

Exam Questions N10-009

CompTIA Network+ Exam

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



NEW QUESTION 1

- (Exam Topic 1)

Which of the following TCP ports is used by the Windows OS for file sharing?

- A. 53
- B. 389
- C. 445
- D. 1433

Answer: C

Explanation:

TCP port 445 is used by the Windows OS for file sharing. It is also known as SMB (Server Message Block) or CIFS (Common Internet File System) and allows users to access files, printers, and other shared resources on a network. References:

<https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smb>

NEW QUESTION 2

- (Exam Topic 1)

An administrator is writing a script to periodically log the IPv6 and MAC addresses of all the devices on a network segment. Which of the following switch features will MOST likely be used to assist with this task?

- A. Spanning Tree Protocol
- B. Neighbor Discovery Protocol
- C. Link Aggregation Control Protocol
- D. Address Resolution Protocol

Answer: B

Explanation:

Short explanation

The switch feature that is most likely to be used to assist with logging IPv6 and MAC addresses of devices on a network segment is Neighbor Discovery Protocol (NDP). NDP is used by IPv6 to discover and maintain information about other nodes on the network, including their IPv6 and MAC addresses. By periodically querying NDP, the administrator can log this information for auditing purposes.

References:

➤ CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.1: Compare and contrast TCP and UDP ports, protocols, and their purposes.

NEW QUESTION 3

- (Exam Topic 1)

Branch users are experiencing issues with videoconferencing. Which of the following will the company MOST likely configure to improve performance for these applications?

- A. Link Aggregation Control Protocol
- B. Dynamic routing
- C. Quality of service
- D. Network load balancer
- E. Static IP addresses

Answer: C

Explanation:

To improve performance for videoconferencing, the company should configure Quality of Service (QoS). This technology allows for the prioritization of network traffic, ensuring that videoconferencing traffic is given higher priority and therefore better performance. Link Aggregation Control Protocol (LACP), Dynamic routing, Network load balancer, and Static IP addresses are not directly related to improving performance for videoconferencing.

References:

➤ Network+ N10-007 Certification Exam Objectives, Objective 2.6: Given a scenario, implement and configure the appropriate wireless security and implement the appropriate QoS concepts.

NEW QUESTION 4

- (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 5

- (Exam Topic 1)

Which of the following is used to prioritize Internet usage per application and per user on the network?

- A. Bandwidth management
- B. Load balance routing
- C. Border Gateway Protocol
- D. Administrative distance

Answer: A

Explanation:

Bandwidth management is used to prioritize Internet usage per application and per user on the network. This allows an organization to allocate network resources to mission-critical applications and users, while limiting the bandwidth available to non-business-critical applications. References: Network+ Certification Study Guide, Chapter 2: Network Operations

NEW QUESTION 6

- (Exam Topic 1)

A network administrator is installing a wireless network at a client's office. Which of the following IEEE 802.11 standards would be BEST to use for multiple simultaneous client access?

- A. CDMA
- B. CSMA/CD
- C. CSMA/CA
- D. GSM

Answer: C

Explanation:

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is an IEEE 802.11 standard that would be best to use for multiple simultaneous client access on a wireless network. CSMA/CA is a media access control method that allows multiple devices to share the same wireless channel without causing collisions or interference. It works by having each device sense the channel before transmitting data and waiting for an acknowledgment from the receiver after each transmission. If the channel is busy or no acknowledgment is received, the device will back off and retry later with a random delay. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-csma-ca.html>

NEW QUESTION 7

- (Exam Topic 1)

A technician is connecting multiple switches to create a large network for a new office. The switches are unmanaged Layer 2 switches with multiple connections between each pair. The network is experiencing an extreme amount of latency. Which of the following is MOST likely occurring?

- A. Ethernet collisions
- B. A DDoS attack
- C. A broadcast storm
- D. Routing loops

Answer: C

Explanation:

A broadcast storm is most likely occurring when connecting multiple unmanaged Layer 2 switches with multiple connections between each pair. A broadcast storm is a situation where broadcast packets flood a network segment and consume all the available bandwidth. It can be caused by loops in the network topology, where broadcast packets are endlessly forwarded by switches without any loop prevention mechanism. Unmanaged switches do not support features such as Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) that can detect and block loops. References: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10556-16.html>

NEW QUESTION 8

- (Exam Topic 1)

A technician is installing multiple UPS units in a major retail store. The technician is required to keep track of all changes to new and old equipment. Which of the following will allow the technician to record these changes?

- A. Asset tags
- B. A smart locker
- C. An access control vestibule
- D. A camera

Answer: A

Explanation:

Asset tags will allow the technician to record changes to new and old equipment when installing multiple UPS units in a major retail store. Asset tags are labels or stickers that are attached to physical assets such as computers, printers, servers, or UPS units. They usually contain information such as asset name, serial number, barcode, QR code, or RFID chip that can be scanned or read by an asset management system or software. Asset tags help track inventory, location, status, maintenance, and ownership of assets. References: <https://www.camcode.com/asset-tags/asset-tagging-guide/>

NEW QUESTION 9

- (Exam Topic 1)

A technician is installing a new fiber connection to a network device in a datacenter. The connection from the device to the switch also traverses a patch panel connection. The chain of connections is in the following order:

Device
LC/LC patch cable Patch panel
Cross-connect fiber cable Patch panel
LC/LC patch cable Switch

The connection is not working. The technician has changed both patch cables with known working patch cables. The device had been tested and was working properly before being installed. Which of the following is the MOST likely cause of the issue?

- A. TX/RX is reversed
- B. An incorrect cable was used
- C. The device failed during installation
- D. Attenuation is occurring

Answer: A

Explanation:

The most likely cause of the issue where the fiber connection from a device to a switch is not working is that the TX/RX (transmit/receive) is reversed. When connecting fiber optic cables, it is important to ensure that the TX of one device is connected to the RX of the other device and vice versa. If the TX/RX is reversed, data cannot be transmitted successfully.

References:

➤ CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 5: Network Operations, Objective 5.1: Given a scenario, use appropriate documentation and diagrams to manage the network.

NEW QUESTION 10

- (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 10

- (Exam Topic 1)

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 (Service Set Identifier) is a feature that should be configured to allow different wireless access through the same equipment. SSID is the name of a wireless network that identifies it from other networks in the same area. A wireless access point (AP) can support multiple SSIDs with different security settings and network policies. For example, a store owner can create one SSID for business equipment and another SSID for patron use, and assign different passwords, VLANs, and QoS levels for each SSID. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70931-multiple-ssid.html>

NEW QUESTION 15

- (Exam Topic 1)

A technician is configuring a network switch to be used in a publicly accessible location. Which of the following should the technician configure on the switch to prevent unintended connections?

- A. DHCP snooping
- B. Geofencing
- C. Port security
- D. Secure SNMP

Answer: C

Explanation:

Port security is a feature that restricts input to a switch port by limiting and identifying MAC addresses of the devices allowed to access the port. This prevents unintended connections from unauthorized devices or spoofed MAC addresses. Port security can also be configured to take actions such as shutting down the port or sending an alert when a violation occurs. 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/td/docs/switches/lan/catalyst9500/software/release/16-10/configuration_guide/se

NEW QUESTION 20

- (Exam Topic 1)

A network administrator is configuring a load balancer for two systems. Which of the following must the administrator configure to ensure connectivity during a failover?

- A. VIP

- B. NAT
- C. APIPA
- D. IPv6 tunneling
- E. Broadcast IP

Answer: A

Explanation:

A virtual IP (VIP) address must be configured to ensure connectivity during a failover. A VIP address is a single IP address that is assigned to a group of servers or network devices. When one device fails, traffic is automatically rerouted to the remaining devices, and the VIP address is reassigned to the backup device, allowing clients to continue to access the service without interruption.

References:

➤ CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 6: Network Servers, p. 300

NEW QUESTION 21

- (Exam Topic 1)

Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

- A. SSO
- B. TACACS+
- C. Zero Trust
- D. Separation of duties
- E. Multifactor authentication

Answer: B

Explanation:

TACACS+ (Terminal Access Controller Access Control System Plus) can be used to centrally manage credentials for various types of administrative privileges on configured network devices. This protocol separates authentication, authorization, and accounting (AAA) functions, providing more granular control over access to network resources.

References:

➤ Network+ N10-007 Certification Exam Objectives, Objective 4.2: Given a scenario, implement secure network administration principles.

NEW QUESTION 26

- (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 29

- (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 33

- (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 38

- (Exam Topic 1)

A network administrator is designing a new datacenter in a different region that will need to communicate to the old datacenter with a secure connection. Which of the following access methods would provide the BEST security for this new datacenter?

- A. Virtual network computing
- B. Secure Socket Shell
- C. In-band connection
- D. Site-to-site VPN

Answer: D

Explanation:

Site-to-site VPN provides the best security for connecting a new datacenter to an old one because it creates a secure tunnel between the two locations, protecting data in transit. References: CompTIA Network+ Certification Study Guide, Chapter 5: Network Security.

NEW QUESTION 40

- (Exam Topic 1)

A technician needs to configure a Linux computer for network monitoring. The technician has the following information:

Linux computer details:

Interface	IP address	MAC address
eth0	10.1.2.24	A1:B2:C3:F4:E5:D6

Switch mirror port details:

Interface	IP address	MAC address
eth1	10.1.2.3	A1:B2:C3:D4:E5:F6

After connecting the Linux computer to the mirror port on the switch, which of the following commands should the technician run on the Linux computer?

- A. `ifconfig eth0 promisc`
- B. `ifconfig eth1 up`
- C. `ifconfig eth0 10.1.2.3`
- D. `ifconfig eth1 hw ether A1:B2:C3:D4:E5:F6`

Answer: A

Explanation:

The `ifconfig eth0 promisc` command should be run on the Linux computer to enable promiscuous mode, which allows the computer to capture all network traffic passing through the switch mirror port. References: CompTIA Network+ Certification Study Guide, Chapter 7: Network Devices.

NEW QUESTION 44

- (Exam Topic 1)

A company hired a technician to find all the devices connected within a network. Which of the following software tools would BEST assist the technician in completing this task?

- A. IP scanner
- B. Terminal emulator
- C. NetFlow analyzer
- D. Port scanner

Answer: A

Explanation:

To find all devices connected within a network, a technician can use an IP scanner. An IP scanner sends a ping request to all IP addresses within a specified range and then identifies the active devices that respond to the request.

NEW QUESTION 49

- (Exam Topic 1)

An engineer is configuring redundant network links between switches. Which of the following should the engineer enable to prevent network stability issues?

- A. 802.1Q
- B. STP
- C. Flow control
- D. CSMA/CD

Answer: B

Explanation:

Spanning Tree Protocol (STP) should be enabled when configuring redundant network links between switches. STP ensures that only one active path is used at a time, preventing network loops and stability issues.

References:

NEW QUESTION 50

- (Exam Topic 1)

Which of the following provides redundancy on a file server to ensure the server is still connected to a LAN even in the event of a port failure on a switch?

- A. NIC teaming
- B. Load balancer
- C. RAID array
- D. PDUs

Answer: A

Explanation:

NIC teaming, also known as network interface card teaming or link aggregation, allows multiple network interface cards to be grouped together to provide redundancy and increased throughput. In the event of a port failure on a switch, NIC teaming ensures that the file server remains connected to the LAN by automatically switching to another network interface card.

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

NEW QUESTION 51

- (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 53

- (Exam Topic 1)

A technician is assisting a user who cannot connect to a network resource. The technician first checks for a link light. According to troubleshooting methodology, this is an example of:

- A. using a bottom-to-top approach.
- B. establishing a plan of action.
- C. documenting a finding.
- D. questioning the obvious.

Answer: A

Explanation:

Using a bottom-to-top approach means starting from the physical layer and moving up the OSI model to troubleshoot a network problem. Checking for a link light is a physical layer check that verifies the connectivity of the network cable and device. References:

<https://www.professormesser.com/network-plus/n10-007/troubleshooting-methodologies-2/>

NEW QUESTION 58

- (Exam Topic 1)

A systems administrator needs to improve WiFi performance in a densely populated office tower and use the latest standard. There is a mix of devices that use 2.4 GHz and 5 GHz. Which of the following should the systems administrator select to meet this requirement?

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

Answer: B

Explanation:

* 802.11 ax is the latest WiFi standard that improves WiFi performance in densely populated environments and supports both 2.4 GHz and 5 GHz bands. 802.11ac is the previous standard that only supports 5 GHz band. 802.11g and 802.11n are older standards that support 2.4 GHz band only or both bands respectively.

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.techtarget.com/searchnetworking/tip/Whats-the-difference-between-80211ax-vs-80211ac>

NEW QUESTION 60

- (Exam Topic 1)

Which of the following service models would MOST likely be used to replace on-premises servers with a cloud solution?

- A. PaaS
- B. IaaS
- C. SaaS
- D. Disaster recovery as a Service (DRaaS)

Answer: B

Explanation:

IaaS stands for Infrastructure as a Service, which is a cloud service model that provides virtualized computing resources over the Internet, such as servers, storage, networking, and operating systems. IaaS allows customers to replace their on-premises servers with cloud servers that can be scaled up or down on demand and pay only for what they use. PaaS stands for Platform as a Service, which provides customers with a cloud-based platform for developing, testing, and deploying applications without managing the underlying infrastructure. SaaS stands for Software as a Service, which provides customers with access to cloud-based software applications over the Internet without installing or maintaining them on their devices. Disaster recovery as a Service (DRaaS) is a type of cloud service that provides customers with backup and recovery solutions for their data and applications in case of a disaster.

NEW QUESTION 61

- (Exam Topic 1)

Which of the following systems would MOST likely be found in a screened subnet?

- A. RADIUS
- B. FTP
- C. SQL
- D. LDAP

Answer: B

Explanation:

FTP (File Transfer Protocol) is a system that would most likely be found in a screened subnet. A screened subnet, or triple-homed firewall, is a network architecture where a single firewall is used with three network interfaces. It provides additional protection from outside cyber attacks by adding a perimeter network to isolate or separate the internal network from the public-facing internet. A screened subnet typically hosts systems that need to be accessed by both internal and external users, such as web servers, email servers, or FTP servers. References: <https://www.techtarget.com/searchsecurity/definition/screened-subnet#:~:text=A%20screened%20subnet%2C%1>

NEW QUESTION 66

- (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 67

- (Exam Topic 2)

A SaaS provider has decided to leave an unpatched VM available via a public DMZ port. With which of the following concepts is this technique MOST closely associated?

- A. Insider threat
- B. War driving
- C. Evil twin
- D. Honeypot

Answer: D

Explanation:

A honeypot is a decoy system that is intentionally left vulnerable or exposed to attract attackers and divert them from the real targets. A honeypot can also be used to collect information about the attackers' techniques and motives. In the scenario, the SaaS provider has left an unpatched VM available via a public DMZ port, which could be a honeypot technique to lure attackers and monitor their activities. References: <https://www.comptia.org/blog/what-is-a-honeypot>

NEW QUESTION 68

- (Exam Topic 2)

A network technician was troubleshooting an issue for a user who was being directed to cloned websites that were stealing credentials. The URLs were correct for the websites but an incorrect IP address was revealed when the technician used ping on the user's PC. After checking the settings, the technician found the DNS

server address was incorrect Which of the following describes the issue?

- A. Rogue DHCP server
- B. Misconfigured HSRP
- C. DNS poisoning
- D. Exhausted IP scope

Answer: C

Explanation:

DNS poisoning is a type of attack that modifies the DNS records of a domain name to point to a malicious IP address instead of the legitimate one. This can result in users being directed to cloned websites that are stealing credentials, even if they enter the correct URL for the website. The incorrect DNS server address on the user's PC could be a sign of DNS poisoning, as the attacker could have compromised the DNS server or spoofed its response to redirect the user's queries.

References: <https://www.comptia.org/blog/what-is-dns-poisoning>

NEW QUESTION 70

- (Exam Topic 2)

Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site. Which of the following will BEST provide this functionality?

- A. Client-to-site VPN
- B. Third-party VPN service
- C. Site-to-site VPN
- D. Split-tunnel VPN

Answer: C

Explanation:

A site-to-site VPN is a type of VPN that connects two or more remote offices securely over an untrustworthy network, such as the Internet. A site-to-site VPN allows each office to access network shares and resources at the other site, as if they were on the same local network. A site-to-site VPN encrypts and tunnels the traffic between the offices, ensuring privacy and integrity of the data. References: <https://www.comptia.org/blog/what-is-a-site-to-site-vpn>

NEW QUESTION 75

- (Exam Topic 2)

A wireless network was installed in a warehouse for employees to scan crates with a wireless handheld scanner. The wireless network was placed in the corner of the building near the ceiling for maximum coverage However users in the offices adjacent to the warehouse have noticed a large amount of signal overlap from the new network Additionally warehouse employees report difficulty connecting to the wireless network from the other side of the building; however they have no issues when they are near the antenna Which of the following is MOST likely the cause?

- A. The wireless signal is being refracted by the warehouse's windows
- B. The antenna's power level was set too high and is overlapping
- C. An omnidirectional antenna was used instead of a unidirectional antenna
- D. The wireless access points are using channels from the 5GHz spectrum

Answer: C

Explanation:

An omnidirectional antenna was used instead of a unidirectional antenna, which is most likely the cause of the wireless network issues. An omnidirectional antenna provides wireless coverage in all directions from the antenna, which can cause signal overlap with adjacent offices and interference with other wireless networks. A unidirectional antenna, on the other hand, provides wireless coverage in a specific direction from the antenna, which can reduce signal overlap and interference and increase signal range and quality. A unidirectional antenna would be more suitable for a warehouse environment where users are located on one side of the building¹. References:

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

NEW QUESTION 76

- (Exam Topic 2)

An organization wants to implement a method of centrally managing logins to network services. Which of the following protocols should the organization use to allow for authentication, authorization and auditing?

- A. MS-CHAP
- B. RADIUS
- C. LDAPS
- D. RSTP

Answer: B

Explanation:

RADIUS (Remote Authentication Dial-In User Service) is a protocol that should be used by the organization to allow for authentication, authorization, and auditing of network services. RADIUS is an AAA (Authentication, Authorization, and Accounting) protocol that manages network access by verifying user credentials, granting access permissions, and logging user activities. RADIUS uses a client-server model where a RADIUS client (such as a router, switch, or VPN server) sends user information to a RADIUS server (such as an authentication server) for verification and authorization. The RADIUS server can also send accounting information to another server for billing or reporting purposes. References:

<https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838>

NEW QUESTION 80

- (Exam Topic 2)

A technician is implementing a new wireless network to serve guests at a local office. The network needs to provide Internet access but disallow associated stations from communicating with each other. Which of the following would BEST accomplish this requirement?

- A. Wireless client isolation
- B. Port security
- C. Device geofencing
- D. DHCP snooping

Answer: A

Explanation:

Wireless client isolation is a feature on wireless routers that limits the connectivity between wireless devices connected to the same network. It prevents them from accessing resources on other wireless or wired devices, as a security measure to reduce attacks and threats. This feature can be useful for guest and BYOD SSIDs, but it can also be disabled on the router's settings. References:
<https://www.howtogeek.com/179089/lock-down-your-wi-fi-network-with-your-routers-wireless-isolation-option>

NEW QUESTION 83

- (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 distributes by the OHCP 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 84

- (Exam Topic 2)

A network technician has multimode fiber optic cable available in an existing IDF. Which of the following Ethernet standards should the technician use to connect the network switch to the existing fiber?

- A. 10GBaseT
- B. 1000BaseT
- C. 1000BaseSX
- D. 1000BaseLX

Answer: C

Explanation:

1000BaseSX is an Ethernet standard that should be used to connect the network switch to the existing multimode fiber optic cable. 1000BaseSX is a Gigabit Ethernet standard that uses short-wavelength laser (850 nm) over multimode fiber optic cable. It can support distances up to 550 meters depending on the cable type and quality. It is suitable for short-range network segments such as campus or building backbone networks. References:
<https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/produ>

NEW QUESTION 85

- (Exam Topic 2)

A network administrator is talking to different vendors about acquiring technology to support a new project for a large company. Which of the following documents will MOST likely need to be signed before information about the project is shared?

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

Answer: B

Explanation:

NDA stands for Non-Disclosure Agreement, which is a legal contract between two or more parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by others. A network administrator may need to sign an NDA before sharing information about a new project with different vendors, as the project may involve sensitive or proprietary data that the company wants to protect from competitors or unauthorized use. References: <https://www.adobe.com/sign/esignature-resources/sign-nda.html>

NEW QUESTION 87

- (Exam Topic 2)

A network technician is installing an analog desk phone for a new receptionist After running a new phone line, the technician now needs to cnmp on a new connector. Which of the following connectors would MOST likely be used in this case?

- A. DB9
- B. RJ11
- C. RJ45
- D. DB25

Answer: B

Explanation:

RJ11 is a type of connector that is commonly used for analog phone lines. RJ11 has four wires and six positions, but only two or four of them are used. A technician can crimp an RJ11 connector to a new phone line to install an analog desk phone for a new receptionist. References:
<https://www.comptia.org/blog/what-is-rj11>

NEW QUESTION 89

- (Exam Topic 2)

A network technician is investigating an issue with handheld devices in a warehouse. Devices have not been connecting to the nearest APs, but they have been connecting to an AP on the far side of the warehouse. Which of the following is the MOST likely cause of this issue?

- A. The nearest APs are configured for 802.11g.
- B. An incorrect channel assignment is on the nearest APs.
- C. The power level is too high for the AP on the far side.
- D. Interference exists around the AP on the far side.

Answer: C

Explanation:

The power level is a setting that determines how strong the wireless signal is from an access point (AP). If the power level is too high for an AP on the far side of a warehouse, it can cause interference and overlap with other APs on the same channel or frequency. This can result in handheld devices not connecting to the nearest APs, but connecting to the AP on the far side instead. A technician should adjust the power level of the AP on the far side to reduce interference and improve connectivity. References:
<https://www.comptia.org/blog/what-is-power-level>

NEW QUESTION 92

- (Exam Topic 2)

Which of the following security devices would be BEST to use to provide mechanical access control to the MDF/IDF?

- A. A smart card
- B. A key fob
- C. An employee badge
- D. A door lock

Answer: D

Explanation:

A door lock would be the best security device to use to provide mechanical access control to the MDF/IDF. A door lock is a device that prevents unauthorized access to a physical area by requiring a key, a code, a card, a biometric scan, or a combination of these factors to open it. A door lock can provide mechanical access control to the MDF/IDF, which are rooms that house network equipment such as switches, routers, servers, or patch panels. A door lock can prevent unauthorized persons from tampering with or stealing the network equipment or data. References:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_6.html

NEW QUESTION 94

- (Exam Topic 2)

A network technician is investigating an issue with a desktop that is not connecting to the network. The desktop was connecting successfully the previous day, and no changes were made to the environment. The technician locates the switchport where the device is connected and observes the LED status light on the switchport is not lit even though the desktop is turned on Other devices that are plugged into the switch are connecting to the network successfully Which of the following is MOST likely the cause of the desktop not connecting?

- A. Transceiver mismatch
- B. VLAN mismatch
- C. Port security
- D. Damaged cable
- E. Duplex mismatch

Answer: D

Explanation:

A damaged cable is most likely the cause of the desktop not connecting to the network. A damaged cable can cause physical layer issues such as loss of signal, attenuation, interference, or crosstalk. These issues can prevent the desktop from establishing a link with the switch and result in the LED status light on the switchport being off. Other possible causes of physical layer issues are faulty connectors, ports, or transceivers. References:
<https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/14119-37.html>

NEW QUESTION 98

- (Exam Topic 2)

An organization with one core and five distribution switches is transitioning from a star to a full-mesh topology Which of the following is the number of additional network connections needed?

- A. 5
- B. 7
- C. 10
- D. 15

Answer: C

Explanation:

10 additional network connections are needed to transition from a star to a full-mesh topology. A star topology is a network topology where each device is connected to a central device, such as a switch or a hub. A full-mesh topology is a network topology where each device is directly connected to every other device. The number of connections needed for a full-mesh topology can be calculated by the formula $n(n-1)/2$, where n is the number of devices. In this case, there are six devices (one core and five distribution switches), so the number of connections needed for a full-mesh topology is $6(6-1)/2 = 15$. Since there are already five connections in the star topology (one from each distribution switch to the core switch), the number of additional connections needed is $15 - 5 = 10$. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>

NEW QUESTION 101

- (Exam Topic 2)

A network technician is configuring a new firewall for a company with the necessary access requirements to be allowed through the firewall. Which of the following would normally be applied as the LAST rule in the firewall?

- A. Secure SNMP
- B. Port security
- C. Implicit deny
- D. DHCP snooping

Answer: C

Explanation:

Implicit deny is a firewall rule that blocks all traffic that is not explicitly allowed by other rules. Implicit deny is usually applied as the last rule in the firewall to ensure that only the necessary access requirements are allowed through the firewall and that any unwanted or malicious traffic is rejected. Implicit deny can also provide a default security policy and a baseline for auditing and logging purposes.

Secure SNMP is a protocol that allows network devices to send event messages to a centralized server or console for logging and analysis. Secure SNMP can be used to monitor and manage the status, performance, and configuration of network devices. Secure SNMP can also help to detect and respond to potential problems or faults on the network. However, secure SNMP is not a firewall rule; it is a network management protocol.

Port security is a feature that allows a switch to restrict the devices that can connect to a specific port based on their MAC addresses. Port security can help to prevent unauthorized access, spoofing, or MAC flooding attacks on the switch. However, port security is not a firewall rule; it is a switch feature.

DHCP snooping is a feature that allows a switch to filter DHCP messages and prevent rogue DHCP servers from assigning IP addresses to devices on the network. DHCP snooping can help to prevent IP address conflicts, spoofing, or denial-of-service attacks on the network. However, DHCP snooping is not a firewall rule; it is a switch feature.

NEW QUESTION 105

- (Exam Topic 2)

A network requirement calls for segmenting departments into different networks. The campus network is set up with users of each department in multiple buildings. Which of the following should be configured to keep the design simple and efficient?

- A. MDIX
- B. Jumbo frames
- C. Port tagging
- D. Flow control

Answer: C

Explanation:

Port tagging is a technique that involves adding a tag or identifier to the frames or packets that belong to a certain VLAN. A VLAN is a logical segment of a network that isolates traffic between different groups of devices. Port tagging allows devices on different physical ports or switches to communicate with each other as if they were on the same port or switch. Port tagging can help keep the design simple and efficient by reducing the number of physical ports and switches needed to segment departments into different networks. References: <https://www.comptia.org/blog/what-is-port-tagging>

NEW QUESTION 108

- (Exam Topic 2)

Which of the following OSI model layers is where conversations between applications are established, coordinated, and terminated?

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

Answer: A

Explanation:

Reference: <https://www.techtarget.com/searchnetworking/definition/OSI#:~:text=The%20session%20layer,and%20termina>

The session layer is where conversations between applications are established, coordinated, and terminated. It is responsible for creating, maintaining, and ending sessions between different devices or processes. The physical layer deals with the transmission of bits over a medium. The presentation layer formats and translates data for different applications. The data link layer provides reliable and error-free delivery of frames within a network.

NEW QUESTION 113

- (Exam Topic 2)

A network administrator needs to implement an HDMI over IP solution. Which of the following will the network administrator MOST likely use to ensure smooth video delivery?

- A. Link aggregation control
- B. Port tagging
- C. Jumbo frames
- D. Media access control

Answer: C

Explanation:

Giants are packets that exceed the configured MTU (Maximum Transmission Unit) of a switchport or interface, which causes them to be dropped or fragmented by the switch or router. The MTU is the maximum size of a packet that can be transmitted without fragmentation on a given medium or protocol. Giants can indicate misconfiguration or mismatch of MTU values between devices or interfaces on a network, which can cause performance issues or errors. CRC errors are errors that occur when the cyclic redundancy check (CRC) value of a packet does not match the calculated CRC value at the destination, which indicates corruption or alteration of data during transmission due to noise, interference, faulty cabling, etc., but not necessarily exceeding MTU values. Runts are packets that are smaller than the minimum size allowed by the medium or protocol, which causes them to be dropped or ignored by the switch or router. Flooding is a technique where a switch sends packets to all ports except the source port when it does not have an entry for the destination MAC address in its MAC address table, which can cause congestion or broadcast storms on a network.

NEW QUESTION 118

- (Exam Topic 2)

A systems administrator is running a VoIP network and is experiencing jitter and high latency. Which of the following would BEST help the administrator determine the cause of these issues?

- A. Enabling RADIUS on the network
- B. Configuring SNMP traps on the network
- C. Implementing LDAP on the network
- D. Establishing NTP on the network

Answer: B

Explanation:

SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a network management system (NMS) for monitoring and configuration purposes. SNMP traps are unsolicited messages sent by network devices to the NMS when certain events or conditions occur, such as errors, failures, or thresholds. Configuring SNMP traps on the network would best help the administrator determine the cause of jitter and high latency on a VoIP network, as they would provide real-time alerts and information about the network performance and status. Enabling RADIUS on the network is not relevant to troubleshooting VoIP issues, as RADIUS is a protocol that provides authentication, authorization, and accounting services for network access. Implementing LDAP on the network is also not relevant to troubleshooting VoIP issues, as LDAP is a protocol that provides directory services for storing and querying information about users, groups, devices, etc. Establishing NTP on the network is not directly related to troubleshooting VoIP issues, as NTP is a protocol that synchronizes the clocks of network devices.

NEW QUESTION 119

- (Exam Topic 2)

A technician is deploying a low-density wireless network and is contending with multiple types of building materials. Which of the following wireless frequencies would allow for the LEAST signal attenuation?

- A. 2.4GHz
- B. 5GHz
- C. 850MHz
- D. 900MHz

Answer: A

Explanation:

* 2.4 GHz is the wireless frequency that would allow for the least signal attenuation when deploying a low-density wireless network with multiple types of building materials. Signal attenuation is the loss of signal strength or quality as it travels through a medium or over a distance. Signal attenuation can be affected by various factors such as distance, interference, reflection, refraction, diffraction, scattering, or absorption. Generally, lower frequencies have less signal attenuation than higher frequencies because they can penetrate obstacles better and travel farther. Therefore, 2.4GHz would have less signal attenuation than 5GHz, 850MHz, or 900MHz. References:
<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html>

NEW QUESTION 124

- (Exam Topic 2)

A company that uses VoIP telephones is experiencing intermittent issues with one-way audio and dropped conversations. The manufacturer says the system will work if ping times are less than 50ms. The company has recorded the following ping times:

10ms	10ms	10ms	100ms	70ms	5ms	5ms	80ms	100ms	5ms	5ms
------	------	------	-------	------	-----	-----	------	-------	-----	-----

Which of the following is MOST likely causing the issue?

- A. Attenuation
- B. Latency
- C. VLAN mismatch
- D. Jitter

Answer: D

Explanation:

Jitter is most likely causing the issue of intermittent one-way audio and dropped conversations for the company that uses VoIP telephones. Jitter is a variation in delay of packets arriving at the destination. It can cause choppy or distorted audio quality for VoIP applications, especially over WAN links that have limited bandwidth and high latency. The recommended jitter for VoIP is less than 10ms. The company has recorded ping times that exceed 50ms, which indicates high jitter and latency on their network. References:
<https://www.voip-info.org/voip-jitter/> 1

NEW QUESTION 129

- (Exam Topic 2)

A technician is connecting DSL for a new customer. After installing and connecting the on-premises equipment, the technician verifies DSL synchronization. When connecting to a workstation, however, the link LEDs on the workstation and modem do not light up. Which of the following should the technician perform during troubleshooting?

- A. Identify the switching loops between the modem and the workstation.
- B. Check for asymmetrical routing on the modem.
- C. Look for a rogue DHCP server on the network.
- D. Replace the cable connecting the modem and the workstation.

Answer: D

Explanation:

If the link LEDs on the workstation and modem do not light up when connecting to a workstation, it could indicate a problem with the cable connecting them. The cable could be damaged, defective, or incompatible with the devices. A technician should replace the cable with a known good one and check if the link LEDs light up. If not, the problem could be with the network interface cards (NICs) on the workstation or modem. References: <https://www.comptia.org/blog/what-is-link-light>

NEW QUESTION 134

- (Exam Topic 2)

A client moving into a new office wants the IP network set up to accommodate 412 network-connected devices that are all on the same subnet. The subnet needs to be as small as possible. Which of the following subnet masks should be used to achieve the required result?

- A. 255.255.0.0
- B. 255.255.252.0
- C. 255.255.254.0
- D. 255.255.255.0

Answer: B

Explanation:

* 255.255.252.1 is a subnet mask that allows for 1022 network-connected devices on the same subnet, which is the smallest subnet that can accommodate 412 devices. The subnet mask determines how many bits are used for the network portion and how many bits are used for the host portion of an IP address. A smaller subnet mask means more bits are used for the network portion and less bits are used for the host portion, which reduces the number of available hosts on the subnet. 255.255.0.0 allows for 65534 hosts on the same subnet, which is too large. 255.255.254.0 allows for 510 hosts on the same subnet, which is also too large. 255.255.255.0 allows for 254 hosts on the same subnet, which is too small.

NEW QUESTION 137

- (Exam Topic 2)

A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

- A. nslookup
- B. netstat -a
- C. ipconfig /a
- D. arp -a

Answer: B

Explanation:

netstat -a is a command that displays information about active TCP connections and listening ports on a system. A network administrator can use netstat -a to check if the database engine is listening on a certain port, as well as verify if there are any connections established to or from that port. References: <https://www.comptia.org/blog/what-is-netstat>

NEW QUESTION 139

- (Exam Topic 2)

A user recently made changes to a PC that caused it to be unable to access websites by both FQDN and IP Local resources, such as the file server remain accessible. Which of the following settings did the user MOST likely misconfigure?

- A. Static IP
- B. Default gateway
- C. DNS entries
- D. Local host file

Answer: B

Explanation:

The default gateway is the setting that the user most likely misconfigured on the PC that caused it to be unable to access websites by both FQDN and IP. The default gateway is a device, usually a router or a firewall, that connects a local network to other networks such as the Internet. It acts as an intermediary between devices on different networks and forwards packets based on their destination IP addresses. If the default gateway is not configured correctly on a PC, it will not be able to communicate with devices outside its local network, such as web servers or DNS servers. References: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/16448-default-gateway.html>

NEW QUESTION 141

- (Exam Topic 2)

A company wants to implement a large number of WAPs throughout its building and allow users to be able to move around the building without dropping their connections Which of the following pieces of equipment would be able to handle this requirement?

- A. A VPN concentrator
- B. A load balancer
- C. A wireless controller
- D. A RADIUS server

Answer: C

Explanation:

A wireless controller would be able to handle the requirement of implementing a large number of WAPs throughout the building and allowing users to move around without dropping their connections. A wireless controller is a device that centrally manages and configures multiple wireless access points (WAPs) on a network. It can provide features such as load balancing, roaming, security, QoS, and monitoring for the wireless network. A wireless controller can also support wireless mesh networks, where some WAPs act as relays for other WAPs to extend the wireless coverage. References: <https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/index.html>

NEW QUESTION 143

- (Exam Topic 3)

A network administrator views a network pcap and sees a packet containing the following:

```
community: public
request-id: 13438
get-response 1.3.6.1.2.1.1.3.0 Value:206801150
```

Which of the following are the BEST ways for the administrator to secure this type of traffic? (Select TWO).

- A. Migrate the network to IPv6.
- B. Implement 802.1 X authentication
- C. Set a private community string
- D. Use SNMPv3.
- E. Incorporate SSL encryption
- F. Utilize IPsec tunneling.

Answer: CD

Explanation:

The packet shown in the image is an SNMP (Simple Network Management Protocol) packet, which is used to monitor and manage network devices. SNMP uses community strings to authenticate requests and responses between SNMP agents and managers. However, community strings are sent in clear text and can be easily intercepted by attackers. Therefore, one way to secure SNMP traffic is to set a private community string that is not the default or well-known value. Another way to secure SNMP traffic is to use SNMPv3, which is the latest version of the protocol that supports encryption and authentication of SNMP messages. References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5: Given a scenario, use remote access methods.

NEW QUESTION 147

- (Exam Topic 3)

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

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

Answer: B

Explanation:

<https://www.practicalnetworking.net/stand-alone/routing-between-vlans/#:~:text=A%20router%20will%20perfo>

NEW QUESTION 151

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 156

- (Exam Topic 3)

Which of the following devices have the capability to allow communication between two different subnetworks? (Select TWO).

- A. IDS
- B. Access point
- C. Layer 2 switch
- D. Layer 3 switch
- E. Router
- F. Media converter

Answer: DE

NEW QUESTION 158

- (Exam Topic 3)

A technician performed a manual reconfiguration of a firewall, and network connectivity was reestablished. Some connection events that were previously sent to a syslog server are no longer being generated by the firewall. Which of the following should the technician perform to fix the issue?

- A. Adjust the proper logging level on the new firewall.
- B. Tune the filter for logging the severity level on the syslog server.
- C. Activate NetFlow traffic between the syslog server and the firewall
- D. Restart the SNMP service running on the syslog server.

Answer: A

Explanation:

Logging level is a setting that determines what types of events are recorded by a device and sent to a syslog server. Different logging levels have different severity levels, ranging from emergency to debug. If the technician performed a manual reconfiguration of the firewall, it is possible that the logging level was changed or reset to a lower level that does not include the connection events that were previously sent to the syslog server. To fix the issue, the technician should adjust the proper logging level on the new firewall to match the desired level of detail and severity for the connection events. References: Network+ Study Guide Objective 3.4: Explain common scanning, monitoring and patching processes and summarize their expected outputs. Subobjective: Syslog.

NEW QUESTION 159

- (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 162

- (Exam Topic 3)

A network device needs to discover a server that can provide it with an IPv4 address. Which of the following does the device need to send the request to?

- A. Default gateway
- B. Broadcast address
- C. Unicast address
- D. Link local address

Answer: B

Explanation:

The DHCP client sends broadcast request packets to the network; the DHCP servers respond with broadcast packets that offer IP parameters, such as an IP address for the client. After the client chooses the IP parameters, communication between the client and server is by unicast packets.

"When a DHCP client boots up, it automatically sends out a DHCP Discover UDP datagram to the broadcast address, 255.255.255.255. This DHCP Discover message asks "Are there any DHCP servers out there?" The client can't send unicast traffic yet, as it doesn't have a valid IP address that can be used."

NEW QUESTION 167

- (Exam Topic 3)

A technician is checking network devices to look for opportunities to improve security. Which of the following tools would BEST accomplish this task?

- A. Wi-Fi analyzer
- B. Protocol analyzer
- C. Nmap
- D. IP scanner

Answer: B

Explanation:

A protocol analyzer is a tool that can capture and analyze network traffic and identify security issues such as unauthorized devices, malicious packets, or misconfigured settings.

A Wi-Fi analyzer is a tool that can measure the signal strength, interference, and channel usage of wireless networks, but it cannot provide detailed information about network security.

Nmap and IP scanner are tools that can scan network hosts and ports for open services, vulnerabilities, or operating systems, but they cannot monitor network traffic in real time.

NEW QUESTION 171

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 172

- (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 175

- (Exam Topic 3)

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

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

Answer: BC

NEW QUESTION 178

- (Exam Topic 3)

Which of the following would be BEST to install to find and block any malicious users within a network?

- A. IDS
- B. IPS
- C. SCADA
- D. ICS

Answer: B

Explanation:

IPS takes action itself to block the attempted intrusion or otherwise remediate the incident. IDS is designed to only provide an alert about a potential incident, which enables a security operations center (SOC) analyst to investigate the event and determine whether it requires further action.

NEW QUESTION 179

- (Exam Topic 3)

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

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

Answer: D

Explanation:

DHCP scope exhaustion means that there are no more available IP addresses in the DHCP server's pool of addresses to assign to new devices on the network. When this happens, the devices will use APIPA (Automatic Private IP Addressing) to self-configure an IP address in the range of 169.254.0.1 to 169.254.255.254. These addresses are not routable and can only communicate with other devices on the same local network.

A rogue DHCP server (A) is an unauthorized DHCP server that can cause IP address conflicts or security issues by assigning IP addresses to devices on the network. A network collision (B) is a situation where two or more devices try to send data on the same network segment at the same time, causing interference and data loss. Incorrect DNS settings © can prevent devices from resolving domain names to IP addresses, but they do not affect the DHCP process.

NEW QUESTION 180

- (Exam Topic 3)

Which of the following devices is used to configure and centrally manage access points installed at different locations?

- A. Wireless controller
- B. Load balancer
- C. Proxy server
- D. VPN concentrator

Answer: A

Explanation:

Access points (APs) can be configured and centrally managed using a wireless LAN controller (WLC). A WLC is a device that connects to multiple APs and provides centralized management and control of those APs. The WLC can be used to configure settings such as wireless network parameters, security settings, and quality of service (QoS) policies. Additionally, the WLC can be used to monitor the status of connected APs, track client connections, and gather statistics on network usage. Some vendors such as Cisco, Aruba, Ruckus, etc. provide wireless LAN controllers as part of their wireless networking solutions.

NEW QUESTION 184

- (Exam Topic 3)

A network technician is troubleshooting an area where the wireless connection to devices is poor. The technician theorizes that the signal-to-noise ratio in the area is causing the issue. Which of the following should the technician do NEXT?

- A. Run diagnostics on the relevant devices.
- B. Move the access point to a different location.
- C. Escalate the issue to the vendor's support team.
- D. Remove any electronics that might be causing interference.

Answer: D

NEW QUESTION 189

- (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 192

- (Exam Topic 3)

Which of the following can be used to limit the ability of devices to perform only HTTPS connections to an internet update server without exposing the devices to the public internet?

- A. Allow connections only to an internal proxy server.
- B. Deploy an IDS system and place it in line with the traffic.
- C. Create a screened network and move the devices to it.
- D. Use a host-based network firewall on each device.

Answer: A

Explanation:

An internal proxy server is a server that acts as an intermediary between internal devices and external servers on the internet. An internal proxy server can be used to limit the ability of devices to perform only HTTPS connections to an internet update server by filtering and forwarding the requests and responses based on predefined rules or policies. An internal proxy server can also prevent the devices from being exposed to the public internet by hiding their IP addresses and providing a layer of security and privacy.

NEW QUESTION 193

- (Exam Topic 3)

SIMULATION

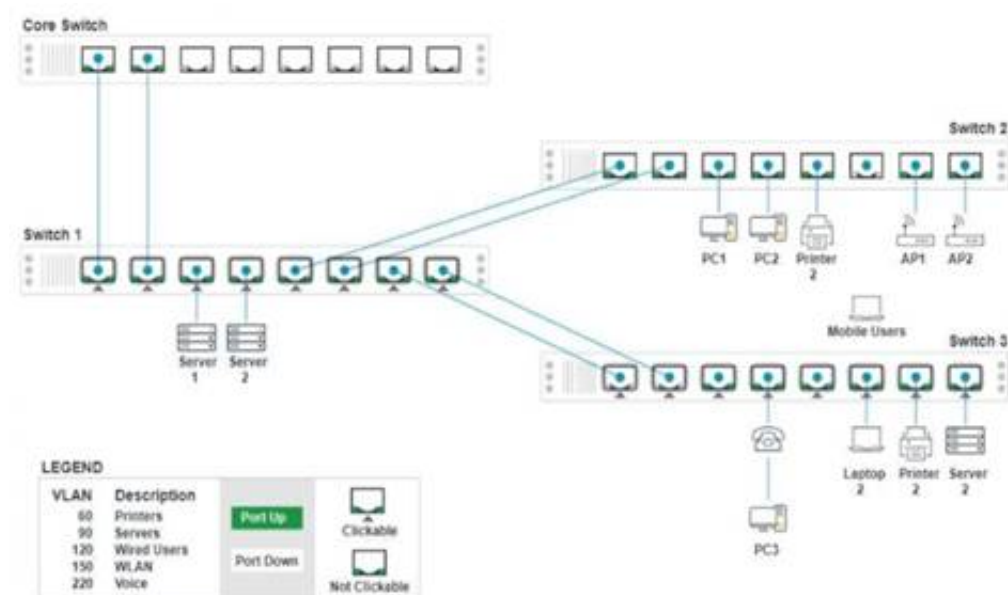
A network technician replaced a switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.

INSTRUCTIONS

Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings:

- Ensure each device accesses only its correctly associated network
- Disable all unused switch ports
- Require fault-tolerant connections between the switches
- Only make necessary changes to complete the above requirements

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



Switch 3 - Port 8 Configuration

Status
Port ☒ Enabled
LACP ☐ Disabled

Wired
Speed ☐ Auto ☐ 100 ☒ 1000
Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

Add VLAN

VLAN 1
Port Tagging

UnTagged
Tagged
UnTagged

VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220

Reset to Default Save Close

Switch 3 - Port 7 Configuration

Status
Port ☒ Enabled
LACP ☐ Disabled

Wired
Speed ☐ Auto ☐ 100 ☒ 1000
Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

Add VLAN

VLAN 1
Port Tagging

UnTagged
Tagged
UnTagged

VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220

Reset to Default Save Close

Switch 3 - Port 6 Configuration

Status

Port ☒ Enabled

LACP ☐ Disabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN150

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1

VLAN 60

VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default

Save

Close

Switch 3 - Port 4 Configuration

Status

Port ☒ Enabled

LACP ☐ Disabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000

Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

+ Add VLAN

VLAN1

Port Tagging

UnTagged

Tagged

UnTagged

VLAN 1

VLAN 60

VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default

Save

Close

Switch 3 - Port 1 Configuration

Status

Port ☒ Enabled
LACP ☐ Disabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000
Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

Add VLAN

VLAN1

Port Tagging

UnTagged
Tagged
Un Tagged

VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220

Reset to Default
Save
Close

Switch 1 - Port 7 Configuration

Status

Port ☒ Enabled
LACP ☒ Enabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000
Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

Add VLAN

VLAN60

Port Tagging

Tagged

VLAN90

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

VLAN220

Port Tagging

Tagged

Reset to Default
Save
Close

Switch 1 - Port 8 Configuration

Status

Port ☒ Enabled
LACP ☒ Enabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000
Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

Add VLAN

VLAN60

Port Tagging

Tagged

VLAN90

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

VLAN220

Port Tagging

Tagged

Reset to Default
Save
Close

Switch 1 - Port 6 Configuration

Status

Port ☒ Enabled
LACP ☒ Enabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000
Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

Add VLAN

VLAN60

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

Reset to Default
Save
Close

Switch 1 - Port 2 Configuration

Status

Port ☒ Enabled
LACP ☒ Enabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000
Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

Add VLAN

VLAN60

Port Tagging

Tagged

VLAN90

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

VLAN220

Port Tagging

Tagged

Reset to Default
Save
Close

Switch 1 - Port 1 Configuration

Status

Port ☒ Enabled
LACP ☒ Enabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000
Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

Add VLAN

VLAN60

Port Tagging

Tagged

VLAN90

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

VLAN220

Port Tagging

Tagged

Reset to Default
Save
Close

Switch 1 - Port 5 Configuration

Status

Port ☒ Enabled
LACP ☒ Enabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000
Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

Add VLAN

VLAN60

Port Tagging

Tagged

VLAN120

Port Tagging

Tagged

VLAN150

Port Tagging

Tagged

Reset to Default Save Close

Switch 1 - Port 4 Configuration

Status

Port ☒ Enabled
LACP ☐ Disabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000
Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

Add VLAN

VLAN90

Port Tagging

UnTagged

VLAN 1

VLAN 60

VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default Save Close

Switch 1 - Port 3 Configuration

Status

Port ☒ Enabled
LACP ☐ Disabled

Wired

Speed ☐ Auto ☐ 100 ☒ 1000
Duplex ☐ Auto ☐ Half ☒ Full

VLAN Configuration

Add VLAN

VLAN90

Port Tagging

UnTagged

VLAN 1

VLAN 60

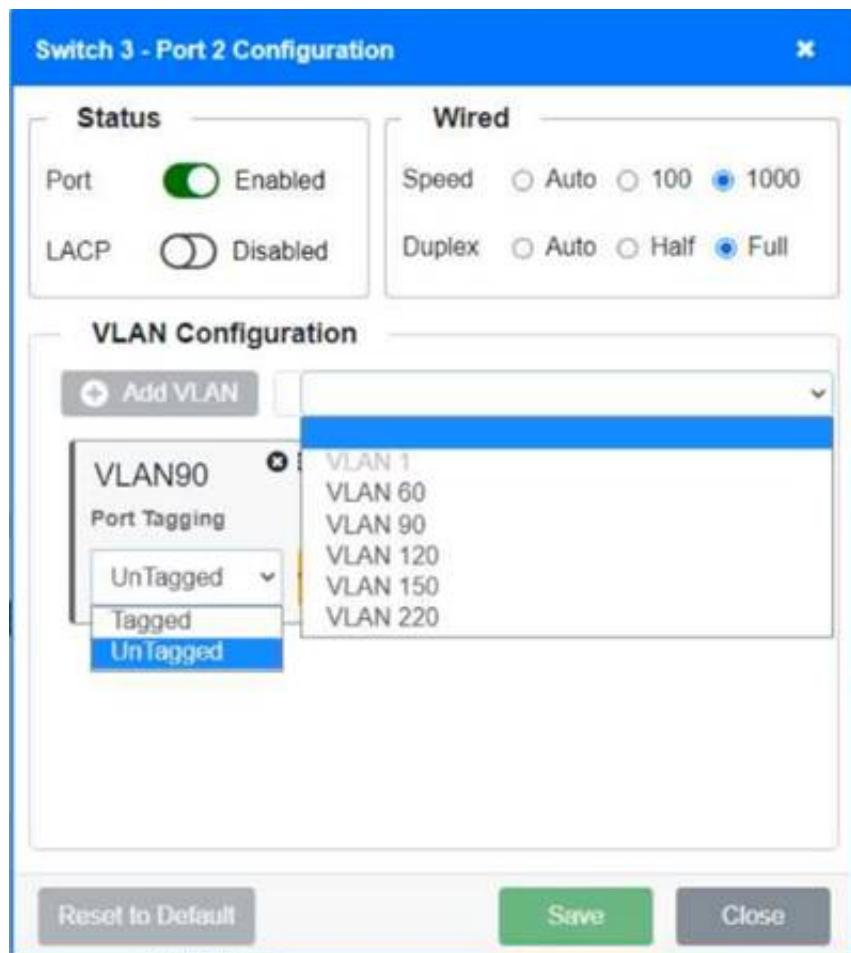
VLAN 90

VLAN 120

VLAN 150

VLAN 220

Reset to Default Save Close



The image shows a configuration window for 'Switch 3 - Port 2'. It has two tabs: 'Status' and 'Wired'. In the 'Status' tab, 'Port' is 'Enabled' and 'LACP' is 'Disabled'. In the 'Wired' tab, 'Speed' is '1000' and 'Duplex' is 'Full'. Below these is a 'VLAN Configuration' section with an 'Add VLAN' button and a list of VLANs: VLAN 1, VLAN 60, VLAN 90, VLAN 120, VLAN 150, and VLAN 220. A dropdown menu for 'Port Tagging' is open, showing 'UnTagged', 'Tagged', and 'UnTagged' (selected). At the bottom are 'Reset to Default', 'Save', and 'Close' buttons.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Switch 1 and Switch 2 is the only two switches that can be configured. Only switches linked together with there switch ports needs to be "tagged" and "LACP" needs to be enabled. The other ports must be untagged with no LACP enabled. You only need to assign the correct vlan via each port. 'Speed and Duplex' needs to be Speed=1000 and Duplex=Full, with is by default.

<https://resources.infosecinstitute.com/topic/what-are-tagged-and-untagged-ports/>

NEW QUESTION 194

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 196

- (Exam Topic 3)

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

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

Answer: A

Explanation:

To determine if a client's network cable issues may be causing intermittent connectivity, the help desk technician can run the show interface command on the switch. This command allows the technician to view the status and statistics of the various interfaces on the switch, including the physical link status and the number of transmitted and received packets. If the interface is experiencing a large number of errors or dropped packets, this could indicate a problem with the network cable or with the connection between the client's device and the switch.

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

NEW QUESTION 200

- (Exam Topic 3)

A new global ISP needs to connect from central offices in North America to the United Kingdom. Which of the following would be the BEST cabling solution for this project?

- A. Single-mode
- B. Coaxial
- C. Cat 6a
- D. Twinaxial

Answer: A

Explanation:

For a new global ISP to connect from central offices in North America to the United Kingdom, the best cabling solution would be single-mode fiber optic cable. Single-mode fiber optic cable is a type of cable that is used to transmit data over long distances using light signals. It is typically used in long-haul communication networks, such as those that connect different countries or continents.

NEW QUESTION 204

- (Exam Topic 3)

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

Switch 1:

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

Switch 2:

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

Switch 3:

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

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

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

Answer: AE

NEW QUESTION 206

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 208

- (Exam Topic 3)

Which of the following protocols can be routed?

- A. FCoE
- B. Fibre Channel

- C. iSCSI
- D. NetBEUI

Answer: C

Explanation:

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

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

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

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

NEW QUESTION 213

- (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 214

- (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 218

- (Exam Topic 3)

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

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

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

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

Answer: A

NEW QUESTION 223

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 226

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 230

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 231

- (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 233

- (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 236

- (Exam Topic 3)

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

- A. Spanning Tree Protocol is enabled on the switch.
- B. VLAN trunking is enabled on the switch.

- C. Port security is configured on the switch.
- D. Dynamic ARP inspection is configured on the switch.

Answer: C

NEW QUESTION 237

- (Exam Topic 3)

A company cell phone was stolen from a technician's vehicle. The cell phone has a passcode, but it contains sensitive information about clients and vendors. Which of the following should also be enabled?

- A. Factory reset
- B. Autolock
- C. Encryption
- D. Two-factor authentication

Answer: C

NEW QUESTION 239

- (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 240

- (Exam Topic 3)

A technician is trying to determine whether an LACP bundle is fully operational. Which of the following commands will the technician MOST likely use?

- A. show interface
- B. show config
- C. how route
- D. show arp

Answer: A

Explanation:

https://www.cisco.com/c/en/us/td/docs/optical/cpt/r9_3/command/reference/cpt93_cr/cpt93_cr_chapter_01000.h

NEW QUESTION 244

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 246

- (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 251

- (Exam Topic 3)

Which of the following is an advanced distance vector routing protocol that automates routing tables and also uses some features of link-state routing protocols?

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

Answer: C

Explanation:

EIGRP is an advanced distance vector routing protocol that is able to automatically update routing tables and also uses features of link-state routing protocols, such as the ability to send updates about the current topology of the network. EIGRP also has the ability to use a variety of algorithms to determine the best route for a packet to take, allowing for more efficient routing across the network.

NEW QUESTION 254

- (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 258

- (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 259

- (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 263

- (Exam Topic 3)

A network administrator is trying to add network redundancy for the server farm. Which of the following can the network administrator configure to BEST provide this capability?

- A. VRRP
- B. DNS
- C. UPS
- D. RPO

Answer: A

Explanation:

VRRP is an open standard protocol, which is used to provide redundancy in a network. It is a network layer protocol (protocol number-112). The number of routers (group members) in a group acts as a virtual logical router which will be the default gateway of all the local hosts. If one router goes down, one of the other group members can take place for the responsibilities for forwarding the traffic.

NEW QUESTION 265

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 268

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 272

- (Exam Topic 3)

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

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

Answer: C

Explanation:

A helper address is an IP address that is configured on a router interface to forward DHCP broadcast messages to a DHCP server on another LAN. A DHCP broadcast message is a message that a workstation sends when it needs to obtain an IP address from a DHCP server. Since broadcast messages are not routed across different networks, a helper address is needed to relay the DHCP broadcast message to the DHCP server on another network. References:

<https://www.comptia.org/training/books/network-n10-008-study-guide> (page 199)

NEW QUESTION 277

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 282

- (Exam Topic 3)

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

- A. Fiber
- B. Leased line

- C. Satellite
- D. Metro optical

Answer: C

Explanation:

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

NEW QUESTION 283

- (Exam Topic 3)

Which of the following can have multiple VLAN interfaces?

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

Answer: B

NEW QUESTION 286

- (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 291

- (Exam Topic 3)

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

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

Answer: AC

Explanation:

To achieve this, you should do two things:

- Tag the three VLANs across the uplink port that connects to another switch or router. This will allow data packets from different VLANs to cross over into other networks.
- Untag an individual VLAN per device port that connects to an end device. This will assign each device to its expected network without additional connections.

NEW QUESTION 293

- (Exam Topic 3)

A network administrator is troubleshooting a client's device that cannot connect to the network. A physical inspection of the switch shows the RJ45 is connected. The NIC shows no activity lights. The network administrator moves the device to another location and connects to the network without issues. Which Of the following tools would be the BEST option for the network administrator to use to further troubleshoot?

- A. Tone generator
- B. Multimeter
- C. Optical time-domain reflectometer
- D. Cable tester

Answer: D

Explanation:

A cable tester is a tool that can verify the integrity and functionality of a network cable. It can measure the electrical characteristics of the cable, such as resistance, capacitance, and impedance, and detect any faults or defects, such as shorts, opens, or crosstalk. A cable tester can help the network administrator troubleshoot the problem by determining if the cable is faulty or not. A tone generator is a tool that can send an audible signal through a cable to help locate and identify it. A multimeter is a tool that can measure voltage, current, and resistance of electrical circuits. An optical time-domain reflectometer (OTDR) is a tool that can test the quality and length of fiber optic cables.

References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.3: Given a scenario, use the appropriate tool to support wired or wireless networks.

NEW QUESTION 296

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 299

- (Exam Topic 3)

A new office space is being designed. The network switches are up, but no services are running yet. A network engineer plugs in a laptop configured as a DHCP client to a switch. Which of the following IP addresses should be assigned to the laptop?

- A. 10.1.1.1
- B. 169.254.1.128
- C. 172.16.128.128
- D. 192.168.0.1

Answer: B

Explanation:

When a DHCP client is connected to a network and no DHCP server is available, the client can automatically configure a link-local address in the 169.254.0.0/16 range using the Automatic Private IP Addressing (APIPA) feature. So, the correct answer is option B, 169.254.1.128. This is also known as an APIPA address. Reference: CompTIA Network+ Study Guide, Exam N10-007, Fourth Edition, by Todd Lammle (Chapter 4: IP Addressing)

NEW QUESTION 303

- (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 306

- (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 311

- (Exam Topic 3)

An ISP configured an internet connection to provide 20Mbps, but actual data rates are occurring at 10Mbps and causing a significant delay in data transmission. Which of the following specifications should the ISP check?

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

Answer: A

Explanation:

Throughput is the actual amount of data that can be transferred over a network in a given time. Throughput can be affected by various factors such as congestion, interference, errors, or hardware limitations. If the throughput is lower than the configured internet connection speed, it can cause a significant delay in data

transmission. The ISP should check the throughput and identify the source of the problem.

References: Network+ Study Guide Objective 2.2: Explain the concepts and characteristics of routing and switching.

NEW QUESTION 315

- (Exam Topic 3)

Which of the following is the NEXT step to perform network troubleshooting after identifying an issue?

- A. Implement a solution.
- B. Establish a theory.
- C. Escalate the issue.
- D. Document the findings.

Answer: B

Explanation:

1 Identify the Problem. 2 Develop a Theory.

3 Test the Theory. 4 Plan of Action.

5 Implement the Solution.

6 Verify System Functionality. 7 Document the Issue.

NEW QUESTION 317

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 322

- (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 324

- (Exam Topic 3)

A network administrator is adding a new switch to the network. Which of the following network hardening techniques would be BEST to use once the switch is in production?

- A. Disable unneeded ports
- B. Disable SSH service
- C. Disable MAC filtering
- D. Disable port security

Answer: A

NEW QUESTION 325

- (Exam Topic 3)

A network technician is performing tests on a potentially faulty network card that is installed in a server. Which of the following addresses will MOST likely be used during traffic diagnostic tests?

- A. 10.10.10.10
- B. 127.0.0.1
- C. 192.168.0.1
- D. 255.255.255.0

Answer: B

Explanation:

* 127.1.1.1 is the loopback address, it is used to test the functionality of a network card by sending traffic to the card and then verifying that it is received properly. This address is used because it is guaranteed to always point to the local host, regardless of the network configuration. The IP address range for loopback addresses is 127.0.0.0/8.

NEW QUESTION 327

- (Exam Topic 3)

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

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

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

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

Answer: A

Explanation:

<https://www.tunnelsup.com/subnet-calculator/> IP Address: 172.28.85.95/27

Netmask: 255.255.255.224

Network Address: 172.28.85.64

Usable Host Range: 172.28.85.65 - 172.28.85.94

Broadcast Address: 172.28.85.95

NEW QUESTION 328

- (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 332

- (Exam Topic 3)

A network security engineer locates an unapproved wireless bridge connected to the corporate LAN that is broadcasting a hidden SSID, providing unauthenticated access to internal resources. Which of the following types of attacks BEST describes this finding?

- A. Rogue access point Most Voted
- B. Evil twin
- C. ARP spoofing
- D. VLAN hopping

Answer: A

Explanation:

A rogue access point is an illegitimate access point plugged into a network to create a bypass from outside into the legitimate network. By contrast, an evil twin is a copy of a legitimate access point.

NEW QUESTION 337

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

RBAC is a method of restricting network access based on the roles of individual users within the organization. With RBAC, users are granted access only to the resources they need to perform their specific job functions. This approach reduces the risk of unauthorized access, provides greater visibility into user activity, and simplifies network management.

Changing the default permissions to implicit deny may improve security, but it could also cause issues for legitimate users who require access to specific resources. Configuring uniform ACLs and NAC for contractors is a step in the right direction, but it may not be enough to address the overall lack of a formal process for granting network permissions. Deploying an RDP server to centralize access to the network is not a viable solution, as it would not address the root cause of the security incidents.

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

NEW QUESTION 339

- (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 343

- (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 344

- (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 349

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 351

- (Exam Topic 3)

Two users on a LAN establish a video call. Which of the following OSI model layers ensures the initiation coordination, and termination of the call?

- A. Session
- B. Physical
- C. Transport

D. Data link

Answer: A

Explanation:

The OSI model layer that ensures the initiation, coordination, and termination of a video call is the session layer. The session layer is responsible for establishing, maintaining, and terminating communication sessions between two devices on a network.

NEW QUESTION 354

- (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 358

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 359

- (Exam Topic 3)

After HVAC failures caused network outages, the support team decides to monitor the temperatures of all the devices. The network administrator cannot find a command that will display this information. Which of the following will retrieve the necessary information?

- A. SNMP OID values
- B. NetFlow data export
- C. Network baseline configurations
- D. Security information and event management

Answer: A

Explanation:

The network administrator can use the Simple Network Management Protocol (SNMP) to monitor the temperatures of all the devices. SNMP is a widely-used protocol for managing and monitoring network devices, such as routers, switches, servers, and other networking equipment. SNMP allows network administrators to gather information about the performance and status of devices on the network, including temperature readings.

To retrieve the temperature information, the administrator will have to configure SNMP on the devices and configure SNMP manager software on their computer. Once the SNMP manager software is configured, it will be able to send SNMP requests to the devices and retrieve information such as temperature, voltage, fan speeds, etc. Many network devices have built-in SNMP support, and the administrator may also need to install SNMP agent software on the devices to enable SNMP monitoring.

The administrator can also use some specific command or tool like IPMI (Intelligent Platform Management Interface) or DCIM (Data Center Infrastructure Management) tools for monitoring the temperatures of all the devices.

NEW QUESTION 362

- (Exam Topic 3)

A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds hundreds of CRC errors on an interface. Which of the following is the MOST likely cause of these errors?

- A. A bad wire on the Cat 5e cable
- B. The wrong VLAN assignment to the switchport
- C. A misconfigured QoS setting on the router
- D. Both sides of the switch trunk set to full duplex

Answer: A

NEW QUESTION 363

- (Exam Topic 3)

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

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

Answer: D

Explanation:

Confidentiality is the property of preventing unauthorized access or disclosure of data. Encryption is a method of transforming data into an unreadable format that can only be decrypted by authorized parties who have the correct key. Encryption can increase the confidentiality of data communication across the network by making it harder for attackers to intercept or eavesdrop on the data. References: Network+ Study Guide Objective 4.1: Summarize the purposes of physical security devices. Subobjective: Encryption.

NEW QUESTION 368

- (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 network. 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 370

- (Exam Topic 3)

A network administrator is planning a WLAN for a soccer stadium and was advised to use MU-MIMO to improve connection performance in high-density areas.

The project requires compatibility with clients

connecting using 2.4GHz or 5GHz frequencies. Which of the following would be the BEST wireless standard for this project?

- A. 80211ac
- B. 802.11ax
- C. 802.11g
- D. 80211n

Answer: B

NEW QUESTION 372

- (Exam Topic 3)

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

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

Answer: D

Explanation:

BGP stands for Border Gateway Protocol and it is used to exchange routing information between autonomous systems (AS) on the Internet. A perimeter router is a router that connects an AS to another AS or to the Internet. Therefore, BGP is the best suited routing protocol for a perimeter router.

References: Network+ Study Guide Objective 2.4: Compare and contrast the characteristics of network topologies, types and technologies.

NEW QUESTION 373

- (Exam Topic 3)

A network technician is configuring a wireless access point and wants to only allow company-owned devices to associate with the network. The access point uses PSKs,

and a network authentication system does not exist on the network. Which of the following should the technician implement?

- A. Captive portal
- B. Guest network isolation
- C. MAC filtering
- D. Geofencing

Answer: C

Explanation:

MAC filtering is a method of allowing only company-owned devices to associate with the network by using their MAC addresses as identifiers. A MAC address is a unique identifier assigned to each network interface card (NIC) by the manufacturer. MAC filtering can be configured on the wireless access point to allow or deny access based on the MAC address of the device. This way, only devices with known MAC addresses can connect to the network. References:
<https://www.comptia.org/training/books/network-n10-008-study-guide> (page 323)

NEW QUESTION 375

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

N10-009 Practice Exam Features:

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