of-band access uses a dedicated network connection or a separate communication channel, such as a dial-up or cellular connection, to provide access to network devices and systems. This allows an administrator to access the management network even if the primary network connection is unavailable or impaired. Out-of-band access is a good solution for providing a redundant link to the management network in an incident response scenario because it can be used to access the network even if the primary connection is unavailable or impaired.

NEW QUESTION 70

- (Exam Topic 3)

Several employees have expressed concerns about the company monitoring their internet activity when they are working from home. The company wants to mitigate this issue and reassure employees that their private internet activity is not being monitored. Which of the following would satisfy company and employee needs?

- A. Split tunnel
- B. Full tunnel
- C. Site-to-site tunnel
- D. Virtual desktop

Answer: A

Explanation:

Split tunnel is a configuration that allows a remote user to access both the local network and the Internet at the same time. In a split tunnel configuration, only traffic destined for the corporate network is sent through the VPN tunnel, while all other traffic is sent directly to the Internet. This allows the remote user to access the Internet without the company's VPN server being able to monitor or intercept their traffic. Using a split tunnel configuration can help the company to mitigate employee concerns about internet activity being monitored and reassure employees that their private internet activity is not being monitored.

NEW QUESTION 71

- (Exam Topic 3)

Which of the following would MOST likely utilize PoE?

- A. A camera
- B. A printer
- C. A hub
- D. A modem

Answer: A

Explanation:

A camera is most likely to utilize PoE (Power over Ethernet). PoE is a technology that allows electrical power to be delivered over Ethernet cables. It is used to power a variety of devices, such as cameras, phones, access points, and other networking equipment. Cameras are particularly well-suited for PoE because they are often installed in locations where it is difficult or impossible to run electrical power. By using PoE, cameras can be powered directly over the Ethernet cable, eliminating the need for separate power cables and outlets. Other devices, such as printers, hubs, and modems, are less likely to utilize PoE because they typically do not need to be powered over Ethernet. These devices are usually powered by AC (alternating current) power and are typically connected to a power outlet rather than an Ethernet cable.

NEW QUESTION 74

- (Exam Topic 3)

Which of the following is an example of on-demand scalable hardware that is typically housed in the vendor's data center?

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

Answer: B

NEW QUESTION 78

- (Exam Topic 3)

A systems operator is granted access to a monitoring application, configuration application, and timekeeping application. The operator is denied access to the financial and project management applications by the system's security configuration. Which of the following BEST describes the security principle in use?

- A. Network access control
- B. Least privilege
- C. Multifactor authentication
- D. Separation of duties

Answer: D

NEW QUESTION 81

- (Exam Topic 3)

Which of the following is the MOST cost-effective alternative that provides proper cabling and supports gigabit Ethernet devices?

- A. Twisted cable with a minimum Cat 5e certification
- B. Multimode fiber with an SC connector
- C. Twinaxial cabling using an F-type connector
- D. Cable termination using TIA/EIA-568-B

Answer: A

Explanation:

twisted cable with a minimum Cat 5e certification is the MOST cost-effective alternative that provides proper cabling and supports gigabit Ethernet devices.

NEW QUESTION 83

- (Exam Topic 3)

A company with multiple routers would like to implement an HA network gateway with the least amount of downtime possible. This solution should not require changes on the gateway setting of the network clients. Which of the following should a technician configure?

- A. Automate a continuous backup and restore process of the system's state of the active gateway.
- B. Use a static assignment of the gateway IP address on the network clients.
- C. Configure DHCP relay and allow clients to receive a new IP setting.
- D. Configure a shared VIP and deploy VRRP on the routers.

Answer: D

Explanation:

The open standard protocol Virtual Router Redundancy Protocol (VRRP) is similar to HSRP, the differences mainly being in terminology and packet formats. In VRRP, the active router is known as the master, and all other routers in the group are known as backup routers. There is no specific standby router; instead, all backup routers monitor the status of the master, and in the event of a failure, a new master router is selected from the available backup routers based on priority.

NEW QUESTION 85

- (Exam Topic 3)

Which of the following would be the MOST cost-effective recovery solution for a company's lower-priority applications?

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

Answer: C

NEW QUESTION 89

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 93

- (Exam Topic 3)

When accessing corporate network resources, users are required to authenticate to each application they try to access. Which of the following concepts does this BEST represent?

- A. SSO
- B. Zero Trust
- C. VPN
- D. Role-based access control

Answer: B

NEW QUESTION 96

- (Exam Topic 3)

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

- A. 10GBASE-SW
- B. 10GBASE-LR
- C. 10GBASE-LX4 over multimode fiber
- D. 10GBASE-SR

Answer: B

Explanation:

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

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

NEW QUESTION 98

- (Exam Topic 3)

A security administrator is trying to prevent incorrect IP addresses from being assigned to clients on the network. Which of the following would MOST likely prevent this and allow the network to continue to operate?

- A. Configuring DHCP snooping on the switch
- B. Preventing broadcast messages leaving the client network
- C. Blocking ports 67/68 on the client network
- D. Enabling port security on access ports

Answer: A

Explanation:

To prevent incorrect IP addresses from being assigned to clients on the network and allow the network to continue to operate, the security administrator should consider configuring DHCP (Dynamic Host Configuration Protocol) snooping on the switch. DHCP snooping is a security feature that is used to prevent unauthorized DHCP servers from operating on a network. It works by allowing the switch to monitor and validate DHCP traffic on the network, ensuring that only legitimate DHCP messages are forwarded to clients. This can help to prevent incorrect IP addresses from being assigned to clients, as it ensures that only authorized DHCP servers are able to provide IP addresses to clients on the network.

NEW QUESTION 99

- (Exam Topic 3)

A technician discovered that some information on the local database server was changed during a file transfer to a remote server. Which of the following should concern the technician the MOST?

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

Answer: B

Explanation:

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

NEW QUESTION 100

- (Exam Topic 3)

Which of the following is used to provide disaster recovery capabilities to spin up an critical devices using internet resources?

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

Answer: A

NEW QUESTION 102

- (Exam 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 103

- (Exam Topic 3)

A company is undergoing expansion but does not have sufficient rack space in its data center. Which of the following would be BEST to allow the company to host its new equipment without a major investment in facilities?

- A. Using a colocation service
- B. Using available rack space in branch offices
- C. Using a flat network topology
- D. Reorganizing the network rack and installing top-of-rack switching

Answer: A

Explanation:

A colocation service is a service that provides rack space, power, cooling, security, and connectivity for a company's network equipment in a data center. A colocation service can be used when a company does not have sufficient rack space in its own data center and does not want to invest in building or expanding its own facilities. By using a colocation service, a company can host its new equipment in a professional and reliable environment without a major investment in facilities. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 414)

NEW QUESTION 106

- (Exam Topic 3)

A Wi-Fi network was originally configured to be able to handle interference from a microwave oven. The microwave oven was recently removed from the office. Now the network administrator wants to optimize the system to maximize the range of the signal. The main sources of signal degradation are the numerous cubicles and wooden walls between the WAP and the intended destination. Which of the following actions should the administrator take?

- A. Implement CDMA.
- B. Change from omni to directional.
- C. Change the SSID.
- D. Change the frequency.

Answer: D

Explanation:

- the microwave was already removed from the office
- the signal is OK now
- Notice that the question mentions "numerous cubicles and wooden walls" - meaning the signal now won't have the interference as before
- KEY POINT: the admin wants to "maximize the range of the signal:"

Manually change the frequency to 2.4 GHz for more reliable speeds and range. While 5 GHz gives you a stronger signal, it doesn't travel through walls or ceilings as well, so it doesn't give you the best range.

"Microwave ovens: Older microwave ovens, which might not have sufficient shielding, can emit relatively high-powered signals in the 2.4GHz band, resulting in significant interference with WLAN devices operating in the 2.4GHz band."

NEW QUESTION 108

- (Exam Topic 3)

A company wants to add a local redundant data center to its network in case of failure at its primary location. Which of the following would give the LEAST amount of redundancy for the company's network?

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

Answer: A

NEW QUESTION 113

- (Exam Topic 3)

A large metropolitan city is looking to standardize the ability for police department laptops to connect to the city government's VPN. The city would like a wireless solution that provides the largest coverage across the city with a minimal number of transmission towers. Latency and overall bandwidth needs are not high priorities. Which of the following would BEST meet the city's needs?

- A. 5G
- B. LTE
- C. Wi-Fi 4
- D. Wi-Fi 5
- E. Wi-Fi 6

Answer: B

NEW QUESTION 118

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 119

- (Exam Topic 3)

Which of the following is considered a physical security detection device?

- A. Cameras
- B. Biometric readers
- C. Access control vestibules
- D. Locking racks

Answer: A

NEW QUESTION 122

- (Exam Topic 3)

A network administrator wants to test the throughput of a new metro Ethernet circuit to verify that its performance matches the requirements specified in the SLA. Which of the following would BEST help measure the throughput?

- A. iPerf
- B. Ping
- C. NetFlow
- D. Netstat

Answer: A

NEW QUESTION 127

- (Exam Topic 3)

An administrator would like to allow Windows clients from outside the office to access workstations without using third-party software. Which of the following access methods would meet this requirement?

- A. Remote desktop gateway
- B. Split tunnel
- C. Site-to-site VPN
- D. VNC

Answer: A

Explanation:

To allow Windows clients from outside the office to access workstations without using third-party software, the administrator can use the Remote Desktop Protocol (RDP). RDP is a built-in feature of the Windows operating system that allows users to remotely connect to and control other Windows computers over a network connection.

To use RDP, the administrator will need to enable the Remote Desktop feature on the workstations that need to be accessed, and ensure that the appropriate firewall rules are in place to allow RDP traffic to pass through. The administrator will also need to provide the remote users with the necessary credentials to access the workstations.

Once RDP is set up and configured, the remote users can use the Remote Desktop client on their own computers to connect to the workstations and access them as if they were physically present in the office. This allows the administrator to provide remote access to the workstations without the need for any additional software or third-party tools.

NEW QUESTION 132

- (Exam Topic 3)

Which of the following BEST describes a split-tunnel client-to-server VPN connection?

- A. The client sends all network traffic down the VPN tunnel
- B. The client has two different IP addresses that can be connected to a remote site from two different ISPs to ensure availability
- C. The client sends some network traffic down the VPN tunnel and other traffic to the local gateway.
- D. The client connects to multiple remote sites at the same time

Answer: C

Explanation:

In a split-tunnel VPN, the client can access both the local network and the remote network simultaneously, with some network traffic sent through the VPN tunnel and other traffic sent to the local gateway. This approach allows for more efficient use of bandwidth and reduces the load on the VPN server. It also allows the client to continue accessing local resources while connected to the remote network.

NEW QUESTION 136

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 137

- (Exam Topic 3)

A network administrator is implementing process changes based on recommendations following a recent penetration test. The testers used a method to gain access to the network that involved exploiting a publicly available and fixed remote code execution vulnerability in the VPN appliance. Which of the following should the administrator do to BEST prevent this from happening again?

- A. Change default passwords on internet-facing hardware.
- B. Implement robust ACLs with explicit deny-all entries.
- C. Create private VLANs for management plane traffic.
- D. Routinely upgrade all network equipment firmware.

Answer: D

Explanation:

Firmware is the software that runs on network equipment such as routers, switches, and VPN appliances. Firmware updates often contain bug fixes, security patches, and performance improvements that can prevent or mitigate vulnerabilities and attacks. By routinely upgrading all network equipment firmware, a network administrator can ensure that the network devices are running the latest and most secure versions of firmware and avoid exploiting known and fixed remote code execution vulnerabilities in the VPN appliance. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 462)

NEW QUESTION 140

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 142

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 146

- (Exam Topic 3)

A network administrator is setting up a new phone system and needs to define the location where VoIP phones can download configuration files. Which of the following DHCP services can be used to accomplish this task?

- A. Scope options
- B. Exclusion ranges
- C. Lease time
- D. Relay

Answer: A

Explanation:

To define the location where VoIP phones can download configuration files, the network administrator can use scope options within the Dynamic Host Configuration Protocol (DHCP) service. Scope options are a set of values that can be configured within a DHCP scope, which defines a range of IP addresses that can be leased to clients on a network. One of the scope options that can be configured is the option for the location of the configuration file server, which specifies the URL or IP address of the server where the configuration files can be downloaded.

<https://pbxbook.com/voip/dhcpcfg.html>

NEW QUESTION 151

- (Exam Topic 3)

An engineer needs to verify the external record for SMTP traffic. The engineer logged in to the server and entered the nslookup command. Which of the following commands should the engineer send before entering the DNS name?

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

Answer: D

NEW QUESTION 156

- (Exam Topic 3)

An IT technician installs five old switches in a network. In addition to the low port rates on these switches, they also have improper network configurations. After three hours, the network becomes overwhelmed by continuous traffic and eventually shuts down. Which Of the following is causing the issue?

- A. Broadcast storm
- B. Collisions
- C. IP settings
- D. Routing loops

Answer: A

Explanation:

A broadcast storm is a situation where a network is flooded with broadcast packets, which are sent to all devices on the network. This can consume bandwidth, cause congestion, and degrade performance. A broadcast storm can be caused by improper network configurations, such as loops or misconfigured switches. In this scenario, the old switches may have created loops or failed to filter broadcast packets, resulting in a broadcast storm that overwhelmed the network.

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 157

- (Exam 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 161

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 162

- (Exam Topic 3)

A company, which is located in a coastal town, retrofitted an office building for a new data center. The underground fiber optics were brought in and connected to the switches in the basement network MDF. A server data center was built on the fifth floor with the two rooms vertically connected by fiber optics. Which of the following types of environmental sensors is MOST needed?

- A. Temperature sensor in the network MDF
- B. Water sensor in the network MDF
- C. Temperature sensor in the data center
- D. Water sensor in the data center

Answer: B

Explanation:

A water sensor is a type of environmental sensor that detects the presence of water or moisture in an area. A water sensor is most needed in a network main distribution frame (MDF) that is located in a basement near underground fiber-optic cables. A network MDF is a central point where all the network connections converge and where network equipment such as switches and routers are located. If water leaks into the basement and damages the fiber-optic cables or the network equipment, it can cause network outages, performance degradation, or data loss. A water sensor can alert the network administrator of any water intrusion and help prevent or minimize the damage. References:

<https://www.comptia.org/training/books/network-n10-008-study-guide> (page 446)

NEW QUESTION 163

- (Exam Topic 3)

A network engineer receives the following when connecting to a switch to configure a port:

```
telnet 10.1.200.1
Connecting to 10.1.200.1...Could not open connection to the host, on port 23: Connect failed.
```

Which of the following is the MOST likely cause for the failure?

- A. The network engineer is using the wrong protocol
- B. The network engineer does not have permission to configure the device
- C. SNMP has been secured with an ACL
- D. The switchport the engineer is trying to configure is down

Answer: D

NEW QUESTION 164

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 167

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5: Given a scenario, use remote access methods.

NEW QUESTION 171

- (Exam Topic 3)

A client who shares office space and an IT closet with another company recently reported connectivity issues throughout the network. Multiple third-party vendors regularly perform on-site maintenance in the shared IT closet. Which of the following security techniques would BEST secure the physical networking equipment?

- A. Disabling unneeded switchports
- B. Implementing role-based access
- C. Changing the default passwords
- D. Configuring an access control list

Answer: B

Explanation:

Role-based access is a security technique that assigns permissions and privileges to users or groups based on their roles or functions within an organization. Role-based access can help secure the physical networking equipment by limiting who can access, modify, or manage the devices in the shared IT closet. Only authorized personnel with a valid role and credentials should be able to access the networking equipment. Disabling unneeded switchports is a security technique that prevents unauthorized devices from connecting to the network by turning off unused ports on a switch. Changing the default passwords is a security technique that prevents unauthorized access to network devices by replacing the factory-set passwords with strong and unique ones. Configuring an access control list is a security technique that filters network traffic by allowing or denying packets based on criteria such as source and destination IP addresses, ports, or protocols. References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.2: Given a scenario, use appropriate network hardening techniques.

NEW QUESTION 174

- (Exam Topic 3)

Given the following Information:

Connection	Cable length	Cable type	Configuration
PC A to switch 1	394ft (120m)	Cat 5	Straight through
Switch 1 to switch 2	3.3ft (1m)	Cat 6	Crossover
Switch 2 to PC B	16ft (5m)	Cat 5	Straight through

Which of the following would cause performance degradation between PC A and PC B'?

- A. Attenuation
- B. Interference
- C. Decibel loss
- D. Incorrect pinout

Answer: D

NEW QUESTION 178

- (Exam Topic 3)

Which of the following issues are present with RIPv2? (Select TWO).

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

Answer: BC

Explanation:

The disadvantages of RIP (Routing Information Protocol) include the following.

---Outdated, insecure, and slow. This is your parents' protocol. It was a thing before the Web was born.

---The more well-known problem of the 15 hop limitation in which data must travel

---Convergence time is terrible for information propagation in a network

---Metrics. It determines the number of hops from source to destination, and gives no regard to other factors when determining the best path for data to travel

---Overhead. A good example would be routing tables. These are broadcast at half-minute intervals to other routers regardless of whether the data has changed or not. It's essentially like those old cartoons where the town guard in the walled city cries out, '10 o' the clock and all is well!'.
RIPv2 introduced more security and reduced broadcast traffic, which is relevant for some available answers here.

NEW QUESTION 180

- (Exam Topic 3)

Which of the following would be BEST suited for use at the access layer in a three-tier architecture system?

- A. Router
- B. Multilayer switch
- C. Layer 2 switch
- D. Access point

Answer: C

Explanation:

A layer 2 switch is a device that forwards traffic based on MAC addresses within a single network segment or VLAN. A layer 2 switch is best suited for use at the access layer in a three-tier architecture system. The access layer is the layer that connects end devices such as computers, printers, and phones to the network. A layer 2 switch can provide fast and efficient switching for end devices without adding complexity or overhead to the network. References: <https://www.comptia.org/training/books/network-n10-008-study-guide> (page 139)

NEW QUESTION 182

- (Exam Topic 3)

A company is utilizing multifactor authentication for data center access. Which of the following is the MOST effective security mechanism against physical intrusions due to stolen credentials?

- A. Biometrics security hardware
- B. Access card readers
- C. Access control vestibule
- D. Motion detection cameras

Answer: C

NEW QUESTION 186

- (Exam Topic 3)

Which of the following would be the MOST likely attack used to bypass an access control vestibule?

- A. Tailgating
- B. Phishing
- C. Evil twin
- D. Brute-force

Answer: A

Explanation:

Tailgating is when someone follows an authorized person into a restricted area without having the proper credentials. This is usually done by pretending to be with the authorized person, or by offering assistance. Tailgating is a social engineering attack and does not require any technical skill.

NEW QUESTION 189

- (Exam Topic 3)

Which of the following DHCP settings would be used to ensure a device gets the same IP address each time it is connected to the network?

- A. Scope options
- B. Reservation
- C. Exclusion
- D. Relay
- E. Pool

Answer: A

NEW QUESTION 194

- (Exam Topic 3)

Which of the following protocols uses Dijkstra's algorithm to calculate the LOWEST cost between routers?

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

Answer: B

Explanation:

OSPF stands for Open Shortest Path First and is a link-state routing protocol that uses Dijkstra's algorithm to calculate the lowest cost between routers. OSPF assigns a cost value to each link based on factors such as bandwidth, delay, or reliability, and builds a map of the network topology. OSPF then uses Dijkstra's algorithm to find the shortest path from each router to every other router in the network¹. RIP stands for Routing Information Protocol and is a distance-vector routing protocol that uses hop count as the metric to find the best path. BGP stands for Border Gateway Protocol and is a path-vector routing protocol that uses attributes such as AS path, local preference, or origin to select the best route. EIGRP stands for Enhanced Interior Gateway Routing Protocol and is a hybrid routing protocol that uses a composite metric based on bandwidth, delay, load, and reliability.

References: 1 Dijkstra's algorithm - Wikipedia (https://en.wikipedia.org/wiki/Dijkstra%27s_algorithm)

NEW QUESTION 196

- (Exam Topic 3)

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

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

Answer: B

Explanation:

Traffic policing is a mechanism that monitors the traffic in any network and enforces a bandwidth limit by discarding packets that exceed a certain rate¹. This can reduce congestion and ensure fair allocation of bandwidth among different applications or users. However, discarding packets can also affect the performance and quality of some applications, especially those that are sensitive to packet loss, such as voice or video.

Traffic shaping is a congestion control mechanism that delays packets that exceed a certain rate instead of discarding them¹. This can smooth out traffic bursts and avoid packet loss, but it also introduces latency and jitter. Traffic shaping can be beneficial for applications that can tolerate some delay but not packet loss, such as file transfers or streaming.

Traffic marking is a mechanism that assigns different priority levels to packets based on their type, source, destination, or other criteria². This can help to

differentiate between different classes of service and apply different policies or treatments to them. However, traffic marking does not enforce bandwidth limits by itself; it only provides information for other mechanisms to act upon.

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

NEW QUESTION 198

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 199

- (Exam Topic 3)

Several users with older devices are reporting intermittent connectivity while in an outdoor patio area. After some research, the network administrator determines that an outdoor WAP might help with the issue. However, the company does not want the signal to bleed into the building and cause interference. Which of the following should the network administrator perform to BEST resolve the issue?

- A. Disable the SSID broadcast on the WAP in the patio area.
- B. Install a WAP and enable 5GHz only within the patio area.
- C. Install a directional WAP in the direction of the patio.
- D. Install a repeater on the back wall of the patio area.

Answer: C

NEW QUESTION 201

- (Exam 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 204

- (Exam Topic 3)

A security engineer is installing a new IOS on the network. The engineer has asked a network administrator to ensure all traffic entering and leaving the router interface is available for the IDS. Which of the following should the network administrator do?

- A. Install a network tap for the IDS
- B. Configure ACLs to route traffic to the IDS.
- C. Install an additional NIC into the IDS
- D. Install a loopback adapter for the IDS.
- E. Add an additional route on the router for the IDS.

Answer: A

Explanation:

a network tap is a way of connecting an IDS out of band, which means it does not interfere with the normal network traffic. A network tap allows you to view a copy of the network traffic transmitted over the media being tapped.

NEW QUESTION 206

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

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

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

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

NEW QUESTION 208

- (Exam Topic 3)

A technician is tasked with setting up a mail server and a DNS server. The mail port should be secured and have the ability to transfer large files. Which of the following ports should be opened? (Select TWO).

- A. 22
- B. 53
- C. 110
- D. 389
- E. 995
- F. 3389

Answer: BE

Explanation:

Port 53 is used for DNS, which is a service that translates domain names into IP addresses. Port 995 is used for POP3S, which is a protocol for receiving email messages securely. POP3S supports large file transfers and encryption. Therefore, these two ports should be opened for the mail server and the DNS server project

NEW QUESTION 213

- (Exam 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 217

- (Exam Topic 3)

Which of the following records can be used to track the number of changes on a DNS zone?

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

Answer: A

Explanation:

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

NEW QUESTION 222

- (Exam Topic 3)

Which of the following protocols would enable a company to upgrade its internet connection by acquiring its own public IP prefixes and autonomous system number?

- A. EIGRP
- B. BGP
- C. IPv6
- D. MPLS

Answer: B

Explanation:

BGP is a routing protocol that is used to exchange routing information between different autonomous systems (ASes) on the internet. An autonomous system is a network or group of networks that is under the same administrative control and uses a common routing protocol. By acquiring its own public IP prefixes and autonomous system number, a company can use BGP to advertise these prefixes to other ASes and establish its own internet connection. This would enable the company to have more control over its internet connection and potentially improve its connectivity. EIGRP (Enhanced Interior Gateway Routing Protocol) is a routing protocol used within a single autonomous system, so it would not be used to establish a connection to the internet. IPv6 is a version of the Internet Protocol (IP) used to identify devices on a network. It is not a routing protocol and would not be used to establish an internet connection. MPLS (Multi-Protocol Label Switching) is a networking technology that is used to route packets between different networks. It is not a routing protocol and would not be used to establish an internet connection.

NEW QUESTION 227

- (Exam Topic 3)

A network administrator is investigating a network event that is causing all communication to stop. The network administrator is unable to use SSH to connect to the switch but is able to gain access using the serial console port. While monitoring port statistics, the administrator sees the following:

Total Rx (bps)	23,041,464	Total Tx (bps)	621,032
Unicast Rx (Pkts/sec)	102,465	Unicast Tx (Pkts/sec)	66
B/Mcast Rx (Pkts/sec)	21,456.465	B/Mcast Tx (Pkts/sec)	7
Utilization Rx	2.3%	Utilization Tx	0.06%

Which of the following is MOST likely causing the network outage?

- A. Duplicate IP address
- B. High collisions
- C. Asynchronous route
- D. Switch loop

Answer: B

NEW QUESTION 229

- (Exam Topic 3)

The following DHCP scope was configured for a new VLAN dedicated to a large deployment of 325 IoT sensors:

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

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

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

Answer: B

NEW QUESTION 230

- (Exam 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 231

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 236

- (Exam Topic 3)

A network technician is troubleshooting a new web server connectivity issue. The network technician discovers the following on the support ticket

- The server's IP address can be pinged from the client PCs,
- Access to the web resource works correctly when on the server's console.
- No clients can access the servers data via URL.

- The server does not have a firewall configured
- No ACLs are preventing connectivity from the client's network.
- All services on the server are operating normally, which was confirmed by the server team. Which of the following actions will resolve the issue?

- A. Reset port security on the switchport connecting the server.
- B. Adjust the web server's NTP settings to match the client settings.
- C. Configure A records for the web server.
- D. Install the correct MIB on the web server

Answer: C

Explanation:

The problem is likely related to DNS resolution, as the clients are able to ping the server's IP address but not access the web resource via URL. The other answers do not address this issue. Configuring A records for the web server will ensure that clients are able to access the web resource via its domain name.

NEW QUESTION 237

- (Exam Topic 3)

A network administrator is looking at switch features and is unsure whether to purchase a model with PoE. Which of the following devices that commonly utilize PoE should the administrator consider? (Select TWO)

- A. VoIP phones
- B. Cameras
- C. Printers
- D. Cable modems
- E. Laptops
- F. UPSs

Answer: AB

Explanation:

Power over Ethernet (PoE) is a technology that allows network-connected devices to receive power over the same Ethernet cables that are used for data transfer. PoE is commonly used to power devices such as VoIP phones and cameras, making it an ideal choice for network administrators looking for a cost-effective solution. PoE is not typically used for other devices such as printers, cable modems, laptops, and UPSs.

NEW QUESTION 240

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 243

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 246

- (Exam Topic 3)

At which of the following OSI model layers does a MAC filter list for a wireless infrastructure operate?

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

Answer: D

Explanation:

A MAC filter list is a security feature that allows or denies access to a wireless network based on the MAC address of the device. A MAC address is a unique identifier assigned to a network interface card (NIC) at the physical layer of the OSI model. However, MAC filtering operates at the data link layer of the OSI model, where MAC addresses are used to encapsulate and deliver data frames between devices on the same network segment.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.1: Given a scenario, install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

NEW QUESTION 251

- (Exam 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 256

- (Exam Topic 3)

Which of the following situations would require an engineer to configure subinterfaces?

- A. In a router-on-a-stick deployment with multiple VLANs
- B. In order to enable inter-VLAN routing on a multilayer switch
- C. When configuring VLAN trunk links between switches
- D. After connecting a router that does not support 802.1Q VLAN tags

Answer: A

Explanation:

A router-on-a-stick is a configuration that allows a single router interface to route traffic between multiple VLANs on a network. A router-on-a-stick requires sub-interfaces to be configured on the router interface, one for each VLAN. Each sub-interface is assigned a VLAN ID and an IP address that belongs to the corresponding VLAN subnet. The router interface is connected to a switch port that is configured as a trunk port, which allows traffic from multiple VLANs to pass through. The router then performs inter-VLAN routing by forwarding packets between the sub-interfaces based on their destination IP addresses.

Inter-VLAN routing is a process that allows devices on different VLANs to communicate with each other. Inter-VLAN routing can be performed by a router-on-a-stick configuration, as explained above, or by a multilayer switch that has routing capabilities. A multilayer switch does not require sub-interfaces to be configured for inter-VLAN routing; instead, it uses switch virtual interfaces (SVIs) that are associated with each VLAN. An SVI is a logical interface that represents a VLAN on a switch and has an IP address that belongs to the VLAN subnet. The switch then performs inter-VLAN routing by forwarding packets between the SVIs based on their destination IP addresses.

VLAN trunking is a method that allows traffic from multiple VLANs to be carried over a single link between switches or routers. VLAN trunking requires the use of a tagging protocol, such as 802.1Q, that adds a header to each frame that identifies its VLAN ID. VLAN trunking does not require sub-interfaces to be configured on the switches or routers; instead, it uses trunk ports that are configured to allow or deny traffic from specific VLANs. The switches or routers then forward packets between the trunk ports based on their VLAN IDs.

* 802.1 Q is a standard that defines how VLAN tagging and trunking are performed on Ethernet networks.

* 802.1Q adds a 4-byte header to each frame that contains a 12-bit field for the VLAN ID and a 3-bit field for the priority level. 802.1Q does not require sub-interfaces to be configured on the switches or routers; instead, it uses trunk ports that are configured to support 802.1Q tagging and untagging. The switches or routers then forward packets between the trunk ports based on their VLAN IDs and priority levels.

NEW QUESTION 261

- (Exam Topic 3)

A company joins a bank's financial network and establishes a connection to the clearinghouse servers in the range 192.168.124.0/27. An IT technician then realizes the range exists within the VM pool at the data center. Which of the following is the BEST way for the technician to connect to the bank's servers?

- A. NAT
- B. PAT
- C. CIDR
- D. SLAAC

Answer: A

NEW QUESTION 264

- (Exam 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 268

- (Exam Topic 3)

Which of the following attacks, if successful, would provide a malicious user who is connected to an isolated guest network access to the corporate network?

- A. VLAN hopping
- B. On-path attack
- C. IP spoofing
- D. Evil twin

Answer: A

Explanation:

The attack which, if successful, would provide a malicious user who is connected to an isolated guest network access to the corporate network is VLAN hopping. VLAN hopping is an attack technique which involves tricking a switch into sending traffic from one VLAN to another. This is done by sending specially crafted packets, which force the switch to send traffic from one VLAN to another, thus allowing the malicious user to gain access to the corporate network. VLAN hopping is an attack technique which involves tricking a switch into sending traffic from one VLAN to another. This is done by sending specially crafted packets, which force the switch to send traffic from one VLAN to another, thus allowing the malicious user to gain access to the corporate network. According to the CompTIA Network+ N10-008 Exam Guide VLAN hopping is a type of attack that is used to gain access to network resources that are not meant to be accessible by a user on a guest network.

NEW QUESTION 272

- (Exam Topic 3)

An administrator would like to have two servers at different geographical locations provide fault tolerance and high performance while appearing as one URL to users. Which of the following should the administrator implement?

- A. Load balancing
- B. Multipathing
- C. NIC teaming
- D. Warm site

Answer: A

Explanation:

Load balancing is a technique that can be used to provide fault tolerance and high performance while appearing as one URL to users. It is achieved by distributing the workload across multiple servers, which are usually located in different geographical locations. This allows for high performance and fault tolerance, as if one server fails, the other will take its place. Additionally, the multiple servers appear as one URL to the users, eliminating the need for the users to switch between servers.

NEW QUESTION 276

- (Exam Topic 3)

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

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

Answer: D

Explanation:

SSID stands for Service Set Identifier and is the name of a wireless network. A wireless access point (WAP) can support multiple SSIDs, which allows different wireless access through the same equipment. For example, the store owner can create one SSID for business equipment and another SSID for patron use, and assign different security settings and bandwidth limits for each SSID. MIMO stands for Multiple Input Multiple Output and is a technology that uses multiple antennas to improve wireless performance. TKIP stands for Temporal Key Integrity Protocol and is an encryption method for wireless networks. LTE stands for Long Term Evolution and is a cellular network technology.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.1: Given a scenario, install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

NEW QUESTION 277

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 281

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 284

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 287

- (Exam 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 290

- (Exam Topic 3)

A network administrator is investigating a performance issue on a dual-link connection—VPN and MPLS—to a partner network. The MPLS is the primary path, and the VPN is used as a backup. While communicating, the delay is measured at 18ms, which is higher than the 6ms expected when the MPLS link is operational but lower than the 30ms expected for the VPN connection. Which of the following will MOST likely point to the root cause of the issue?

- A. Checking the routing tables on both sides to ensure there is no asymmetric routing
- B. Checking on the partner network for a missing route pointing to the VPN connection
- C. Running iPerf on both sides to confirm the delay that is measured is accurate
- D. Checking for an incorrect VLAN assignment affecting the MPLS traffic

Answer: A

Explanation:

Asymmetric routing can occur when two routers have different paths for the same two hosts, resulting in increased latency and possible packet loss. According to the CompTIA Network+ Study Manual, "If the path from the source to the destination is not the same in both directions, the packets will take different routes and the latency can increase significantly." To confirm this, the network administrator should check the routing tables on both sides of the connection and ensure that the same path is used in both directions.

NEW QUESTION 294

- (Exam Topic 3)

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

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

Answer: E

NEW QUESTION 298

- (Exam 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 303

- (Exam Topic 3)

An organization set up its offices so that a desktop is connected to the network through a VoIP phone. The VoIP vendor requested that voice traffic be segmented separately from non-voice traffic. Which of the following would allow the organization to configure multiple devices with network isolation on a single switch port?

- A. Subinterfaces
- B. Link aggregation
- C. Load balancing
- D. Tunneling

Answer: A

NEW QUESTION 307

- (Exam 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 308

- (Exam Topic 3)

A network engineer is monitoring a fiber uplink to a remote office and notes the uplink has been operating at 100% capacity for a long duration. Which of the following performance metrics is MOST likely to be impacted with sustained link saturation?

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

Answer: A

Explanation:

When a fiber uplink is operating at 100% capacity for an extended period of time, it can cause sustained link saturation. This can impact the network's performance by increasing latency. Latency is the time it takes for a packet to travel from the source to its destination. When there is link saturation, packets may have to wait in a queue before being transmitted, which increases the time it takes for them to reach their destination. As a result, users may experience delays or timeouts when accessing network resources.

Other metrics such as jitter, speed, and bandwidth are also important, but they are not as directly impacted by sustained link saturation as latency.

NEW QUESTION 309

- (Exam Topic 3)

An engineer was asked to update an MX record for an upcoming project. Which of the following server types is MOST likely to be in scope for the project?

- A. Email
- B. Web
- C. File
- D. Database

Answer: A

Explanation:

An MX record is a type of DNS record that specifies the mail server responsible for accepting email messages on behalf of a domain name. Therefore, an engineer who needs to update an MX record is most likely working on an email server project

NEW QUESTION 310

- (Exam 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 315

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

N10-009 Practice Exam Features:

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

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