Exam Questions N10-009

CompTIA Network+ Exam

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

NEW QUESTION 1
- (Topic 3)
Which of the following can have multiple VLAN interfaces?

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

Answer: B

NEW QUESTION 2
- (Topic 3)
Which of the following is the MOST appropriate use case for the deployment of a clientless VPN?

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

Answer: A

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

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

Answer: C

Explanation:
An SVI, or switched virtual interface, is a logical interface that is created on a Layer 3- capable device, such as a multilayer switch or a router. An SVI is associated with a VLAN and can be used to route traffic between different VLANs on the same device or across multiple devices. An SVI can also provide management access, security features, and quality of service (QoS) for the VLAN. An SVI is different from a physical interface, which is a port that connects to a physical device or network. A physical interface can be used for trunking, which is a method of carrying multiple VLANs over a single link, or for connecting to a single VLAN. An SVI is also different from a subinterface, which is a logical division of a physical interface that can be assigned to different VLANs.
References:
? VLANs and Trunking – N10-008 CompTIA Network+ : 2.11
? Switched Virtual Interfaces – N10-008 CompTIA Network+ : 2.22

NEW QUESTION 4
- (Topic 3)
A network is experiencing extreme latency when accessing a particular website. Which of the following commands will BEST help identify the issue?

A. ipconfig
B. netstat
C. tracert
D. ping

Answer: C

NEW QUESTION 5
- (Topic 3)
A technician is trying to install a VolP phone, but the phone is not turning on. The technician checks the cable gong from the phone to the switch, and the cable is good. Which of the following actions IS needed for this phone to work?

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

Answer: A

NEW QUESTION 6
- (Topic 3)
Which of the following IP packet header fields is the mechanism for ending loops at Layer 3?

A. Checksum
B. Type
C. Time-to-live
D. Protocol

Answer: C

Explanation:
The time-to-live (TTL) field is the mechanism for ending loops at Layer 3, which is the network layer of the OSI model. The TTL field is an 8-bit field that indicates the maximum time or number of hops that an IP packet can travel before it is discarded. Every time an IP packet passes through a router, the router decrements the TTL value by one. If the TTL value reaches zero, the router drops the packet and sends an ICMP message back to the source, informing that the packet has expired. This way, the TTL field prevents an IP packet from looping endlessly in a network with routing errors or cycles123.
The other options are not mechanisms for ending loops at Layer 3. The checksum field is a 16-bit field that is used to verify the integrity of the IP header. The checksum field is calculated by adding all the 16-bit words in the header and taking the one's complement of the result. If the checksum field does not match the calculated value, the IP packet is considered corrupted and discarded12. The type field, also known as the type of service (TOS) or differentiated services code point (DSCP) field, is an 8-bit field that is used to specify the quality of service (QoS) or priority of the IP packet. The type field can indicate how the packet should be handled in terms of delay, throughput, reliability, or cost12. The protocol field is an 8-bit field that is used to identify the transport layer protocol that is encapsulated in the IP packet. The protocol field can indicate whether the payload is a TCP segment, a UDP datagram, an ICMP message, or another protocol12.

NEW QUESTION 7
- (Topic 3)
Which of the following types of attacks can be used to gain credentials by setting up rogue APs with identical corporate SSIDs?

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

Answer: B

NEW QUESTION 8
- (Topic 3)
A network engineer needs to create a subnet that has the capacity for five VLANs. with the following number of clients lo 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 9
- (Topic 3)
A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light
does not come on. Which of the following should a technician try first to troubleshoot this issue?

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

Answer: A

Explanation:
One of the most common causes of fiber connectivity issues is the reversal of the fibers. This means that the transmit (TX) and receive (RX) ports on one end of the fiber link are not matched with the corresponding ports on the other end. For example, if the TX port on one device is connected to the TX port on another device, and the same for the RX ports, then the devices will not be able to communicate with each other. This can result in no indicator light, no link, or no data transmission12.
To troubleshoot this issue, the technician should first try to reverse the fibers. This can be done by swapping the connectors at one end of the fiber patch cable, or by using a crossover adapter or cable that reverses the polarity of the fibers. The technician should then check if the indicator light comes on and if the devices can communicate properly12. The other options are not the first steps to troubleshoot this issue. Reterminating the fibers is a time-consuming and costly process that should be done only if there is evidence of physical damage or poor quality of the termination. Verifying the fiber size is not relevant in this scenario, as multimode fiber is compatible with multimode fiber, and any mismatch in core diameter or bandwidth would result in high attenuation, not complete loss of signal. Examining the cable runs for visual faults is a useful technique, but it requires a special tool called a visual fault locator (VFL) that emits a visible red light through the fiber and shows any breaks or bends along the cable. However, a VFL cannot detect polarity issues or connector problems, so it is not sufficient to troubleshoot this issue

NEW QUESTION 10
- (Topic 3)
Which of the following protocols is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links?

A. OSPF

B. RIPv2
C. QoS
D. STP

Answer: A

NEW QUESTION 10
- (Topic 3)
A technician is troubleshooting network connectivity from a wall jack. Readings from a multimeter indicate extremely low ohmic values instead of the rated impedance from the switchport. Which of the following is the MOST likely cause of this issue?

A. Incorrect transceivers
B. Faulty LED
C. Short circuit
D. Upgraded OS version on switch

Answer: C

Explanation:
A short circuit is a condition where two conductors in a circuit are connected unintentionally, creating a low resistance path for the current. This causes the voltage to drop and the current to increase, which can damage the circuit or cause a fire. A multimeter can measure the resistance or impedance of a circuit, and if it shows extremely low values, it indicates a short circuit.

NEW QUESTION 11
- (Topic 3)
Which of the following technologies would MOST likely De used to prevent the loss of connection between a virtual server and network storage devices?

A. Multipathing
B. VRRP
C. Port aggregation
D. NIC teaming

Answer: D

Explanation:
NIC teaming is a technology that allows multiple network interface cards (NICs) to work together as a single logical interface, providing redundancy and load balancing. This can prevent the loss of connection between a virtual server and network storage devices if one of the NICs fails or becomes disconnected.
References: [CompTIA Network+ Certification Exam Objectives], Domain 2.0 Networking Concepts, Objective 2.5: Explain the purposes and use cases for advanced networking devices, Subobjective: NIC bonding/teaming

NEW QUESTION 13
- (Topic 3)
A large number of PCs are obtaining an APIPA IP address, and a number of new computers were added to the network. Which of the following is MOST likely causing the PCs to obtain an APIPA address?

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

Answer: D

Explanation:
DHCP scope exhaustion means that there are no more available IP addresses in the DHCP server's pool of addresses to assign to new devices on the network. When this happens, the devices will use APIPA (Automatic Private IP Addressing) to self-configure an IP address in the range of 169.254.0.1 to 169.254.255.2541. These addresses are not routable and can only communicate with other devices on the same local network.
A rogue DHCP server (A) is an unauthorized DHCP server that can cause IP address conflicts or security issues by assigning IP addresses to devices on the network. A network collision (B) is a situation where two or more devices try to send data on the same network segment at the same time, causing interference and data loss. Incorrect DNS settings © can prevent devices from resolving domain names to IP addresses, but they do not affect the DHCP process.

NEW QUESTION 17
- (Topic 3)
While troubleshooting a network, a VoIP systems engineer discovers a significant inconsistency in the amount of time required for data to reach its destination and return. Which of the following terms best describes this issue?

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

Answer: C

Explanation:
Jitter is the variation in the delay of data packets over a network. It is caused by factors such as network congestion, routing changes, packet loss, or improper queuing. Jitter affects the quality of VoIP calls because it can cause gaps, distortion, or out-of-order delivery of voice data. Jitter can be measured by the difference between the expected and actual arrival times of packets2. To reduce jitter, VoIP systems use buffers to store and reorder packets before playing them back. However, too much buffering can also increase latency, which is the total time it takes for data to travel from one point to another3.
References2 - VoIP Troubleshooting: 5 Fixes for Common Connection Issues - Nextiva3 - Troubleshooting VoIP — Is it You or the Network? - PingPlotter

NEW QUESTION 20
- (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 24
- (Topic 3)
Which of the following is a valid and cost-effective solution to connect a fiber cable into a network switch without available SFP ports?

A. Use a media converter and a UTP cable
B. Install an additional transceiver module and use GBICs
C. Change the type of connector from SC to F-type
D. Use a loopback adapter to make the connection

Answer: A

NEW QUESTION 27
- (Topic 3)
Which of the following DNS records maps an alias to a true name?

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

Answer: D

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

NEW QUESTION 31
- (Topic 3)
A network administrator is reviewing the network device logs on a syslog server. The messages are normal but the stamps on the messages are incorrect. Which of the following actions should the administrator take to ensure the log message time stamps are correct?

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

Answer: A

NEW QUESTION 32
- (Topic 3)
Which of the following BEST describes a north-south traffic flow?

A. A public internet user accessing a published web server
B. A database server communicating with another clustered database server
C. A Layer 3 switch advertising routes to a router
D. A management application connecting to managed devices

Answer: A

Explanation:
A north-south traffic flow is a term used to describe the communication between a user or device outside the network and a server or service inside the network. For example, a public internet user accessing a published web server is a north-south traffic flow. This type of traffic flow typically crosses the network perimeter and requires security measures such as firewalls and VPNs. References: CompTIA Network+ N10-008 Certification Study Guide, page 16; The Official CompTIA Network+ Student Guide (Exam N10-008), page 1- 9.
North-south traffic flow refers to the flow of traffic between the internal network of an organization and the external world. This type of traffic typically flows from the internet to the organization's internal network, and back again.
Examples of north-south traffic flow include:
? A public internet user accessing a published web server
? A remote employee connecting to a VPN
? An email client sending email to an external server
? A customer connecting to an e-commerce website

References:
? CompTIA Network+ N10-008 Exam Objectives, Version 5.0, August 2022, page 12
? CompTIA Network+ Certification Study Guide, Seventh Edition, Todd Lammle, Sybex, 2022, page 17

NEW QUESTION 35
- (Topic 3)
Which of the following, in addition to a password, can be asked of a user for MFA?

A. PIN
B. Favorite color
C. Hard token
D. Mother's maiden name

Answer: A

Explanation:
MFA stands for Multi-Factor Authentication, which is a method of verifying the identity of a user by requiring two or more pieces of evidence that belong to different categories: something the user knows, something the user has, or something the user is. A password is something the user knows, and it is usually combined with another factor such as a PIN (Personal Identification Number) or a hard token (a physical device that generates a one- time code) that the user has. A favorite color or a mother’s maiden name are not suitable for MFA, as they are also something the user knows and can be easily guessed or compromised.
References
? 1: Multi-Factor Authentication – N10-008 CompTIA Network+ : 3.1
? 2: CompTIA Network+ Certification Exam Objectives, page 13
? 3: CompTIA Network+ N10-008 Certification Study Guide, page 250
? 4: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 14

NEW QUESTION 36
- (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 39
- (Topic 3)
Network traffic is being compromised by DNS poisoning every time a company's router is connected to the internet. The network team detects a non-authorized DNS server being assigned to the network clients and remediates the incident by setting a trusted DNS server, but the issue occurs again after internet exposure. Which of the following best practices should be implemented on the router?

A. Change the device's default password.
B. Disable router advertisement guard.
C. Activate control plane policing.
D. Disable unneeded network services.

Answer: A

NEW QUESTION 40
- (Topic 3)
A company has multiple offices around the world. The computer rooms in some office locations are too warm Dedicated sensors are in each room, but the process of checking each sensor takes a long time. Which of the following options can the company put In place to automate temperature readings with internal resources?

A. Implement NetFlow.
B. Hire a programmer to write a script to perform the checks
C. Utilize ping to measure the response.
D. Use SNMP with an existing collector server

Answer: D

Explanation:
SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a management server. By using SNMP, the company can set up an SNMP agent on each sensor, which will report its temperature readings to an existing collector server. This will enable the company to monitor the temperatures of all their sensors in real-time without the need for manual checks. Additionally, SNMP's scalability means that even if the company adds more rooms or sensors, the existing system can be easily expanded to accommodate them.

NEW QUESTION 41
- (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 44
- (Topic 3)
A network engineer designed and implemented a new office space with the following characteristics:

Building construction type:	Brick
Layout:	10,764sq ft (1,000sq m) commercial office space
Users:	50
Servers:	2
Laptops:	50

One month after the office space was implemented, users began reporting dropped signals when entering another room and overall poor connections to the 5GHz network. 'which of the following should the engineer do to best resolve the issue?

A. use non-overlapping channels
B. Reconfigure the network to support 2.4GHz_
C. Upgrade to WPA3.
D. Change to directional antennas-

Answer: D

Explanation:
The best solution to resolve the issue of dropped signals and poor connections to the 5GHz network is to change to directional antennas. Directional antennas are antennas that focus the wireless signal in a specific direction, increasing the range and strength of the signal. Directional antennas are suitable for environments where there are obstacles or interference that can weaken or block the wireless signal. In the image, the office space has several walls and doors that can reduce the signal quality of the 5GHz network, which has a shorter wavelength and higher frequency than the 2.4GHz network. By using directional antennas, the network engineer can aim the wireless signal towards the desired areas and avoid the signal loss caused by the walls and doors. References: CompTIA Network+ N10-008 Certification Study Guide, page 76; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-19.

NEW QUESTION 49
- (Topic 3)
A network administrator needs to monitor traffic on a specific port on a switch. Which of the following should the administrator configure to accomplish the task?

A. Port security
B. Port tagging
C. Port mirroring
D. Media access control

Answer: C

Explanation:
Port mirroring is a technique that allows a network administrator to monitor the traffic on a specific port on a switch by sending a copy of the packets seen on that port to another port where a monitoring device is connected1. Port mirroring can be used to analyze and debug data, diagnose errors, or perform security audits on the network without affecting the normal operation of the switch

NEW QUESTION 53
- (Topic 3)
Which of the following is the most secure connection used to inspect and provide controlled internet access when remote employees are connected to the corporate network?

A. Site-to-site VPN
B. Full-tunnel VPN
C. Split-tunnel VPN
D. SSH

Answer: B

Explanation:
A full-tunnel VPN is a type of virtual private network (VPN) that encrypts and routes all the traffic from the remote device to the corporate network, regardless of the destination or protocol. This provides a secure connection for the remote employees to access the corporate resources, as well as inspect and control the internet access through the corporate firewall and proxy servers. A full-tunnel VPN also prevents any leakage of sensitive data or exposure to malicious attacks from the public internet. A full-tunnel VPN is more secure than a split-tunnel VPN, which only encrypts and routes the traffic destined for the corporate network, while allowing the traffic for other destinations to bypass the VPN and use the local internet connection. A site-to-site VPN is a type of VPN that connects two or more

networks, such as branch offices or data centers, over the internet. It is not suitable for connecting individual remote employees to the corporate network. SSH stands for Secure Shell, and it is a protocol that allows secure remote login and command execution over an encrypted channel. It is not a type of VPN, and it does not provide
controlled internet access. References: CompTIA Network+ N10-008 Cert Guide, Chapter 5, Section 5.3

NEW QUESTION 58
- (Topic 3)
A network administrator is concerned about a rainbow table being used to help access network resources. Which of the following must be addressed to reduce the likelihood of a rainbow table being effective?

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

Answer: A

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

NEW QUESTION 60
- (Topic 3)
A technician is working on a ticket for a user in the human resources department who received a new PC that does not connect to the internet. All users in human resources can access the
internet. The technician can ping the PC from the human resources router but not from the IT network. Which of the following is the most likely cause of the issue?

A. Duplicate IP address
B. Misconfigured RIP
C. Improper VLAN assignment
D. Incorrect default gateway

Answer: D

Explanation:
An incorrect default gateway can cause a PC to not connect to the internet, because the default gateway is the device that routes traffic from the local network to other networks. If the PC has a wrong default gateway configured, it may not be able to reach the internet router or the IT network router. The technician can ping the PC from the human resources router because they are on the same local network, but not from the IT network router because they are on different networks.
A duplicate IP address can cause a PC to not communicate with other devices on the same network, because the IP address is the unique identifier of a device on a network. If two devices have the same IP address, they may cause IP conflicts and packet loss. However, a duplicate IP address would not prevent the technician from pinging the PC from the human resources router, because they are on the same network.
A misconfigured RIP can cause a router to not learn or advertise routes to other networks, because RIP is a routing protocol that dynamically exchanges routing information between routers. If a router has a wrong RIP configuration, it may not be able to reach or share routes with other routers. However, a misconfigured RIP would not affect the PC's connectivity to the internet, because the PC does not use RIP.
An improper VLAN assignment can cause a PC to not communicate with other devices on the same or different networks, because a VLAN is a logical segmentation of a network that isolates traffic based on criteria such as function, security, or performance. If a PC is assigned to a wrong VLAN, it may not be able to access the resources or services that it needs. However, an improper VLAN assignment would not prevent the technician from pinging the PC from the human resources router, because they are on the same physical network.
References
What is a Default Gateway?
What's an IP Conflict and How Do You Resolve It? What is RIP (Routing Information Protocol)?
What is a VLAN? How to Set Up a VLAN Network
CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION 61
- (Topic 3)
A network engineer needs to change an entire subnet of SLAAC-configured workstation addresses. Which of the following methods would be the best for the engineer to use?

A. Change the address prefix in ARP in order for the workstations to retrieve their new addresses.
B. Change the address prefix in a router in order for the router to advertise the new prefix with an ND.
C. Change the address prefix scope in a DHCP server in order for the workstations to retrieve their new addresses.
D. Change the workstations' address prefix manually because an automated method does not exist.

Answer: B

Explanation:
SLAAC (Stateless Address Autoconfiguration) is a mechanism that enables each host on the network to auto-configure a unique IPv6 address without any device keeping track of which address is assigned to which node12. SLAAC uses link-local addresses and the interface's MAC address or a random number to generate the host portion of the IPv6 address2. SLAAC also relies on Router Solicitation (RS) and Router Advertisement (RA) messages to obtain the network prefix and other information from a router12. Therefore, to change an entire subnet of SLAAC-configured workstation addresses, the network engineer needs to change the address prefix in a router and let the router advertise the new prefix with an ND (Neighbor Discovery) message. This way, the workstations will receive the new prefix and update their IPv6 addresses accordingly3.
References1 - IPv6 Stateless Address Auto-configuration (SLAAC) | NetworkAcademy.io2 - IPv6 SLAAC – Stateless Address Autoconfiguration - Study-CCNA3 - Mastering IPv6
SLAAC Concepts and Configuration - Cisco Press

NEW QUESTION 65
- (Topic 3)
To access production applications and data, developers must first connect remotely to a different server From there, the developers are able to access production data Which of the following does this BEST represent?

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

Answer: E

NEW QUESTION 67
- (Topic 3)
Which of the following ports is a secure protocol?

A. 20
B. 23
C. 443
D. 445

Answer: C

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

NEW QUESTION 69
- (Topic 3)
During a risk assessment which of the following should be considered when planning to mitigate high CPU utilization of a firewall?

A. Recovery time objective
B. Uninterruptible power supply
C. NIC teaming
D. Load balancing

Answer: D

Explanation:
The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs. This does nothing to help with CPU utilization. Load balancing does this.

NEW QUESTION 71
- (Topic 3)
Which of the following should be used to manage outside cables that need to be routed to various multimode uplinks?

A. Fiber distribution panel
B. 110 punchdown block
C. PDU
D. TIA/EIA-568A patch bay
E. Cat 6 patch panel

Answer: A

Explanation:
A fiber distribution panel is a device that provides a central location for connecting and managing fiber optic cables and optical modules. It can support various types and speeds of fiber optic links, including multimode uplinks. Therefore, a fiber distribution panel should be used to manage outside cables that need to be routed to various multimode uplinks.

NEW QUESTION 75
- (Topic 3)
A Chief Executive Officer and a network administrator came to an agreement With a vendor to purchase new equipment for the data center A document was drafted so all parties would be Informed about the scope of the project before It started. Which of the following terms BEST describes the document used?

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

Answer: B

Explanation:
The document used to inform all parties about the scope of the project before it starts is likely a project charter.
A project charter is a document that outlines the key aspects of a project, including the project's objectives, scope, stakeholders, and resources. It serves as a

formal agreement between the project team and the stakeholders, and helps to define the project's goals and constraints.
A project charter typically includes information about the project's scope, including the specific deliverables that are expected and any constraints or limitations that may impact the project. It may also include details about the project team and stakeholders, the project schedule and budget, and the roles and responsibilities of each party.
By creating a project charter, the Chief Executive Officer and the network administrator can ensure that all parties involved in the project have a clear understanding of the project's goals and objectives, and can help to prevent misunderstandings or miscommunications during the project.
What is in a project charter?
A project charter is a formal short document that states a project exists and provides project managers with written authority to begin work. A project charter document describes a project to create a shared understanding of its goals, objectives and resource requirements before the project is scoped out in detail.
What are the 5 elements of the project charter?
What Are the Contents of a Project Charter? A project charter should always include an overview, an outline of scope, an approximate schedule, a budget estimate, anticipated risks, and key stakeholders

NEW QUESTION 80
- (Topic 3)
Network connectivity in an extensive forest reserve was achieved using fiber optics. A network fault was detected, and now the repair team needs to check the integrity of the fiber cable. Which of me following actions can reduce repair time?

A. Using a tone generator and wire map to determine the fault location
B. Using a multimeter to locate the fault point
C. Using an OTDR In one end of the optic cable to get the liber length information
D. Using a spectrum analyzer and comparing the current wavelength with a working baseline

Answer: C

NEW QUESTION 83
- (Topic 3)
Which of the following issues are present with RIPv2? (Select TWO).

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

Answer: BC

Explanation:
The disadvantages of RIP (Routing Information Protocol) include the following.
---Outdated, insecure, and slow. This is your parents' protocol. It was a thing before the Web was born.
---The more well-known problem of the 15 hop limitation in which data must travel
---Convergence time is terrible for information propagation in a network
---Metrics. It determines the number of hops from source to destination, and gives no regard to other factors when determining the best path for data to travel
---Overhead. A good example would be routing tables. These are broadcast at half-minute intervals to other routers regardless of whether the data has changed or not. It's essentially like those old cartoons where the town guard in the walled city cries out, '10 o' the clock and all is well!'.
RIPv2 introduced more security and reduced broadcast traffic, which is relevant for some available answers here.

NEW QUESTION 84
- (Topic 3)
A network technician is troubleshooting a connectivity issue. All users within the network report that they are unable to navigate to websites on the internet; however, they can still access local network resources. The technician issues a command and receives the following results:

```
Pinging comptia.com [172.67.217.56] with 32 bytes of data:
Reply from 172.67.217.56: TTL expired in transit.
Reply from 172.67.217.56: TTL expired in transit.
Reply from 172.67.217.56: TTL expired in transit.
Reply from 172.67.217.56: TTL expired in transit.
```

Which of the following best explains the result of this command?

A. Incorrect VLAN settings
B. Upstream routing loop
C. Network collisions
D. DNS misconfiguration

Answer: D

Explanation:
The users are unable to navigate to websites on the internet but can access local network resources, indicating a possible DNS issue. The ping command result showing “TTL expired in transit” suggests that packets are not reaching their destination due to a DNS misconfiguration that is not resolving website names into IP addresses correctly3. A possible solution is to check and correct the DNS server settings on the network devices4.
References: 3: What does “TTL expired in transit” mean?54: CompTIA Network+ N10-008 Cert Guide - Chapter 14: Network Monitoring2

NEW QUESTION 89
- (Topic 3)
A firewall administrator observes log entries of traffic being allowed to a web server on port 80 and port 443. The policy for this server is to only allow traffic on port

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

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

Answer: A

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

NEW QUESTION 93
- (Topic 3)
An employee working in a warehouse facility is experiencing interruptions in mobile applications while walking around the facility. According to a recent site survey, the WLAN comprises autonomous APs that are directly connected to the internet, providing adequate signal coverage. Which of the following is the BEST solution to improve network stability?

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

Answer: A

Explanation:
Client roaming refers to the ability of a wireless device to seamlessly connect to a different access point (AP) as the user moves around the facility. This can help to improve network stability and reduce interruptions in mobile applications. An extended service deployment is a type of wireless network configuration that uses multiple APs to cover a large area, such as a warehouse facility. By using a wireless controller to manage the APs, the network can be better optimized for client roaming, which can improve network stability.
"Roaming With multiple WAPs in an ESS, clients will connect to whichever WAP has the strongest signal. As clients move through the space covered by the broadcast area, they will change WAP connections seamlessly, a process called roaming."

NEW QUESTION 97
- (Topic 3)
A technician was cleaning a storage closet and found a box of transceivers labeled 8Gbps. Which of the following protocols uses those transceivers?

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

Answer: C

Explanation:
The transceivers labeled 8Gbps are likely to be used with the Fibre Channel protocol. Fibre Channel is a high-speed networking technology that is primarily used to connect storage devices to servers in storage area networks (SANs). It is capable of transmitting data at speeds of up to 8 Gbps (gigabits per second), and uses specialized transceivers to transmit and receive data over fiber optic cables.
Coaxial over Ethernet (CoE) is a networking technology that uses coaxial cables to transmit data, and is not related to the transceivers in question. Internet Small Computer Systems Interface (iSCSI) is a protocol that allows devices to communicate over a network using the SCSI protocol, and does not typically use specialized transceivers. Gigabit interface converter (GBIC) is a type of transceiver used to transmit and receive data over fiber optic cables, but it is not capable of transmitting data at 8 Gbps.

NEW QUESTION 99
- (Topic 3)
A company wants to invest in new hardware for the core network infrastructure. The management team requires that the infrastructure be capable of being repaired in less than 60 minutes if any major part fails. Which of the following metrics is MOST likely associated with this requirement?

A. RPO
B. MTTR
C. FHRP
D. MTBF

Answer: B

Explanation:
MTTR is directly related to how quickly a system can be repaired if any major part fails3. The management team requires that the infrastructure be capable of being repaired in less than 60 minutes, which means they have a low MTTR requirement.
MTTR stands for Mean Time To Repair and is a metric used to measure the average amount of time it takes to repair a failed component or system. In this case, the requirement is for the infrastructure to be capable of being repaired in less than 60 minutes if any major part fails, which means the MTTR should be less than 60 minutes.

NEW QUESTION 102
- (Topic 3)
A technician is setting up DNS records on local servers for the company's cloud DNS to enable access by hostname. Which of the following records should be

used?

A. A
B. MX
C. CNAME
D. NS

Answer: A

Explanation:
An A record, also known as an address record, is a type of DNS record that maps a hostname to an IPv4 address. An A record is used to resolve a domain name to an IP address, so that clients can connect to the server or service by using the domain name instead of the IP address. For example, an A record can map www.example.com to 192.0.2.1.
An A record is the most common type of DNS record for cloud DNS, as it allows the company to use a custom domain name for their cloud services, such as web hosting, email, or storage. An A record can also be used to create subdomains, such as blog.example.com or mail.example.com, that point to different IP addresses or servers. The other options are not correct because they are not the best type of DNS record for cloud DNS. They are:
? MX. MX stands for mail exchange, and it is a type of DNS record that specifies the
mail servers that are responsible for receiving and delivering email messages for a domain name. MX records are used for email services, but they are not sufficient for cloud DNS, as they do not map a hostname to an IP address.
? CNAME. CNAME stands for canonical name, and it is a type of DNS record that specifies an alias name for another domain name. CNAME records are used to create multiple names for the same IP address or server, such as www.example.com and example.com. CNAME records are useful for cloud DNS, but they are not the best type, as they depend on another A record to resolve the IP address.
? NS. NS stands for name server, and it is a type of DNS record that delegates a DNS zone to an authoritative server. NS records are used to specify which DNS servers are responsible for answering queries for a domain name or a subdomain. NS records are essential for cloud DNS, but they are not the best type, as they do not map a hostname to an IP address.
References1: DNS records overview | Google Cloud2: Network+ (Plus) Certification | CompTIA IT Certifications3: ClouDNS: What is a DNS record?

NEW QUESTION 105
- (Topic 3)
A network team is getting reports that air conditioning is out in an IDF. The team would like to determine whether additional network issues are occurring. Which of the following should the network team do?

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

Answer: D

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

NEW QUESTION 107
- (Topic 3)
All packets arriving at an interface need to be fully analyzed. Which of me following features should be used to enable monitoring of the packets?

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

Answer: D

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

NEW QUESTION 112
- (Topic 3)
A company has a geographically remote office. In order to connect to the internet, the company has decided to use a satellite WAN link. Which of the following is the GREATEST concern for this type of connection?

A. Duplex
B. Collisions
C. Jitter
D. Encapsulation

Answer: C

Explanation:
itter is the variation in latency or delay of packets in a network. Satellite WAN links have high latency and are prone to jitter, which can affect the quality of voice and video applications. Jitter is the greatest concern for this type of connection

NEW QUESTION 115
- (Topic 3)
An engineer is using a tool to run an ICMP sweep of a network to find devices that are online. When reviewing the results, the engineer notices a number of workstations that are currently verified as being online are not listed in the report.
The tool was configured to scan using the following information: Network address: 172.28.16.0
CIDR: /22
The engineer collected the following information from the client workstation: IP address: 172.28.17.206
Subnet mask: 255.255.252.0
Which of the following MOST likely explains why the tool is failing to detect some workstations?

A. The scanned network range is incorrect.
B. The subnet mask on the client is misconfigured.
C. The workstation has a firewall enabled.
D. The tool is unable to scan remote networks.

Answer: C

Explanation:
A firewall is a device or software that filters and controls the incoming and outgoing network traffic based on predefined rules. A firewall can block ICMP packets, which are used for ping and other diagnostic tools. If the workstation has a firewall enabled, it may not respond to the ICMP sweep and appear as offline. The engineer should check the firewall settings on the workstation and allow ICMP traffic if needed.
References: Network+ Study Guide Objective 4.1: Given a scenario, use the appropriate tool.

NEW QUESTION 119
- (Topic 3)
A security team would like to use a system in an isolated network to record the actions of potential attackers. Which of the following solutions is the security team implementing?

A. Perimeter network
B. Honeypot
C. Zero trust infrastructure
D. Network segmentation

Answer: B

Explanation:
The solution that the security team is implementing to record the actions of potential attackers in an isolated network is a honeypot. A honeypot is a decoy system that simulates a real network or service, but has no actual value or function. A honeypot is designed to attract and trap attackers who try to infiltrate or compromise the network, and then monitor and analyze their behavior and techniques. A honeypot can help the security team learn about the attackers' motives, methods, and tools, and improve their defense
strategies accordingly. References: CompTIA Network+ N10-008 Certification Study Guide, page 358; The Official CompTIA Network+ Student Guide (Exam N10-008), page 14-1.

NEW QUESTION 121
- (Topic 3)
A network administrator is setting up a web-based application for a company. The application needs to be continually accessible to all end users.
Which of the following would best ensure this need is fulfilled?

A. NIC teaming
B. Cold site
C. Snapshots
D. High availability

Answer: D

Explanation:
High availability is a quality of a system or component that assures a high level of operational performance for a given period of time. High availability means that an IT system, component, or application can operate at a high level, continuously, without intervention, for a given time period. High-availability infrastructure is configured to deliver quality performance and handle different loads and failures with minimal or zero downtime. High availability is important for web-based applications, as it ensures that the application is always accessible to the end users, even in the event of a server or component failure. High availability can be achieved by eliminating single points of failure, implementing redundancy, load balancing, and failover mechanisms.

NEW QUESTION 126
- (Topic 3)
An engineer needs to verity the external record tor SMTP traffic. The engineer logged in to the server and entered the nslookup command. Which of the following commands should the engineer send before entering the DNS name?

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

Answer: D

NEW QUESTION 129
- (Topic 3)
A network technician is troubleshooting a connection to a web server. The Technician Is unable to ping the server but is able to verify connectivity to the web service using Tenet. Which of the following protocols is being blocked by me firewall?

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

Answer: C

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

NEW QUESTION 132
- (Topic 3)
A network administrator wants to know which systems on the network are at risk of a known vulnerability. Which of the following should the administrator reference?

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

Answer: E

Explanation:
A Common Vulnerabilities and Exposures (CVE) is a publicly available database of known security vulnerabilities and exposures that affect various software and hardware products. A CVE entry provides a standardized identifier, a brief description, and references to related sources of information for each vulnerability or exposure. A network administrator can reference the CVE database to check if any of the systems on the network are affected by a known vulnerability, and if so, what are the potential impacts and mitigations.
A Service Level Agreement (SLA) is a contract between a service provider and a customer that defines the expected level and quality of service, such as availability, performance, and security. An SLA does not provide information on specific vulnerabilities or exposures affecting the systems or services.
A Patch Management Policy is a set of rules and procedures that govern how patches are applied to systems and software to fix bugs, improve functionality, or address security issues. A patch management policy can help prevent or reduce the risk of vulnerabilities or exposures, but it does not provide information on specific vulnerabilities or exposures affecting the systems or software.
A Non-Disclosure Agreement (NDA) is a legal contract between two or more parties that prohibits the disclosure of confidential or proprietary information to unauthorized parties. An NDA does not provide information on specific vulnerabilities or exposures affecting the systems or information.
A Site Survey Report is a document that summarizes the results of a physical inspection and assessment of a network site, such as the layout, infrastructure, equipment, and environmental conditions. A site survey report can help identify and resolve potential network issues, such as interference, signal strength, or coverage, but it does not provide information on specific vulnerabilities or exposures affecting the network devices or software.
References
What is CVE?
What is a Service Level Agreement (SLA)? Guide to Enterprise Patch Management Planning
NDA, MSA, SOW and SLA. Confidentiality agreements when you outsource QA Site Survey Report

NEW QUESTION 134
- (Topic 3)
Which of the following is a requirement when certifying a network cabling as Cat 7?

A. Ensure the patch panel is certified for the same category.
B. Limit 10Gb transmissions to 180ft (55m).
C. Use F-type connectors on the network terminations.
D. Ensure the termination standard is TIA/EIA-568-A.

Answer: D

Explanation:
Category 7 (Cat 7) is a cabling standard that supports 10GBASE-T Ethernet connections up to 100 meters (328 feet). In order for a cabling system to be certified as Cat 7, all components, including the patch panel, must meet the TIA/EIA-568-A standard. This standard requires the use of shielded cables with F-type connectors for the network terminations. Reference: CompTIA Network+ Study Manual, 8th Edition, page 158.

NEW QUESTION 139
- (Topic 3)
Which of the following is a valid alternative to maintain a deployed proxy technology while saving physical space in the data center by moving the network service to the virtualization infrastructure?

A. NFV
B. SDWAN
C. Networking as code
D. VIP

Answer: A

Explanation:
The valid alternative to maintain a deployed proxy technology while saving physical space in the data center by moving the network service to the virtualization

infrastructure is NFV (Network Function Virtualization). NFV is a technique that allows network functions, such as proxies, firewalls, routers, or load balancers, to be implemented as software applications running on virtual machines or containers. NFV reduces the need for dedicated hardware devices and improves scalability and flexibility of network
services. References: CompTIA Network+ N10-008 Certification Study Guide, page 440; The Official CompTIA Network+ Student Guide (Exam N10-008), page 16-11.
NFV can be used to virtualize a wide variety of network functions, including proxy servers. By virtualizing proxy servers, organizations can save physical space in the data center and
improve the scalability and efficiency of their networks.
To virtualize a proxy server using NFV, an organization would need to deploy a virtualization platform, such as VMware ESXi or Microsoft Hyper-V. The organization would then need to install a virtual proxy server appliance on the virtualization platform.
Once the virtual proxy server appliance is installed, it can be configured and used just like a physical proxy server.
NFV is a relatively new technology, but it is quickly gaining popularity as organizations look for ways to improve the efficiency and scalability of their networks.

NEW QUESTION 142
- (Topic 3)
After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect
take to troubleshoot the issue?

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

Answer: A

Explanation:
Cat 8 keystones are shielded to prevent interference from external sources, but they also require proper grounding to avoid interference from within the cable. Wrapping the end connections with copper tape before terminating them is one way to ensure a good ground connection and reduce interference. Using passthrough modular crimping plugs, connecting the RX/TX wires to different pins, or running a speed test on a slow device are not relevant or effective steps to troubleshoot the issue.
References:
? CompTIA Network+ N10-008 Certification Study Guide, page 191
? CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 362
? CAT8 RJ45 Keystone Problem : r/HomeNetworking2
? How to Terminate Cat8 Shielded Keystone Jacks3

NEW QUESTION 146
- (Topic 3)
A technician is concerned about unauthorized personnel moving assets that are installed in a data center server rack. The technician installs a networked sensor that sends an alert when the server rack door is opened. Which of the following did the technician install?

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

Answer: D

Explanation:
Tamper detection is a physical security feature that can alert the technician when someone opens the server rack door without authorization. Tamper detection sensors can be installed inside the equipment or on the rack itself, and they can send an alert via email, SMS, or other methods. Tamper detection can help prevent unauthorized access, theft, or damage to the network assets.
References:
? Physical Security – N10-008 CompTIA Network+ : 4.51

NEW QUESTION 150
- (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 154
- (Topic 3)
A network engineer is concerned about VLAN hopping happening on the network. Which of the following should the engineer do to address this concern?

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

Answer: B

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

NEW QUESTION 155
- (Topic 3)
A network administrator installed a new data and VoIP network. Users are now experiencing poor call quality when making calls. Which of the following should the administrator do to increase VoIP performance?

A. Configure a voice VLAN.
B. Configure LACP on all VoIP phones.
C. Configure PoE on the network.
D. Configure jumbo frames on the network.

Answer: A

Explanation:
"Benefits of Voice VLAN
It ensures that your VoIP (Voice over Internet Phone) devices do not have to contend directly with all the broadcasts and other traffic from the data VLAN. A voice VLAN can simplify network configuration in some circumstances."
https://community.fs.com/blog/auto-voip-vs-voice-vlan-what-s-the-difference.html Jumbo Frames
"When jumbo frames on a VoIP/UC network are enabled, it can cause the same kind of
delay to your network transmissions."
"VoIP uses will always not benefit from jumbo frame, as VoIP like gaming, is latency and time sensitive. Jumbo Frame for Internet Purpose: You will not see any performance boost as the files that came across the internet does not support jumbo frame."
https://www.ankmax.com/newsinfo/1358641.html#:~:text=VoIP%20uses%20will%20always%20not,does%20not%20support%20jumbo%20frame.
"To summarize this general best practice guide, you should NOT enable jumbo frame feature as a general home user."

NEW QUESTION 159
- (Topic 3)
A network administrator received complaints of intermittent network connectivity issues. The administrator investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?

A. Enable spanning tree.
B. Configure port security.
C. Change switch port speed limits.
D. Enforce 802. IQ tagging.

Answer: A

Explanation:
Spanning tree is a protocol that prevents network loops by dynamically disabling or enabling switch ports based on the network topology. Network loops can cause intermittent connectivity issues, such as broadcast storms, MAC address table instability, and multiple frame transmission. By enabling spanning tree, the network administrator can ensure that there is only one active path between any two network devices at any given time. References:
? CompTIA Network+ N10-008 Certification Exam Objectives, page 91
? CompTIA Network+ Cert Guide: Switching and Virtual LANs, page 172

NEW QUESTION 161
- (Topic 3)
A network administrator is configuring a firewall to allow for a new cloud-based email server. The company standard is to use SMTP to route email traffic. Which of the following ports, by default, should be reserved for this purpose?

A. 23
B. 25
C. 53
D. 110

Answer: B

Explanation:
Port 25, by default, should be reserved for SMTP traffic to allow for a new cloud-based email server. SMTP stands for Simple Mail Transfer Protocol, which is a network protocol that enables email communication between mail servers and clients. SMTP uses port 25 as its default port for sending and receiving email messages over TCP/IP networks. A cloud-based email server is an email server that is hosted on a cloud service provider's infrastructure, rather than on-premise or in-house. A cloud-based email server can offer advantages such as scalability, reliability, security, and cost-effectiveness. To allow for a new cloud-based email server, a firewall should be configured to open port 25 for SMTP traffic. References: [CompTIA Network+ Certification Exam Objectives], What Is SMTP? | Mailtrap Blog, Cloud Email Server: What Is It & How Does It Work? | Zoho Mail

NEW QUESTION 165
- (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. IQ
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 170
- (Topic 3)
Which of the following types of connections would need to be set up to provide access from the internal network to an external network so multiple satellite offices can communicate securely using various ports and protocols?

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

Answer: D

NEW QUESTION 172
- (Topic 3)
Which of the following fouling protocols is generally used by major ISPs for handing large- scale internet traffic?

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

Answer: D

NEW QUESTION 175
- (Topic 3)
A large metropolitan city is looking to standardize the ability tor 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 180
- (Topic 3)
A customer has an attached USB printer that needs to be shared with other users. The desktop team set up printer sharing. Now, the network technician needs to obtain the necessary information about the PC and share it with other users so they can connect to the printer. Which of the following commands should the technician use to get the required information? (Select TWO).

A. arp
B. route
C. netstat
D. tcpdump
E. hostname
F. ipconfig

Answer: EF

Explanation:
The hostname and ipconfig commands should be used to get the required information about the PC and share it with other users so they can connect to the printer. The hostname command displays the name of the computer on a network. The ipconfig command displays the IP configuration of the computer, including its IP address, subnet mask, default gateway, and DNS servers. These information are necessary for other users to locate and connect to the shared printer on the network. For example, other users can use the UNC path \\hostname\printername or \\ipaddress\printername to access the shared printer. References: [CompTIA Network+ Certification Exam Objectives], How to Share a Printer in Windows 10

NEW QUESTION 181
- (Topic 3)
When accessing corporate network resources, users are required to authenticate to each application they try to access. Which of the following concepts does this BEST represent?

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

Answer: B

NEW QUESTION 183
- (Topic 3)
A company realizes that only half of its employees work in the office, and the employees who work from home no longer need a computer at the office. Which of the following security measures should the network administrator implement when removing a computer from a cubicle?

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

Answer: D

Explanation:
The best security measure to implement when removing a computer from a cubicle is to remove the employee's network access. This will prevent the employee from accessing any network resources or data from the computer, as well as prevent any unauthorized users from using the computer to access the network. Removing the employee's network access can be done by deleting or disabling the user account, revoking the credentials, or changing the permissions.
The other options are not as effective or necessary as removing the employee's network access. They are:
•Disabling DHCP on the computer being removed will prevent the computer from obtaining an IP address from the network, but it will not prevent the computer from using a static IP address or accessing the network through another device.
•Placing the switch port in a private VLAN will isolate the computer from other devices on the network, but it will not prevent the computer from accessing the network through another port or device.
•Applying a firewall rule to block the computer's IP address will prevent the computer from communicating with the network, but it will not prevent the computer from changing its IP address or accessing the network through another device.
References
1: CompTIA Network+ N10-008 Cert Guide - O'Reilly Media 2: Network+ (Plus) Certification | CompTIA IT Certifications
3: 10 Ways to Secure Office Workstations - Computer Security

NEW QUESTION 185
- (Topic 3)
Which of the following is a characteristic of the application layer?

A. It relies upon other layers for packet delivery.
B. It checks independently for packet loss.
C. It encrypts data in transit.
D. It performs address translation.

Answer: A

Explanation:

The application layer is the highest layer of the OSI model, and it provides the interface between the user and the network. It does not handle the details of packet delivery, such as addressing, routing, error checking, or encryption. Those functions are performed by the lower layers of the OSI model. The application layer only focuses on the format, content, and presentation of the data.
References:
? Understanding the OSI Model – N10-008 CompTIA Network+ : 1.11
? CompTIA Network+ Certification Exam Objectives, page 92

NEW QUESTION 187
- (Topic 3)
Users report they cannot reach any websites on the internet. An on-site network engineer is able to duplicate the issue on a different PC. The network engineer then tries to ping a website and receives the following message:
Ping request could not find host www.google.com. Please check the name and try again. Which of the following is the next step the engineer should take?

A. Ping 127. 0. 0. 1 to test local hardware.
B. Test the website from outside the company.
C. Ping internal name server functionality.
D. Check internet firewall logs for blocked DNS traffi

Answer: C

Explanation:

The error message "Ping request could not find host www.google.com" indicates that the network engineer's PC cannot resolve the hostname www.google.com to its corresponding IP address. This means that there is a problem with the DNS (Domain Name System) service, which is responsible for translating hostnames to IP addresses and vice versa. The DNS service can be provided by internal or external name servers, depending on the network configuration.
The next step the engineer should take is to ping the internal name server functionality, which means to test if the PC can communicate with the name server that is configured in its network settings, and if the name server can resolve internal hostnames, such as those of the company's servers or devices. To do this, the engineer can use the following commands:
? To find out the IP address of the name server, use ipconfig /all and look for the DNS Servers entry.
? To ping the name server, use ping <name server IP address> and check if the packets are sent and received successfully.
? To test the name resolution, use nslookup <internal hostname> and check if the name server returns the correct IP address.
If the ping or the nslookup commands fail, it means that the internal name server is not working properly, and the engineer should troubleshoot the name server configuration or connectivity. If the ping and the nslookup commands succeed, it means that the internal name server is working properly, but there is a problem

with the external name resolution, and the engineer should check the internet firewall logs for blocked DNS traffic, or test the website from outside the company.
ReferencesWindows 10 can’t resolve hostnames - ping with IP works but not with hostnamePing request could not find host xyz.local. Please check the name and try againDNS problem, nslookup works, ping doesn’t Users are connected to a switch on an Ethernet interface of a campus router. The service provider is connected to the serial 1 interface on the router. The output of the interfaces is:
E1/0: 192.168.8.1/24 S1: 192.168.7.252/30

NEW QUESTION 188
- (Topic 3)
Clients have reported slowness between a branch and a hub location. The senior engineer suspects asymmetrical routing is causing the issue. Which of the following should the engineer run on both the source and the destination network devices to validate this theory?

A. traceroute
B. ping
C. route
D. nslookup

Answer: A

Explanation:

Asymmetric routing occurs when traffic does not traverse the same path in both directions of a conversation. This can cause problems when there are stateful devices, such as firewalls or NAT devices, in the path that expect the traffic to be symmetrical. Asymmetric routing can also result in suboptimal TCP performance, as TCP assumes that the SYN and ACK packets take the same path1.
To validate the theory of asymmetric routing, the engineer should run the traceroute command on both the source and the destination network devices. The traceroute command shows the route that packets take to reach a destination, by displaying the IP addresses and hostnames of the routers along the path, as well as the time taken for each hop. By comparing the output of the traceroute command from both ends, the engineer can determine if the traffic is taking different paths in each direction, and identify where the asymmetry occurs2.
The ping command is not sufficient to validate the theory of asymmetric routing, as it only tests the connectivity and latency between two devices, but does not show the intermediate hops or the path taken by the packets. The route command shows the routing table of a device, but does not show the actual path taken by the packets. The nslookup command resolves a hostname to an IP address, or vice versa, but does not show the route or the connectivity between two devices.
ReferencesHow to Find & Fix Asymmetric Routing Issues | AuvikIdentifying and Troubleshooting Asymmetric Routing in WAAS - Cisco Community

NEW QUESTION 193
- (Topic 3)
An administrator needs to ensure an access switch is sending the appropriate logs to the network monitoring server. Which of the following logging levels is most appropriate for the access layer switch?

A. Level 0
B. Level 2
C. Level 5
D. Level 7

Answer: C

Explanation:

Logging levels are used to categorize the severity and importance of log messages generated by network devices. The lower the level, the higher the priority. Level 0 is the most critical, while level 7 is the most verbose and least important. Level 5 is the default logging level for most Cisco devices, and it corresponds to notifications. Notifications are messages that indicate normal but significant events, such as interface status changes, configuration changes, or system restarts. These messages are useful for monitoring the health and performance of the network, and they do not generate excessive traffic or consume too much memory or CPU resources. Therefore, level 5 is the most appropriate logging level for an access layer switch, which connects end devices to the network and does not need to log debug or informational messages.
ReferencesHow to configure logging in Cisco IOSCisco Guide to Harden Cisco IOS DevicesCisco Privilege Levels – Explanation and Configuration

NEW QUESTION 196
- (Topic 3)
A network administrator walks into a data center 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 type of physical security attack in which an unauthorized person follows an authorized person into a restricted area, such as a data center, without proper identification or authentication. Tailgating can allow attackers to access sensitive data, equipment, or network resources, or to plant malicious devices or software. The network administrator prevented tailgating by stopping and directing the unknown person to the security desk, where they would have to verify their identity and purpose.
ReferencesDigital Threats and Cyberattacks at the Network LevelNetwork attacks and how to prevent them

NEW QUESTION 198
- (Topic 3)
A technician is configuring a wireless access point in a public space for guests to use. Which of the following should the technician configure so that only approved connections are

allowed?

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

Answer: B

Explanation:

A captive portal is a web page that requires users to authenticate or accept terms of service before they can access the internet through a wireless access point. A captive portal can be used to control who can use the wireless network, limit the bandwidth or time of usage, or display advertisements or information. A captive portal is a common feature of public wireless networks, such as those in hotels, airports, cafes, or libraries. A captive portal can prevent unauthorized or malicious users from accessing the network or consuming network resources.
ReferencesPublic Wireless Access Points Definition | Law InsiderAre Public Wi-Fi Networks Safe? What You Need To Know

NEW QUESTION 203
- (Topic 3)
A technician reviews a network performance report and finds a high level of collisions happening on the network. At which of the following layers of the OSI model would these collisions be found?

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

Answer: A

Explanation:

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

NEW QUESTION 205
- (Topic 3)
Which of the following would be increased by adding encryption to data communication across the network?

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

Answer: D

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

NEW QUESTION 206
- (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 210
- (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 211
- (Topic 3)
A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks does the technician need to install?
? 110
? 66

A. BiX
B. Krone

Answer: A

Explanation:
A 110 block is a type of punch-down block that is used to terminate twisted-pair cables in Ethernet networks. It is a non-proprietary standard that is widely used in structured cabling systems for voice and data applications. A 110 block can support up to 100 MHz of bandwidth and can be used with Cat 3, Cat 5, Cat 5e, and Cat 6 cables12.
A 66 block is another type of punch-down block that is mainly used for telephone wiring. It is an older and less reliable standard than the 110 block and does not support high-speed data transmission3. A BiX block is a proprietary punch-down block that is developed by NORDX/CDT and is mostly used in Canada. It can support up to 250 MHz of bandwidth and can be used with Cat 5e and Cat 6 cables4. A Krone block is another proprietary punch-down block that is developed by ADC Krone and is mostly used in Europe. It can support up to 100 MHz of bandwidth and can be used with Cat 5 and Cat 5e cables. Therefore, the best option for the customer who wants to use non-proprietary standards is the 110 block.

NEW QUESTION 216
- (Topic 3)
A network administrator is reviewing north-south traffic to determine whether a security threat exists. Which of the following explains the type of traffic the administrator is reviewing?

A. Data flowing between application servers
B. Data flowing between the perimeter network and application servers
C. Data flowing in and out of the data center
D. Data flowing between local on-site support and backup servers

Answer: C

Explanation:
North-south traffic is any communication between components of a data center and another system, which is physically out of the boundary of the data center. It is also referred to as client-server traffic, as it usually involves requests from end users or external applications to the data center resources. For example, when a user accesses a web application hosted in a data center, the traffic between the user's browser and the web server is considered north-south traffic.

NEW QUESTION 218
- (Topic 3)
A network technician needs to install patch cords from the UTP patch panel to the access switch for a newly occupied set of offices. The patch panel is not labeled for easy jack identification. Which of the following tools provides the easiest way to identify the appropriate patch panel port?

A. Toner
B. Laptop
C. Cable tester
D. Visual fault locator

Answer: A

Explanation:
A toner is a tool that generates an audible signal that can be traced by a probe. A network technician can use a toner to identify the appropriate patch panel port by connecting the toner to one end of the patch cord and using the probe to scan the patch panel until the signal is detected. A toner is the easiest way to identify the patch panel port when the patch panel is not labeled, as it does not require a laptop, a cable tester, or a visual fault locator.
A toner can also be used to locate breaks or shorts in a cable, or to verify continuity. References:
? Using a Toner and Probe - CompTIA Network+ Certification (N10-008): The Total
Course Video
? CompTIA Network+ Certification Exam Objectives, page 141

NEW QUESTION 221
- (Topic 3)
Which of the following is a document that states what the minimum performance expectations are within a network?

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

Answer: B

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

NEW QUESTION 222
- (Topic 3)
A store owner would like to have secure wireless access available for both business equipment and patron use. Which of the following features should be configured to allow different wireless access through the same equipment?

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

Answer: D

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

NEW QUESTION 227
- (Topic 3)
A network manager wants to view network traffic for devices connected to a switch. A network engineer connects an appliance to a free port on the switch and needs to configure the switch port connected to the appliance. Which of the following is the best option for the engineer to enable?

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

Answer: B

Explanation:
Port mirroring is a feature that allows a switch to copy the traffic from one or more ports to another port, where a network analyzer or a monitoring device can capture and analyze the traffic. Port mirroring is useful for troubleshooting and security purposes, as it allows the network engineer to see the traffic that is passing through the switch without affecting the normal operation of the network.
References
? 1: Port Mirroring - CompTIA Network+ Certification (N10-008): The Total Course [Video]
? 2: CompTIA Network+ Certification Exam Objectives, page 5
? 3: CompTIA Network+ N10-005: 2.1 – Port Mirroring - Professor Messer IT Certification Training Courses
? 4: CompTIA Network+ N10-005: 1.4 – Port Mirroring

NEW QUESTION 228
- (Topic 3)
A network administrator is creating a subnet for a remote office that has 53 network devices. An additional requirement is to use the most efficient subnet. Which of the following CIDR notations indicates the appropriate number of IP addresses with the LEAST amount of unused addresses? (Choose Correct option and give explanation directly from CompTIA Network+ Study guide or documents)

A. /24
B. /26
C. /28
D. /32

Answer: B

Explanation:
This CIDR notation indicates that there are 64 IP addresses, of which 62 are usable for network devices. This provides the LEAST amount of unused addresses, making it the most efficient subnet for a remote office with 53 network devices. According to the CompTIA Network+ Study Guide, "Subnetting allows you to divide one large network into smaller, more manageable networks or subnets."

NEW QUESTION 229
- (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 230
- (Topic 3)
Which of the following can be used to validate domain ownership by verifying the presence of pre-agreed content contained in a DNS record?

A. SOA

B. SRV
C. AAA
D. TXT

Answer: D

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

NEW QUESTION 232
- (Topic 3)
Which of the following is a major difference between a router and a Layer 3 switch?

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

Answer: A

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

NEW QUESTION 235
- (Topic 3)
A network technician is planning a network scope. The web server needs to be within 12.31 69.1 to 12.31.69.29. Which of the following would meet this requirement?

A. Lease time
B. Range reservation
C. DNS
D. Superscope

Answer: A

NEW QUESTION 238
- (Topic 3)
A network administrator is getting reports of some internal users who cannot connect to network resources. The users slate 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 240
- (Topic 3)
Classification using labels according to information sensitivity and impact in case of unauthorized access or leakage is a mandatory component of:

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

Answer: C

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

NEW QUESTION 243
- (Topic 3)
A user is unable to reach any resources on the internet. A technician goes to the site and obtains the following output from the workstation:

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

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

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

Answer: A

Explanation:
The route command is used to view and manipulate the IP routing table in Windows operating systems456 The routing table contains information about how to reach different network destinations. The output from the workstation shows that the routing table does not have a default gateway, which is a router that forwards packets to other networks that are not directly connected to the local network. A default gateway is usually specified by a route with a destination of 0.0.0.0 and a netmask of 0.0.0.0, which matches any IP address. To correct the issue, the technician can use the route ADD command to add a default gateway to the routing table. The syntax of the command is:
route ADD <destination> MASK <netmask> <gateway> metric <metric>
The destination and netmask parameters should be 0.0.0.0 to indicate a default route. The gateway parameter should be the IP address of the router that can reach the internet, which is 10.10.51.10 in this case. The metric parameter is an optional value that indicates the cost or preference of the route, which can be used to choose between multiple routes to the same destination. A lower metric means a higher preference. The metric parameter can be any integer between 1 and 9999. In this case, the metric parameter can be 35 or any other value.
Therefore, the correct command is:
route ADD 0.0.0.0 MASK 0.0.0.0 10.10.51.10 metric 35

NEW QUESTION 244
- (Topic 3)
A technician is configuring a bandwidth-monitoring tool that supports payloads of 1,600 bytes. Which of the following should the technician configure for this tool?

A. LACP
B. Flow control
C. Port mirroring
D. Jumbo frames

Answer: D

Explanation:
Jumbo frames are Ethernet frames that can carry more than the standard 1,500 bytes of payload data. Jumbo frames can support payloads of up to 9,000 bytes, depending on the network device and configuration. Jumbo frames can improve network performance by reducing the overhead of packet headers and increasing the efficiency of data transmission. Jumbo frames can also reduce the CPU utilization of the sender and receiver devices, as they require fewer interrupts and processing cycles. However, jumbo frames also have some drawbacks, such as increased latency, fragmentation, and compatibility issues. Therefore, jumbo frames should be used with caution and only in networks that support them end-to-end.
A technician who is configuring a bandwidth-monitoring tool that supports payloads of 1,600 bytes should enable jumbo frames for this tool, as this would allow the tool to capture and analyze more data per frame and provide more accurate and detailed results. However, the technician should also ensure that the network devices and interfaces that the tool is connected to also support jumbo frames, and that the MTU (maximum transmission unit) is set to the same value across the network path.
ReferencesWhat are Jumbo Frames?How to Enable Jumbo FramesCompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION 248
- (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 249
- (Topic 3)
Which of the following best describes what an organization would use port address translation for?

A. VLANs on the perimeter
B. Public address on the perimeter router
C. Non-routable address on the perimeter router
D. Servers on the perimeter

Answer: B

Explanation:
The best answer is B. Public address on the perimeter router.
Port address translation (PAT) is a function that allows multiple users within a private network to make use of a minimal number of IP addresses. Its basic function is to share a single IP public address between multiple clients who need to use the Internet publicly. It is an extension of network address translation (NAT)1.
PAT works by creating dynamic NAT mapping, in which a global (public) IP address and a unique port number are selected. The router keeps a NAT table entry for every unique combination of the private IP address and port, with translation to the global address and a unique port number2.
Therefore, an organization would use PAT for having a public address on the perimeter router, which can be shared by many hosts on the private network using different port numbers. This can reduce the bandwidth consumption and cost of the organization's internet connection, as well as provide some security benefits by hiding the internal network structure3.
The other options are not correct because:
? VLANs on the perimeter are not related to PAT, as they are used to segment the network into logical groups based on different criteria, such as function, security, or performance4.
? Non-routable address on the perimeter router would not allow the organization to access the Internet or the cloud, as non-routable addresses are not valid on the public network and cannot be translated by PAT5.
? Servers on the perimeter are not a reason to use PAT, as servers usually have static IP addresses and do not need to share a public address with other hosts. Servers on the perimeter may use NAT, but not PAT, to map their private IP addresses to a public IP address2.

NEW QUESTION 253
- (Topic 3)
Which of the following security concepts is related to ensuring that encrypted data is not edited while in transit?

A. Zero trust
B. Integrity
C. Availability
D. Confidentiality

Answer: B

Explanation:
Integrity is the security concept that is related to ensuring that encrypted data is not edited while in transit. Integrity is one of the three main goals of information security, along with confidentiality and availability. Integrity means that data is protected from unauthorized modification or corruption during storage, processing, or transmission. Integrity can be achieved by using various techniques, such as hashing, digital signatures, checksums, or message authentication codes (MACs). These techniques can verify the authenticity and validity of the data by detecting any changes or tampering that may have occurred. References: [CompTIA Network+ Certification Exam Objectives], What Is Data Integrity? | Definition & Examples | Forcepoint

NEW QUESTION 257
- (Topic 3)
A false camera is installed outside a building to assist with physical security. Which of the following is the device assisting?

A. Detection
B. Recovery
C. Identification
D. Prevention

Answer: A

NEW QUESTION 261
- (Topic 3)
Which of the following network devices can perform routing between VLANs?

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

Answer: B

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

NEW QUESTION 263
- (Topic 3)
Which of the following OSI model layers are responsible for handling packets from the sources to the destination and checking for errors? (Select two).

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

Answer: CD

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

NEW QUESTION 265
- (Topic 3)
A global company has acquired a local company. The companies are geographically separate. The IP address ranges for the two companies are as follows:
· Global company: 10.0.0.0/16
· Local company: 10.0.0.0/24
Which of the following can the network engineer do to quickly connect the two companies?

A. Assign static routing to advertise the local company's network.
B. Assign an overlapping IP address range to both companies.
C. Assign a new IP address range to the local company.
D. Assign a NAT range to the local company.

Answer: C

Explanation:
Assigning a new IP address range to the local company is the best option to quickly connect the two companies without causing any IP address conflicts or overlaps. This option requires reconfiguring the local company’s network devices and updating the routing tables on both sides, but it avoids the need for any NAT or static routing solutions that may introduce additional complexity, cost, or performance issues12 References1: Connecting Networks with Overlapping IP Ranges 2: What Is Network Address Translation (NAT)?

NEW QUESTION 270
- (Topic 3)
Which of the following most likely determines the size of a rack for installation? {Select two).

A. KVM size
B. Switch depth
C. Hard drive size
D. Cooling fan speed
E. Outlet amperage
F. Server height

Answer: BF

Explanation:
The size of a rack for installation depends on several factors, such as the available space, the power and cooling requirements, and the dimensions of the equipment to be installed. Two of the most important dimensions to consider are the switch depth and the server height. Switch depth refers to the length of the switch from front to back, which determines how much space is needed inside the rack. Server height refers to the vertical space occupied by the server, which is measured in rack units (RU) or U. One rack unit is equal to 1.75 inches. The height of the rack should be able to accommodate the total number of rack units needed for the servers and other devices, as well as some extra space for cable management and airflow. References: CompTIA Network+ N10-008 Cert Guide, Chapter 2, Section 2.5

NEW QUESTION 271
- (Topic 3)
A security engineer is installing a new IOS on the network. The engineer has asked a network administrator to ensure all traffic entering and leaving the router interface is available for the IDS. Which of the following should the network administrator do?

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

Answer: A

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

NEW QUESTION 272
- (Topic 3)
A network administrator is connecting two Layer 2 switches in a network These switches must transfer data in multiple networks. Which of the following would fulfill this requirement?

A. Jumbo frames
B. 802. IQ tagging
C. Native VLAN
D. Link aggregation

Answer: B

Explanation:
The technique that would fulfill the requirement of transferring data in multiple networks is 802.1Q tagging. 802.1Q tagging is a method of adding a tag or identifier to Ethernet frames that indicate which VLAN (Virtual Local Area Network) they belong to. VLANs are logical subdivisions of a network that allow devices in different physical locations or segments to communicate as if they were in the same network. VLANs improve network performance, security, and management by reducing broadcast traffic, isolating sensitive data, and grouping devices by function or department. By using 802.1Q tagging, two Layer 2 switches can exchange data from multiple VLANs over a single trunk link, without mixing or losing the VLAN information. References: CompTIA Network+ N10-008 Certification Study Guide, page 64; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-12.

NEW QUESTION 277
- (Topic 3)
At which of the following OSI model layers does routing occur?

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

Answer: D

NEW QUESTION 282
- (Topic 3)
Which of the following record types would be used to define where SIP is found?

A. SRV
B. CNAME
C. A
D. MX

Answer: C

Explanation:
The record type that would be used to define where SIP (Session Initiation Protocol) is found is A (Address). A record is a type of DNS (Domain Name System) record that maps a domain name to an IPv4 address. SIP is a protocol that enables voice over IP (VoIP) communication, such as voice calls or video conferencing. SIP uses domain names to identify endpoints or servers involved in a communication session. Therefore, an A record is needed to resolve the domain name of a SIP endpoint or server to its IPv4 address. References: CompTIA Network+ N10-008 Certification Study Guide, page 154; The Official CompTIA Network+ Student Guide (Exam N10-008), page 6-8.

NEW QUESTION 286
- (Topic 3)
Which of the following requires network devices to be managed ustng a different set of IP addresses?

A. Console
B. Split tunnel
C. Jump box
D. Out of band

Answer: D

Explanation:
Out of band management is a process for accessing and managing network devices and infrastructure at remote locations through a separate management plane from the production network. Out of band management requires network devices to be managed using a different set of IP addresses than the ones used for in-band management or data traffic. This provides a secure and dedicated alternate access method to administer connected devices and IT assets without using the corporate LAN.

NEW QUESTION 291
- (Topic 3)
While working in a coffee shop, an attacker watches a user log in to a corporate system and writes down the user's log-in credentials. Which of the following social engineering attacks is this an example of?

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

Answer: A

Explanation:

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

NEW QUESTION 294
- (Topic 3)
A network manager wants to set up a remote access system for the engineering staff. Access to this system will be over a public IP and secured with an ACL. Which of the following best describes this system?

A. VPN
B. Secure Shell
C. Jump server
D. API

Answer: C

Explanation:
A jump server is a system that allows remote access to internal devices through a single, secure device on the public network. A jump server can be configured with an access control list (ACL) to limit who can access the system and what devices they can connect to. A jump server can also use secure protocols such as SSH or VPN to encrypt the communication between the remote user and the internal device. A jump server is different from a VPN, which creates a virtual private network between the remote user and the internal network. A jump server is also different from a secure shell, which is a protocol that allows remote command execution and file transfer. An API is an application programming interface that allows software components to interact with each other.
References:
? Other Network Appliances – SY0-601 CompTIA Security+ : 3.31

NEW QUESTION 296
- (Topic 3)
A company's management team wants to implement NAC on the wired and wireless networks. Which of the following is an authentication component that must be used in this solution?

A. IPSec
B. 802.1X
C. EAP
D. TACACS+

Answer: B

Explanation:
802.1X is an authentication component that must be used in a network access control (NAC) solution. NAC is a method of enforcing security policies on devices that want to access a network, by verifying their identity, compliance, and authorization. 802.1X is a standard that defines how to provide authentication for devices trying to connect to a LAN or WLAN. It uses the Extensible Authentication Protocol (EAP) to exchange authentication information between the device (supplicant), the network access device (authenticator), and the authentication server (typically RADIUS or TACACS+). 802.1X can prevent unauthorized devices from accessing the network, and can also assign them to different VLANs or apply different policies based on their role or group.
IPSec is a protocol suite that provides encryption, authentication, and integrity for IP packets. It can be used to create secure VPN tunnels between networks or hosts. IPSec is not an authentication component for NAC, but rather a security component for protecting data in transit.
EAP is a framework that supports multiple authentication methods, such as passwords, certificates, tokens, or biometrics. EAP is used by 802.1X to provide authentication for network access, but it is not a component by itself. EAP requires a carrier protocol, such as 802.1X, to transport the authentication messages.
TACACS+ is a protocol that provides authentication, authorization, and accounting (AAA) services for network devices or users. It can be used as an authentication server for 802.1X, but it is not an authentication component for NAC by itself. TACACS+ requires a client-server protocol, such as 802.1X, to communicate with the network access device. ReferencesWhat is 802.1X Network Access Control (NAC)?Compare TACACS + and RADIUS802.1X: What EXACTLY is it regarding WPA and EAP?CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008)

NEW QUESTION 297
- (Topic 3)
A company is designing a new complex. The primary and alternate data centers will be in separate buildings 6.2mi (10km) apart and will be connected via fiber. Which of the following types of SFP is the best choice?

A. 10GBASE-SR
B. 10000BASE-LX
C. 10GBASE-LR
D. 1000BASE-SX

Answer: C

Explanation:
10GBASE-LR is the best choice for connecting two data centers that are 6.2 miles (10 km) apart via fiber, because it supports a maximum distance of 6.2 miles (10 km) over single- mode fiber. 10GBASE-SR and 1000BASE-SX are designed for short-range connections over multi-mode fiber, and they can only reach up to 1,312 feet (400 m) and 1,804 feet (550 m), respectively. 10000BASE-LX is a typo and does not exist as a standard. References:
? Network Transceivers – CompTIA Network+ N10-007 – 2.11
? CompTIA Network+ Certification Exam Objectives2

NEW QUESTION 299
- (Topic 3)
A WAN technician reviews activity and identifies newly installed hardware that is causing outages over an eight-hour period. Which of the following should be considered FIRST?

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

Answer: D

NEW QUESTION 302
- (Topic 3)
Which of the following does OSPF use to communicate routing updates?

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

Answer: C

Explanation:
OSPF uses multicast to communicate routing updates among routers within the same area. OSPF routers send and receive link-state advertisements (LSAs) using IP multicast addresses 224.0.0.5 (all OSPF routers) and 224.0.0.6 (all OSPF designated routers) 1. Multicast allows OSPF to send routing updates efficiently and selectively, without flooding the entire network or requiring acknowledgments from every router

NEW QUESTION 305
- (Topic 3)
At which of the following OSI model layers does a MAC filter list for a wireless infrastructure operate?

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

Answer: D

Explanation:
A MAC filter list is a security feature that allows or denies access to a wireless network based on the MAC address of the device. A MAC address is a unique identifier assigned to a network interface card (NIC) at the physical layer of the OSI model. However, MAC filtering operates at the data link layer of the OSI model, where MAC addresses are used to encapsulate and deliver data frames between devices on the same network segment.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.1: Given a scenario, install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

NEW QUESTION 308
- (Topic 3)
Which of the following has the capability to centrally manage configuration, logging, and firmware versioning for distributed devices?

A. WLAN controller
B. Load balancer
C. SIEM solution
D. Syslog server

Answer: A

Explanation:
A WLAN controller is a device that manages and controls multiple wireless access points (WAPs) in a wireless LAN (WLAN). A WLAN controller has the capability to centrally manage configuration, logging, and firmware versioning for distributed WAPs. A WLAN controller can also provide load balancing, security, and quality of service (QoS) for the WLAN.
References: Network+ Study Guide Objective 3.1: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 313
- (Topic 3)
A company needs to virtualize a replica of its internal physical network without changing the logical topology and the way that devices behave and are managed. Which of the following technologies meets this requirement?

A. NFV
B. SDWAN
C. VIP
D. MPLS

Answer: A

Explanation:
Network Function Virtualization (NFV) is a technology that allows for the virtualization of a replica of a network's physical topology and the way it behaves without changing the logical topology and the way that devices are managed. NFV allows for the virtualization of network functions such as routers, firewalls, and switches, resulting in increased flexibility and scalability. This makes NFV an ideal technology for companies looking to virtualize a replica of their internal physical network.

NEW QUESTION 314
- (Topic 3)

A network contains 25 access points. Which of the following devices would be best to change configurations on all the devices remotely?

A. WLAN controller
B. Load balancer
C. Bridge
D. Layer 3 switch

Answer: A

Explanation:
A WLAN controller is a device that can centrally manage and configure multiple access points in a wireless network. A WLAN controller can change settings on all the devices remotely, such as SSIDs, security policies, firmware updates, and channel assignments. A WLAN controller can also monitor the performance and status of the access points and provide load balancing and fault tolerance

NEW QUESTION 317
- (Topic 3)
An engineer was asked to update an MX record for an upcoming project. Which of the following server types is MOST likely to be in scope for the project?

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

Answer: A

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

NEW QUESTION 322
- (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 324
- (Topic 3)
An organization set up its offices so that a desktop is connected to the network through a VoIP phone. The VoIP vendor requested that voice traffic be segmented separately from non-voice traffic. Which of the following would allow the organization to configure multiple devices with network isolation on a single switch port?

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

Answer: A

NEW QUESTION 327
- (Topic 3)
An IT technician successfully connects to the corporate wireless network at a hank. 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 staff1. 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 332

- (Topic 3)
A network technician is installing a wireless network in an office building. After performing a site survey, the technician determines the area is very saturated on the 2.4GHz and the 5GHz bands. Which of the following wireless standards should the network technician implement?

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

Answer: B

Explanation:
* 802.11 ax is the latest wireless standard that operates in both the 2.4GHz and the 5GHz bands. It offers higher throughput, lower latency, and improved efficiency compared to previous standards. It also uses technologies such as OFDMA and MU-MIMO to reduce interference and increase capacity in dense environments. Therefore, 802.11 ax is the best choice for a wireless network in an office building with high saturation on both bands. References
? Part 3 of current page talks about the benefits of 802.11 ax and how it improves network performance in congested areas1.
? CompTIA Network+ N10-008 Exam Cram covers the wireless standards and their characteristics in Chapter 5. It also provides practice questions and explanations for the exam.

NEW QUESTION 333
.....

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