CompTIA

Exam Questions N10-009

CompTIA Network+ Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Topic 3)
Which of the following would most likely affect design considerations when building out an IDF?

A. The source panel amperage
B. The fire suppression system
C. The humidity levels
D. The cable transmission speeds

Answer: B

Explanation:
The fire suppression system is a design consideration when building out an IDF because it can affect the safety and reliability of the network equipment and cabling. A fire suppression system is a system that detects and extinguishes fires in a building, using water, gas, or chemicals. Depending on the type of fire suppression system, it can have different impacts on the IDF design, such as:
? Water-based systems, such as sprinklers, can damage the network equipment and cabling if they are activated by a fire or a false alarm. Therefore, the IDF should be designed to protect the equipment and cabling from water exposure, such as using waterproof cabinets, drip pans, and conduits.
? Gas-based systems, such as clean agent systems, can displace the oxygen in the IDF and cause suffocation for anyone inside. Therefore, the IDF should be designed to allow for ventilation and air circulation, as well as warning signs and alarms to alert anyone in the IDF before the gas is released.
? Chemical-based systems, such as dry chemical systems, can leave a residue on the network equipment and cabling that can affect their performance and lifespan. Therefore, the IDF should be designed to minimize the contact between the chemical and the equipment and cabling, as well as provide a means for cleaning and restoring them after a fire.
The other options are not correct because:
? The source panel amperage is not a design consideration when building out an IDF, as it is determined by the electrical circuit and the power needs of the network equipment and cabling. The source panel amperage does not affect the layout, location, or protection of the IDF.
? The humidity levels are not a design consideration when building out an IDF, as they are controlled by the HVAC system and the ventilation of the IDF. The humidity levels do not affect the layout, location, or protection of the IDF.
? The cable transmission speeds are not a design consideration when building out an IDF, as they are determined by the type and quality of the network cabling and the network equipment. The cable transmission speeds do not affect the layout, location, or protection of the IDF.

NEW QUESTION 2
- (Topic 3)
Which of the following compromises internet-connected devices and makes them vulnerable to becoming part of a botnet? (Select TWO).

A. Deauthentication attack
B. Malware infection
C. IP spoofing
D. Firmware corruption
E. Use of default credentials
F. Dictionary attack

Answer: BE

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)
Which of the following is the MOST appropriate use case for the deployment of a clientless VPN?

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

Answer: A

NEW QUESTION 5
- (Topic 3)
A network technician is troubleshooting a port channel issue. When logging in to one of the switches, the technician sees the following information displayed:

Native VLAN mismatch detected on interface g0/1
Which of the following layers of the OSI model is most likely to be where the issue resides?

A. Layer 2
B. Layer 3
C. Layer 5
D. Layer 6

Answer: A

Explanation:
Layer 2 of the OSI model is the data link layer, which is responsible for transferring data between adjacent nodes on a network. It uses protocols such as Ethernet, PPP, and HDLC to encapsulate data into frames and add MAC addresses for source and destination identification. It also uses protocols such as STP, LACP, and CDP to manage the physical links and prevent loops, aggregate bandwidth, and discover neighboring devices12
A native VLAN mismatch is a common Layer 2 issue that occurs when two switches are connected by a trunk port, but have different native VLANs configured on their interfaces. A native VLAN is the VLAN that is assigned to untagged frames on a trunk port. If the native VLANs do not match, the switches will drop the untagged frames and generate an error message. This can cause connectivity problems and security risks on the network345
To resolve a native VLAN mismatch, the network technician should ensure that both switches have the same native VLAN configured on their trunk ports, or use a different port mode such as access or general.

NEW QUESTION 6
- (Topic 3)
A network is experiencing extreme latency when accessing a particular website. Which of the following commands will BEST help identify the issue?

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

Answer: C

NEW QUESTION 7
- (Topic 3)
A technician is trying to install a VoIP phone, but the phone is not turning on. The technician checks the cable gong from the phone to the switch, and the cable is good. Which of the following actions IS needed for this phone to work?

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

Answer: A

NEW QUESTION 8
- (Topic 3)
A network administrator is given the network 80.87.78.0/26 for specific device assignments. Which of the following describes this network?

A. 80.87.78 0 - 80.87.78.14
B. 80.87.78 0 - 80.87.78.110
C. 80.87.78 1 - 80.87.78.62
D. 80.87.78.1 - 80.87.78.158

Answer: C

Explanation:
The network 80.87.78.0/26 is a Class A network with a subnet mask of /26, which means that it contains 26 bits of network information and 6 bits of host information.
The range of valid host addresses for this network is 80.87.78.1 to 80.87.78.62. Any addresses outside of this range are reserved for special purposes or are not used.

NEW QUESTION 9
- (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 10
- (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 10
- (Topic 3)
A technician is expanding a wireless network and adding new access points. The company requires that each access point broadcast the same SSID. Which of the following should the technician implement for this requirement?

A. MIMO
B. Roaming
C. Channel bonding
D. Extended service set

Answer: D

Explanation:
An extended service set (ESS) is a wireless network that consists of two or more access points (APs) that share the same SSID and are connected by a distribution system, such as a switch or a router. An ESS allows wireless clients to roam seamlessly between different APs without losing connectivity or changing network settings. An ESS can also increase the coverage area and capacity of a wireless network

NEW QUESTION 11
- (Topic 3)
The following DHCP scope was configured for a new VLAN dedicated to a large deployment of 325 loT sensors:

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

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

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

Answer: B

NEW QUESTION 14
- (Topic 3)
A network administrator is trying to create a subnet, which is the most efficient size possible, for 31 laptops. Which of the following network subnets would be best in this situation?

A. 10.10.10.0/24
B. 10.10.10.0/25
C. 10.10.10.0/26
D. 10.10.10.0/27

Answer: D

Explanation:
A /27 subnet mask has 32 IP addresses, of which 30 are usable for hosts. This is the smallest subnet that can accommodate 31 laptops, as the other options have either too few or too many IP addresses. A /27 subnet mask is equivalent to 255.255.255.224 in decimal notation, and has a wildcard mask of 0.0.0.31. The network address is 10.10.10.0, and the broadcast address is 10.10.10.31. The usable host range is 10.10.10.1 to 10.10.10.30.
References
1: Subnet Cheat Sheet – 24 Subnet Mask, 30, 26, 27, 29, and other IP Address CIDR Network References
2: IP Subnet Calculator

NEW QUESTION 16
- (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 18
- (Topic 3)
Which of the following is the best action to take before sending a network router to be recycled as electronic waste?

A. Turn on port security.
B. Shred the switch hard drive.
C. Back up and erase the configuration.
D. Remove the company asset ID tag.

Answer: C

Explanation:
Before disposing of a network router, it is important to back up and erase the configuration to prevent unauthorized access to sensitive data and network settings. A network router may contain information such as passwords, IP addresses, firewall rules, VPN settings, and other network parameters that could be exploited by hackers or malicious users. By backing up the configuration, you can preserve the network settings for future reference or reuse. By erasing the configuration, you can wipe out the data and restore the router to its factory default state.

NEW QUESTION 19
- (Topic 3)
Which of the following is an advantage of using the cloud as a redundant data center?

A. The process of changing cloud providers is easy.
B. Better security for company data is provided.
C. The initial capital expenses are lower.
D. The need for backups is eliminated.

Answer: C

Explanation:
Using the cloud as a redundant data center means that the company does not need to invest in building and maintaining a physical backup site, which can be costly and time- consuming. Instead, the company can pay for the cloud services as needed, which can reduce the initial capital expenses and operational costs. However, this does not mean that the other options are true. Changing cloud providers may not be easy due to compatibility, contractual, or regulatory issues. Security for company data may not be better in the cloud, depending on the cloud provider's policies and practices. The need for backups is not eliminated, as the cloud data still needs to be protected from loss, corruption, or unauthorized access.
References:
? Part 1 of current page talks about how Bing is your AI-powered copilot for the web and provides various examples of how it can help you with different tasks, such as writing a joke, creating a table, or summarizing research. However, it does not mention anything about using the cloud as a redundant data center.
? Part 2 of current page shows the search results for "ai powered search bing chat", which include web, image, and news results. However, none of these results seem to be relevant to the question, as they are mostly about Bing's features, products, or announcements, not about cloud computing or data centers.
? Therefore, I cannot find the answer or the explanation from the current page. I have to use my own knowledge and information from other sources to verify the answer and provide a short but comprehensive explanation. I will cite these sources using numerical references.
? : CompTIA Network+ Certification Exam Objectives, Version 8.0, Domain 3.0: Network Operations, Objective 3.4: Given a scenario, use appropriate resources to support configuration management, Subobjective 3.4.2: Cloud-based configuration management, https://www.comptia.jp/pdf/comptia-network-n10-008-exam-objectives.pdf
? : Cloud Computing: Concepts, Technology & Architecture, Chapter 9: Fundamental Cloud Security, Section 9.1: Cloud Security Threats, https://ptgmedia.pearsoncmg.com/images/9780133387520/samplepages/9780133 387520.pdf
? : Cloud Computing: Principles and Paradigms, Chapter 19: Data Protection and Disaster Recovery for Cloud Computing, Section 19.1: Introduction, https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470940105.ch19

NEW QUESTION 21
- (Topic 3)
Which of the following documents is MOST likely to be associated with identifying and documenting critical applications?

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

Answer: D

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

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

NEW QUESTION 24
- (Topic 3)
A security engineer is trying to connect cameras to a 12-port PoE switch, but only eight cameras turn on. Which of the following should the engineer check first?

A. Ethernet cable type
B. Voltage
C. Transceiver compatibility
D. DHCP addressing

Answer: B

Explanation:
The most likely reason why only eight cameras turn on is that the PoE switch does not
have enough power budget to supply all 12 cameras. The engineer should check the voltage and wattage ratings of the PoE switch and the cameras, and make sure they are compatible and sufficient. The Ethernet cable type, transceiver compatibility, and DHCP addressing are less likely to cause this problem, as they would affect the data transmission rather than the power delivery.
References:
? CompTIA Network+ N10-008 Certification Study Guide, page 181
? CompTIA Network+ N10-008 Cert Guide, Deluxe Edition, page 352
? PoE Troubleshooting: The Common PoE Errors and Solutions3

NEW QUESTION 25
- (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 29
- (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 31
- (Topic 3)
Users are reporting poor wireless performance in some areas of an industrial plant The wireless controller is measuring a tow EIRP value compared to me recommendations noted on me most recent site survey. Which of the following should be verified or replaced for the EIRP value to meet the site survey's specifications? (Select TWO).

A. AP transmit power
B. Channel utilization
C. Signal loss
D. Update ARP tables
E. Antenna gain
F. AP association time

Answer: AE

Explanation:
? AP transmit power: You should check if your APs have sufficient power output and adjust them if needed. You should also make sure they are not exceeding regulatory limits for your region.
? Antenna gain: You should check if your antennas have adequate gain for your coverage area and replace them if needed. You should also make sure they are aligned properly and not obstructed by any objects.

In the scenario described, the wireless controller is measuring a low EIRP value compared to the recommendations noted in the most recent site survey. EIRP is the combination of the power transmitted by the access point and the antenna gain. Therefore, to increase the EIRP value to meet the site survey's specifications, the administrator should verify or replace the AP transmit power (option A) and the antenna gain (option E). This can be achieved by adjusting the transmit power settings on the AP or by replacing the AP's antenna with one that has a higher gain

NEW QUESTION 36
- (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 37
- (Topic 3)
A user calls the IT department to report being unable to log in after locking the computer The user resets the password, but later in the day the user is again unable to log in after locking the computer Which of the following attacks against the user IS MOST likely taking place?

A. Brute-force
B. On-path
C. Deauthentication
D. Phishing

Answer: A

NEW QUESTION 42
- (Topic 3)
In which of the following components do routing protocols belong in a software-defined network?

A. Infrastructure layer
B. Control layer
C. Application layer
D. Management plane

Answer: B

Explanation:
A software-defined network (SDN) is a network architecture that decouples the control plane from the data plane and centralizes the network intelligence in a software controller. The control plane is the part of the network that makes decisions about how to route traffic, while the data plane is the part of the network that forwards traffic based on the control plane's instructions. The control layer is the layer in an SDN that contains the controller and the routing protocols that communicate with the network devices. The control layer is responsible for managing and configuring the network devices and providing them with the necessary information to forward traffic. References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 378)

NEW QUESTION 45
- (Topic 3)
An IT administrator is creating an alias to the primary customer's domain. Which of the following DNS record types does this represent?

A. CNAME
B. MX
C. A
D. PTR

Answer: A

Explanation:
A CNAME record is a type of DNS record that maps an alias name to a canonical name, or the primary domain name. A CNAME record is used to create subdomains or alternative names for the same website, without having to specify the IP address for each alias. For example, a CNAME record can map www.example.com to example.com, or mail.example.com to example.com. References: CompTIA Network+ N10-008 Cert Guide, Chapter 2, Section 2.4

NEW QUESTION 48
- (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 51
- (Topic 3)
A wireless technician is working to upgrade the wireless infrastructure for a company. The company currently uses the 802.11g wireless standard on all access points. The company requires backward compatibility and is requesting the least expensive solution. Which of the following should the technician recommend to the company?

A. 802.11a
B. 802.11ac
C. 802Hax
D. 802.11n

Answer: D

Explanation:
* 802.11n is a wireless standard that supports data rates up to 600 Mbps and operates in both 2.4 GHz and 5 GHz frequency bands. 802.11n is backward compatible with 802.11g, which operates only in 2.4 GHz band. 802.11n is the least expensive solution that can upgrade the wireless infrastructure for the company, as it does not require replacing all the access points or wireless devices

NEW QUESTION 55
- (Topic 3)
A network administrator needs to monitor traffic on a specific port on a switch. Which of the following should the administrator configure to accomplish the task?

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

Answer: C

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

NEW QUESTION 57
- (Topic 3)
A technician is investigating why a PC cannot reach a file server with the IP address 192.168.8.129. Given the following TCP/IP network configuration:

Link-local IPv6 address	fe80::28e4:a7cc:a55e:4bea
IPv4 address	192.168.8.105
Subnet mask	255.255.255.128
Default gateway	192.168.8.1

Which of the following configurations on the PC is incorrect?

A. Subnet mask
B. IPv4 address
C. Default gateway
D. IPv6 address

Answer: C

Explanation:
The default gateway is the IP address of the router that connects the PC to other networks. The default gateway should be on the same subnet as the PC's IPv4 address. However, in this case, the default gateway is 192.168.9.1, which is on a different subnet than the PC's IPv4 address of 192.168.8.15. Therefore, the default gateway configuration on the PC is incorrect and prevents the PC from reaching the file server on another subnet.

NEW QUESTION 60
- (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 64
- (Topic 3)
A network administrator is working to configure a new device to provide Layer 2 connectivity to various endpoints including several WAPs. Which of the following devices will the administrator MOST likely configure?

A. WLAN controller
B. Cable modem
C. Load balancer
D. Switch
E. Hub

Answer: D

Explanation:
A switch is a device that provides Layer 2 connectivity to various endpoints by forwarding frames based on MAC addresses. A switch can also connect to several WAPs (wireless access points) to provide wireless connectivity to wireless devices.

NEW QUESTION 65
- (Topic 3)
A technician is working on a ticket for a user in the human resources department who received a new PC that does not connect to the internet. All users in human resources can access the
internet. The technician can ping the PC from the human resources router but not from the IT network. Which of the following is the most likely cause of the issue?

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

Answer: D

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

NEW QUESTION 67
- (Topic 3)
A technician completed troubleshooting and was able to fix an issue. Which of the following is the BEST method the technician can use to pass along the exact steps other technicians should follow in case the issue arises again?

A. Use change management to build a database
B. Send an email stating that the issue is resolved.
C. Document the lessons learned
D. Close the ticket and inform the users.

Answer: C

Explanation:
Documenting the lessons learned is the best method for passing along the exact steps other technicians should follow in case the issue arises again. Lessons learned are the knowledge and experience gained from completing a project or solving a problem. Documenting the lessons learned helps to capture the best practices, challenges, solutions, and recommendations for future reference and improvement. Documenting the lessons learned can also help to update the knowledge base, standard operating procedures, or policies related to the issue. References: [CompTIA Network+ Certification Exam Objectives], Lessons Learned: Definition & Examples for Project Managers

NEW QUESTION 70
- (Topic 3)
A company's web server is hosted at a local ISP. This is an example of:

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

Answer: D

NEW QUESTION 74
- (Topic 3)
A technician is deploying a new SSID for an industrial control system. The control devices require the network to use encryption that employs TKIP and a symmetrical password to connect. Which of the following should the technician configure to ensure compatibility with the control devices?

A. WPA2-Enterprise
B. WPA-Enterprise
C. WPA-PSK
D. WPA2-PSK

Answer: C

Explanation:
"WPA uses Temporal Key Integrity Protocol (TKIP) for enhanced encryption. TKIP uses RC4 for the encryption algorithm, and the CompTIA Network+ exam may reference TKIP-RC4 in a discussion of wireless."
" WPA2 uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) for integrity checking and Advanced Encryption Standard (AES) for encryption. On the Network+ exam, you might find this referenced as simply CCMP-AES"

NEW QUESTION 78
- (Topic 3)
A company is designing a SAN and would like to use STP as its medium for communication. Which of the following protocols would BEST suit me company's needs?

A. SFTP
B. Fibre Channel
C. iSCSI
D. FTP

Answer: B

Explanation:
A SAN also employs a series of protocols enabling software to communicate or prepare data for storage. The most common protocol is the Fibre Channel Protocol (FCP), which maps SCSI commands over FC technology. The iSCSI SANs will employ an iSCSI protocol that maps SCSI commands over TCP/IP.
STP (Spanning Tree Protocol) is a protocol used to prevent loops in Ethernet networks, and it is not a medium for communication in a storage area network (SAN). However, Fibre Channel is a protocol that is specifically designed for high-speed data transfer in SAN environments. It is a dedicated channel technology that provides high throughput and low latency, making it ideal for SANs. Therefore, Fibre Channel would be the best protocol for the company to use for its SAN. SFTP (Secure File Transfer Protocol), iSCSI (Internet Small Computer System Interface), and FTP (File Transfer Protocol) are protocols used for transferring files over a network and are not suitable for use in a SAN environment.

NEW QUESTION 82
- (Topic 3)
Which of the following would be BEST suited for a long cable run with a 40Gbps bandwidth?

A. Cat 5e
B. Cat 6a
C. Cat 7
D. Cat 8

Answer: C

Explanation:
Cat 7 is a type of twisted-pair copper cable that supports up to 40 Gbps bandwidth and up to 100 meters cable length. Cat 7 is suitable for long cable runs that require high-speed data transmission. Cat 7 has better shielding and crosstalk prevention than lower categories of cables.
References: Network+ Study Guide Objective 1.5: Compare and contrast network cabling types, features and their purposes.

NEW QUESTION 86
- (Topic 3)
A network technician is attempting to increase throughput by configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch. Which of the following is the BEST choice concerning speed and duplex for all interfaces that are participating in the link aggregation?

A. Half duplex and 1GB speed
B. Full duplex and 1GB speed
C. Half duplex and 10OMB speed
D. Full duplex and 100MB speed

Answer: B

Explanation:
The best choice for configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch is to use full duplex and 1GB speed for all interfaces that are participating in the link aggregation. This will allow for maximum throughput, as the full duplex connection will enable simultaneous sending and receiving of data, and the 1GB speed will ensure that the data is transferred quickly. According to the CompTIA Network+ Study Guide, “Full-duplex Ethernet allows the network adapter to transmit and receive data simultaneously, which can result in double the bandwidth of half-duplex Ethernet.” Additionally, the official text states, “Ethernet and Fast Ethernet use different speeds for data transmission, with Ethernet being 1,000 megabits (1 gigabit) per second and Fast Ethernet being 100 megabits per second.”

NEW QUESTION 90
- (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 93
- (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 96
- (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 101
- (Topic 3)
A network engineer is troubleshooting application connectivity issues between a server and a client. The network engineer needs to view the certificate exchange between the two hosts. Which of the following tools should the network engineer use?

A. dig
B. tcpdump
C. nmap
D. traceroute

Answer: B

Explanation:
tcpdump is a tool that can capture and analyze network traffic, including the certificate exchange between two hosts. It can display the contents of packets, such as the SSL/TLS handshake, which involves the exchange of certificates. dig is a tool that can query DNS servers for domain name information. nmap is a tool that can scan ports and services on a network. traceroute is a tool that can show the path and hops between a source and a destination.

NEW QUESTION 106
- (Topic 3)
Which of the following commands can be used to display the IP address, subnet address, gateway address, and DNS address on a Windows computer?

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

Answer: D

Explanation:
The ipconfig command is a utility that allows you to view and modify the network configuration of a Windows computer. By running the command "ipconfig /all", you can view detailed information about the network configuration of your computer, including the IP address, subnet mask, default gateway, and DNS server addresses.
Option A (netstat -a) is a command that displays active network connections and their status, but it does not display IP address or other network configuration information. Option B (ifconfig) is a command used on Linux and Unix systems to view and modify network configuration, but it is not available on Windows. Option C (ip addr) is a command used on Linux and Unix systems to view and modify network configuration, but it is not available on Windows.

NEW QUESTION 108
- (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 111
- (Topic 3)
A company has a geographically remote office. In order to connect to the internet, the company has decided to use a satellite WAN link. Which of the following is the GREATEST concern for this type of connection?

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

Answer: C

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

NEW QUESTION 112
- (Topic 3)
Which of the following would be used to enforce and schedule critical updates with supervisory approval and include backup plans in case of failure?

A. Business continuity plan
B. Onboarding and offboarding policies
C. Acceptable use policy
D. System life cycle
E. Change management

Answer: A

NEW QUESTION 115
- (Topic 3)
To comply with an industry regulation, all communication destined to a secure server should be logged and archived on a storage device. Which of the Mowing can be configured to fulfill this requirement?

A. QoS traffic classification
B. Port mirroring
C. Flow control
D. Link Aggregation Control Protocol

Answer: B

NEW QUESTION 116
- (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 120
- (Topic 3)
An organization has a security staff shortage and must prioritize efforts in areas where the staff will have the most impact. In particular, the focus is to avoid expending resources on identifying non-relevant events. A security analyst is reviewing web server logs and sees the following:

```
202.180.155.1 - [14/Jan/2021:04:12:28 -0200] "GET /img/us.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:28 -0200] "GET /img/org.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:29 -0200] "GET /img/org2.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:29 -0200] "GET /img/org3.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:30 -0200] "GET /img/org4.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:31 -0200] "GET /img/directors.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:31 -0200] "GET /img/directors2.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:32 -0200] "GET /img/directors3.gif" 404 295
202.180.155.1 - [14/Jan/2021:04:12:33 -0200] "GET /img/directors4.gif" 404 295
```

Which of the following should the analyst recommend?

A. Configuring the web server log to filter out 404 errors on image files
B. Updating firewall rules to block 202.180.155.1
C. Resyncing the network time server and monitoring logs for future anomalous behavior
D. Checking with the penetration testing team to see if the team ran any scans on January 14, 2021

Answer: A

Explanation:
This answer will help the organization to avoid expending resources on identifying non- relevant events, as the 404 errors on image files are not indicative of any security threat or issue, but rather a misconfiguration or a broken link on the web server. The 404 errors on image files are also very frequent and repetitive, as shown by the web server log, which can clutter the log and make it harder to spot any relevant events. By filtering out these errors, the analyst can focus on more important events and reduce the noise in the log. The other answers are not as good as A, because they either do not address the problem of identifying non-relevant events, or they are based on incorrect assumptions or information. For example:
? B. Updating firewall rules to block 202.180.155.1 is not a good answer, because the IP address 202.180.155.1 is not doing anything malicious or suspicious, but rather requesting image files that do not exist on the web server. Blocking this IP address will not improve the security of the web server, but rather create unnecessary firewall rules and possibly deny legitimate access to the web server.
? C. Resyncing the network time server and monitoring logs for future anomalous behavior is not a good answer, because there is no evidence that the network time server is out of sync or causing any problems. The web server log shows that the entries are all within a few minutes of each other, which is normal and expected. Resyncing the network time server will not help the analyst to identify non-relevant events, but rather waste time and resources on an unrelated task.
? D. Checking with the penetration testing team to see if the team ran any scans on January 14, 2021 is not a good answer, because the web server log does not show any signs of a penetration test or a scan. The log shows only 404 errors on image files, which are not typical of a penetration test or a scan, which would usually target different types of files, ports, or vulnerabilities. Checking with the penetration testing team will not help the analyst to identify non-relevant events, but rather distract the analyst from the actual events and possibly create false alarms.
https://www.professormesser.com/network-plus/n10-008/n10-008-video/general-network-troubleshooting-n10-008/

NEW QUESTION 122
- (Topic 3)
An infrastructure company is implementing a cabling solution to connect sites on multiple continents. Which of the following cable types should the company use for this project?

A. Cat 7
B. Single-mode
C. Multimode
D. Cat 6

Answer: B

Explanation:
Single-mode fiber is a type of optical fiber that has a small core diameter and allows only one mode of light to propagate. This reduces signal attenuation and increases transmission distance, making it suitable for long-distance communication networks.
Single-mode fiber can carry data over thousands of kilometers without requiring repeaters or amplifiers. Single-mode fiber is also immune to electromagnetic interference and has a higher bandwidth than multimode fiber. Therefore, single-mode fiber is the best cable type for connecting sites on multiple continents.
References: [CompTIA Network+ Certification Exam Objectives], [Single-mode optical fiber - Wikipedia]
Single-mode fiber optic cable uses a single ray of light to transmit data. This allows it to achieve very low attenuation and high bandwidth.
Multimode fiber optic cable uses multiple rays of light to transmit data. This results in higher attenuation and lower bandwidth than single-mode cable.
Twisted pair copper cable uses two insulated copper wires to transmit data. It is less expensive than fiber optic cable, but it has higher attenuation and lower bandwidth. When choosing a cable type for a long-distance application, it is important to consider the following factors:
? Attenuation: The amount of signal loss that occurs over the length of the cable.
? Bandwidth: The amount of data that can be transmitted over the cable per second.
? Cost: The cost of the cable and installation.
Single-mode fiber optic cable is the best choice for long-distance applications because it
has the lowest attenuation and highest bandwidth of any cable type. However, it is also the most expensive cable type.

NEW QUESTION 125
- (Topic 3)
A network engineer is concerned about VLAN hopping happening on the network. Which of the following should the engineer do to address this concern?

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

Answer: B

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

NEW QUESTION 129
- (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 133
- (Topic 3)
A network administrator installed a new data and VoIP network. Users are now experiencing poor call quality when making calls. Which of the following should the administrator do to increase VoIP performance?

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

Answer: A

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

NEW QUESTION 135
- (Topic 3)
A network technician is investigating why a core switch is logging excessive amounts of data to the syslog server. The running configuration of the switch showed the following logging information:
ip ssh logging events logging level debugging logging host 192.168.1.100 logging synchronous
Which of the following changes should the technician make to best fix the issue?

A. Update the logging host IP.
B. Change to asynchronous logging.
C. Stop logging SSH events.
D. Adjust the logging level.

Answer: D

Explanation:
The logging level debugging is the highest level of logging, which means that the switch will log every possible event, including low-priority and verbose messages. This can result in excessive amounts of data being sent to the syslog server, which can affect the performance and storage of the server. To fix the issue, the technician should adjust the logging level to a lower value, such as informational, warning, or error, depending on the desired level of detail and severity. This will reduce the amount of log data generated by the switch and only send the relevant and necessary messages to the syslog server.
https://betterstack.com/community/guides/logging/log-levels-explained/

NEW QUESTION 138
- (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 143
- (Topic 3)
Which of the following protocols should be used when Layer 3 availability is of the highest concern?

A. LACP
B. LDAP
C. FHRP
D. DHCP

Answer: C

Explanation:
FHRP stands for First Hop Redundancy Protocol, which is a group of protocols that allow routers or switches to provide backup or failover for the default gateway in a network. FHRP ensures that the network traffic can reach its destination even if the primary gateway fails or becomes unavailable. Some examples of FHRP protocols are HSRP, VRRP, and GLBP.
References
? 1: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 18
? 2: CompTIA Network+ N10-008 Certification Practice Test, question 9
? 3: CompTIA Network+ Study Guide: Exam N10-008, 5th Edition, page 263
? 4: CompTIA Network+ (N10-008) Practice Exam w/PBQ & Solution, question 5
? 5: What's on the CompTIA Network+ 008 certification? | CompTIA, section 3.1

NEW QUESTION 146
- (Topic 3)
An attacker sends more connection requests than a server can handle, causing the server to crash- Which of the following types of attacks is this an example of?

A. ARP poisoning
B. Denial-of-service
C. MAC flooding
D. On-path

Answer: B

Explanation:
A denial-of-service (DoS) attack is an example of an attack where an attacker sends more connection requests than a server can handle, causing the server to crash. A DoS attack is a type of cyberattack that aims to disrupt the normal functioning of a network service or resource by overwhelming it with excessive or malformed traffic. A DoS attack can prevent legitimate users from accessing the service or resource, resulting in degraded performance, unavailability, or data loss. A DoS attack can target various network layers, protocols, or components, such as servers, routers, firewalls, or applications. References: [CompTIA Network+ Certification Exam Objectives], What Is a Denial-of-Service (DoS) Attack? | Cisco

NEW QUESTION 151
- (Topic 3)
A company with multiple routers would like to implement an HA network gateway with the least amount of downtime possible. This solution should not require changes on the gateway setting of the network clients. Which of the following should a technician configure?

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

Answer: D

Explanation:

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

NEW QUESTION 154
- (Topic 3)
A coffee shop owner hired a network consultant to provide recommendations for installing a new wireless network. The coffee shop customers expect high speeds even when the network is congested. Which of the following standards should the consultant recommend?

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

Answer: B

Explanation:
802.11ax is the latest and most advanced wireless standard, providing higher speeds, lower latency, and more capacity than previous standards. It also supports OFDMA, which allows multiple devices to share a channel and reduce congestion. The other options are older standards that have lower bandwidth, range, and efficiency than 802.11ax. Therefore, 802.11ax is the best option for the coffee shop owner who wants to provide high speeds even when the network is congested.

NEW QUESTION 158
- (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 162
- (Topic 3)
When accessing corporate network resources, users are required to authenticate to each application they try to access. Which of the following concepts does this BEST represent?

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

Answer: B

NEW QUESTION 164
- (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 166
- (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 168
- (Topic 3)
A technician is configuring a wireless access point in a public space for guests to use. Which of the following should the technician configure so that only approved connections are
allowed?

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

Answer: B

Explanation:

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

NEW QUESTION 173
- (Topic 3)
Which of the following is used when a workstation sends a DHCP broadcast to a server on another LAN?

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

Answer: C

Explanation:
A helper address is an IP address that is configured on a router interface to forward DHCP broadcast messages to a DHCP server on another LAN. A DHCP broadcast message is a message that a workstation sends when it needs to obtain an IP address from a DHCP server. Since broadcast messages are not routed across different networks, a helper address is needed to relay the DHCP broadcast message to the DHCP server on another network. References: https://www.comptia.org/training/books/network-n10-008- study-guide (page 199)

NEW QUESTION 178
- (Topic 3)
A network administrator needs to add access points to the network because coverage in some areas is improper. Which of the following should the administrator do first?

A. Interference analysis
B. Wireless survey
C. Traffic analysis
D. Packet capture

Answer: B

Explanation:
A wireless survey is the first step that a network administrator should do before adding access points to the network. A wireless survey is a process of collecting data about the wireless environment, such as signal strength, channel usage, interference, and coverage. A wireless survey can help the network administrator to determine the optimal locations and configurations for the access points to provide the best possible coverage and performance for the wireless network. A wireless survey can also help to identify and troubleshoot any issues that may cause improper coverage in some areas.
https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html

NEW QUESTION 180
- (Topic 3)
An organization has experienced an increase in malicious spear-phishing campaigns and wants to mitigate the risk of hyperlinks from inbound emails.
Which of the following appliances would best enable this capability?

A. Email protection gateway
B. DNS server
C. Proxy server
D. Endpoint email client
E. Sandbox

Answer: A

Explanation:
An email protection gateway is an appliance that can filter and block malicious emails and attachments before they reach the recipients. An email protection gateway can mitigate the risk of hyperlinks from inbound emails by scanning the links for malicious content, rewriting the links to point to a safe domain, or blocking the links altogether. An email protection gateway can also perform other functions such as spam filtering, antivirus scanning, encryption, and data loss prevention.
A DNS server, a proxy server, an endpoint email client, and a sandbox are not appliances that can enable this capability, as they have different purposes and functions.
References
? 1: CompTIA Network+ N10-008 Certification Study Guide, page 304
? 2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 15
? 3: CompTIA Network+ N10-008 Certification Practice Test, question 5
? 4: Email Protection Gateway – N10-008 CompTIA Network+ : 3.2

NEW QUESTION 181
- (Topic 3)
A network administrator needs to set up a file server to allow user access. The organization uses DHCP to assign IP addresses. Which of the following is the best solution for the administrator to set up?

A. A separate scope for the file server using a 132 subnet
B. A reservation for the server based on the MAC address
C. A static IP address within the DHCP IP range
D. A SLAAC for the server

Answer: B

Explanation:
A reservation for the server based on the MAC address means that the DHCP server will assign a specific IP address to the file server every time it requests one, based on its MAC address. This way, the file server will have a consistent IP address that users can access, without the need to manually configure it or use a separate scope. A reservation also ensures that the IP address of the file server will not be given to any other device by the DHCP server

NEW QUESTION 186
- (Topic 3)
Many IP security cameras use RTSP to control media playback. Which of the following default transport layer port numbers does RTSP use?

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

Answer: B

Explanation:
RTSP stands for Real Time Streaming Protocol and is an application-level network protocol designed for controlling media playback on streaming media servers. RTSP uses the default transport layer port number 554 for both TCP and UDP1. Port 445 is used for SMB (Server Message Block), a protocol for file and printer sharing. Port 587 is used for SMTP (Simple Mail Transfer Protocol), a protocol for sending email messages. Port 5060 is used for SIP (Session Initiation Protocol), a protocol for initiating and managing multimedia sessions.
References: 1 Real Time Streaming Protocol - Wikipedia (https://en.wikipedia.org/wiki/Real_Time_Streaming_Protocol)

NEW QUESTION 187
- (Topic 3)
Two users on a LAN establish a video call. Which of the following OSI model layers ensures the initiation coordination, and termination of the call?

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

Answer: A

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

NEW QUESTION 191
- (Topic 3)
A network administrator is testing performance improvements by configuring channel bonding on an 802.Hac AP. Although a site survey detected the majority of

the 5GHz frequency spectrum was idle, being used only by the company's WLAN and a nearby government radio system, the AP is not allowing the administrator to manually configure a large portion of the 5GHz frequency range. Which of the following would be BEST to configure for the WLAN being tested?

A. Upgrade the equipment to an AP that supports manual configuration of the ElRP power settings.
B. Switch to 802.11
C. disable channel auto-selection, and enforce channel bonding on the configuration.
D. Set up the AP to perform a dynamic selection of the frequency according to regulatory requirements.
E. Deactivate the band 5GHz to avoid Interference with the government radio

Answer: C

NEW QUESTION 192
- (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 197
- (Topic 3)
Which of the following describes the BEST device to configure as a DHCP relay?

A. Bridge
B. Router
C. Layer 2 switch
D. Hub

Answer: B

Explanation:
Normally, routers do not forward broadcast traffic. This means that each broadcast domain must be served by its own DHCP server. On a large network with multiple subnets, this would mean provisioning and configuring many DHCP servers. To avoid this scenario, a DHCP relay agent can be configured to provide forwarding of DHCP traffic between subnets. Routers that can provide this type of forwarding are described as RFC 1542 compliant. The DHCP relay intercepts broadcast DHCP frames, applies a unicast address for the appropriate DHCP server, and forwards them over the interface for the subnet containing the server. The DHCP server can identify the original IP subnet from the packet and offer a lease from the appropriate scope. The DHCP relay also performs the reverse process of directing responses from the server to the appropriate client subnet.

NEW QUESTION 201
- (Topic 3)
A store owner would like to have secure wireless access available for both business equipment and patron use. Which of the following features should be configured to allow different wireless access through the same equipment?

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

Answer: D

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

NEW QUESTION 205
- (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 207
- (Topic 3)
An engineer is designing a network topology for a company that maintains a large on- premises private cloud. A design requirement mandates internet-facing hosts to be partitioned off from the internal LAN and internal server IP ranges. Which Of the following
defense strategies helps meet this requirement?

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

Answer: A

Explanation:
A screened subnet is a network segment that is isolated from both the internal LAN and the Internet by firewalls. A screened subnet can be used to host internet-facing hosts such as web servers, email servers, or DNS servers. A screened subnet provides an additional layer of security and prevents direct access to the internal network from the Internet.
References: Network+ Study Guide Objective 3.1: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 208
- (Topic 3)
Which of the following should be used to associate an IPv6 address with a domain name?

A. AAAA
B. A
C. SOA
D. TXT

Answer: A

Explanation:
An AAAA record is a type of DNS record that maps a domain name to an IPv6 address. It is similar to an A record, which maps a domain name to an IPv4 address, but it uses a 128-bit address instead of a 32-bit one. An AAAA record allows a domain name to be resolved by both IPv4 and IPv6 clients, and it is necessary for accessing websites and services that use IPv6.

NEW QUESTION 210
- (Topic 3)
Classification using labels according to information sensitivity and impact in case of unauthorized access or leakage is a mandatory component of:

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

Answer: C

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

NEW QUESTION 214
- (Topic 3)
A user is unable to reach any resources on the internet. A technician goes to the site and obtains the following output from the workstation:

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

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

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

Answer: A

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

NEW QUESTION 219
- (Topic 3)
Which of the following bandwidth management techniques uses buffers al the client side to prevent TCP retransmissions from occurring when the ISP starts to drop packets of specific types that exceed the agreed traffic rate?

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

Answer: D

NEW QUESTION 222
- (Topic 3)
An attacker targeting a large company was able to inject malicious A records into internal name resolution servers. Which of the following attack types was MOST likely used?

A. DNS poisoning
B. On-path
C. IP spoofing
D. Rogue DHCP

Answer: A

NEW QUESTION 227
- (Topic 3)
A company's data center is hosted at its corporate office to ensure greater control over the security of sensitive data. During times when there are increased workloads, some of the company’s non-sensitive data is shifted to an external cloud provider. Which of the following cloud deployment models does this describe?

A. Hybrid
B. Community
C. Public
D. Private

Answer: A

NEW QUESTION 230
- (Topic 3)

An organization is interested in purchasing a backup solution that supports the organization's goals. Which of the following concepts would specify the maximum duration that a given service can be down before impacting operations?

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

Answer: B

Explanation:
The maximum duration that a given service can be down before it impacts operations is often referred to as the Recovery Time Objective (RTO). RTO is a key consideration in any backup and disaster recovery plan, as it determines how quickly the organization needs to be able to recover from a disruption or failure. It is typically expressed in terms of time, and it helps to inform the design and implementation of the backup solution. For example, if an organization has a critical service that must be available 24/7, it may have a very low RTO, requiring that the service be restored within a matter of minutes or even seconds. On the other hand, if the service can be down for a longer period of time without significantly impacting operations, the organization may have a higher RTO. When selecting a backup solution, it is important to consider the organization's RTO requirements and ensure that the solution is capable of meeting those needs. A solution that does not meet the organization's RTO requirements may not be sufficient to ensure the availability of critical services in the event of a disruption or failure.

NEW QUESTION 235
- (Topic 3)
A network administrator is preparing answers for an annual risk assessment that is required for compliance purposes. Which of the following would be an example of an internal threat?

A. An approved vendor with on-site offices
B. An infected client that pulls reports from the firm
C. A malicious attacker from within the same country
D. A malicious attacker attempting to socially engineer access into corporate offices

Answer: A

Explanation:
Insider threat= insider threat is defined as the threat that an employee or a contractor will use his or her authorized access, wittingly or unwittingly, to do harm

NEW QUESTION 239
- (Topic 3)
An office area contains two PoE-enabled WAPs. After the area was remodeled, new cable uplinks were installed in the ceiling above the fluorescent lights. However, after the WAPs were reconnected, users reported slowness and application errors. An intern reviewed the network and discovered a lot of CRC errors. A network engineer reviewed the intern's work and realized UTP cabling was used. Which of the following is the MOST likely cause of the CRC errors?

A. Insufficient power at the antennas
B. PoE and UTP incompatibility
C. Electromagnetic interference
D. Wrong cable pinout

Answer: C

Explanation:
"EMI is a problem when cables are installed near electrical devices, such as air conditioners or fluorescent light fixtures. If a network medium is placed close enough to such a device, the signal within the cable might become corrupt. Network media vary in their resistance to the effects of EMI. Standard unshielded twisted-pair (UTP) cable is susceptible to EMI, whereas fiber cable, with its light transmissions, is resistant to EMI. When deciding on a particular medium, consider where it will run and the impact EMI can have on the installation."

NEW QUESTION 242
- (Topic 3)
A virtual machine has the following configuration:
· IPv4 address: 169.254.10.10
· Subnet mask: 255.255.0.0
The virtual machine can reach colocated systems but cannot reach external addresses on the internet. Which of the following is most likely the root cause?

A. The subnet mask is incorrect.
B. The DHCP server is offline.
C. The IP address is an RFC1918 private address.
D. The DNS server is unreachable.

Answer: B

Explanation:
The IP address 169.254.10.10 is an APIPA (Automatic Private IP Addressing) address, which is assigned by the operating system when a DHCP server is not available or reachable. APIPA addresses are in the range of 169.254.0.0/16, and they allow the device to communicate with other devices on the same local network, but not with external networks or the internet. Therefore, the most likely root cause of the virtual machine’s connectivity issue is that the DHCP server is offline or malfunctioning, and the virtual machine cannot obtain a valid IP address from it.
References
? 1: CompTIA Network+ N10-008 Certification Study Guide, page 86
? 2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 9
? 3: CompTIA Network+ N10-008 Certification Practice Test, question 4

NEW QUESTION 245
- (Topic 3)

Which of the following routing protocols should be implemented to create a route between a local area network and an ISP?

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

Answer: A

Explanation:
BGP stands for Border Gateway Protocol, and it is a routing protocol that is used to exchange routing information between different autonomous systems (AS) on the Internet. An AS is a network or a group of networks that are under the same administrative control and share a common routing policy. BGP is used to create routes between local area networks and Internet service providers (ISPs), as well as between different ISPs. BGP is considered an exterior gateway protocol (EGP), as opposed to an interior gateway protocol (IGP) such as EIGRP, RIP, or OSPF, which are used to create routes within an AS. References: CompTIA Network+ N10-008 Cert Guide, Chapter 3, Section 3.4

NEW QUESTION 250
- (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 254
- (Topic 3)
A consultant is working with two international companies. The companies will be sharing cloud resources for a project. Which of the following documents would provide an agreement on how to utilize the resources?

A. MOU
B. NDA
C. AUP
D. SLA

Answer: A

Explanation:
A memorandum of understanding (MOU) is a document that describes an agreement between two or more parties on how to utilize shared resources for a project. An MOU is not legally binding, but it outlines the expectations and responsibilities of each party involved in the collaboration. An MOU can be used when two international companies want to share cloud resources for a project without creating a formal contract. References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 405)

NEW QUESTION 255
- (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 257
- (Topic 3)
Which of the following is the DNS feature that controls how long a lookup is stored in cache on a server?

A. CNAME
B. TTL
C. SOA
D. SRV

Answer: B

Explanation:
TTL stands for Time to Live, and it is a field on DNS records that controls how long each record is valid and cached by the DNS resolver before it expires and requests a new one. The TTL value is measured in seconds, and it affects how quickly DNS changes propagate across the Internet. A lower TTL means that the DNS resolver will refresh the record more frequently, but it also increases the load on the DNS servers. A higher TTL means that the DNS resolver will cache the record longer, but it also delays the update of the record.

NEW QUESTION 258
- (Topic 3)
A customer hired a network consultant to install a new wireless network with the following specifications:
* 2.4GHz
* 11Mbps
* 20MHz
Which of the following standards best fits these requirements?

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

Answer: B

Explanation:
The 802.11b standard is a wireless networking protocol that operates in the 2.4GHz frequency band and supports a maximum data rate of 11Mbps. It uses a 20MHz channel width and a direct-sequence spread spectrum (DSSS) modulation technique2. The 802.11b standard was released in 1999 and is backward compatible with the original 802.11 standard3. The other standards do not match the specifications given by the customer. 802.11ac operates in the 5GHz band and supports higher data rates up to 6.9Gbps.
* 802.11g also operates in the 2.4GHz band but supports data rates up to 54Mbps. 802.11n can operate in both 2.4GHz and 5GHz bands and supports data rates up to 600Mbps. It also uses a wider channel width of 40MHz and a multiple-input multiple-output (MIMO) technology3.
References2 - 802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a - Lifewire3 - Introduction to WLAN Frequency Bands | Engineering Education (EngEd …

NEW QUESTION 259
- (Topic 3)
A cafeteria is lacing lawsuits related to criminal internet access that was made over its guest network. The marketing team, however, insists on keeping the cafeteria phone number as the wireless passphrase. Which of the following actions would Improve wireless security while accommodating the marketing team and accepting the terms of use?

A. Setting WLAN security to use EAP-TLS
B. Deploying a captive portal tor user authentication
C. Using geofencing to limit the area covered by the WLAN
D. Configuring guest network isolation

Answer: B

Explanation:
A captive portal is a web page that is presented to a user before they are allowed to access a network. It is used to authenticate users and to ensure that all users have accepted the terms of use for the network. By deploying a captive portal, the cafeteria can require users to enter their phone number as the passphrase, while still providing an additional layer of security. Reference: CompTIA Network+ Study Guide, 8th Edition, page 182.

NEW QUESTION 264
- (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 269
- (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 271
- (Topic 3)
Which of the following policies outlines the software and hardware requirements for using personally owned devices to conduct business?

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

Answer: C

Explanation:
The policy that outlines the software and hardware requirements for using personally owned devices to conduct business is BYOD (Bring Your Own Device). BYOD is a practice that allows employees to use their own devices, such as laptops, tablets, or smartphones, to access corporate resources and applications. BYOD can offer benefits such as increased productivity, flexibility, and satisfaction for employees, as well as reduced costs for employers. However, BYOD also poses challenges and risks, such as security, compatibility, and support issues. Therefore, a BYOD policy is needed to define the rules and expectations for using personal devices in a business environment. A BYOD policy typically covers topics such as device eligibility, security requirements, acceptable use, data ownership, privacy, and liability. References: CompTIA Network+ N10-008 Certification Study Guide, page 362; The Official CompTIA Network+ Student Guide (Exam N10-008), page 14-2.

NEW QUESTION 276
- (Topic 3)
A network consultant is setting up a new wireless infrastructure. The new infrastructure is primarily focused on supporting legacy equipment that does not support the newest standards. Which of the following frequency ranges will the consultant most likely have to support?

A. 2.4GHz
B. 5GHz
C. 5.9GHz
D. 6GHz

Answer: A

Explanation:
The most likely frequency range that the network consultant will have to support is 2.4GHz. This is because the most common legacy wireless standards, 802.11b and 802.11g, use the 2.4GHz range1. IEEE 802.11a uses 5GHz exclusively, and 5.9GHz and 6GHz are not widely used by legacy equipment. Therefore, A. 2.4GHz is the correct answer.
https://www.networkcomputing.com/networking/wireless-beginners-part-1-rf-and-waves

NEW QUESTION 280
- (Topic 3)
A company wants to add a local redundant data center to its network in case of failure at its primary location. Which of the following would give the LEAST amount of redundancy for the company's network?

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

Answer: A

NEW QUESTION 284
- (Topic 3)
Which of the following authentication protocols should be used when securing a basic wireless network? (Select two).

A. WPA2
B. RDP
C. WPA

D. SSL
E. SNMP
F. EAP

Answer: AF

Explanation:
WPA2 and EAP are two authentication protocols that can be used to secure a basic wireless network. WPA2 stands for Wi-Fi Protected Access 2 and it is a security standard that provides strong encryption and authentication for wireless networks. WPA2 supports two modes: personal and enterprise. In personal mode, WPA2 uses a pre-shared key (PSK) that is shared among all wireless devices. In enterprise mode, WPA2 uses an authentication server, such as a RADIUS server, to verify the identity of each wireless device. EAP stands for Extensible Authentication Protocol and it is a framework that allows different methods of authentication to be used over wireless networks. EAP works with WPA2 enterprise mode to provide more flexibility and security for wireless authentication. EAP supports various methods, such as EAP-TLS, EAP-FAST, PEAP, and LEAP, that use certificates, passwords, or tokens to authenticate wireless devices.

NEW QUESTION 289
- (Topic 3)
An administrator is attempting to add a new system to monitoring but is unsuccessful. The administrator notices the system is similar to another one on the network; however, the new one has an updated OS version. Which of the following should the administrator consider updating?

A. Management information bases
B. System baseline
C. Network device logs
D. SNMP traps

Answer: A

NEW QUESTION 290
- (Topic 3)
A network administrator is checking to see if anything has changed. Which of the following steps of the troubleshooting methodology is involved?

A. Identify the problem.
B. Test the theory.
C. Establish a theory.
D. Document findings.

Answer: B

Explanation:
According to the CompTIA troubleshooting methodology1, testing the theory is the step where the network administrator verifies if the problem is caused by a specific factor or change. This step involves checking the system logs, running diagnostic tools, or performing other tests to confirm or eliminate the possible cause.
References:
? Troubleshooting Methodology | IT Support and Help Desk | CompTIA1

NEW QUESTION 293
- (Topic 3)
A network administrator is troubleshooting a client's device that cannot connect to the network. A physical inspection of the switch shows the RJ45 is connected. The NIC shows no activity lights. The network administrator moves the device to another location and connects to the network without issues. Which Of the following tools would be the BEST option for the network administrator to use to further troubleshoot?

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

Answer: D

Explanation:
A cable tester is a tool that can verify the integrity and functionality of a network cable. It can measure the electrical characteristics of the cable, such as resistance, capacitance, and impedance, and detect any faults or defects, such as shorts, opens, or crosstalk. A cable tester can help the network administrator troubleshoot the problem by determining if the cable is faulty or not. A tone generator is a tool that can send an audible signal through a cable to help locate and identify it. A multimeter is a tool that can measure voltage, current, and resistance of electrical circuits. An optical time-domain reflectometer (OTDR) is a tool that can test the quality and length of fiber optic cables.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.3: Given a scenario, use the appropriate tool to support wired or wireless networks.

NEW QUESTION 297
- (Topic 3)
Which of the following indicates a computer has reached end-of-support?

A. The computer does not have any users.
B. The antivirus protection is expired.
C. The operating system license is expired.
D. No more patches or bug fixes are available indefinitely.

Answer: D

Explanation:
No more patches or bug fixes are available indefinitely. This indicates that a computer has reached end-of-support, which means that the manufacturer or vendor

of the hardware or software no longer provides technical assistance, updates, or security fixes for the product12. This can expose the computer to potential security risks and compatibility issues with newer technologies

NEW QUESTION 300
- (Topic 3)
A network technician is performing tests on a potentially faulty network card that is installed in a server. Which of the following addresses will MOST likely be used during traffic diagnostic tests?

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

Answer: B

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

NEW QUESTION 303
- (Topic 3)
Which of the following would be BEST suited for use at the access layer in a three-tier architecture system?

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

Answer: C

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

NEW QUESTION 304
- (Topic 3)
A network engineer needs to enable device monitoring using authentication and encryption. Which of the following protocols offers this option?

A. ESP
B. SNMPv3
C. NetFIow
D. SSLv3

Answer: B

Explanation:
SNMPv3 is a protocol that offers device monitoring using authentication and encryption. SNMP stands for Simple Network Management Protocol, and it is a standard way of collecting and organizing information about network devices, such as routers, switches, servers, printers, and so on. SNMPv3 is the latest version of SNMP, and it provides enhanced security features, such as data integrity, data origin authentication, data confidentiality, and access control. SNMPv3 can use different algorithms to encrypt and authenticate the communication between the network management system and the network devices12. References:
? Network Monitoring Tools – CompTIA Network+ N10-006 – 2.12
? CompTIA Network+ N10-008 Certification Exam Objectives, page 93

NEW QUESTION 308
- (Topic 3)
A technician is checking network devices to look for opportunities to improve security Which of the following toots would BEST accomplish this task?

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

Answer: B

Explanation:
A protocol analyzer is a tool that can capture and analyze network traffic and identify security issues such as unauthorized devices, malicious packets, or misconfigured settings.
A Wi-Fi analyzer is a tool that can measure the signal strength, interference, and channel usage of wireless networks, but it cannot provide detailed information about network security.
Nmap and IP scanner are tools that can scan network hosts and ports for open services, vulnerabilities, or operating systems, but they cannot monitor network traffic in real time.

NEW QUESTION 312
- (Topic 3)

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

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

Answer: C

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

NEW QUESTION 316
- (Topic 3)
To find the best subnet mask that meets the requirement of six usable IP addresses, we need to calculate the number of host bits and the number of host addresses for each option. The number of host bits is the number of 0s in the binary representation of the subnet mask, and the number of host addresses is 2^host bits - 2 (the -2 is to exclude the network address and the broadcast address). The option that has the smallest number of host addresses that is greater than or equal to six is the best choice. Here are the calculations for each option:

A. 255.255.255.128Binary: 11111111.11111111.11111111.10000000Host bits: 7Host addresses: 2^7 - 2 = 126 - 2 = 124This option has too many host addresses for the requirement.
B. 255.255.255.192Binary: 11111111.11111111.11111111.11000000Host bits: 6Host addresses: 2^6 - 2 = 64 - 2 = 62This option also has too many host addresses for the requirement.
C. 255.255.255.224Binary: 11111111.11111111.11111111.11100000Host bits: 5Host addresses: 2^5 - 2 = 32 - 2 = 30This option has the smallest number of host addresses that is greater than or equal to six, so this is the best choice.
D. 255.255.255.240Binary: 11111111.11111111.11111111.11110000Host bits: 4Host addresses: 2^4 - 2 = 16 - 2 = 14This option has fewer host addresses than the requirement, so this is not a valid choice.

Answer: C

Explanation:
This subnet mask will allow you to have six usable IP addresses in each subnet, with a minimum of wasted addresses. You can use the following formula to calculate the number of subnets and the subnet ID for each subnet:
Number of subnets = 2^network bits Subnet ID = (subnet number - 1) x number of host addresses + network address
The network bits are the number of 1s in the binary representation of the subnet mask, and the network address is the first address in the range. For example, if your range is 192.168.1.0/27, then the network bits are 27, the network address is 192.168.1.0, and the number of host addresses is 30. Therefore, the number of subnets is 2^27, and the subnet ID for the first subnet is (1 - 1) x 30 + 192.168.1.0 = 192.168.1.0. The subnet ID for the second subnet is (2 - 1) x 30 + 192.168.1.0 = 192.168.1.32, and so on.
References
? Subnet masks are covered in Objective 1.4 of the CompTIA Network+ N10-008 certification exam1.
? Subnet masks can be calculated based on binary and CIDR-block notations2.
? Subnet masks can be used to determine the number of host bits and host addresses3.
1: CompTIA Network+ Certification Exam Objectives, page 4 2: IPv4 Subnet Masks – N10- 008 CompTIA Network+ : 1.41 3: Calculating IPv4 Subnets and Hosts – N10-008 CompTIA Network+ : 1.44

NEW QUESTION 320
- (Topic 3)
A network is secured and is only accessible via TLS and IPSec VPNs. Which of the following would need to be present to allow a user to access network resources on a laptop without logging in to the VPN application?

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

Answer: A

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

NEW QUESTION 321
- (Topic 3)
An organization set up its offices so that a desktop is connected to the network through a VoIP phone. The VoIP vendor requested that voice traffic be segmented separately from non-voice traffic. Which of the following would allow the organization to configure multiple devices with network isolation on a single switch port?

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

Answer: A

NEW QUESTION 322
- (Topic 3)

An IT technician successfully connects to the corporate wireless network at a hank. While performing some tests, the technician observes that the physical address of the DHCp server has changed even though the network connection has not been lost. Which of the following would BEST explain this change?

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

Answer: D

Explanation:
A rogue server is a DHCP server on a network that is not under the administrative control of the network staff1. It may provide incorrect IP addresses or other network configuration information to devices on the network, causing them to lose connectivity or be vulnerable to attacks2. The physical address of the DHCP server may change if a rogue server takes over the role of assigning IP addresses to devices on the network. This can be detected by monitoring DHCP traffic or using tools such as RogueChecker2.

NEW QUESTION 326
- (Topic 3)
An ISP configured an internet connection to provide 20Mbps, but actual data rates are occurring at 10Mbps and causing a significant delay in data transmission. Which of the following specifications should the ISP check?

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

Answer: A

Explanation:
Throughput is the actual amount of data that can be transferred over a network in a given time. Throughput can be affected by various factors such as congestion, interference, errors, or hardware limitations. If the throughput is lower than the configured internet connection speed, it can cause a significant delay in data transmission. The ISP should check the throughput and identify the source of the problem.
References: Network+ Study Guide Objective 2.2: Explain the concepts and characteristics of routing and switching.

NEW QUESTION 327
- (Topic 3)
Users have reported an issue connecting to a server over the network. A workstation was recently added to the network and configured with a shared USB printer. Which of the following is most likely causing the issue?

A. The switch is oversubscribed and cannot handle the additional throughput.
B. The printer is tying up the server with DHCP discover messages
C. The web server's back end was designed for only single-threaded applications.
D. The workstation was configured with a static IP that is the same as the server.

Answer: D

Explanation:
The workstation was configured with a static IP that is the same as the server is the most likely cause of the issue where users are unable to access any network resources. A static IP address is an IP address that is manually assigned to a device and does not change over time. A static IP address can be useful for devices that need to be easily identified or accessed on a network, such as servers or printers. However, if two devices on the same network have the same static IP address, it can cause an IP address conflict. An IP address conflict occurs when two devices try to use the same IP address at the same time, resulting in network communication errors or failures. An IP address conflict can prevent users from accessing any network resources that rely on the IP address for identification or routing. References: [CompTIA Network+ Certification Exam
Objectives], What Is an IP Address Conflict? | HowStuffWorks

NEW QUESTION 332
- (Topic 3)
A help desk supervisor reviews the following excerpt of a call transcript:

```
Agent: Thanks for calling the help desk. What can I help you with today?
Customer: I have been trying to connect to www.awesome-website.com all morning, but I can't get to it.
Agent: Let me see if I can reach it from my end. Give me a moment, please.
Customer: Sure. Thanks for helping.
Agent: It's my pleasure. And indeed, it seems like I can't reach that website either.
Customer: I guess that means that it isn't just me, then.
```

Which of the following was the agent trying to accomplish with this exchange?

A. The agent was questioning the obvious.
B. The agent was verifying full system functionality
C. The agent was identifying potential effects.
D. The agent was trying to duplicate the problem.

Answer: D

Explanation:
The agent was trying to duplicate the problem by asking the user to perform the same steps that led to the issue. This is a common troubleshooting technique that helps the agent to identify the root cause of the problem and verify if it is reproducible or intermittent. By duplicating the problem, the agent can also gather more information about the symptoms and error messages that the user encountered. References: [CompTIA Network+ Certification Exam Objectives], [Troubleshooting Methodology - CompTIA Network+ N10-007 - 1.4 | Professor Messer IT Certification Training Courses]

NEW QUESTION 336
- (Topic 3)
Which of the following would a network administrator configure to set NTP settings for a specific subnet within DHCP?

A. Reservation
B. Lease time
C. Scope options
D. Exclusion range

Answer: C

Explanation:
The network administrator would configure scope options to set NTP settings for a specific subnet within DHCP. Scope options are settings that apply to a range of IP addresses that are assigned by a DHCP server. Scope options can include parameters such as default gateway, DNS server, and NTP server. By configuring the NTP server option for a specific scope, the network administrator can ensure that the devices in that subnet synchronize their clocks with the same time source. References: CompTIA Network+ N10-008 Certification Study Guide, page 121; The Official CompTIA Network+ Student Guide (Exam N10-008), page 5-11.

NEW QUESTION 340
- (Topic 3)
Which of the following devices have the capability to allow communication between two different subnetworks? (Select TWO).

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

Answer: DE

NEW QUESTION 342
- (Topic 3)
A technician thinks one of the router ports is flapping. Which of the following available resources should the technician use in order to determine if the router is flapping?

A. Audit logs
B. NetFlow
C. Syslog
D. Traffic logs

Answer: C

Explanation:
Syslog is a protocol that allows network devices to send event messages to a centralized server or console for logging and analysis1. Syslog can help a technician to determine if a router port is flapping by providing timestamps, severity levels, and
descriptions of the events that occur on the router, such as interface up or down, link state change, or error messages. Syslog can also help to identify the cause and frequency of the port flapping and troubleshoot the issue.
Audit logs are records of actions or events that occur on a system or network, such as user login, file access, configuration change, or policy violation. Audit logs can help to monitor and verify the activities and behaviors of users, devices, or applications on a system or network. Audit logs can also help to detect and investigate security incidents, compliance issues, or performance problems. However, audit logs do not provide detailed information about router port flapping.
NetFlow is a protocol that collects and analyzes network traffic data for monitoring and troubleshooting purposes2. NetFlow can help to identify the sources, destinations, volumes, and types of traffic on a network. NetFlow can also help to optimize network performance, security, and capacity planning. However, NetFlow does not provide detailed information about router port flapping.
Traffic logs are records of network traffic that pass through a device or application, such as a firewall, proxy, or web server. Traffic logs can help to monitor and filter the network traffic based on rules or policies. Traffic logs can also help to detect and prevent malicious traffic, such as malware, attacks, or unauthorized access. However, traffic logs do not provide detailed information about router port flapping.

NEW QUESTION 346
- (Topic 3)
Which of the following diagrams would most likely include specifications about fiber connector types?

A. Logical
B. Physical
C. Rack
D. Routing

Answer: B

Explanation:
A physical diagram is a type of diagram that shows the physical layout and connections of the network devices and components, such as routers, switches, cables, and connectors. A physical diagram may include specifications about the fiber connector types, such as LC, SC, FC, ST, MPO, etc., that are used to link the fiber optic cables and devices. A physical diagram can help to visualize the network topology, troubleshoot network problems, and plan network changes

NEW QUESTION 348
- (Topic 3)
Which of the following must be functioning properly in order for a network administrator to create an accurate timeline during a troubleshooting process?

A. NTP

B. IP helper
C. Syslog
D. MySQL

Answer: C

NEW QUESTION 353
.....

Relate Links

100% Pass Your N10-009 Exam with Exambible Prep Materials

https://www.exambible.com/N10-009-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/