CompTIA

Exam Questions N10-009

CompTIA Network+ Exam

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

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

Answer: B

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

NEW QUESTION 3
- (Topic 3)
An organization has a security requirement that all network connections can be traced back to a user. A network administrator needs to identify a solution to implement on the wireless network. Which of the following is the best solution?

A. Implementing enterprise authentication
B. Requiring the use of PSKs
C. Configuring a captive portal for users
D. Enforcing wired equivalent protection

Answer: A

Explanation:
Enterprise authentication is a method of securing wireless networks that uses an external authentication server, such as RADIUS, to verify the identity of users and devices. Enterprise authentication can provide user traceability by logging the network connections and activities of each authenticated user. This can help the organization meet its security requirement and comply with any regulations or policies that mandate user accountability12.
References:
? CompTIA Network+ N10-008 Certification Exam Objectives, page 83
? CompTIA Network+ Cert Guide: Wireless Networking, page 13

NEW QUESTION 4
- (Topic 3)
A user in a branch office reports that access to all files has been lost after receiving a new PC. All other users in the branch can access fileshares. The IT engineer who is troubleshooting this incident is able to ping the workstation from the branch router, but the machine cannot ping the router. Which of the following is MOST likely the cause of the incident?

A. Incorrect subnet mask
B. Incorrect DNS server
C. Incorrect IP class
D. Incorrect TCP port

Answer: A

NEW QUESTION 5
- (Topic 3)
A customer needs six usable IP addresses. Which of the following best meets this requirement?

A. 255.255.255.128
B. 255.255.255.192
C. 255.255.255.224
D. 255.255.255.240

Answer: C

NEW QUESTION 6
- (Topic 3)
A technician is monitoring a network interface and notices the device is dropping packets. The cable and interfaces, however, are in working order. Which of the following is MOST likely the cause?

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

Answer: C

NEW QUESTION 7
- (Topic 3)
A technician removes an old PC from the network and replaces it with a new PC that is unable to connect to the LAN. Which of the Mowing is MOST likely the cause of the issue?

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

Answer: A

Explanation:
It is most likely that the issue is caused by port security, as this is a feature that can prevent new devices from connecting to the LAN. Port tagging, port aggregation, and port mirroring are all features that are used to manage traffic on the network, but they are not related to the connectivity of new devices. If the technician has configured port security on the network and the new PC does not meet the security requirements, it will not be able to connect to the LAN.

NEW QUESTION 8
- (Topic 3)
During the troubleshooting of an E1 line, the point-to-point link on the core router was accidentally unplugged and left unconnected for several hours. However, the network management team was not notified. Which of the following could have been configured to allow early detection and possible resolution of the issue?

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

Answer: A

Explanation:
Traps are unsolicited messages sent by network devices to a network management system (NMS) when an event or a change in status occurs. Traps can help notify the network management team of any issues or problems on the network, such as a link failure or a device reboot. Traps can also trigger actions or alerts on the NMS, such as sending an email or logging the event. MIB stands for Management Information Base and is a database of information that can be accessed and managed by an NMS using SNMP (Simple Network Management Protocol). OID stands for Object Identifier and is a unique name that identifies a specific variable in the MIB. Baselines are measurements of normal network performance and behavior that can be used for comparison and analysis. References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5: Given a scenario, use remote access methods.

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

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

Answer: A

NEW QUESTION 10
- (Topic 3)
Which of the following fiber connector types is the most likely to be used on a network interface card?

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

Answer: A

Explanation:
LC (local connector) is the most likely fiber connector type to be used on a network interface card, because it is a small form factor connector that can fit more interfaces on a single card. LC connectors use square connectors that have a locking mechanism on the top, similar to an RJ45 copper connector. LC connectors are also compatible with SFP (small form-factor pluggable) modules that are often used to link a gigabit Ethernet port with a fiber network12.
References:
? Optical Fiber Connectors – CompTIA Network+ N10-007 – 2.11
? CompTIA Network+ Certification Exam Objectives2

NEW QUESTION 12
- (Topic 3)
A network technician wants to find the shortest path from one node to every other node in the network. Which of the following algorithms will provide the FASTEST convergence time?

A. A static algorithm
B. A link-state algorithm
C. A distance-vector algorithm
D. A path-vector algorithm

Answer: B

Explanation:
A link-state algorithm is a routing algorithm that uses information about the state of each link in the network to calculate the shortest path from one node to every other node. A link-state algorithm requires each router to maintain a complete map of the network topology and exchange link-state advertisements with its neighbors periodically or when a change occurs. A link-state algorithm uses a mathematical formula called Dijkstra's algorithm to find the shortest path based on the link costs. A link-state algorithm provides the fastest convergence time because it can quickly detect and adapt to network changes. References: [CompTIA Network+ Certification Exam Objectives], [Link-state routing protocol - Wikipedia]

NEW QUESTION 15
- (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 16
- (Topic 3)
Which of the following would be used to adjust resources dynamically for a virtual web server under variable loads?

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

Answer: B

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

NEW QUESTION 17
- (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 22
- (Topic 3)
A network technician needs to ensure that all files on a company's network can be moved in a safe and protected manner without interception from someone who is not the intended recipient. Which of the following would allow the network technician to meet these requirements?

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

Answer: D

NEW QUESTION 24
- (Topic 3)
The Chief Executive Officer of a company wants to ensure business operations are not disrupted in the event of a disaster. The solution must have fully redundant equipment, real-time synchronization, and zero data loss. Which Of the following should be prepared?

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

Answer: C

Explanation:
A hot site is a backup site that is fully equipped and ready to take over the operations of the primary site in the event of a disaster. A hot site has real-time synchronization with the primary site and can provide zero data loss. A hot site is the most expensive and reliable option for disaster recovery.
References: Network+ Study Guide Objective 5.3: Explain common scanning, monitoring and patching processes and summarize their expected outputs.

NEW QUESTION 29
- (Topic 3)
Which of the following routing technologies is used to prevent network failure at the gateway by protecting data traffic from a failed router?

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

Answer: D

Explanation:
FHRP stands for First Hop Redundancy Protocol, and it is a group of protocols that allow routers to work together to provide backup or failover for the default gateway in a network. FHRP can prevent network failure at the gateway by protecting data traffic from a failed router and ensuring that there is always an active router to forward packets. Some examples of FHRP protocols are HSRP, VRRP, and GLBP12.
References: 1: CompTIA Network+ N10-008 Cert Guide - Chapter 13: Routing Protocols32: First Hop Redundancy Protocols (FHRP) Explained4

NEW QUESTION 34
- (Topic 3)
Due to space constraints in an IDF, a network administrator can only a do a single switch to
accommodate three data networks. The administrator needs a configuration that will allow each device to access its expected network without additional connections. The configuration must also allow each device to access the rest of the network. Which of the following should the administrator do to meet these requirements? (Select TWO).

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

Answer: AC

Explanation:
To achieve this, you should do two things:

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

NEW QUESTION 36
- (Topic 3)
A technician is troubleshooting reports that a networked printer is unavailable. The printer's IP address is configured with a DHCP reservation, but the address cannot be pinged from the print server in the same subnet. Which of the following is MOST likely the cause of me connectivity failure?

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

Answer: D

NEW QUESTION 41
- (Topic 3)
A VOIP phone is plugged in to a port but cannot receive calls. Which Of the following needs to be done on the port to address the issue?

A. Trunk all VLANs on the port.
B. Configure the native VLAN.
C. Tag the traffic to voice VLAN.
D. Disable VLANs.

Answer: C

Explanation:
To enable a VOIP phone to receive calls on a port, the traffic needs to be tagged to the voice VLAN that is configured on the switch. This allows the phone to communicate with the voice network and the PBX server. Tagging the traffic also separates the voice traffic from the data traffic that may be coming from a computer connected to the phone. The port should be configured to tag the traffic for the voice VLAN and untag the traffic for the data VLAN1. Trunking all VLANs on the port is unnecessary and may cause security issues. Configuring the native VLAN is not relevant for this issue. Disabling VLANs would prevent the phone from working at all.
References:
Optical Fiber Connectors – CompTIA Network+ N10-007 – 2.13
? VoIP and computer on separate VLANs through one cable1

NEW QUESTION 42
- (Topic 3)
Which of the following is the IEEE link cost for a Fast Ethernet interface in STP calculations?

A. 2
B. 4
C. 19
D. 100

Answer: D

Explanation:
The IEEE standard for link cost for a Fast Ethernet interface is 100, and for a Gigabit Ethernet interface is 19. These values are based on the bandwidth of the interface, with lower values indicating a higher-bandwidth interface.

NEW QUESTION 46
- (Topic 3)
A network technician needs to ensure the company's external mail server can pass reverse lookup checks. Which of the following records would the technician MOST likely configure? (Choose Correct option and give explanation directly from CompTIA Network+ Study guide or documents)

A. PTR
B. AAAA
C. SPF
D. CNAME

Answer: A

Explanation:
A PTR (Pointer) record is used to map an IP address to a domain name, which is necessary for reverse lookup checks. Reverse lookup checks are performed by external mail servers to verify the identity of the sender of the email. By configuring a PTR record, the network technician can ensure that the company's external mail server can pass these checks. According to the CompTIA Network+ Study Guide, "A PTR record is used to map an IP address to a domain name, and it is often used for email authentication."

NEW QUESTION 47
- (Topic 3)
A technician received a report that some users in a large, 30-floor building are having intermittent connectivity issues. Users on each floor have stable connectivity, but do not have connectivity to other floors. Which of the following devices is MOST likely causing the issue?

A. User devices
B. Edge devices
C. Access switch

D. Core switch

Answer: D

Explanation:
A core switch is the most likely device causing the issue where users on each floor have stable connectivity, but do not have connectivity to other floors. A core switch is a high-performance switch that connects multiple access switches in a network. An access switch is a switch that connects end devices, such as computers and printers, to the network. A core switch acts as the backbone of the network, providing interconnection and routing between different subnets or VLANs. If the core switch is malfunctioning or misconfigured, it can prevent communication between different segments of the network, resulting in intermittent connectivity issues. References: [CompTIA Network+ Certification Exam Objectives], Core Switch vs Access Switch: What Are the Differences?

NEW QUESTION 48
- (Topic 3)
A network technician has determined the cause of a network disruption. Which of the following is the NEXT step for the technician to perform?

A. Validate the findings in a top-to-bottom approach
B. Duplicate the issue, if possible
C. Establish a plan of action to resolve the issue
D. Document the findings and actions

Answer: C

NEW QUESTION 52
- (Topic 3)
Which of the following describes traffic going in and out of a data center from the internet?

A. Demarcation point
B. North-South
C. Fibre Channel
D. Spine and leaf

Answer: B

NEW QUESTION 56
- (Topic 3)
A malicious user is using special software 10 perform an on-path attack. Which of the following best practices should be configured to mitigate this threat?

A. Dynamic ARP inspection
B. Role-based access
C. Control plane policing
D. MAC filtering

Answer: A

NEW QUESTION 60
- (Topic 3)
A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks does the technician need to install?

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

Answer: A

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

NEW QUESTION 65
- (Topic 3)
A network resource was accessed by an outsider as a result of a successful phishing
campaign. Which of the following strategies should be employed to mitigate the effects of phishing?

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

Answer: A

Explanation:
Multifactor authentication is a security measure that requires users to provide multiple pieces of evidence before they can access a network resource. This could include requiring users to enter a username, password, and a code sent to the user's mobile phone before they are allowed access. This ensures that the user is

who they say they are, reducing the risk of malicious actors gaining access to network resources as a result of a successful phishing campaign.

NEW QUESTION 67
- (Topic 3)
Which of the following protocols uses Dijkstra's algorithm to calculate the LOWEST cost between routers?

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

Answer: B

Explanation:
OSPF stands for Open Shortest Path First and is a link-state routing protocol that uses Dijkstra's algorithm to calculate the lowest cost between routers. OSPF assigns a cost value to each link based on factors such as bandwidth, delay, or reliability, and builds a map of the network topology. OSPF then uses Dijkstra's algorithm to find the shortest path from each router to every other router in the network1. RIP stands for Routing Information Protocol and is a distance-vector routing protocol that uses hop count as the metric to find the best path. BGP stands for Border Gateway Protocol and is a path-vector routing protocol that uses attributes such as AS path, local preference, or origin to select the best route. EIGRP stands for Enhanced Interior Gateway Routing Protocol and is a hybrid routing protocol that uses a composite metric based on bandwidth, delay, load, and reliability.
References: 1 Dijkstra's algorithm - Wikipedia (https://en.wikipedia.org/wiki/Dijkstra%27s_algorithm)

NEW QUESTION 69
- (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 72
- (Topic 3)
Which of the following network cables involves bouncing light off of protective cladding?

A. Twinaxial
B. Coaxial
C. Single-mode
D. Multimode

Answer: D

Explanation:
Multimode fiber optic cables use multiple paths of light that bounce off the cladding, which is a layer of glass or plastic that surrounds the core of the cable.
https://www.explainthatstuff.com/fiberoptics.html

NEW QUESTION 77
- (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 82
- (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 85
- (Topic 3)
A network technician recently installed 35 additional workstations. After installation, some users are unable to access network resources. Many of the original workstations that are experiencing the network access issue were offline when the new workstations were turned on. Which of the following is the MOST likely cause of this issue?

A. Incorrect VLAN setting
B. Insufficient DHCP scope
C. Improper NIC setting
D. Duplicate IP address

Answer: B

NEW QUESTION 87
- (Topic 3)
The lack of a formal process to grant network permissions to different profiles of employees and contractors is leading to an increasing number of security incidents Non-uniform and overly permissive network accesses are being granted. Which of the following would be the MOST appropriate method to improve the security of the environment?

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

Answer: D

Explanation:
The most appropriate method to improve the security of the environment would be to implement role-based access control (RBAC). With RBAC, users are granted access to the network based on their role within the organization. This allows for more granular access control, as different roles may require different levels of access. Additionally, this ensures that users only have access to the resources they need and no more. This helps to reduce the risk of unauthorized access or misuse of the network. References and further information can be found in the CompTIA Network+ Study Manual, Chapter 8, Access Control.
RBAC is a method of restricting network access based on the roles of individual users within the organization. With RBAC, users are granted access only to the resources they need to perform their specific job functions. This approach reduces the risk of unauthorized access, provides greater visibility into user activity, and simplifies network management. Changing the default permissions to implicit deny may improve security, but it could also cause issues for legitimate users who require access to specific resources. Configuring uniform ACLs and NAC for contractors is a step in the right direction, but it may not be enough to address the overall lack of a formal process for granting network permissions. Deploying an RDP server to centralize access to the network is not a viable solution, as it would not address the root cause of the security incidents.
Therefore, the most appropriate option is to implement role-based access control. Reference: CompTIA Network+ Study Guide, Fourth Edition, Chapter 7, section 7.4.

NEW QUESTION 89
- (Topic 3)
A network technician is having issues connecting an loT sensor to the internet The WLAN settings were enabled via a custom command line, and a proper IP address assignment was received on the wireless interlace. However, when trying to connect to the internet, only HTTP redirections are being received when data Is requested. Which of the following will point to the root cause of the Issue?

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

Answer: C

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

NEW QUESTION 91
- (Topic 3)
A network administrator wants to test the throughput of a new metro Ethernet circuit to verify that its performance matches the requirements specified m the SLA. Which of the following would BEST help measure the throughput?

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

Answer: A

NEW QUESTION 94
- (Topic 3)
A network administrator is decommissioning a server. Which of the following will the network administrator MOST likely consult?

A. Onboarding and off boarding policies
B. Business continuity plan
C. Password requirements
D. Change management documentation

Answer: D

NEW QUESTION 99
- (Topic 3)
Which of the following would be the BEST choice to connect branch sites to a main office securely?

A. VPN headend
B. Proxy server
C. Bridge
D. Load balancer

Answer: A

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

NEW QUESTION 103
- (Topic 3)
Which of the following types of data center architectures will MOST likely be used in a large SDN and can be extended beyond the data center?

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

Answer: D

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

NEW QUESTION 106
- (Topic 3)
An online gaming company needs a cloud solution that will allow for more virtual resources to be deployed when tournaments are held. The number of users who access the service increases during tournaments. The company also needs the resources to return to baseline levels once the resources are not needed in order to reduce cost. Which of the following cloud concepts would provide the best solution?

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

Answer: D

Explanation:
Elasticity is the ability of a cloud service to automatically adjust the amount of resources allocated to meet the changing demand of the users. Elasticity enables a cloud service to scale up or down resources quickly and efficiently, without requiring manual intervention or planning. Elasticity is ideal for scenarios where the demand is unpredictable, dynamic, or seasonal, such as online gaming tournaments. By using elasticity, the online gaming company can ensure optimal performance and user experience during peak times, while also saving costs and avoiding overprovisioning during off-peak times.
The other options are not correct because they do not address the specific needs of the online gaming company. They are:
•Scalability is the ability of a cloud service to handle an increase or decrease in the demand of the users by adding or removing resources. Scalability is similar to elasticity, but it is more manual, planned, and predictive, while elasticity is automatic, prompt, and reactive. Scalability is suitable for scenarios where the demand is steady, predictable, or gradual, such as a growing business or a long-term project.
•Hybrid is a type of cloud model that combines two or more clouds, such as on-premises private, hosted private, or public, that can be centrally managed to enable interoperability for various use cases. Hybrid cloud can offer benefits such as flexibility, security, and cost- efficiency, but it does not directly address the need for dynamic resource allocation for the online gaming company.
•Multitenancy is a feature of cloud services that allows multiple users or customers to share the same physical or virtual resources, such as servers, databases, or applications, while maintaining isolation and privacy. Multitenancy can offer benefits such as efficiency, scalability, and cost-effectiveness, but it does not directly address the need for dynamic resource allocation for the online gaming company.
References
1: Understand cloud concepts | Microsoft Press Store 2: What Is Hybrid Cloud? - Cisco
3: Difference between Elasticity and Scalability in Cloud Computing 4: Scalability and Elasticity in Cloud Computing - GeeksforGeeks

NEW QUESTION 109
- (Topic 3)
During an annual review of policy documents, a company decided to adjust its recovery time frames. The company agreed that critical applications can be down for no more than six hours, and the acceptable amount of data loss is no more than two hours. Which of the following should be documented as the RPO?

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

Answer: A

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

NEW QUESTION 112
- (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 117
- (Topic 3)
A network administrator is in the process of installing 35 PoE security cameras. After the administrator installed and tested the new cables, the administrator installed the cameras. However, a small number of the cameras do not work. Which of the following is the most likely reason?

A. Incorrect wiring standard
B. Power budget exceeded
C. Signal attenuation
D. Wrong voltage

Answer: B

Explanation:
The power budget is the total amount of power that a PoE switch or injector can provide to the connected PoE devices. If the power budget is exceeded, some of the PoE devices may not receive enough power to function properly. To troubleshoot this issue, the network administrator should check the power consumption of each PoE device and the power capacity of the PoE switch or injector.
References:
? PoE Troubleshooting: The Common PoE Errors and Solutions1
? Security Camera Won't Work - Top 10 Solutions to Fix2
? CompTIA Network+ N10-008 Exam Objectives https://www.comptia.org/certifications/network#examdetails

NEW QUESTION 122
- (Topic 3)
A network administrator Is looking at switch features and is unsure whether to purchase a model with PoE Which of the following devices that commonly utilize PoE should the administrator consider? (Select TWO)

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

Answer: AB

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

NEW QUESTION 125
- (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 127
- (Topic 3)
A network deployment engineer is deploying a new single-channel 10G optical connection. Which of the following optics should the engineer MOST likely use to satisfy this requirement?

A. QSFP
B. QSFP+
C. SFP
D. SFP+

Answer: D

Explanation:
SFP+ is a type of optical transceiver that supports 10G single-channel transmission over fiber optic cables. SFP+ stands for small form-factor pluggable plus, and it is compatible with SFP slots on switches and routers.

NEW QUESTION 132
- (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 137
- (Topic 3)
A technician is configuring a static IP address on a new device in a newly created subnet. The work order specifies the following requirements:
• The IP address should use the highest address available in the subnet.
• The default gateway needs to be set to 172.28.85.94.
• The subnet mask needs to be 255.255.255.224.
Which of the following addresses should the engineer apply to the device?

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

Answer: A

Explanation:
https://www.tunnelsup.com/subnet-calculator/
IP Address: 172.28.85.95/27 Netmask: 255.255.255.224
Network Address: 172.28.85.64
Usable Host Range: 172.28.85.65 - 172.28.85.94
Broadcast Address: 172.28.85.95

NEW QUESTION 139
- (Topic 3)
Which of the following is a benefit of the spine-and-leaf network topology?

A. Increased network security
B. Stable network latency
C. Simplified network management

D. Eliminated need for inter-VLAN routing

Answer: A

NEW QUESTION 140
- (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 143
- (Topic 3)
Which of the following would be used to forward requests and replies between a DHCP server and client?

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

Answer: B

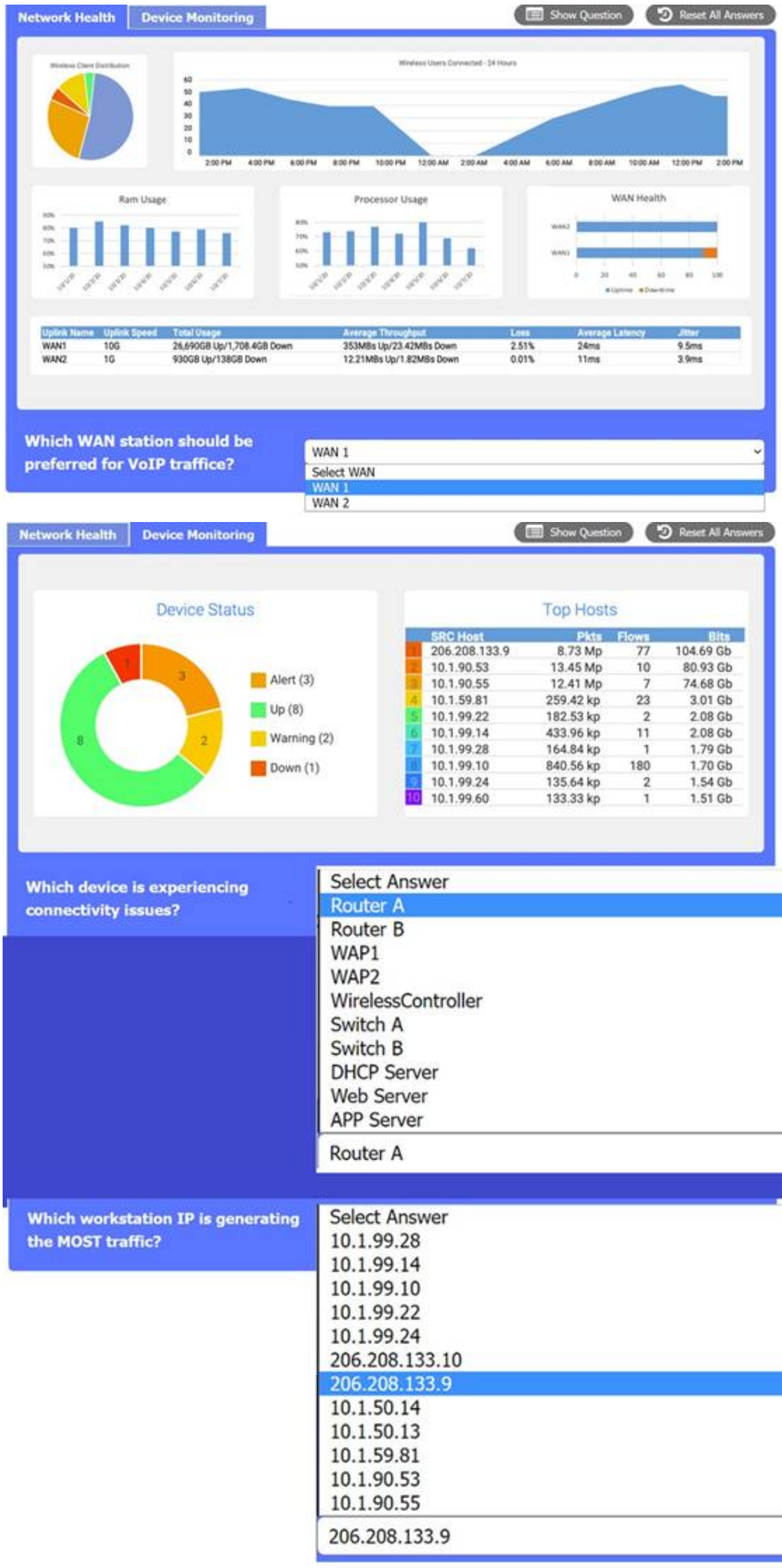
NEW QUESTION 145
- (Topic 3)
A technician is equipped with a tablet, a smartphone, and a laptop to troubleshoot a switch with the help of support over the phone. However, the technician is having issues interconnecting all these tools in troubleshooting the switch. Which Of the following should the technician use to gain connectivity?

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

Answer: A

Explanation:
A PAN stands for Personal Area Network and it is a type of network that connects devices within a small range, such as a few meters. A PAN can use wireless technologies such as Bluetooth or Wi-Fi to interconnect devices such as tablets, smartphones, and laptops. A technician can use a PAN to gain connectivity among these tools and troubleshoot the switch.
References: Network+ Study Guide Objective 1.2: Explain devices, applications, protocols and services at their appropriate OSI layers.

NEW QUESTION 149
SIMULATION - (Topic 3)
After a recent power outage, users are reporting performance issues accessing the application servers. Wireless users are also reporting intermittent Internet issues.
INSTRUCTIONS
Click on each tab at the top of the screen. Select a widget to view information, then
use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Network Health:
WAN 2 appears to have a lower average latency and loss percentage, which would make it the preferred WAN station for VoIP traffic. VoIP traffic requires low latency and packet loss to ensure good voice quality and reliability. WAN 1 seems to have higher RAM and processor usage, which could also affect the performance of VoIP traffic.
Here's the summary of the key metrics for WAN 1 and WAN 2 from the image provided:

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

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

A screenshot of a computer
Description automatically generated

NEW QUESTION 151
- (Topic 3)
Which of me following security controls indicates unauthorized hardware modifications?

A. Biometric authentication
B. Media device sanitization
C. Change management policy
D. Tamper-evident seals

Answer: A

NEW QUESTION 156
- (Topic 3)

A company has been added to an unapproved list because of spam. The network administrator confirmed that a workstation was infected by malware. Which of the following processes did the administrator use to identify the root cause?

A. Traffic analysis
B. Availability monitoring
C. Baseline metrics
D. Network discovery

Answer: A

Explanation:
One possible process that the administrator used to identify the root cause of the spam issue is traffic analysis. Traffic analysis is a technique that monitors and analyzes the network traffic that flows between devices or applications. Traffic analysis can help troubleshoot network problems by identifying the source, destination, volume, frequency, and content of the network packets12.
To use traffic analysis to identify the root cause of the spam issue, the administrator could follow these steps:
? Install a traffic analysis tool on the server or a device that is connected to the same
network as the server, such as Wireshark3, tcpdump4, or Microsoft Network Monitor5.
? Start capturing the network traffic and filter it by using the IP address or hostname
of the server, or by using a specific port or protocol that is used by the email service, such as SMTP (port 25), POP3 (port 110), or IMAP (port 143).
? Analyze the filtered traffic and look for any signs of abnormal or malicious activity, such as high volume of outgoing emails, unknown recipients, suspicious attachments, or spam keywords.
? Trace back the source of the spam emails to the infected workstation by using its IP address or MAC address.
? Isolate and clean up the infected workstation by using an antivirus or malware removal tool.
The other options are not processes that the administrator used to identify the root cause of the spam issue. Availability monitoring is a technique that measures and reports the uptime and downtime of a network device or service. Availability monitoring can help troubleshoot network problems by detecting any failures or outages that affect the network performance. Baseline metrics are a set of standard measurements that establish the normal behavior or performance of a network device or service. Baseline metrics can help troubleshoot network problems by comparing the current state of the network with the expected state and identifying any deviations or anomalies. Network discovery is a technique that scans and maps the network devices and services that are connected to a network. Network discovery can help troubleshoot network problems by providing a comprehensive and updated view of the network topology and configuration.

NEW QUESTION 159
- (Topic 3)
An on-call network technician receives an automated email alert stating that a power supply on a firewall has just powered down. Which of the following protocols would best allow for this level of detailed device monitoring?

A. TFTP
B. TLS
C. SSL
D. SNMP

Answer: D

Explanation:
SNMP stands for Simple Network Management Protocol, and it is a protocol that allows network devices to communicate their status, performance, and configuration information to a central management system. SNMP can be used to monitor and manage various aspects of network devices, such as CPU usage, memory utilization, interface statistics, temperature, voltage, power supply, etc. SNMP can also generate alerts or notifications when certain events or thresholds are reached, such as a power supply failure, a link down, or a high traffic volume. SNMP is widely used for network monitoring and troubleshooting purposes, as it provides a comprehensive and detailed view of the network health and performance.
The other options are not correct because they are not protocols that allow for detailed device monitoring. They are:
? TFTP. TFTP stands for Trivial File Transfer Protocol, and it is a protocol that allows for simple and fast file transfer between network devices. TFTP is often used to transfer configuration files, firmware updates, or boot images to network devices, such as routers, switches, or firewalls. TFTP does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.
? TLS. TLS stands for Transport Layer Security, and it is a protocol that provides encryption and authentication for data transmission over a network. TLS is often used to secure web traffic, email, or other applications that use TCP as the transport protocol. TLS does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.
? SSL. SSL stands for Secure Sockets Layer, and it is a protocol that provides encryption and authentication for data transmission over a network. SSL is the predecessor of TLS, and it is still used to secure some web traffic, email, or other applications that use TCP as the transport protocol. SSL does not provide any monitoring or management capabilities for network devices, nor does it generate any alerts or notifications.
References1: What is SNMP? - Definition from WhatIs.com2: Network+ (Plus) Certification
| CompTIA IT Certifications3: What is TFTP? - Definition from WhatIs.com4: What is TLS? - Definition from WhatIs.com5: What is SSL? - Definition from WhatIs.com

NEW QUESTION 161
- (Topic 3)
An ISP is unable to provide services to a user in a remote area through cable and DSL. Which of the following is the NEXT best solution to provide services without adding external infrastructure?

A. Fiber
B. Leased line
C. Satellite
D. Metro optical

Answer: C

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

NEW QUESTION 166

- (Topic 3)
Which of the following steps of the troubleshooting methodology would most likely include checking through each level of the OSI model after the problem has been identified?

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

Answer: C

Explanation:
Creating a plan of action is the step of the troubleshooting methodology that would most likely include checking through each level of the OSI model after the problem has been identified. According to the web search results, the troubleshooting methodology consists of the following steps: 12
? Define the problem: Identify the symptoms and scope of the problem, and gather relevant information from users, devices, and logs.
? Establish a theory: Based on the information collected, hypothesize one or more possible causes of the problem, and rank them in order of probability.
? Test the theory: Test the most probable cause first, and if it is not confirmed, eliminate it and test the next one. Repeat this process until the root cause is found or a new theory is needed.
? Create a plan of action: Based on the confirmed cause, devise a solution that can resolve the problem with minimal impact and risk. The solution may involve checking through each level of the OSI model to ensure that all layers are functioning properly and that there are no configuration errors, physical damages, or logical inconsistencies34
? Implement the solution: Execute the plan of action, and monitor the results. If the problem is not solved, revert to the previous state and create a new plan of action.
? Verify functionality: Confirm that the problem is fully resolved and that the network is restored to normal operation. Perform preventive measures if possible to avoid recurrence of the problem.
? Document the findings: Record the problem description, the solution, and the outcome. Update any relevant documentation, such as network diagrams, policies, or procedures.
References1: Troubleshooting Methods for Cisco IP Networks 2: Troubleshooting Methodologies - CBT IT Certification Training 3: How to use the OSI Model to Troubleshoot Networks 4: How is the OSI model used in troubleshooting? – Sage-Answer

NEW QUESTION 168
- (Topic 3)
Which of the following describes when an active exploit is used to gain access to a network?

A. Penetration testing
B. Vulnerability testing
C. Risk assessment
D. Posture assessment
E. Baseline testing

Answer: A

Explanation:
Penetration testing is a type of security testing that is used to assess the security of a system or network by actively exploiting known vulnerabilities. It is used to simulate an attack on the system and identify any weaknesses that may be exploited by malicious actors. As stated in the CompTIA Security+ Study Guide, "penetration testing is a type of security assessment that attempts to gain unauthorized access to networks and systems by exploiting security vulnerabilities."

NEW QUESTION 173
- (Topic 3)
Which of the following is MOST appropriate for enforcing bandwidth limits when the performance of an application is not affected by the use of buffering but is heavily impacted by packet drops?

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

Answer: B

Explanation:
Traffic policing is a mechanism that monitors the traffic in any network and enforces a bandwidth limit by discarding packets that exceed a certain rate1. This can reduce congestion and ensure fair allocation of bandwidth among different applications or users. However, discarding packets can also affect the performance and quality of some applications, especially those that are sensitive to packet loss, such as voice or video. Traffic shaping is a congestion control mechanism that delays packets that exceed a certain rate instead of discarding them1. This can smooth out traffic bursts and avoid packet loss, but it also introduces latency and jitter. Traffic shaping can be beneficial for applications that can tolerate some delay but not packet loss, such as file transfers or streaming.
Traffic marking is a mechanism that assigns different priority levels to packets based on their type, source, destination, or other criteria2. This can help to differentiate between different classes of service and apply different policies or treatments to them. However, traffic marking does not enforce bandwidth limits by itself; it only provides information for other mechanisms to act upon.
Traffic classification is a process that identifies and categorizes packets based on their characteristics, such as protocol, port number, payload, or behavior. This can help to distinguish between different types of traffic and apply appropriate policies or actions to them. However, traffic classification does not enforce bandwidth limits by itself; it only provides input for other mechanisms to use.

NEW QUESTION 176
- (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 179
- (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 180
- (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 185
- (Topic 3)
Which of the following most likely occurs when an attacker is between the target and a legitimate server?

A. IP spoofing
B. VLAN hopping
C. Rogue DHCP
D. On-path attack

Answer: D

Explanation:
An on-path attack (also known as a man-in-the-middle attack) is a type of security attack where the attacker places themselves between two devices (often a web browser and a web server) and intercepts or modifies communications between the two1. The attacker can then collect information as well as impersonate either of the two agents. For example, an on-path attacker could capture login credentials, redirect traffic to malicious sites, or inject malware into legitimate web pages.
The other options are not correct because they describe different types of attacks:
•IP spoofing is the practice of forging the source IP address of a packet to make it appear as if it came from a trusted or authorized source2.
•VLAN hopping is a technique that allows an attacker to access a VLAN that they are not authorized to access by sending packets with a modified VLAN tag3.
•Rogue DHCP is a scenario where an unauthorized DHCP server offers IP configuration parameters to clients on a network, potentially causing network disruption or redirection to malicious sites4.
References
2: Understanding Targeted Attacks: What is a Targeted Attack? 3: Types of attacks - Security on the web | MDN
1: What is an on-path attacker? | Cloudflare
4: [What is a Rogue DHCP Server? - Definition from Techopedia]

NEW QUESTION 186
- (Topic 3)
An AP uses a 98ft (30m) Cat 6 cable to connect to an access switch. The cable is wired through a duct close to a three-phase motor installation. Anytime the three-phase is turned on, all users connected to the switch experience high latency on the network. Which Of the following is MOST likely the cause Of the issue?

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

Answer: A

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

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

NEW QUESTION 188
- (Topic 3)
A user reports that a crucial fileshare is unreachable following a network upgrade that was completed the night before. A network technician confirms the problem exists. Which of the following
troubleshooting Steps should the network technician perform NEXT?

A. Establish a theory of probable cause.
B. Implement a solution to fix the problem.
C. Create a plan of action to resolve the problem.
D. Document the problem and the solution.

Answer: A

Explanation:
Establishing a theory of probable cause is the third step in the general troubleshooting process, after identifying the problem and gathering information. Establishing a theory of probable cause involves using the information gathered to formulate one or more possible explanations for the problem and testing them to verify or eliminate them. In this scenario, the network technician has confirmed the problem exists
and should proceed to establish a theory of probable cause based on the information available, such as the network upgrade that was completed the night before.
Implementing a solution to fix the problem is the fifth step in the general troubleshooting process, after establishing a plan of action. Implementing a solution involves applying the chosen method or technique to resolve the problem and verifying its effectiveness. In this scenario, the network technician has not established a plan of action yet and should not implement a solution without knowing the cause of the problem.
Creating a plan of action to resolve the problem is the fourth step in the general troubleshooting process, after establishing a theory of probable cause. Creating a plan of action involves selecting the best method or technique to address the problem based on the available resources, constraints, and risks. In this scenario, the network technician has not established a theory of probable cause yet and should not create a plan of action without knowing the cause of the problem.
Documenting the problem and the solution is the seventh and final step in the general troubleshooting process, after implementing preventive measures. Documenting the problem and the solution involves recording the details of the problem, its symptoms, its cause, its solution, and its preventive measures for future reference and improvement. In this scenario, the network technician has not implemented preventive measures yet and should not document the problem and the solution without resolving and preventing it.

NEW QUESTION 193
- (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 195
- (Topic 3)
After router and device configurations are applied, internet access is not possible. Which of the following is the most likely cause?

A. The Ethernet interface was configured with an incorrect IP address.
B. The router was configured with an incorrect loopback address.
C. The router was configured with an incorrect default gateway.
D. The serial interface was configured with the incorrect subnet mas

Answer: C

Explanation:

The default gateway is the IP address of the router that connects a network to the internet or another network. The default gateway is usually configured on the devices that need to access the internet or other networks, such as PCs, servers, or routers. If the router was configured with an incorrect default gateway, it would not be able to forward packets to the correct destination, and internet access would not be possible.
The other options are not the most likely causes of the issue. The Ethernet interface is the physical port that connects a device to a network using a cable. If the Ethernet interface was configured with an incorrect IP address, it would cause a problem with the local network connectivity, not the internet access. The loopback address is a special IP address that refers to the device itself, usually used for testing or troubleshooting purposes. If the router was configured with an incorrect loopback address, it would not affect the internet access, as the loopback address is not used for routing packets to other networks. The serial interface is another type of physical port that connects a device to a network using a serial cable, often used for WAN connections. If the serial interface was configured with the incorrect subnet mask, it would cause a problem with the WAN connectivity, not the internet access, as the subnet mask is used to determine the network and host portions of an IP address.
ReferencesWhat is a Default Gateway? | HowStuffWorksWhat is an Ethernet Interface? - Definition from TechopediaWhat is a Loopback Address? - Definition from TechopediaWhat is a Serial Interface? - Definition from Techopedia

NEW QUESTION 197

- (Topic 3)
Which of the following use cases would justify the deployment of an mGRE hub-and-spoke topology?

A. An increase in network security using encryption and packet encapsulation
B. A network expansion caused by an increase in the number of branch locations to the headquarters
C. A mandatory requirement to increase the deployment of an SDWAN network
D. An improvement in network efficiency by increasing the useful packet payload

Answer: B

Explanation:

mGRE (Multipoint GRE) is a type of GRE (Generic Routing Encapsulation) tunnel that allows a single interface to support multiple tunnel endpoints, instead of having to configure a separate point-to-point tunnel for each destination. mGRE simplifies the configuration and management of large-scale VPN networks, such as DMVPN (Dynamic Multipoint VPN), which is a Cisco technology that uses mGRE, NHRP (Next Hop Resolution Protocol), and IPsec to create secure and dynamic VPN connections between a hub and multiple spokes1.
A network expansion caused by an increase in the number of branch locations to the headquarters would justify the deployment of an mGRE hub-and-spoke topology, because it would reduce the complexity and overhead of configuring and maintaining multiple point- to-point tunnels between the hub and each spoke. mGRE would also enable spoke-to- spoke communication without having to go through the hub, which would improve the network performance and efficiency23.
The other options are not directly related to the use case of mGRE hub-and-spoke topology. An increase in network security using encryption and packet encapsulation can be achieved by using IPsec, which is a separate protocol that can be applied to any type of GRE tunnel, not just mGRE. A mandatory requirement to increase the deployment of an SDWAN network can be met by using various technologies and vendors, not necessarily mGRE or DMVPN. An improvement in network efficiency by increasing the useful packet payload can be achieved by using various techniques, such as compression, fragmentation, or QoS, not specifically mGRE.
ReferencesUnderstanding Cisco Dynamic Multipoint VPN - DMVPN, mGRE, NHRPMGRE Easy Steps - Cisco CommunityWhat is DMVPN (Dynamic Multipoint VPN), NHRP, mGRE and How to configu - Cisco Community

NEW QUESTION 200
- (Topic 3)
After a firewall replacement, some alarms and metrics related to network availability stopped updating on a monitoring system relying on SNMP. Which of the following should the network
administrator do first?

A. Modify the device's MIB on the monitoring system.
B. Configure syslog to send events to the monitoring system.
C. Use port mirroring to redirect traffic to the monitoring system.
D. Deploy SMB to transfer data to the monitoring syste

Answer: A

Explanation:

SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a monitoring system and provide information about their status, performance, and configuration. SNMP relies on MIBs (Management Information Bases), which are collections of objects that define the types of information that can be accessed or modified on a device1.
When a firewall replacement occurs, the new firewall may have a different MIB than the old one, which means that the monitoring system may not be able to recognize or interpret the data sent by the new firewall. This can cause some alarms and metrics related to network availability to stop updating on the monitoring system. To fix this, the network administrator should modify the device’s MIB on the monitoring system, so that it matches the MIB of the new firewall and can correctly process the SNMP data2.
The other options are not relevant to the issue. Configuring syslog to send events to the monitoring system would not affect the SNMP data, as syslog is a different protocol that sends log messages from network devices to a central server. Using port mirroring to redirect traffic to the monitoring system would not help, as port mirroring is a technique that copies traffic from one port to another for analysis or troubleshooting purposes, but does not change the format or content of the traffic. Deploying SMB to transfer data to the monitoring system would not work, as SMB is a protocol that allows file sharing and access between network devices, but does not support SNMP data.
ReferencesGrafana & Prometheus SNMP: advanced network monitoring guideConfiguring Windows Systems for Monitoring with SNMP - ScienceLogic

NEW QUESTION 201
- (Topic 3)
Which of the following is most closely associated with attempting to actively prevent network intrusion?

A. IDS
B. Firewall
C. IPS
D. VPN

Answer: C

Explanation:

An intrusion prevention system (IPS) is a network security tool that continuously monitors network traffic for malicious activity and takes action to prevent it, such as reporting, blocking, or dropping it. An IPS is different from an intrusion detection system (IDS), which only detects and alerts about threats, but does not stop them. A firewall is a device or software that filters network traffic based on predefined rules, but it does not analyze the traffic for anomalies or signatures of known attacks. A VPN is a virtual private network that creates a secure tunnel between two endpoints, but it does not prevent intrusions from within the network or from compromised endpoints.
ReferencesWhat is an Intrusion Prevention System (IPS)? | FortinetWhat is an Intrusion Prevention System? - Palo Alto Networks

NEW QUESTION 202
- (Topic 3)
A network administrator is creating a VLAN that will only allow executives to connect to a data source. Which of the following is this scenario an example of?

A. Availability
B. Confidentiality
C. Internal threat
D. External threat
E. Integrity

Answer: B

Explanation:

Confidentiality is the principle of preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information1. By creating a VLAN that will only allow executives to connect to a data source, the network administrator is implementing a form of network segmentation that enhances the confidentiality of the data. This prevents unauthorized users or processes from accessing or modifying the data, which could compromise its integrity or availability. Confidentiality is one of the components of the CIA triad, a widely used information security model that guides the efforts and policies aimed at keeping data secure234.
ReferencesDefending Your Network: A Comprehensive Guide to VLAN Hopping AttacksThe CIA triad: Definition, components and examples | CSO OnlineExecutive Summary — NIST SP 1800-25 documentationThe CIA Triad — Confidentiality, Integrity, and Availability ExplainedConfidentiality, Integrity and Availability - DevQA.io

NEW QUESTION 205
- (Topic 3)
A user cannot connect to the network, although others in the office are unaffected. The network technician sees that the link lights on the NIC are not on. The technician needs to check which switchport the user is connected to, but the cabling is not labeled. Which of the following is the best way for the technician to find where the computer is connected?

A. Look up the computer's IP address in the switch ARP table.
B. Use a cable tester to trace the cable.
C. Look up the computer's MAC address in the switch CAM table.
D. Use a tone generator to trace the cable.

Answer: D

Explanation:

A tone generator is a device that emits an audible signal on a wire. A tone probe is a device that detects the signal on the wire. By attaching the tone generator to one end of the cable and using the tone probe to scan the other end, the technician can identify which switchport the cable is connected to. This method does not require any knowledge of the computer’s IP or MAC address, or access to the switch configuration. It is also faster and more reliable than physically tracing the cable or disconnecting the cable and looking for the link light to go out on the switch.
ReferencesHow to find what port im connected to on a switch from my PC?Switch Port Monitoring Guide - ComparitechFinding Out Which Network Switch Port My Computer is Connected

NEW QUESTION 209
- (Topic 3)
A customer runs a DNS lookup service and needs a network technician to reconfigure the network to improve performance. The customer wants to ensure that servers are accessed based on whichever one is topographically closest to the destination. If the server does not respond, then the next topographically closest server should respond Which of the following does the technician need to configure to meet the requirements?

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

Answer: B

Explanation:
Anycast addressing is a network addressing and routing methodology in which a single destination address has multiple routing paths to two or more endpoint destinations. Routers will select the desired path on the basis of number of hops, distance, lowest cost, latency measurements or based on the least congested route. Anycast addressing is designed to provide high availability and low latency for services that have multiple instances across the world, such as DNS servers. By using anycast addressing, the customer can ensure that servers are accessed based on whichever one is topographically closest to the destination. If the server does not respond, then the next topographically closest server should respond. References: [CompTIA Network+ Certification Exam Objectives], [Anycast - Wikipedia]

NEW QUESTION 214
- (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 219
- (Topic 3)
A network administrator has received calls every day for the past few weeks from three users who cannot access the network. The administrator asks all the users to reboot their PCs, but the same users still cannot access the system. The following day, three different users report the same issue, and the administrator asks them all to reboot their PCs; however, this does not fix the issue. Which of the following is MOST likely occurring?

A. Incorrect firewall settings
B. Inappropriate VLAN assignment
C. Hardware failure
D. Overloaded CAM table in switch
E. DHCP scope exhaustion

Answer: E

NEW QUESTION 224
- (Topic 3)
A hacker used a packet sniffer on the network to capture the hardware address of the server. Which of the following types of attacks can the hacker perform now?

A. Piggybacking
B. MAC spoofing
C. Evil twin
D. VLAN hopping

Answer: B

Explanation:
MAC spoofing is a technique that allows a hacker to change the media access control (MAC) address of their network interface card (NIC) to impersonate another device on the network. By capturing the hardware address of the server, the hacker can spoof their MAC address to match the server's and bypass any MAC-based security measures, such as MAC filtering or MAC authentication. MAC spoofing can also be used to perform man-in- the-middle attacks, where the hacker intercepts and alters the traffic between two devices on the network. References: CompTIA Network+ N10-008 Cert Guide, Chapter 7, Section 7.3

NEW QUESTION 226
- (Topic 3)
A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds hundreds of CRC errors on an interface. Which of the following is the MOST likely cause of these errors?

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

Answer: A

NEW QUESTION 231
- (Topic 3)
A company wants to implement a disaster recovery site for non-critical applications, which can tolerate a short period of downtime. Which of the following types of sites should the company implement to achieve this goal?

A. Hot
B. Cold
C. warm
D. Passive

Answer: C

Explanation:
The type of site that the company should implement for non-critical applications that can tolerate a short period of downtime is a warm site. A warm site is a disaster recovery site that has some pre-installed equipment and software, but not as much as a hot site, which is fully operational and ready to take over the primary site's functions in case of a disaster. A warm site requires some time and effort to activate and synchronize with the primary site, but not as much as a cold site, which has no equipment or software installed and requires a lot of configuration and testing. A passive site is not a common term for a disaster recovery site, but it could refer to a site that only receives backups from the primary site and does not actively participate in the network operations. References: CompTIA Network+ N10- 008 Certification Study Guide, page 347; The Official CompTIA Network+ Student Guide (Exam N10-008), page 13-10.

NEW QUESTION 232
- (Topic 3)
A network technician is selecting new network hardware, and availability is the main concern. Which of the following availability concepts should the technician consider?

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

Answer: A

Explanation:
The availability concept that the network technician should consider when selecting new network hardware is RTO (Recovery Time Objective). RTO is a metric that defines the maximum acceptable time for restoring a system or service after a disruption or failure. RTO is based on the impact and cost of downtime for the business and its customers. RTO helps determine the level of redundancy and backup needed for network hardware to ensure high availability and minimize downtime. References: CompTIA Network+ N10-008 Certification Study Guide, page 346; The Official CompTIA Network+ Student Guide (Exam N10-008), page 13-9.

NEW QUESTION 235
- (Topic 3)

Which of the following devices and encapsulations are found at the data link layer? (Select two).

A. Session
B. Frame
C. Firewall
D. Switch
E. Packet
F. Router

Answer: BD

Explanation:
A frame is a unit of data that is transmitted at the data link layer of the OSI model. A frame consists of a header, a payload, and a trailer. The header contains information such as the source and destination MAC addresses, the frame type, and the error detection code. The payload contains the data from the upper layer protocols, such as IP packets. The trailer contains the frame check sequence, which is used to verify the integrity of the frame. A switch is a device that operates at the data link layer of the OSI model. A switch forwards frames based on the MAC addresses of the devices connected to its ports. A switch can create separate collision domains and reduce network congestion. A switch can also implement VLANs, which are logical groups of devices that share the same broadcast domain, regardless of their physical location. A session is a logical connection between two or more devices that allows the exchange of data at the transport layer of the OSI model. A session is not a device or an encapsulation at the data link layer. A firewall is a device that operates at the network layer or the application layer of the OSI model. A firewall filters packets based on the IP addresses, ports, protocols, or application rules. A firewall is not a device or an encapsulation at the data link layer. A packet is a unit of data that is transmitted at the network layer of the OSI model. A packet consists of a header and a payload. The header contains information such as the source and destination IP addresses, the protocol type, and the hop count. The payload contains the data from the upper layer protocols, such as TCP segments. A packet is not an encapsulation at the data link layer. A router is a device that operates at the network layer of the OSI model. A router forwards packets based on the IP addresses and the routing table. A router can create separate broadcast domains and connect different networks. A router is not a device or an
encapsulation at the data link layer. References: CompTIA Network+ N10-008 Cert Guide, Chapter 2, Section 2.2 and CompTIA Network+ N10-008 Cert Guide, Chapter 3, Section 3.1

NEW QUESTION 238
- (Topic 3)
Which of the following authentication methods requires a user to enter a password and scan a fingerprint?

A. Single sign-on
B. Kerberos
C. Multifactor
D. Network access control

Answer: C

Explanation:
Multifactor authentication is a method of verifying a user’s identity by requiring more than one factor, such as something the user knows, something the user has, or something the user is. A password is something the user knows, and a fingerprint is something the user is. Therefore, a user who needs to enter a password and scan a fingerprint is using multifactor authentication.

NEW QUESTION 243
- (Topic 3)
Which of the following ports should be used to securely receive mail that is synchronized across multiple devices?

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

Answer: D

NEW QUESTION 248
- (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 253
- (Topic 3)

The results of a recently completed site survey indicate a significant, undesired RSSI in the parking lot and other exterior areas near the like to mitigate access to the wireless network in exterior access areas. The current access point settings are listed in the following table:

Name	Power	Antenna type	Channel	SSID	Passphrase
AP1	High	Omnidirectional	1	Corp01	P$ssw0rd
AP2	Medium	Omnidirectional	6	Corp01	P$ssw0rd
AP3	Medium	Directional	9	Corp01	P$ssw0rd

Which of the following is the BEST step for the technician to take to resolve the issue?

A. Reconfigure AP2 and AP3 for non-overlapping channels
B. Implement directional antennas on AP1 and AP2.
C. Raise the power settings on AP2 and AP3.
D. Change the SSID on AP1 and AP2.

Answer: B

Explanation:
Implementing directional antennas on AP1 and AP2 is the best step for the technician to take to resolve the issue of undesired RSSI in the parking lot and other exterior areas near the building. RSSI stands for received signal strength indicator, which is a measure of how well a device can receive a wireless signal from an access point (AP). An AP is a device that provides wireless connectivity to a network. An antenna is a device that radiates or receives electromagnetic waves. A directional antenna is an antenna that focuses the wireless signal in a specific direction, resulting in higher gain and longer range. By using directional antennas on AP1 and AP2, which are located near the exterior walls of the building, the technician can reduce the wireless signal leakage to the outside areas and improve the wireless coverage inside the building. References: [CompTIA Network+ Certification Exam Objectives], What Is RSSI and How Does It Affect Wireless Networks?, Directional Antennas: Everything You Need to Know

NEW QUESTION 255
- (Topic 3)
A newly installed multifunction copier needs to be set up so scanned documents can be emailed to recipients. Which of the following ports from the copier's IP address should be allowed?

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

Answer: B

Explanation:
Port 25 is the port number that is commonly used for Simple Mail Transfer Protocol (SMTP), which is a protocol that allows sending and receiving email messages over a network1. Port 25 from the copier’s IP address should be allowed so that scanned documents can be emailed to recipients.
Port 22 is the port number that is commonly used for Secure Shell (SSH), which is a protocol that allows secure and encrypted remote access and control of a device over a network1. Port 22 from the copier’s IP address is not necessary for emailing scanned documents.
Port 53 is the port number that is commonly used for Domain Name System (DNS), which is a protocol that allows resolving domain names to IP addresses and vice versa on a network1. Port 53 from the copier’s IP address is not necessary for emailing scanned documents.
Port 80 is the port number that is commonly used for Hypertext Transfer Protocol (HTTP), which is a protocol that allows transferring web pages and other resources over a network1. Port 80 from the copier’s IP address is not necessary for emailing scanned documents.

NEW QUESTION 258
- (Topic 3)
Which of the following connector types would be used to connect to the demarcation point and provide network access to a cable modem?

A. F-type
B. RJ45
C. LC
D. RJ11

Answer: A

Explanation:
An F-type connector is a type of coaxial connector that is commonly used to connect a cable modem to the demarcation point, which is the point at which the cable provider's network ends and the customer's network begins. The F-type connector is a threaded connector that is typically used for television, cable modem, and satellite antenna connections.

NEW QUESTION 259
- (Topic 3)
Which of the following can be used to decrease latency during periods of high utilization of a firewall?

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

Answer: B

Explanation:

NIC Teaming, also known as load balancing and failover (LBFO), allows multiple network adapters on a computer to be placed into a team for the following purposes:
(https://www.bing.com/search?q=what+is+nic+teaming+used+for%3F&form=QBLH&sp=- 1&pq=what+is+nic+teaming+used+for&sc=10-28&qs=n&sk=&cvid=13882A9A9B584D8099F4ABCAD034E821&ghsh=0&ghacc=0&ghpl=)

NEW QUESTION 261
- (Topic 3)
A network administrator is trying to add network redundancy for the server farm. Which of the following can the network administrator configure to BEST provide this capability?

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

Answer: A

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

NEW QUESTION 262
- (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 265
- (Topic 3)
Due to a surge in business, a company is onboarding an unusually high number of salespeople. The salespeople are assigned desktops that are wired to the network. The last few salespeople to be onboarded are able to access corporate materials on the network but not sales-specific resources. Which of the following is MOST likely the cause?

A. The switch was configured with port security.
B. Newly added machines are running into DHCP conflicts.
C. The IPS was not configured to recognize the new users.
D. Recently added users were assigned to the wrong VLAN

Answer: D

NEW QUESTION 270
- (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 274
- (Topic 3)
An engineer needs to restrict the database servers that are in the same subnet from communicating with each other. The database servers will still need to communicate with the application servers in a different subnet. In some cases, the database servers will be clustered, and the servers will need to communicate with other cluster members. Which of the following technologies will be BEST to use to implement this filtering without creating rules?

A. Private VLANs
B. Access control lists
C. Firewalls
D. Control plane policing

Answer: A

Explanation:
"Use private VLANs: Also known as port isolation, creating a private VLAN is a method of restricting switch ports (now called private ports) so that they can communicate only with a particular uplink. The private VLAN usually has numerous private ports and only one uplink, which is usually connected to a router, or firewall."

NEW QUESTION 278
- (Topic 3)
A user reports that a new VoIP phone works properly but the computer that is connected to the phone cannot access any network resources. Which of the following MOST Likely needs to be configured correctly to provide network connectivity to the computer?

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

Answer: D

Explanation:
VLAN (virtual LAN) tags are used to identify packets as belonging to a particular VLAN. VLANs are used to segment a network into logical sub-networks, and each VLAN is assigned a unique VLAN tag. If the VLAN tag is not configured correctly, the computer may not be able to access network resources.

NEW QUESTION 279
- (Topic 3)
A technician needs to set up a wireless connection that utilizes MIMO on non-overlapping channels. Which of the following would be the best choice?

A. 802.11a
B. 802.11b
C. 802.11g
D. 802.11n

Answer: D

Explanation:
802.11n is the best choice for setting up a wireless connection that utilizes MIMO on non-overlapping channels. 802.11n is a wireless standard that offers faster speeds and longer range than previous standards. 802.11n uses multiple-input multiple- output (MIMO) technology, which allows multiple antennas to transmit and receive multiple spatial streams of data simultaneously. MIMO can improve wireless performance, reliability, and capacity by exploiting multipath propagation and spatial diversity. 802.11n also uses non-overlapping channels in both the 2.4 GHz and 5 GHz frequency bands to
avoid interference and increase bandwidth. Non-overlapping channels are channels that do not share any part of their frequency spectrum with other channels.
References: [CompTIA Network+ Certification Exam Objectives], 802.11n - Wikipedia

NEW QUESTION 283
- (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 285
- (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 286
- (Topic 3)
Logs show an unauthorized IP address entering a secure part of the network every night at 8:00 pm. The network administrator is concerned that this IP address will cause an issue to a critical server and would like to deny the IP address at the edge of the network. Which of the following solutions would address these concerns?

A. Changing the VLAN of the web server
B. Changing the server's IP address
C. Implementing an ACL
D. Instating a rule on the firewall connected to the web server

Answer: D

NEW QUESTION 289
- (Topic 3)
A building was recently remodeled in order to expand the front lobby. Some mobile users have been unable to connect to the available network jacks within the new lobby, while others have had no issues. Which of the following is the MOST likely cause of the connectivity issues?

A. LACP
B. Port security
C. 802.11ax
D. Duplex settings

Answer: B

Explanation:
Port security is a feature that allows a network device to limit the number and type of MAC addresses that can access a port. Port security can prevent unauthorized devices from connecting to the network through an available network jack. Therefore, port security is the most likely cause of the connectivity issues for some mobile users in the new lobby.

NEW QUESTION 292
- (Topic 3)
Which of the following routing protocols has routes that are classified with an administrative distance of 110?

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

Answer: B

Explanation:
Administrative distance is a measure of the trustworthiness of a routing protocol. The smaller the administrative distance value, the more reliable the protocol. Each routing protocol has its own default administrative distance value. OSPF has a default administrative distance of 110, which means it is more reliable than RIP (120) but less reliable than EIGRP (90) or BGP (20).
References := Administrative Distance of Routing Protocols - Networks Training, What is Administrative Distance? - Cisco, Adjust Administrative Distance for Route Selection in Cisco IOS Routers …, Administrative Distance (AD) and Autonomous System (AS)

NEW QUESTION 293
- (Topic 3)
A network technician is selecting a replacement for a damaged fiber cable that goes directly to an SFP transceiver on a network switch. Which of the following cable connectors should be used?

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

Answer: C

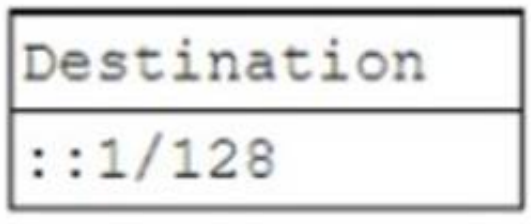
NEW QUESTION 298
- (Topic 3)
An IT administrator received an assignment with the following objectives
• Conduct a total scan within the company's network tor all connected hosts
• Detect all the types of operating systems running on all devices
• Discover all services offered by hosts on the network
• Find open ports and detect security risks.
Which of the following command-line tools can be used to achieve these objectives?

A. nmap
B. arp
C. netatat
D. tcpdump

Answer: A

Explanation:
Nmap (Network Mapper) is a free and open source command line tool that can be used to scan a network for all connected hosts, detect the types of operating systems running on all devices, discover all services offered by hosts on the network, find open ports, and detect security risks. Nmap is commonly used by system administrators and security professionals to audit a network's security and identify possible vulnerabilities. Nmap can be used to discover active hosts, scan ports, fingerprint operating systems, detect running services, and more. Reference: CompTIA Network+ Study Manual, 8th Edition, page 592.

NEW QUESTION 300
- (Topic 3)
An application is not working. When the log files are reviewed, the application continuously tries to reach the following destination:



Which of the following is most likely associated with this IP address?

A. APIPA
B. Default gateway
C. Link local
D. Loopback

Answer: D

Explanation:
The IP address ::1/128 is the loopback address of the local host in IPv6, which is the equivalent of the 127.0.0.1 in IPv4. The loopback address is a virtual interface that loops all traffic back to itself, the local host. The loopback address is used for testing and troubleshooting purposes, such as checking the connectivity and configuration of the network stack. If an application tries to reach the loopback address, it means that it is not communicating with any external network or server, but only with itself.
The other options are not correct because they are not associated with the IP address ::1/128. They are:
? APIPA. APIPA stands for Automatic Private IP Addressing, which is a feature that allows a device to assign itself a private IPv4 address in the range of 169.254.0.0/16 when no DHCP server is available. APIPA does not apply to IPv6 addresses, and it is not related to the loopback address.
? Default gateway. The default gateway is the IP address of the router or device that connects a local network to other networks. The default gateway is usually the first or last usable IP address in a subnet, and it is not the same as the loopback address.
? Link local. Link local addresses are IPv6 addresses that are used for communication within a single network segment or link. Link local addresses have the prefix fe80::/10, and they are not routable or reachable from other networks. Link local addresses are not the same as the loopback address.
References1: Loopback Address - ::1/128 - ipUpTime.net2: Network+ (Plus) Certification | CompTIA IT Certifications3: Reserved IP addresses - Wikipedia

NEW QUESTION 302
- (Topic 3)
A network administrator needs to provide remote clients with access to an internal web application. Which of the following methods provides the highest flexibility and compatibility while encrypting only the connection to the web application?

A. Clientless VPN
B. Virtual desktop
C. Virtual network computing
D. mGRE tunnel

Answer: A

Explanation:
A clientless VPN is a method of providing remote clients with access to an internal web application without installing any additional software or dedicated VPN client on their devices. Instead, users access the VPN through a web browser, utilizing a web portal or gateway provided by the VPN service. This method provides the highest flexibility and compatibility, as it supports various operating systems and devices, and encrypts only the connection to the web application, not the entire traffic of the device.

NEW QUESTION 303
- (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 308
- (Topic 3)

A user reports that the internet seems slow on a workstation, but no other users have reported any issues. The server team confirms the servers are functioning normally. A technician suspects something specific to the user's computer is overutilizing bandwidth. Which of the following commands should the technician use to further investigate the issue?

A. nmap
B. tcpdump
C. netstat
D. nslookup

Answer: C

Explanation:
netstat is a command-line tool that displays network connections, routing tables, interface statistics, and more. It can help the technician identify which processes or applications are using the network bandwidth on the user's computer. netstat can also show the current bandwidth usage in bytes per second for each network interface.
References
? netstat - Wikipedia provides an overview of the netstat tool and its features.
? How to get current bandwidth usage from command line using built-in Linux tools?
- Super User explains how to use netstat and other tools to monitor bandwidth usage on Linux systems.
? Get network utilization from command line - Super User shows how to use typeperf and other tools to monitor bandwidth usage on Windows systems.

NEW QUESTION 311
- (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 314
- (Topic 3)
Given the following Information:

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

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

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

Answer: D

NEW QUESTION 315
- (Topic 3)
Which of the following is an example of on-demand scalable hardware that is typically housed in the vendor's data center?

A. DaaS
B. laaS
C. PaaS
D. SaaS

Answer: B

Explanation:
IaaS is an example of on-demand scalable hardware that is typically housed in the vendor's data center. IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources over the internet. IaaS allows customers to rent servers, storage, network devices, and other hardware components from a cloud service provider, rather than purchasing and maintaining them on-premise. IaaS offers advantages such as scalability, flexibility, cost-effectiveness, and reliability. Customers can adjust their hardware resources according to their needs and pay
only for what they use. Customers can also access their hardware resources from anywhere via a web browser or an API. References: [CompTIA Network+ Certification Exam Objectives], What Is Infrastructure as a Service (IaaS)? | IBM

NEW QUESTION 316
- (Topic 3)
A technician is assisting a user who cannot connect to a website. The technician attempts to ping the default gateway and DNS server of the workstation. According to troubleshooting methodology, this is an example of:

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

Answer: A

NEW QUESTION 318
- (Topic 3)
A network administrator is planning to implement device monitoring to enhance network visibility. The security team requires that the solution provides authentication and encryption.
Which of the following meets these requirements?

A. SIEM
B. Syslog
C. NetFlow
D. SNMPv3

Answer: D

Explanation:
SNMPv3 is a protocol that allows network administrators to monitor and manage network devices such as routers, switches, servers, printers, and more. SNMPv3 provides authentication and encryption features that ensure the security and integrity of the data exchanged between the management station and the network devices. SNMPv3 uses a user-based security model (USM) that supports three levels of security: noAuthNoPriv, authNoPriv, and authPriv. The noAuthNoPriv level provides no authentication or encryption, the authNoPriv level provides authentication but no encryption, and the authPriv level provides both authentication and encryption12.
References
? SNMP is one of the common network monitoring protocols covered in Objective 3.1 of the CompTIA Network+ N10-008 certification exam3.
? SNMPv3 provides authentication and encryption features for network monitoring12.
? SNMPv3 uses a user-based security model with three levels of security12.
1: SNMP - N10-008 CompTIA Network+ : 3.1 - Professor Messer IT Certification Training Courses 2: CompTIA Network+ N10-008 Cert Guide, Chapter 13, page 413 3: CompTIA Network+ Certification Exam Objectives, page 7

NEW QUESTION 320
- (Topic 3)
A customer called the help desk to report a network issue. The customer recently added a hub between the switch and the router in order to duplicate the traffic flow to a logging device. After adding the hub, all the Other network components that were connected to the switch slowed more than expected. Which Of the following is the MOST likely cause Of the issue?

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

Answer: A

Explanation:
A duplex mismatch is a situation where two devices on a network have different duplex settings, such as full-duplex or half-duplex. Full-duplex means that a device can send and receive data simultaneously, while half-duplex means that a device can only send or receive data at a time. A duplex mismatch can cause performance issues, such as collisions, errors, or slow throughput. In this scenario, the customer added a hub between the switch and the router. A hub is a device that operates at half-duplex and broadcasts all traffic to all ports. A switch and a router are devices that operate at full-duplex and forward traffic to specific ports. Therefore, adding a hub between the switch and the router can cause a duplex mismatch and slow down all the other network components that were connected to the switch.
References: https://www.comparitech.com/net-admin/hub-vs-switch-vs-router/ https://www.cisco.com/c/en/us/support/docs/lan-switching/ethernet/10561-3.html

NEW QUESTION 321
- (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 325
- (Topic 3)
Which of the following is an example of on-demand scalable hardware that is typically housed in the vendor's data center?

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

Answer: B

NEW QUESTION 327
- (Topic 3)
Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

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

Answer: B

Explanation:
TACACS+ is used to authenticate users and authorize access to network resources. This protocol provides greater network security by encrypting the authentication credentials and reducing the risk of unauthorized access. According to the CompTIA Network+ Study Manual, “TACACS+ is an authentication protocol used to centralize authentication and authorization for network devices. It is a more secure alternative to Telnet for handling logins and for granting privileges to users.”

NEW QUESTION 330
- (Topic 3)
A network administrator needs to connect two routers in a point-to-point configuration and conserve IP space. Which of the following subnets should the administrator use?

A. /24
B. /26
C. /28
D. /30

Answer: D

Explanation:
A /30 subnet is the smallest possible subnet that can be used for a point-to-point configuration between two routers. A /30 subnet has only two usable host addresses, one for each router, and a network address and a broadcast address. A /30 subnet conserves IP space by minimizing the number of wasted addresses. A /24, /26, or /28 subnet would have more usable host addresses than needed for a point-to-point configuration and would waste IP space.
References:
? Routing Technologies – N10-008 CompTIA Network+ : 2.21
? CompTIA Network+ Certification Exam Objectives, page 10

NEW QUESTION 332
- (Topic 3)
Which of the following is used to provide disaster recovery capabilities to spin up an critical devices using internet resources?

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

Answer: A

NEW QUESTION 335
- (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 339
- (Topic 3)
Which of the following layers of the OSI model receives data from the application layer and converts it into syntax that is readable by other devices on the network?

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

Answer: C

NEW QUESTION 341
- (Topic 3)
A network engineer turned on logging to assist with troubleshooting a suspected configuration issue informative log information?

A. FATAL
B. ERROR
C. DEBUG
D. WARN

Answer: C

Explanation:
DEBUG is the log level that provides the most informative log information for troubleshooting a suspected configuration issue. Logging is a feature that allows network devices to record events and messages related to their operation and status. Logging can help network engineers to monitor, diagnose, and resolve network problems. Log levels are categories that indicate the severity or importance of a log message. Different log levels provide different amounts of detail and verbosity. DEBUG is the lowest log level, which means it provides the most detailed and verbose information about every action and event that occurs on a network device. DEBUG can help network engineers to identify configuration errors, misbehaving processes, or unexpected outcomes. However, DEBUG can also generate a lot of noise and overhead, which can affect the performance and availability of the network device. Therefore, DEBUG should be used sparingly and only when necessary. References: [CompTIA Network+ Certification Exam
Objectives], Understanding Logging Levels - Cisco

NEW QUESTION 345
- (Topic 3)
A technician is trying to determine whether an LACP bundle is fully operational. Which of the following commands will the technician MOST likely use?

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

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/optical/cpt/r9_3/command/reference/cpt93_cr/cpt93
_cr_chapter_01000.html

NEW QUESTION 348
- (Topic 3)
Which of the following uses the link-state routing algorithm and operates within a single autonomous system?

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

Answer: B

Explanation:
OSPF uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks

NEW QUESTION 352
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

N10-009 Practice Exam Features:

* N10-009 Questions and Answers Updated Frequently

* N10-009 Practice Questions Verified by Expert Senior Certified Staff

* N10-009 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* N10-009 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year