

Exam Questions N10-009

CompTIA Network+ Exam

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



NEW QUESTION 1

- (Exam Topic 1)

An IT director is setting up new disaster and HA policies for a company. Limited downtime is critical to operations. To meet corporate requirements, the director set up two different datacenters across the country that will stay current on data and applications. In the event of an outage, the company can immediately switch from one datacenter to another. Which of the following does this BEST describe?

- A. A warm site
- B. Data mirroring
- C. Multipathing
- D. Load balancing
- E. A hot site

Answer: E

Explanation:

A hot site is a fully redundant site that can take over operations immediately if the primary site goes down. In this scenario, the company has set up two different datacenters across the country that are current on data and applications, and they can immediately switch from one datacenter to another in case of an outage.

References:

➤ Network+ N10-008 Objectives: 1.5 Compare and contrast disaster recovery concepts and methodologies.

NEW QUESTION 2

- (Exam Topic 1)

A network technician is installing new software on a Windows-based server in a different geographical location. Which of the following would be BEST for the technician to use to perform this task?

- A. RDP
- B. SSH
- C. FTP
- D. DNS

Answer: A

Explanation:

RDP (Remote Desktop Protocol) is the best option for a network technician to use when installing new software on a Windows-based server in a different geographical location. This protocol allows the technician to connect to the server remotely and control it as if they were physically present.

References:

➤ Network+ N10-007 Certification Exam Objectives, Objective 2.2: Given a scenario, implement the appropriate network-based security and troubleshoot common connectivity issues.

NEW QUESTION 3

- (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 4

- (Exam Topic 1)

Which of the following devices would be used to manage a corporate WLAN?

- A. A wireless NAS
- B. A wireless bridge
- C. A wireless router
- D. A wireless controller

Answer: D

Explanation:

A wireless controller is used to manage a corporate WLAN, providing centralized management and configuration of access points. References: CompTIA Network+ Certification Study Guide, Chapter 8: Wireless Networks.

NEW QUESTION 5

- (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 6

- (Exam Topic 1)

At which of the following OSI model layers would a technician find an IP header?

- A. Layer 1
- B. Layer 2
- C. Layer 3
- D. Layer 4

Answer: C

Explanation:

An IP header can be found at the third layer of the OSI model, also known as the network layer. This layer is responsible for logical addressing, routing, and forwarding of data packets.

References:

➤ CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: Network Models, p. 82

NEW QUESTION 7

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

References:

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

NEW QUESTION 8

- (Exam Topic 1)

A network administrator discovers that users in an adjacent building are connecting to the company's guest wireless network to download inappropriate material. Which of the following can the administrator do to MOST easily mitigate this issue?

- A. Reduce the wireless power levels
- B. Adjust the wireless channels
- C. Enable wireless client isolation
- D. Enable wireless port security

Answer: A

Explanation:

Reducing the wireless power levels can limit the range of the guest wireless network and prevent users in an adjacent building from connecting to it. Adjusting the wireless channels or enabling wireless client isolation will not affect the signal strength or coverage of the guest network. Enabling wireless port security will not work on a guest network that does not use authentication or MAC address filtering. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 2.0 Network Operations, Objective 2.5 Given a scenario, implement appropriate wireless configuration settings; Guest WiFi Security - Cisco Umbrella

NEW QUESTION 9

- (Exam Topic 1)

Access to a datacenter should be individually recorded by a card reader even when multiple employees enter the facility at the same time. Which of the following allows the enforcement of this policy?

- A. Motion detection
- B. Access control vestibules
- C. Smart lockers
- D. Cameras

Answer: B

Explanation:

The most effective security mechanism against physical intrusions due to stolen credentials would likely be a combination of several of these options. However, of the options provided, the most effective security mechanism would probably be an access control vestibule. An access control vestibule is a secure area that is located between the outer perimeter of a facility and the inner secure area. It is designed to provide an additional layer of security by requiring that individuals pass through a series of security checks before being allowed access to the secure area. This could include biometric authentication, access card readers, and motion detection cameras.

Access control vestibules allow the enforcement of the policy that access to a datacenter should be individually recorded by a card reader even when multiple employees enter the facility at the same time. An access control vestibule is a physical security device that consists of two doors with an interlocking mechanism. Only one door can be opened at a time, and only one person can pass through each door. This prevents tailgating or piggybacking, where unauthorized persons follow authorized persons into a secure area. An access control vestibule can also be integrated with a card reader or other authentication system to record each individual's access. References: <https://www.boonedam.us/blog/what-are-access-control-vestibules>

NEW QUESTION 10

- (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)

Several WIFI users are reporting the inability to connect to the network. WLAN users on the guest network are able to access all network resources without any performance issues. The following table summarizes the findings after a site survey of the area in question:

Location	AP 1	AP 2	AP 3	AP 4
SSID	Corp1	Corp1	Corp1/Guest	Corp1/Guest
Channel	2	1	5	11
RSSI	-81dBm	-82dBm	-44dBm	-41dBm
Antenna type	Omni	Omni	Directional	Directional

Which of the following should a wireless technician do NEXT to troubleshoot this issue?

- A. Reconfigure the channels to reduce overlap
- B. Replace the omni antennas with directional antennas
- C. Update the SSIDs on all the APs
- D. Decrease power in AP 3 and AP 4

Answer: A

Explanation:

Based on the site survey table, we can see that AP 2, AP 3, and AP 4 are all broadcasting on the same channel, which can cause interference and affect performance. Therefore, the next step a wireless technician should take to troubleshoot this issue is to reconfigure the channels to reduce overlap. This will help to improve network performance and eliminate any interference.

References:

➤ Network+ N10-007 Certification Exam Objectives, Objective 2.8: Given a scenario, troubleshoot common wireless problems and perform site surveys.

NEW QUESTION 11

- (Exam Topic 1)

Given the following information:

Protocol	Local address	Foreign address	State
TCP	127.0.0.1:57779	Desktop-Open:57780	Established
TCP	127.0.0.1:57780	Desktop-Open:57779	Established

Which of the following command-line tools would generate this output?

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

Answer: D

Explanation:

Tracert is a command-line tool that traces the route of a packet from a source to a destination and displays the number of hops and the round-trip time for each hop. The output shown in the question is an example of a tracert output, which shows five hops with their IP addresses and hostnames (if available) and three latency measurements for each hop in milliseconds. 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.lumen.com/help/en-us/network/traceroute/understanding-the-traceroute-output.html>

NEW QUESTION 15

- (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 16

- (Exam Topic 1)

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

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

Answer: C

Explanation:

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

NEW QUESTION 19

- (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 22

- (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 27

- (Exam Topic 1)

After the A record of a public website was updated, some visitors were unable to access the website. Which of the following should be adjusted to address the issue?

- A. TTL
- B. MX
- C. TXT
- D. SOA

Answer: A

Explanation:

TTL (Time To Live) should be adjusted to address the issue of some visitors being unable to access the website after the A record was updated. TTL is a value that specifies how long a DNS record should be cached by DNS servers and clients before it expires and needs to be refreshed. If the TTL is too high, some DNS servers and clients may still use the old A record that points to the previous IP address of the website, resulting in connection failures. By lowering the TTL, the DNS servers and clients will update their cache more frequently and use the new A record that points to the current IP address of the website. References: <https://www.cloudflare.com/learning/dns/dns-records/dns-ttl/>

NEW QUESTION 28

- (Exam Topic 1)

A technician is installing a cable modem in a SOHO. Which of the following cable types will the technician MOST likely use to connect a modem to the ISP?

- A. Coaxial
- B. Single-mode fiber
- C. Cat 6e
- D. Multimode fiber

Answer: A

Explanation:

Coaxial cable is a type of cable that consists of a central copper conductor surrounded by an insulating layer and a braided metal shield. Coaxial cable is commonly used to connect a cable modem to an ISP by transmitting data over cable television networks. Coaxial cable can support high bandwidth and long distances with minimal interference or attenuation. References: [https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.techopedia.com/definition/4027/coaxial-cable>

NEW QUESTION 30

- (Exam Topic 1)

A technician is deploying a new switch model and would like to add it to the existing network monitoring software. The technician wants to know what metrics can be gathered from a given switch. Which of the following should the technician utilize for the switch?

- A. MIB
- B. Trap
- C. Syslog
- D. Audit log

Answer: A

Explanation:

To determine what metrics can be gathered from a given switch, a technician should utilize the Management Information Base (MIB). The MIB is a database of network management information that is used to manage and monitor network devices. It contains information about device configuration, status, and performance. References: Network+ Certification Study Guide, Chapter 5: Network Security

NEW QUESTION 35

- (Exam Topic 1)

Which of the following ports is commonly used by VoIP phones?

- A. 20
- B. 143
- C. 445
- D. 5060

Answer: D

Explanation:

TCP/UDP port 5060 is commonly used by VoIP phones. It is the default port for SIP (Session Initiation Protocol), which is a signaling protocol that establishes, modifies, and terminates multimedia sessions over IP networks. SIP is widely used for VoIP applications such as voice and video calls. References: <https://www.voip-info.org/session-initiation-protocol/>

NEW QUESTION 37

- (Exam Topic 1)

A technician receives feedback that some users are experiencing high amounts of jitter while using the wireless network. While troubleshooting the network, the technician uses the ping command with the IP address of the default gateway and verifies large variations in latency. The technician thinks the issue may be

interference from other networks and non-802.11 devices. Which of the following tools should the technician use to troubleshoot the issue?

- A. NetFlow analyzer
- B. Bandwidth analyzer
- C. Protocol analyzer
- D. Spectrum analyzer

Answer: D

Explanation:

A spectrum analyzer is a tool that measures the frequency and amplitude of signals in a wireless network. It can be used to troubleshoot issues related to interference from other networks and non-802.11 devices, such as microwave ovens or cordless phones, by identifying the sources and levels of interference in the wireless spectrum. A spectrum analyzer can also help to optimize the channel selection and placement of wireless access points. 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.flukenetworks.com/blog/cabling-chronicles/what-spectrum-analyzer-and-how-do-you-use-it>

NEW QUESTION 40

- (Exam Topic 1)

Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

- A. Scope options
- B. Reservation
- C. Dynamic assignment
- D. Exclusion
- E. Static assignment

Answer: B

Explanation:

A reservation should be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP. A reservation is a feature of DHCP that allows an administrator to assign a fixed IP address to a device based on its MAC address. This way, the device will always receive the same IP address from the DHCP server, even if it is powered off or disconnected from the network for a long time. References: <https://docs.microsoft.com/en-us/windows-server/troubleshoot/configure-dhcp-reservations>

NEW QUESTION 45

- (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 47

- (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 49

- (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 52

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

NEW QUESTION 56

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 60

- (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 62

- (Exam Topic 1)

Which of the following routing protocols is used to exchange route information between public autonomous systems?

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

Answer: B

Explanation:

BGP (Border Gateway Protocol) is a routing protocol used to exchange route information between public autonomous systems (AS). OSPF (Open Shortest Path First), EGRIP (Enhanced Interior Gateway Routing Protocol), and RIP (Routing Information Protocol) are all used for internal routing within a single AS. Therefore, BGP is the correct option to choose for this question.

References:

- Network+ N10-007 Certification Exam Objectives, Objective 3.3: Given a scenario, configure and apply the appropriate routing protocol.
- Cisco: Border Gateway Protocol (BGP) Overview

NEW QUESTION 63

- (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 67

- (Exam Topic 1)

Which of the following factors should be considered when evaluating a firewall to protect a datacenter's east-west traffic?

- A. Replication traffic between an on-premises server and a remote backup facility
- B. Traffic between VMs running on different hosts
- C. Concurrent connections generated by Internet DDoS attacks
- D. VPN traffic from remote offices to the datacenter's VMs

Answer: B

Explanation:

When evaluating a firewall to protect a datacenter's east-west traffic, it is important to consider traffic between VMs running on different hosts. This type of traffic is referred to as east-west traffic and is often protected by internal firewalls. By implementing firewalls, an organization can protect their internal network against threats such as lateral movement, which can be caused by attackers who have breached a perimeter firewall. References: Network+ Certification Study Guide, Chapter 5: Network Security

NEW QUESTION 72

- (Exam Topic 1)

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

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

Answer: A

Explanation:

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

References:

- Network+ N10-007 Certification Exam Objectives, Objective 2.5: Given a scenario, troubleshoot copper cable issues.
- FS: OTDR (Optical Time Domain Reflectometer) Testing Principle and Applications

NEW QUESTION 75

- (Exam Topic 1)

A user reports being unable to access network resources after making some changes in the office. Which of the following should a network technician do FIRST?

- A. Check the system's IP address
- B. Do a ping test against the servers
- C. Reseat the cables into the back of the PC
- D. Ask what changes were made

Answer: D

Explanation:

When a user reports being unable to access network resources after making some changes, the network technician should first ask the user what changes were made. This information can help the technician identify the cause of the issue and determine the appropriate course of action.

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

NEW QUESTION 77

- (Exam Topic 1)

An IT organization needs to optimize speeds for global content distribution and wants to reduce latency in high-density user locations. Which of the following technologies BEST meets the organization's requirements?

- A. Load balancing
- B. Geofencing
- C. Public cloud
- D. Content delivery network
- E. Infrastructure as a service

Answer: D

Explanation:

A content delivery network (CDN) is a distributed network of servers that delivers web content to users based on their geographic location. By replicating content across multiple servers in various locations, a CDN can optimize speed and reduce latency in high-density user locations.

NEW QUESTION 78

- (Exam Topic 1)

Client devices cannot enter a network, and the network administrator determines the DHCP scope is exhausted. The administrator wants to avoid creating a new DHCP pool. Which of the following can the administrator perform to resolve the issue?

- A. Install load balancers
- B. Install more switches
- C. Decrease the number of VLANs
- D. Reduce the lease time

Answer: D

Explanation:

To resolve the issue of DHCP scope exhaustion without creating a new DHCP pool, the administrator can reduce the lease time. By decreasing the lease time, the IP addresses assigned by DHCP will be released back to the DHCP scope more quickly, allowing them to be assigned to new devices.

References:

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

➤ <https://www.networkcomputing.com/data-centers/10-tips-optimizing-dhcp-performance>

NEW QUESTION 80

- (Exam Topic 1)

Which of the following is MOST likely to generate significant East-West traffic in a datacenter?

- A. A backup of a large video presentation to cloud storage for archival purposes
- B. A duplication of a hosted virtual server to another physical server for redundancy
- C. A download of navigation data to a portable device for offline access
- D. A query from an IoT device to a cloud-hosted server for a firmware update

Answer: B

Explanation:

East-West traffic refers to data flows between servers or devices within the same datacenter. When a hosted virtual server is duplicated to another physical server for redundancy, it generates significant East-West traffic as the data is replicated between the two servers. References:

➤ Network+ N10-008 Objectives: 3.3 Given a scenario, implement secure network architecture concepts.

NEW QUESTION 82

- (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 85

- (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 internet¹. 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 86

- (Exam Topic 1)

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

- A. Ensure an implicit permit rule is enabled
- B. Configure the log settings on the firewalls to the central syslog server
- C. Update the firewalls with current firmware and software
- D. Use the same complex passwords on all firewalls

Answer: C

Explanation:

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

NEW QUESTION 88

- (Exam Topic 1)

A network technician is manually configuring the network settings for a new device and is told the network block is 192.168.0.0/20. Which of the following subnets should the technician use?

- A. 255.255.128.0
- B. 255.255.192.0
- C. 255.255.240.0
- D. 255.255.248.0

Answer: C

Explanation:

A subnet mask is a binary number that indicates which bits of an IP address belong to the network portion and which bits belong to the host portion. A slash notation (/n) indicates how many bits are used for the network portion. A /20 notation means that 20 bits are used for the network portion and 12 bits are used for the host portion. To convert /20 to a dotted decimal notation, we need to write 20 ones followed by 12 zeros in binary and then divide them into four octets separated by dots. This gives us 11111111.11111111.11110000.00000000 or 255.255.240.0 in decimal. References:
[https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-\(2-0\)](https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0)), <https://www.techopedia.com/definition/950/subnet-mask>

NEW QUESTION 92

- (Exam Topic 1)

Which of the following technologies provides a failover mechanism for the default gateway?

- A. FHRP
- B. LACP
- C. OSPF
- D. STP

Answer: A

Explanation:

First Hop Redundancy Protocol (FHRP) provides a failover mechanism for the default gateway, allowing a backup gateway to take over if the primary gateway fails. References: CompTIA Network+ Certification Study Guide, Chapter 4: Infrastructure.

NEW QUESTION 93

- (Exam Topic 2)

Which of the following uses the destination IP address to forward packets?

- A. A bridge
- B. A Layer 2 switch
- C. A router
- D. A repeater

Answer: C

Explanation:

A router is a device that uses the destination IP address to forward packets between different networks. A bridge and a Layer 2 switch operate at the data link layer and use MAC addresses to forward frames within the same network. A repeater is a device that amplifies or regenerates signals at the physical layer.

NEW QUESTION 98

- (Exam Topic 2)

A network technician needs to correlate security events to analyze a suspected intrusion. Which of the following should the technician use?

- A. SNMP
- B. Log review
- C. Vulnerability scanning
- D. SIEM

Answer: D

Explanation:

SIEM stands for Security Information and Event Management, which is a tool that collects, analyzes, and correlates data from various network devices and sources to provide alerts and reports on security incidents and events. A network technician can use SIEM to correlate security events to analyze a suspected intrusion, as SIEM can help identify the source, target, method, and impact of an attack, as well as provide recommendations for remediation. References: <https://www.comptia.org/blog/what-is-siem>

NEW QUESTION 101

- (Exam Topic 2)

Which of the following services can provide data storage, hardware options, and scalability to a third-party company that cannot afford new devices?

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

Answer: B

Explanation:

IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources such as servers, storage, and networking over the Internet. IaaS can provide data storage, hardware options, and scalability to a third-party company that cannot afford new devices by allowing them to rent or lease the infrastructure they need from a cloud provider. The company can pay only for what they use and scale up or down as needed. References: <https://www.comptia.org/blog/what-is-iaas>

NEW QUESTION 105

- (Exam Topic 2)

A corporation has a critical system that would cause unrecoverable damage to the brand if it was taken offline. Which of the following disaster recovery solutions should the corporation implement?

- A. Full backups
- B. Load balancing
- C. Hot site
- D. Snapshots

Answer: C

Explanation:

A hot site is the disaster recovery solution that the corporation should implement for its critical system that would cause unrecoverable damage to the brand if it was taken offline. A hot site is a fully operational backup site that can take over the primary site's functions in case of a disaster or disruption. A hot site has all the necessary hardware, software, data, network connections, and personnel to resume normal operations with minimal downtime. A hot site is suitable for systems that require high availability and cannot afford any data loss or interruption. References: <https://www.enterprisestorageforum.com/management/disaster-recovery-site/> 1

NEW QUESTION 106

- (Exam Topic 2)

A network administrator wants to analyze attacks directed toward the company's network. Which of the following must the network administrator implement to assist in this goal?

- A. A honeypot
- B. Network segmentation
- C. Antivirus
- D. A screened subnet

Answer: A

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. A network administrator can implement a honeypot to analyze attacks directed toward the company's network, as a honeypot can help identify the source, target, method, and impact of an attack, as well as provide recommendations for remediation. References: <https://www.comptia.org/blog/what-is-a-honeypot>

NEW QUESTION 110

- (Exam Topic 2)

Which of the following is used to provide networking capability for VMs at Layer 2 of the OSI model?

- A. VPN
- B. VRRP
- C. vSwitch
- D. VIP

Answer: C

Explanation:

A vSwitch (virtual switch) is a software-based switch that provides networking capability for VMs (virtual machines) at Layer 2 of the OSI model. It connects the VMs to each other or to external networks using virtual NICs (network interface cards). A VPN (virtual private network) is a technology that creates a secure tunnel over a public network for remote access or site-to-site connectivity. VRRP (Virtual Router Redundancy Protocol) is a protocol that provides high availability for routers by creating a virtual router with multiple physical routers. A VIP (virtual IP) is an IP address that can be shared by multiple servers or devices for load balancing or failover purposes.

NEW QUESTION 114

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

<https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/15292-scp.html>

NEW QUESTION 117

- (Exam Topic 2)

There are two managed legacy switches running that cannot be replaced or upgraded. These switches do not support cryptographic functions, but they are password protected. Which of the following should a network administrator configure to BEST prevent unauthorized access?

- A. Enable a management access list
- B. Disable access to unnecessary services.
- C. Configure a stronger password for access
- D. Disable access to remote management
- E. Use an out-of-band access method.

Answer: E

Explanation:

Using an out-of-band access method is the best way to prevent unauthorized access to the legacy switches that do not support cryptographic functions. Out-of-band access is a method of accessing a network device through a dedicated channel that is separate from the main network traffic. Out-of-band access can use physical connections such as serial console ports or dial-up modems, or logical connections such as VPNs or firewalls. Out-of-band access provides more security and reliability than in-band access, which uses the same network as the data traffic and may be vulnerable to attacks or failures. References:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book/>

NEW QUESTION 120

- (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 121

- (Exam Topic 2)

A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

- A. Omni
- B. Directional
- C. Yagi
- D. Parabolic

Answer: A

Explanation:

An omni antenna should be used by the AP to provide service in a radius surrounding a radio. An omni antenna is a type of antenna that has a 360-degree horizontal radiation pattern. It can provide wireless coverage in all directions from the antenna with varying degrees of vertical coverage. It is suitable for indoor environments where users are located around the AP1. References: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-omni-vs-direct.html> 1

NEW QUESTION 122

- (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 124

- (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 127

- (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 130

- (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 connect 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 131

- (Exam Topic 2)

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

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

Answer: A

Explanation:

AUP stands for Acceptable Use Policy, which is a policy that defines the rules and guidelines for using a network or service. A guest captive portal is a web page that requires users to agree to the AUP before accessing the Internet or other network resources. This is a common way to enforce security and legal compliance for guest users. References:
https://www.arubanetworks.com/techdocs/Instant_87_WebHelp/Content/instant-ug/captive-portal/captive-portal

NEW QUESTION 136

- (Exam Topic 2)

Which of the following is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines?

- A. Storage array
- B. Type 1 hypervisor
- C. Virtual machine
- D. Guest QS

Answer: B

Explanation:

A type 1 hypervisor is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines. A hypervisor is a software layer that enables virtualization by creating and managing virtual machines (VMs) on a physical host. A type 1 hypervisor, also known as a bare-metal hypervisor or a native hypervisor, runs directly on the host's hardware without requiring an underlying operating system (OS). It provides better performance and security than a type 2 hypervisor, which runs on top of an existing OS and relies on it for hardware access. References:
<https://www.vmware.com/topics/glossary/content/hypervisor>

NEW QUESTION 141

- (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 145

- (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 148

- (Exam Topic 2)

A technician is troubleshooting a workstation's network connectivity and wants to confirm which switchport corresponds to the wall jack the PC is using. Which of the following concepts would BEST help the technician?

- A. Consistent labeling
- B. Change management
- C. Standard work instructions
- D. Inventory management
- E. Network baseline

Answer: A

Explanation:

Consistent labeling would be the concept that would best help the technician to confirm which switchport corresponds to the wall jack the PC is using. Consistent labeling is a practice of using standardized and descriptive labels for network devices, ports, cables, jacks, and other components. It can help with identifying, locating, and troubleshooting network issues. For example, a technician can use consistent labeling to trace a cable from a PC to a wall jack, and then from a patch panel to a switchport. References: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_6.html

NEW QUESTION 153

- (Exam Topic 2)

A network administrator is required to ensure that auditors have read-only access to the system logs, while systems administrators have read and write access to the system logs, and operators have no access to the system logs. The network administrator has configured security groups for each of these functional categories. Which of the following security capabilities will allow the network administrator to maintain these permissions with the LEAST administrative effort?

- A. Mandatory access control
- B. User-based permissions
- C. Role-based access
- D. Least privilege

Answer: C

Explanation:

Role-based access is a security capability that assigns permissions to users based on their roles or functions within an organization. It allows the network administrator to maintain these permissions with the least administrative effort, as they only need to configure the security groups for each role once and then assign users to those groups. Mandatory access control is a security capability that assigns permissions based on security labels or classifications, which requires more administrative effort to maintain. User-based permissions are a security capability that assigns permissions to individual users, which is not scalable or efficient for large organizations. Least privilege is a security principle that states that users should only have the minimum level of access required to perform their tasks, which is not a security capability by itself.

NEW QUESTION 157

- (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 158

- (Exam Topic 2)

A network administrator wants to improve the security of the management console on the company's switches and ensure configuration changes made can be correlated to the administrator who configured them. Which of the following should the network administrator implement?

- A. Port security
- B. Local authentication
- C. TACACS+
- D. Access control list

Answer: C

Explanation:

TACACS+ is a protocol that provides centralized authentication, authorization, and accounting (AAA) for network devices and users. TACACS+ can help improve

the security of the management console on the company's switches by verifying the identity and credentials of the administrators, enforcing granular access policies and permissions, and logging the configuration changes made by each administrator. This way, the network administrator can ensure only authorized and authenticated users can access and modify the switch settings, and also track and correlate the changes made by each user. References: <https://www.comptia.org/blog/what-is-tacacs>

NEW QUESTION 163

- (Exam Topic 2)

A firewall administrator is implementing a rule that directs HTTP traffic to an internal server listening on a non-standard socket Which of the following types of rules is the administrator implementing?

- A. NAT
- B. PAT
- C. STP
- D. SNAT
- E. ARP

Answer: B

Explanation:

The firewall administrator is implementing a PAT (Port Address Translation) rule that directs HTTP traffic to an internal server listening on a non-standard socket. PAT is a type of NAT (Network Address Translation) that allows multiple devices to share a single public IP address by using different port numbers. PAT can also be used to redirect traffic from one port to another port on the same or different IP address. This can be useful for security or load balancing purposes. For example, a firewall administrator can configure a PAT rule that redirects HTTP traffic (port 80) from the public IP address of the firewall to an internal server that listens on a non-standard port (such as 8080) on its private IP address. References: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html>

NEW QUESTION 164

- (Exam Topic 2)

A company requires a disaster recovery site to have equipment ready to go in the event of a disaster at its main datacenter. The company does not have the budget to mirror all the live data to the disaster recovery site. Which of the following concepts should the company select?

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

Answer: C

Explanation:

A warm site is a type of disaster recovery site that has equipment ready to go in the event of a disaster at the main datacenter, but does not have live data or applications. A warm site requires some time and effort to restore the data and services from backups, but it is less expensive than a hot site that has live data and applications. A cold site is a disaster recovery site that has no equipment or data, and requires a lot of time and money to set up after a disaster. A cloud site is a disaster recovery site that uses cloud computing resources to provide data and services, but it may have issues with bandwidth, latency, security, and cost. References: <https://www.comptia.org/blog/what-is-a-warm-site>

NEW QUESTION 169

- (Exam Topic 2)

A network administrator has been directed to present the network alerts from the past week to the company's executive staff. Which of the following will provide the BEST collection and presentation of this data?

- A. A port scan printout
- B. A consolidated report of various network devices
- C. A report from the SIEM tool
- D. A report from a vulnerability scan done yesterday

Answer: C

Explanation:

SIEM stands for Security Information and Event Management, which is a tool that collects, analyzes, and correlates data from various network devices and sources to provide alerts and reports on security incidents and events. A report from the SIEM tool can provide a comprehensive overview of the network alerts from the past week to the executive staff, highlighting any potential threats, vulnerabilities, or anomalies. References: <https://www.comptia.org/blog/what-is-siem>

NEW QUESTION 174

- (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 177

- (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 178

- (Exam Topic 2)

Which of the following technologies allows traffic to be sent through two different ISPs to increase performance?

- A. Fault tolerance
- B. Quality of service
- C. Load balancing
- D. Port aggregation

Answer: C

Explanation:

Load balancing is a technology that allows traffic to be sent through two different ISPs to increase performance. Load balancing is a process of distributing network traffic across multiple servers or links to optimize resource utilization, throughput, latency, and reliability. Load balancing can be implemented at different layers of the OSI model, such as layer 4 (transport) or layer 7 (application). Load balancing can also be used for outbound traffic by using multiple ISPs and routing protocols such as BGP (Border Gateway Protocol) to select the best path for each packet. References:

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/border-gateway-protocol-bgp/prod_white_

NEW QUESTION 179

- (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 181

- (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 10m1s. 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 184

- (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 188

- (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 191

- (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 192

- (Exam Topic 2)

A customer wants to segregate the traffic between guests on a hypervisor. Which of the following does a technician need to configure to meet the requirement?

- A. Virtual switches
- B. OSPF routing
- C. Load balancers
- D. NIC teaming
- E. Fibre Channel

Answer: A

Explanation:

A virtual switch is a software-based switch that connects virtual machines on a hypervisor. A virtual switch can create and manage VLANs, which are logical segments of a network that isolate traffic between different groups of devices. A customer can use virtual switches to segregate the traffic between guests on a hypervisor by creating a separate VLAN for each guest and assigning it to a virtual switch port. References: <https://www.comptia.org/blog/what-is-a-virtual-switch>

NEW QUESTION 196

- (Exam Topic 2)

A small, family-run business uses a single SOHO router to provide Internet and WiFi to its employees. At the start of a new week, employees come in and find their usual WiFi network is no longer available, and there is a new wireless network to which they cannot connect. Given that information, which of the following should have been done to avoid this situation?

- A. The device firmware should have been kept current.
- B. Unsecure protocols should have been disabled.

- C. Parental controls should have been enabled
- D. The default credentials should have been changed

Answer: D

Explanation:

The default credentials are the username and password that come with a device or service when it is first installed or configured. They are often easy to guess or find online, which makes them vulnerable to unauthorized access or attacks. The default credentials should be changed to something unique and strong as soon as possible to avoid this situation. If the default credentials were not changed, someone could have accessed the SOHO router and changed the WiFi settings without the employees' knowledge. References: <https://www.comptia.org/blog/network-security-basics-6-easy-ways-to-protect-your-network>

NEW QUESTION 200

- (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 201

- (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 204

- (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 208

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 213

- (Exam Topic 3)

Which of the following is used to elect an STP root?

- A. A bridge ID
- B. A bridge protocol data unit
- C. Interface port priority
- D. A switch's root port

Answer: B

Explanation:

"Using special STP frames known as bridge protocol data units (BPDUs), switches communicate with other switches to prevent loops from happening in the first place. Configuration BPDUs establish the topology, where one switch is elected root bridge and acts as the center of the STP universe. Each switch then uses the root bridge as a reference point to maintain a loop-free topology."

NEW QUESTION 215

- (Exam Topic 3)

Which of the following needs to be tested to achieve a Cat 6a certification for a company's data cabling?

- A. RJ11
- B. LC ports
- C. Patch panel
- D. F-type connector

Answer: D

NEW QUESTION 216

- (Exam Topic 3)

An administrator is investigating reports of network slowness in a building. While looking at the uplink interface statistics in the switch's CLI, the administrator discovers the uplink is at 100% utilization. However, the administrator is unsure how to identify what traffic is causing the saturation. Which of the following tools should the administrator utilize to identify the source and destination addresses of the traffic?

- A. SNMP
- B. Traps
- C. Syslog
- D. NetFlow

Answer: D

Explanation:

To identify the source and destination addresses of the traffic causing network saturation, the network administrator should use a network protocol analyzer that supports the NetFlow protocol. NetFlow is a network protocol that collects IP traffic information as it enters or exits an interface and sends it to a NetFlow collector for analysis. This data includes the source and destination addresses of the traffic, the ports used, and the number of bytes and packets transferred.

Therefore, the correct answer is option D, NetFlow.

Reference: CompTIA Network+ Study Guide, Exam N10-007, Fourth Edition, by Todd Lammle (Chapter 6: Network Devices)

NEW QUESTION 218

- (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 223

- (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 225

- (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 230

- (Exam Topic 3)

A technician manages a DHCP scope but needs to allocate a portion of the scope's subnet for statically assigned devices. Which of the following DHCP concepts would be BEST to use to prevent IP address conflicts?

- A. Dynamic assignment
- B. Exclusion range
- C. Address reservation
- D. IP helper

Answer: B

Explanation:

To prevent IP address conflicts when allocating a portion of a DHCP scope's subnet for statically assigned devices, it is recommended to use the concept of DHCP exclusion ranges. DHCP exclusion ranges allow a DHCP administrator to specify a range of IP addresses within the scope that should not be assigned to DHCP clients. This can be useful in situations where some devices on the network need to be assigned static IP addresses, as it ensures that the statically assigned addresses do not overlap with addresses assigned by the DHCP server. To set up a DHCP exclusion range, the administrator needs to specify the start and end IP addresses of the range, as well as the subnet mask. The DHCP server will then exclude the specified range of addresses from its pool of available addresses, and will not assign them to DHCP clients. By using DHCP exclusion ranges, the technician can ensure that the statically assigned addresses do not conflict with addresses assigned by the DHCP server, and can prevent IP address conflicts on the network.

Anthony Sequeira

"Another frequent configuration you might make in a DHCP implementation is to configure an exclusion range. This is a portion of the address pool that you never want leased out to clients in the network. Perhaps you have numbered your servers 192.168.1.1–192.168.1.10. Because the servers are statically configured with these addresses, you exclude these addresses from the 192.168.1.0/24 pool of addresses."

Mike Meyers

"Exclusion ranges represent an IP address or range of IP addresses from the pool of addresses that are not to be given out by the DHCP server. Exclusions should be made for the static addresses manually configured on servers and router interfaces, so these IP addresses won't be offered to DHCP clients."

NEW QUESTION 232

- (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 234

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 237

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

NEW QUESTION 239

- (Exam Topic 3)

Which of the following provides guidance to an employee about restricting non-business access to the company's videoconferencing solution?

- A. Acceptable use policy
- B. Data loss prevention
- C. Remote access policy
- D. Standard operating procedure

Answer: A

Explanation:

An acceptable use policy (AUP) is a set of rules that outline the proper and improper use of an organization's resources, such as its videoconferencing solution. An AUP can provide guidance to employees about what is expected of them when using the organization's videoconferencing solution, including restricting non-business access to it.

NEW QUESTION 241

- (Exam Topic 3)

Which of the following OSI model layers would allow a user to access and download files from a remote computer?

- A. Session
- B. Presentation
- C. Network
- D. Application

Answer: D

Explanation:

The application layer of the OSI model (Open Systems Interconnection) is responsible for providing services to applications that allow users to access and download files from a remote computer. These services include file transfer, email, and web access, as well as other related services. In order for a user to access and download files from a remote computer, the application layer must provide the necessary services that allow the user to interact with the remote computer.

NEW QUESTION 246

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 248

- (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 253

- (Exam Topic 3)

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

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

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

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

Answer: A

NEW QUESTION 254

- (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 258

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 259

- (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 261

- (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 263

- (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 265

- (Exam Topic 3)

An administrator needs to connect two laptops directly to each other using 802.11ac but does not have an AP available. Which of the following describes this configuration?

- A. Basic service set
- B. Extended service set
- C. Independent basic service set
- D. MU-MIMO

Answer: C

NEW QUESTION 269

- (Exam Topic 3)

Which of the following commands can be used to display the IP address, subnet address, gateway address, and DNS address on a Windows computer?

- A. netstat -a
- B. ifconfig
- C. ip addr
- D. ipconfig /all

Answer: D

Explanation:

The ipconfig command is a utility that allows you to view and modify the network configuration of a Windows computer. By running the command "ipconfig /all", you can view detailed information about the network configuration of your computer, including the IP address, subnet mask, default gateway, and DNS server addresses.

Option A (netstat -a) is a command that displays active network connections and their status, but it does not display IP address or other network configuration information. Option B (ifconfig) is a command used on Linux and Unix systems to view and modify network configuration, but it is not available on Windows. Option C (ip addr) is a command used on Linux and Unix systems to view and modify network configuration, but it is not available on Windows.

NEW QUESTION 272

- (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 275

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 278

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 280

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

NEW QUESTION 284

- (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 288

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

Answer: AE

NEW QUESTION 292

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 295

- (Exam Topic 3)

A network is secured and is only accessible via TLS and IPSec VPNs. Which of the following would need to be present to allow a user to access network resources on a laptop without logging in to the VPN application?

- A. Site-to-site
- B. Secure Shell
- C. In-band management
- D. Remote desktop connection

Answer: A

Explanation:

A site-to-site VPN is a type of VPN that connects two or more networks over the Internet using a secure tunnel. A site-to-site VPN allows users to access network resources on a laptop without logging in to the VPN application, as long as the laptop is connected to one of the networks in the VPN. A site-to-site VPN is transparent to the users and does not require any additional software or configuration on the client devices. References: Network+ Study Guide Objective 3.4: Explain the purposes and use cases for VPNs.

NEW QUESTION 297

- (Exam Topic 3)

On a network with redundant switches, a network administrator replaced one of the switches but was unable to get a connection with another switch. Which of the following should the administrator check after successfully testing the cable that was wired for TIA/EIA-568A on both ends?

- A. If MDIX is enabled on the new switch

- B. If PoE is enabled
- C. If a plenum cable is being used
- D. If STP is disabled on the switches

Answer: A

Explanation:

Auto-MDIX (or medium dependent interface crossover) is a feature that automatically detects the type of cable connection and configures the interface accordingly (i.e. straight-through or crossover). This ensures that the connection between the two switches is successful. This is referenced in the CompTIA Network+ Study Manual, page 519.

NEW QUESTION 302

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 303

- (Exam Topic 3)

A technician knows the MAC address of a device and is attempting to find the device's IP address. Which of the following should the technician look at to find the IP address? (Select TWO).

- A. ARP table
- B. DHCP leases
- C. IP route table
- D. DNS cache
- E. MAC address table
- F. STP topology

Answer: BE

NEW QUESTION 308

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 313

- (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 318

- (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 322

- (Exam Topic 3)

A network administrator is getting reports of some internal users who cannot connect to network resources. The users state they were able to connect last week, but not today. No changes have been configured on the network devices or server during the last few weeks. Which of the following is the MOST likely cause of the issue?

- A. The client DHCP scope is fully utilized
- B. The wired network is experiencing electrical interference
- C. The captive portal is down and needs to be restarted
- D. SNMP traps are being received
- E. The packet counter on the router interface is high.

Answer: A

NEW QUESTION 325

- (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 330

- (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 333

- (Exam Topic 3)

A network engineer is investigating reports of poor performance on a videoconferencing application. Upon reviewing the report, the engineer finds that available bandwidth at the WAN connection is low.

Which Of the following is the MOST appropriate mechanism to handle this issue?

- A. Traffic shaping
- B. Flow control

- C. NetFlow
- D. Link aggregation

Answer: A

Explanation:

Traffic shaping is a congestion management method that regulates network data transfer by delaying the flow of less important or less desired packets¹. Traffic shaping can help to improve the performance of a videoconferencing application by prioritizing its packets over other types of traffic and smoothing out traffic bursts. Traffic shaping can also help to avoid packet loss and ensure fair allocation of bandwidth among different applications or users.

Flow control is a mechanism that prevents a sender from overwhelming a receiver with more data than it can handle. Flow control can help to avoid buffer overflow and data loss, but it does not prioritize different types of traffic or smooth out traffic bursts. Flow control operates at the data link layer or the transport layer, while traffic shaping operates at the network layer or above.

NetFlow is a protocol that collects and analyzes network traffic data for monitoring and troubleshooting purposes². NetFlow can help to identify the sources, destinations, volumes, and types of traffic on a network, but it does not regulate or shape the traffic flow. NetFlow operates at the network layer or above.

Link aggregation is a technique that combines multiple physical links into one logical link for increased bandwidth, redundancy, and load balancing. Link aggregation can help to improve the performance of a videoconferencing application by providing more available bandwidth at the WAN connection, but it does not prioritize different types of traffic or smooth out traffic bursts. Link aggregation operates at the data link layer.

NEW QUESTION 337

- (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 342

- (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 346

- (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 351

- (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 352

- (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 357

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 358

- (Exam Topic 3)

A systems administrator wants to use the least amount of equipment to segment two departments that have cables terminating in the same room. Which of the following would allow this to occur?

- A. A load balancer
- B. A proxy server
- C. A Layer 3 switch
- D. A hub
- E. A Layer 7 firewall
- F. The RSSI was not strong enough on the link

Answer: C

NEW QUESTION 360

- (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 364

- (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 368

- (Exam Topic 3)

An IT technician successfully connects to the corporate wireless network at a bank. While performing some tests, the technician observes that the physical

address of the DHCP server has changed even though the network connection has not been lost. Which of the following would BEST explain this change?

- A. Server upgrade
- B. Duplicate IP address
- C. Scope exhaustion
- D. Rogue server

Answer: D

Explanation:

A rogue server is a DHCP server on a network that is not under the administrative control of the network staff 1. It may provide incorrect IP addresses or other network configuration information to devices on the network, causing them to lose connectivity or be vulnerable to attacks2. The physical address of the DHCP server may change if a rogue server takes over the role of assigning IP addresses to devices on the network. This can be detected by monitoring DHCP traffic or using tools such as RogueChecker2.

NEW QUESTION 371

- (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 375

- (Exam Topic 3)

Which of the following layers of the OSI model receives data from the application layer and converts it into syntax that is readable by other devices on the network?

- A. Layer 1
- B. Layer 3
- C. Layer 6
- D. Layer 7

Answer: C

NEW QUESTION 377

- (Exam Topic 3)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 382

- (Exam Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 385

- (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 387

- (Exam Topic 3)

A network engineer needs to create a subnet that has the capacity for five VLANs. with the following number of clients to be allowed on each:

VLAN 10	50 users
VLAN 20	35 users
VLAN 30	20 users
VLAN 40	75 users
VLAN 50	130 users

Which of the following is the SMALLEST subnet capable of this setup that also has the capacity to double the number of clients in the future?

- A. 10.0.0.0/21
- B. 10.0.0.0/22
- C. 10.0.0.0/23
- D. 10.0.0.0/24

Answer: B

NEW QUESTION 391

- (Exam Topic 3)

Which of the following can be used to decrease latency during periods of high utilization of a firewall?

- A. Hot site
- B. NIC teaming
- C. HA pair
- D. VRRP

Answer: B

Explanation:

NIC Teaming, also known as load balancing and failover (LBFO), allows multiple network adapters on a computer to be placed into a team for the following purposes: (<https://www.bing.com/search?q=what+is+nic+teaming+used+for%3F&form=QBLH&sp=-1&pq=what+is+nic>)

NEW QUESTION 395

.....

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