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

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

Answer: B

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

NEW QUESTION 4
- (Topic 3)
During an incident, an analyst sends reports regularly to the investigation and leadership teams. Which of the following best describes how Pll should be safeguarded during an incident?

A. Implement data encryption and store the data so only the company has access.
B. Ensure permissions are limited to the investigation team and encrypt the data.
C. Implement data encryption and create a standardized procedure for deleting data that is no longer needed.
D. Ensure the permissions are open only to the company.

Answer: C

Explanation:
PII stands for Personally Identifiable Information, which is any data that can be used to identify, contact, or locate a specific individual, such as name, address, phone number, email, social security number, and so on. PII should be safeguarded during an incident to protect the privacy and security of the individuals involved, and to comply with the legal and ethical obligations of the organization. One way to safeguard PII during an incident is to implement data encryption, which is a process of transforming data into an unreadable format that can only be accessed by authorized parties who have the decryption key. Data encryption can prevent unauthorized access, modification, or disclosure of PII by malicious actors or third parties. Another way to safeguard PII during an incident is to create a standardized procedure for deleting data that is no longer needed, such as after the incident is resolved or the investigation is completed. Deleting data that is no

longer needed can reduce the risk of data breaches, data leaks, or data theft, and can also save storage space and resources. A standardized procedure for deleting data can ensure that the data is erased securely and completely, and that the deletion process is documented and audited.
References
? 1: CompTIA Network+ N10-008 Certification Study Guide, page 304-305
? 2: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 13
? 3: CompTIA Network+ N10-008 Certification Practice Test, question 5
? 4: Data Encryption – N10-008 CompTIA Network+ : 3.1

NEW QUESTION 5
- (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 6
- (Topic 3)
A network administrator needs to create an SVI on a Layer 3-capable device to separate voice and data traffic. Which of the following best explains this use case?

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

Answer: C

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

NEW QUESTION 7
- (Topic 3)
A Chief Information Officer wants to monitor network breaching in a passive, controlled manner. Which of the following would be best to implement?

A. Honeypot
B. Perimeter network
C. Intrusion prevention system
D. Port security

Answer: A

Explanation:
A honeypot is a decoy system that is designed to attract and trap hackers who attempt to breach the network. A honeypot mimics a real system or network, but contains fake or non- sensitive data and applications. A honeypot can be used to monitor network breaching in a passive, controlled manner, as it allows the network administrator to observe the hacker’s behavior, techniques, and tools without compromising the actual network or data. A honeypot can also help to divert the hacker’s attention from the real targets and collect forensic evidence for further analysis or prosecution.

NEW QUESTION 8
- (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 9

- (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 10
- (Topic 3)
A user notifies a network administrator about losing access to a remote file server. The network administrator is able to ping the server and verifies the current firewall rules do not block access to the network fileshare. Which of the following tools would help identify which ports are open on the remote file server?

A. dig
B. nmap
C. tracert
D. nslookup

Answer: B

Explanation:
nmap is the tool that would help identify which ports are open on the remote file server. nmap stands for Network Mapper, which is a free and open-source tool that can perform various network scanning and discovery tasks. nmap can help identify which ports are open on a remote device by sending probes or packets to different ports and analyzing the responses. nmap can also provide information about the operating system, services, versions, firewalls, or vulnerabilities of the remote device. nmap can be useful for network administrators, security professionals, or hackers to monitor, audit, or attack network devices. References: [CompTIA Network+ Certification Exam Objectives], Nmap - Free Security Scanner For Network Exploration & Security Audits

NEW QUESTION 10
- (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 14
- (Topic 3)
A network engineer needs to create a subnet that has the capacity for five VLANs. with the following number of clients lo be allowed on each:

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

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

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

Answer: B

NEW QUESTION 15
- (Topic 3)
A network technician 13 troubleshooting a specific port on a switch. Which of the following commands should the technician use to see the port configuration?

A. show route
B. show Interface
C. show arp
D. show port

Answer: B

Explanation:
To see the configuration of a specific port on a switch, the network technician should use the "show interface" command. This command provides detailed information about the interface, including the current configuration, status, and statistics for the interface.

NEW QUESTION 16
- (Topic 3)
Which of the following protocols is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links?

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

Answer: A

NEW QUESTION 20
- (Topic 3)
Which of the following records can be used to track the number of changes on a DNS zone?

A. SOA
B. SRV
C. PTR
D. NS

Answer: A

Explanation:
The DNS ‘start of authority’ (SOA) record stores important information about a domain or zone such as the email address of the administrator, when the domain was last updated, and how long the server should wait between refreshes. All DNS zones need an SOA record in order to conform to IETF standards. SOA records are also important for zone transfers.

NEW QUESTION 22
- (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 27
- (Topic 3)
Which of the following is most likely to be implemented to actively mitigate intrusions on a host device?

A. HIDS
B. MDS
C. HIPS
D. NIPS

Answer: A

Explanation:
HIDS (host-based intrusion detection system) is a type of security software that monitors and analyzes the activity on a host device, such as a computer or a server. HIDS can detect and alert on intrusions, such as malware infections, unauthorized access, configuration changes, or policy violations. HIDS can also

actively mitigate intrusions by blocking or quarantining malicious processes, files, or network connections1.
HIPS (host-based intrusion prevention system) is similar to HIDS, but it can also prevent intrusions from happening in the first place by enforcing security policies and rules on the host device2. MDS (multilayer switch) is a network device that combines the functions of a switch and a router, and it does not directly protect a host device from intrusions3. NIPS (network-based intrusion prevention system) is a network device that monitors and blocks malicious traffic on the network level, and it does not operate on the host device level4.

NEW QUESTION 30
- (Topic 3)
Which of the following is used to elect an STP root?

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

Answer: B

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

NEW QUESTION 33
- (Topic 3)
An engineer recently decided to upgrade the firmware on a router. During the upgrade, the help desk received calls about a network outage, and a critical ticket was opened. The network manager would like to create a policy to prevent this from happening in the future. Which of the following documents should the manager create?

A. Change management
B. incident response
C. Standard operating procedure
D. System life cycle

Answer: A

NEW QUESTION 35
- (Topic 3)
Which of the following devices Is used to configure and centrally manage access points Installed at different locations?

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

Answer: A

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

NEW QUESTION 38
- (Topic 3)
Which of the following is a valid and cost-effective solution to connect a fiber cable into a network switch without available SFP ports?

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

Answer: A

NEW QUESTION 40
- (Topic 3)
Which of the following focuses on application delivery?

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

Answer: C

Explanation:
SaaS is the cloud computing model that focuses on application delivery. SaaS stands for Software as a Service, which is a cloud computing model that provides software applications over the internet. SaaS allows customers to access and use software applications without installing or maintaining them on their own devices or servers. SaaS offers advantages such as scalability, accessibility, compatibility, and cost-effectiveness.

Customers can use SaaS applications on demand and pay only for what they use. References: [CompTIA Network+ Certification Exam Objectives], What Is Software as a Service (SaaS)? | IBM

NEW QUESTION 42
- (Topic 3)
Which of the following fiber connector types is the most likely to be used on a network interface card?

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

Answer: A

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

NEW QUESTION 46
- (Topic 3)
A network administrator would like to purchase a device that provides access ports to endpoints and has the ability to route between networks. Which of the following would be BEST for the administrator to purchase?

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

Answer: B

NEW QUESTION 50
- (Topic 3)
A customer reports there is no access to resources following the replacement of switches. A technician goes to the site to examine the configuration and discovers redundant links between two switches. Which of the following is the reason the network is not functional?

A. The ARP cache has become corrupt.
B. CSMA/CD protocols have failed.
C. STP is not configured.
D. The switches are incompatible models

Answer: C

Explanation:
The reason the network is not functional is that STP (Spanning Tree Protocol) is not configured on the switches. STP is a protocol that prevents loops in a network topology by blocking redundant links between switches. If STP is not enabled, the switches will forward broadcast frames endlessly, creating a broadcast storm that consumes network resources and disrupts communication. References: CompTIA Network+ N10-008 Certification Study Guide, page 67; The Official CompTIA Network+ Student Guide (Exam N10-008), page 2-14.

NEW QUESTION 53
- (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 54
- (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 55
- (Topic 3)
A network technician wants to deploy a new wireless access point to reduce user latency. Currently, the organization has the following deployed:
Which of the following channels should the new device broadcast on?

A. Channel 3
B. Channel 9
C. Channel 10
D. Channel 11

Answer: D

Explanation:
The best channel for a new wireless access point is one that does not overlap with the existing channels used by other devices. Overlapping channels can cause interference and degrade the performance of the wireless network. According to the web search results, the 2.4 GHz band has 11 channels in the U.S., but only channels 1, 6, and 11 are non- overlapping. Since the existing devices are using channels 1 and 6, the new device should use channel 11 to avoid adjacent-channel interference12
References1: Why Channels 1, 6 and 11? | MetaGeek 2: How to Choose the Best Wi-Fi Channels for Your Network - Lifewire

NEW QUESTION 58
- (Topic 3)
A company has multiple offices around the world. The computer rooms in some office locations are too warm Dedicated sensors are in each room, but the process of checking each sensor takes a long time. Which of the following options can the company put In place to automate temperature readings with internal resources?

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

Answer: D

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

NEW QUESTION 62
- (Topic 3)
The power company notifies a network administrator that it will be turning off the power to the building over the weekend. Which of the following is the BEST solution to prevent the servers from going down?

A. Redundant power supplies
B. Uninterruptible power supply
C. Generator
D. Power distribution unit

Answer: A

NEW QUESTION 65
- (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 68
- (Topic 3)
A VOIP phone is plugged in to a port but cannot receive calls. Which Of the following needs to be done on the port to address the issue?

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

Answer: C

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

NEW QUESTION 70
- (Topic 3)
A network engineer designed and implemented a new office space with the following characteristics:

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

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

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

Answer: D

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

NEW QUESTION 72
- (Topic 3)
A network technician needs to ensure the company's external mail server can pass reverse lookup checks. Which of the following records would the technician MOST likely configure? (Choose Correct option and give explanation directly from CompTIA Network+ Study guide or documents)

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

Answer: A

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

NEW QUESTION 76
- (Topic 3)
Which of the following devices would be used to extend the range of a wireless network?

A. A repeater
B. A media converter
C. A router
D. A switch

Answer: A

Explanation:
A repeater is a device used to extend the range of a wireless network by receiving, amplifying, and retransmitting wireless signals. It is typically used to extend the range of a wireless network in a large area, such as an office building or a campus. Repeaters can also be used to connect multiple wireless networks together, allowing users to move seamlessly between networks. As stated in the CompTIA Network+ Study Manual, "a wireless repeater is used to extend the range of a wireless network by repeating the signal from one access point to another."

NEW QUESTION 78
- (Topic 3)
Which of the following best describe the functions of Layer 2 of the OSI model? (Select two).

A. Local addressing
B. Error preventing
C. Logical addressing
D. Error detecting
E. Port addressing
F. Error correcting

Answer: AD

Explanation:
Layer 2 of the OSI model, also known as the data link layer, is responsible for physical addressing and error detecting. Physical addressing refers to the use of MAC addresses to identify and locate devices on a network segment. Error detecting refers to the use of techniques such as checksums and CRCs to identify and correct errors in the data frames.
References:
? OSI Model | Computer Networking | CompTIA1

NEW QUESTION 81
- (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 86
- (Topic 3)
Which of the following describes traffic going in and out of a data center from the internet?

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

Answer: B

NEW QUESTION 88
- (Topic 3)
Which of the following architectures is used for FTP?

A. Client-server
B. Service-oriented
C. Connection-oriented
D. Data-centric

Answer: A

Explanation:
FTP (File Transfer Protocol) is a client-server based protocol, meaning that the two computers involved communicate with each other in a request-response pattern. The client sends a request to the server and the server responds with the requested data. This type of architecture is known as client-server, and it is used for many different types of applications, including FTP. Other architectures, such as service-oriented, connection- oriented, and data-centric, are not used for FTP.

NEW QUESTION 89
- (Topic 3)
A WAN technician reviews activity and identifies newly installed hardware that is causing outages over an eight-hour period. Which of the following should be considered FIRST?

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

Answer: D

Explanation:
The most likely cause of outages due to newly installed hardware is a misconfiguration of the device settings. Therefore, the first step should be to review the device configuration and check for any errors or inconsistencies that might affect the WAN connectivity. References: Network+ Study Guide Objective 2.1: Explain the importance of network documentation.

NEW QUESTION 91
- (Topic 3)
A network resource was accessed by an outsider as a result of a successful phishing campaign. Which of the following strategies should be employed to mitigate the effects of phishing?

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

Answer: A

Explanation:
Multifactor authentication is a security measure that requires users to provide multiple pieces of evidence before they can access a network resource. This could include requiring users to enter a username, password, and a code sent to the user's mobile phone before they are allowed access. This ensures that the user is who they say they are, reducing the risk of malicious actors gaining access to network resources as a result of a successful phishing campaign.

NEW QUESTION 94
- (Topic 3)
Which of the following protocols uses Dijkstra's algorithm to calculate the LOWEST cost between routers?

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

Answer: B

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

NEW QUESTION 99
- (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 102
- (Topic 3)
A network technician receives a support ticket concerning multiple users who are unable access the company's shared drive. The switch interface that the shared drive Is connected to is displaying die following:

```
GigabitEthernet0/9 is down, line protocol is down (notconnect)
        Hardware is Gigabit Ethernet, address is C800.84bf.9847 (via c800.84bf.9847)
        MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
        reliability 255/255. txload 1/255. rxload 1/255
        Encapsulation ARPA, loopback not set
```

Which of the following is MOST likely the Issue?

A. The switchport Is shut down
B. The cable Is not plugged In.

C. The loopoack Is not set
D. The bandwidth configuration is incorrect.

Answer: A

Explanation:
The switchport is shut down, which means it is administratively disabled and cannot forward traffic. The image shows that the switchport status is “down” and the protocol status is “down”, indicating that there is no physical or logical connection. The cable is plugged in, as shown by the “connected” message under the interface name. The loopback is not set, as shown by the “loopback not set” message under the encapsulation type. The bandwidth configuration is correct, as shown by the “BW 10000 Kbit/sec” message under the MTU size. References: [CompTIA Network+ Certification Exam Objectives], Domain 3.0 Infrastructure, Objective 3.1: Given a scenario, use appropriate networking tools, Subobjective: Command line tools (ping, netstat, tracert, etc.)

NEW QUESTION 106
- (Topic 3)
Users are reporting intermittent Wi-Fi connectivity in specific parts of a building. Which of the following should the network administrator check FIRST when troubleshooting this issue? (Select TWO).

A. Site survey
B. EIRP
C. AP placement
D. Captive portal
E. SSID assignment
F. AP association time

Answer: AC

Explanation:
This is a coverage issue. WAP placement and power need to be checked. Site survey should be done NEXT because it takes a while.

NEW QUESTION 108
- (Topic 3)
A help desk technician is concerned that a client's network cable issues may be causing intermittent connectivity. Which of the following would help the technician determine if this is the issue?

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

Answer: A

Explanation:
To determine if a client's network cable issues may be causing intermittent connectivity, the help desk technician can run the show interface command on the switch.
This command allows the technician to view the status and statistics of the various interfaces on the switch, including the physical link status and the number of transmitted and received packets. If the interface is experiencing a large number of errors or dropped packets, this could indicate a problem with the network cable or with the connection between the client's device and the switch.
"Cisco routers and switches have a show interfaces IOS command that provides interface statistics/status information, including link state (up/down), speed/duplex, send/receive traffic, cyclic redundancy checks (CRCs), and protocol packet and byte counts."

NEW QUESTION 110
- (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 113
- (Topic 3)
Which of the following should be used to manage outside cables that need to be routed to various multimode uplinks?

A. Fiber distribution panel
B. 110 punchdown block
C. PDU

D. TIA/EIA-568A patch bay
E. Cat 6 patch panel

Answer: A

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

NEW QUESTION 114
- (Topic 3)
Network connectivity in an extensive forest reserve was achieved using fiber optics. A network fault was detected, and now the repair team needs to check the integrity of the fiber cable. Which of me following actions can reduce repair time?

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

Answer: C

NEW QUESTION 117
- (Topic 3)
A user took a laptop on a trip and made changes to the network parameters while at the airport. The user can access all internet websites but not corporate intranet websites. Which of the following is the most likely cause of the issue?

A. Duplicate IP address
B. Duplicate SSID
C. Incorrect DNS
D. Incorrect subnet mask

Answer: C

Explanation:
DNS (Domain Name System) is a service that translates domain names into IP addresses. Corporate intranet websites are usually hosted on private IP addresses that are not accessible from the public internet. Therefore, the user's laptop needs to use the correct DNS server that can resolve the intranet domain names to the private IP addresses. If the user changed the network parameters at the airport and did not revert them back, the laptop might be using a public DNS server that does not have the records for the intranet websites. This would cause the user to access all internet websites but not corporate intranet websites.
References:
? An Overview of DNS - N10-008 CompTIA Network+ : 1.61
? DNS Configuration – CompTIA A+ 220-11012
? CompTIA Network+ Certification Exam Objectives, page 53

NEW QUESTION 120
- (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 124
- (Topic 3)
A firewall administrator observes log entries of traffic being allowed to a web server on port 80 and port 443. The policy for this server is to only allow traffic on port 443. The firewall administrator needs to investigate how this change occurred to prevent a reoccurrence. Which of the following should the firewall administrator do next?

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

Answer: A

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

from happening again

NEW QUESTION 126
- (Topic 3)
Which of the following topologies requires me MOST connections when designing a network?

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

Answer: A

NEW QUESTION 130
- (Topic 3)
A network client is trying to connect to the wrong TCP port. Which of the following responses would the client MOST likely receive?

A. RST
B. FIN
C. ICMP Time Exceeded
D. Redirect

Answer: A

NEW QUESTION 134
- (Topic 3)
An employee working in a warehouse facility is experiencing interruptions in mobile applications while walking around the facility. According to a recent site survey, the WLAN comprises autonomous APs that are directly connected to the internet, providing adequate signal coverage. Which of the following is the BEST solution to improve network stability?

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

Answer: A

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

NEW QUESTION 137
- (Topic 3)
A network administrator is decommissioning a server. Which of the following will the network administrator MOST likely consult?

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

Answer: D

NEW QUESTION 142
- (Topic 3)
Which of the following layers of the OSI model has new protocols activated when a user moves from a wireless to a wired connection?

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

Answer: A

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

NEW QUESTION 144
- (Topic 3)
Which of the following cloud components can filter inbound and outbound traffic between cloud resources?

A. NAT gateways

B. Service endpoints
C. Network security groups
D. Virtual private cloud

Answer: C

Explanation:
Network security groups are cloud components that can filter inbound and outbound traffic between cloud resources based on rules and priorities. Network security groups can be applied to virtual machines, subnets, or network interfaces to control the network access and security. Network security groups can allow or deny traffic based on the source, destination, port, and protocol of the packets. Network security groups are different from NAT gateways, service endpoints, and virtual private clouds, which are other cloud components that have different functions and purposes.
References
? 1: Network Security Groups – N10-008 CompTIA Network+ : 3.2
? 2: CompTIA Network+ N10-008 Certification Study Guide, page 329-330
? 3: CompTIA Network+ N10-008 Exam Subnetting Quiz, question 17
? 4: CompTIA Network+ N10-008 Certification Practice Test, question 10

NEW QUESTION 146
- (Topic 3)
An online gaming company needs a cloud solution that will allow for more virtual resources to be deployed when tournaments are held. The number of users who access the service increases during tournaments. The company also needs the resources to return to baseline levels once the resources are not needed in order to reduce cost. Which of the following cloud concepts would provide the best solution?

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

Answer: D

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

NEW QUESTION 148
- (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 150
- (Topic 3)
Which of the following connectors and terminations are required to make a Cat 6 cable that connects from a PC to a non-capable MDIX switch? (Select TWO).

A. T1A-568-A - TIA-568-B
B. TIA-568-B - TIA-568-B
C. RJ11
D. RJ45
E. F-type

Answer: AD

NEW QUESTION 153
- (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 154
- (Topic 3)
A network administrator is in the process of installing 35 PoE security cameras. After the administrator installed and tested the new cables, the administrator installed the cameras. However, a small number of the cameras do not work. Which of the following is the most likely reason?

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

Answer: B

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

NEW QUESTION 159
- (Topic 3)
A security team would like to use a system in an isolated network to record the actions of potential attackers. Which of the following solutions is the security team implementing?

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

Answer: B

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

NEW QUESTION 164
- (Topic 3)
Which of the following allows for an devices within a network to share a highly reliable time source?

A. NTP
B. SNMP
C. SIP
D. DNS

Answer: A

Explanation:
Network Time Protocol (NTP) is a protocol used to maintain a highly accurate and reliable clock time on all devices within a network. NTP works by synchronizing the time of all the devices within a network to a single, highly accurate time source. This allows for the time of all the devices to be kept in sync with each other, ensuring a consistent and reliable time source for all devices within the network.

NEW QUESTION 168

- (Topic 3)
After upgrading to a SOHO router that supports Wi-Fi 6, the user determines throughput has not increased. Which of the following is the MOST likely cause of the issue?

A. The wireless router is using an incorrect antenna type.
B. The user's workstation does not support 802.11 ax.
C. The encryption protocol is mismatched
D. The network is experiencing interference.

Answer: B

Explanation:
The user's workstation does not support 802.11 ax, which is the technical name for Wi-Fi 6. Wi-Fi 6 is a new wireless standard that offers faster speeds, higher capacity, and lower latency than previous standards. However, to take advantage of these
benefits, both the router and the workstation need to support Wi-Fi 6. If the workstation only supports an older standard, such as 802.11 ac or Wi-Fi 5, then the throughput will not increase even if the router supports Wi-Fi 6. References: [CompTIA Network+ Certification Exam Objectives], What is Wi-Fi 6? Here's what you need to know | PCWorld

NEW QUESTION 169
- (Topic 3)
A technician is investigating packet loss to a device that has varying data bursts throughout the day. Which of the following will the technician MOST likely configure to resolve the issue?

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

Answer: A

Explanation:
Ethernet flow control is a mechanism for temporarily stopping the transmission of data on Ethernet family computer networks. The goal of this mechanism is to avoid packet loss in the presence of network congestion.
Flow control is a mechanism that allows a device to regulate the amount of data it receives from another device, ensuring that the receiving device is not overwhelmed with data. If the device experiencing packet loss is receiving large bursts of data at times when it is not able to process it quickly enough, configuring flow control could help prevent packets from being lost.
"In theory, flow control can help with situations like a host that can't keep up with the flow of traffic. It enables the host to send an Ethernet PAUSE frame, which asks the switch to hold up for some amount of time so the host can catch its breath. If the switch can, it'll buffer transmissions until the pause expires, and then start sending again. If the host catches up early, it can send another PAUSE frame with a delay of zero to ask the switch to resume. In practice, flow control can cause latency trouble for modern real-time applications such as VoIP, and the same needs are usually met by QoS"

NEW QUESTION 171
- (Topic 3)
Which of the following can be used to limit the ability of devices to perform only HTTPS connections to an internet update server without exposing the devices to the public internet?

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

Answer: A

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

NEW QUESTION 175
- (Topic 3)
During a recent security audit, a contracted penetration tester discovered the organization uses a number of insecure protocols. Which of the following ports should be disallowed so only encrypted protocols are allowed? (Select TWO).

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

Answer: BC

NEW QUESTION 180
- (Topic 3)
A network administrator wants to know which systems on the network are at risk of a known vulnerability. Which of the following should the administrator reference?

A. SLA

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

Answer: E

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

NEW QUESTION 183
- (Topic 3)
A network administrator is setting up a new phone system and needs to define the location where VoIP phones can download configuration files. Which of the following DHCP services can be used to accomplish this task?

A. Scope options
B. Exclusion ranges
C. Lease time
D. Relay

Answer: A

Explanation:
To define the location where VoIP phones can download configuration files, the network administrator can use scope options within the Dynamic Host Configuration Protocol (DHCP) service. Scope options are a set of values that can be configured within a DHCP scope, which defines a range of IP addresses that can be leased to clients on a network. One of the scope options that can be configured is the option for the location of the configuration file server, which specifies the URL or IP address of the server where the configuration files can be downloaded.
https://pbxbook.com/voip/dhcpcfg.html

NEW QUESTION 188
- (Topic 3)
A network administrator received a report staling a critical vulnerability was detected on an application that is exposed to the internet. Which of the following Is the appropriate NEXT step?

A. Check for the existence of a known exploit in order to assess the risk
B. Immediately shut down the vulnerable application server.
C. Install a network access control agent on the server.
D. Deploy a new server to host the application.

Answer: A

Explanation:
The appropriate next step in this situation would be to check for the existence of a known exploit in order to assess the risk. This is important because it will help the network administrator determine the severity of the vulnerability and the potential impact it could have on the organization. Once the network administrator has assessed the risk, they can then take appropriate action to address the vulnerability. This might include patching the application, deploying a new server to host the application, or implementing other security measures to mitigate the risk. It is generally not advisable to immediately shut down the vulnerable application server, as this could disrupt business operations and cause significant downtime. Similarly, installing a network access control agent on the server may not be the most effective solution, as it would not address the underlying vulnerability.

NEW QUESTION 191
- (Topic 3)
After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect
take to troubleshoot the issue?

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

Answer: A

Explanation:

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

NEW QUESTION 196
- (Topic 3)
A technician is concerned about unauthorized personnel moving assets that are installed in a data center server rack. The technician installs a networked sensor that sends an alert when the server rack door is opened. Which of the following did the technician install?

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

Answer: D

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

NEW QUESTION 199
- (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 200
- (Topic 3)
AGRE tunnel has been configured between two remote sites. Which of the following
features, when configured, ensures me GRE overhead does not affect payload?

A. jumbo frames
B. Auto medium-dependent Interface
C. Interface crossover
D. Collision detection

Answer: A

Explanation:
One of the features that can be configured to ensure that GRE overhead does not affect payload is A. jumbo frames. Jumbo frames are Ethernet frames that have a payload size larger than 1500 bytes, which is the standard maximum transmission unit (MTU) for Ethernet. By using jumbo frames, more data can be sent in each packet, reducing the overhead ratio and improving efficiency.
Auto medium-dependent interface (MDI), interface crossover, and collision detection are features related to Ethernet physical layer connectivity, but they do not affect GRE overhead or payload.

NEW QUESTION 201
- (Topic 3)
Which of the following network types is composed of computers that can all communicate with one another with equal permissions and allows users to directly share what is on or
attached to their computers?

A. Local area network
B. Peer-to-peer network
C. Client-server network
D. Personal area network

Answer: B

Explanation:
A peer-to-peer network is a type of network in which each computer (or node) can communicate directly with any other node, without requiring a central server or authority. Each node can act as both a client and a server, and can share its own resources, such as files, printers, or internet connection, with other nodes. A peer-to-peer network allows users to directly access and exchange what is on or attached to their computers, with equal permissions and responsibilities

NEW QUESTION 206
- (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/

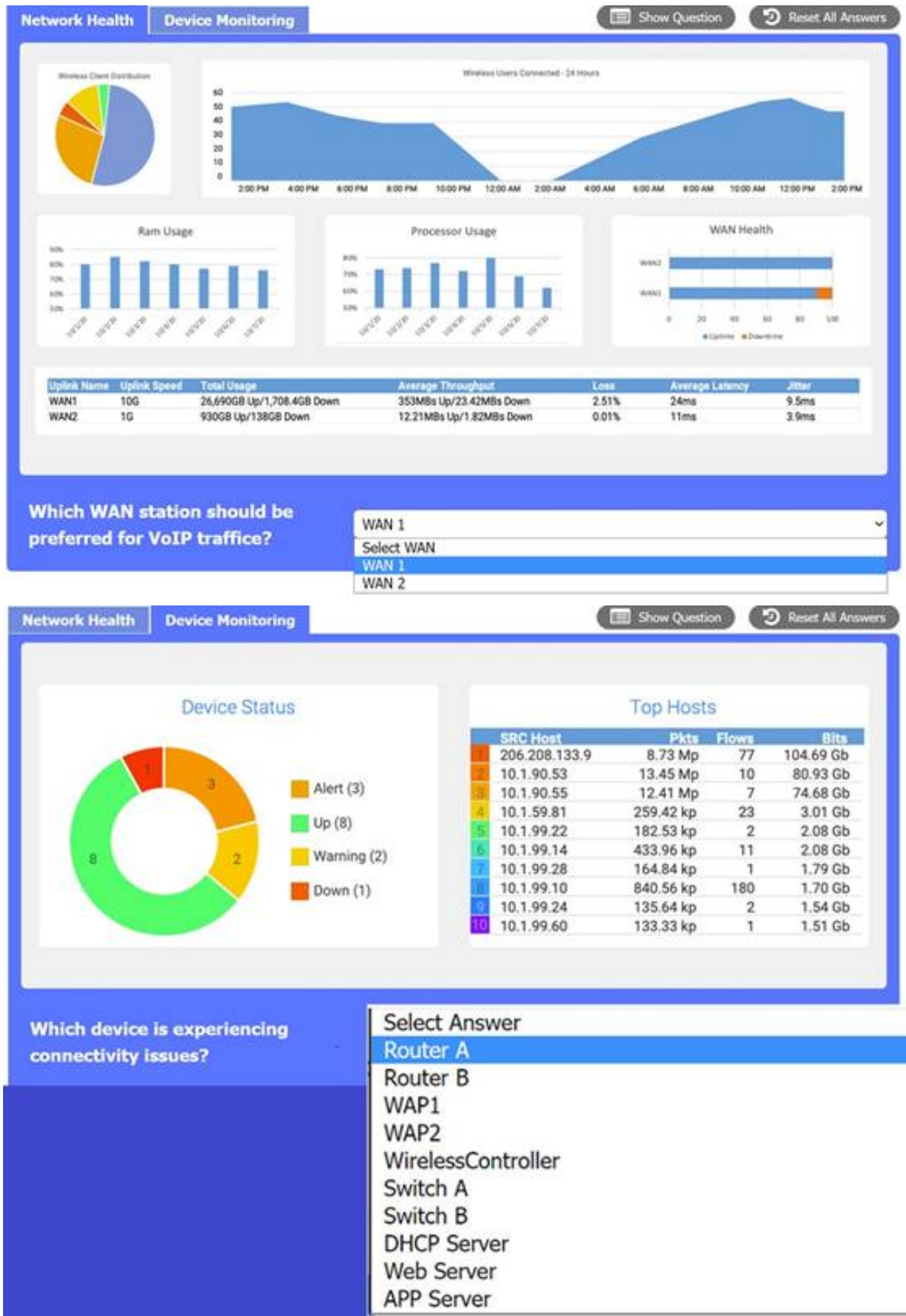
NEW QUESTION 211
- (Topic 3)
Which of the following situations would require an engineer to configure subinterfaces?

A. In a router-on-a-stick deployment with multiple VLANs
B. In order to enable inter-VLAN routing on a multilayer switch
C. When configuring VLAN trunk links between switches
D. After connecting a router that does not support 802.1Q VLAN tags

Answer: A

Explanation:
A router-on-a-stick is a configuration that allows a single router interface to route traffic between multiple VLANs on a network1. A router-on-a-stick requires sub-interfaces to be configured on the router interface, one for each VLAN. Each sub-interface is assigned a VLAN ID and an IP address that belongs to the corresponding VLAN subnet. The router interface is connected to a switch port that is configured as a trunk port, which allows traffic from multiple VLANs to pass through. The router then performs inter-VLAN routing by forwarding packets between the sub-interfaces based on their destination IP addresses. Inter-VLAN routing is a process that allows devices on different VLANs to communicate with each other. Inter-VLAN routing can be performed by a router-on-a-stick configuration, as explained above, or by a multilayer switch that has routing capabilities. A multilayer switch does not require sub-interfaces to be configured for inter-VLAN routing; instead, it uses switch virtual interfaces (SVIs) that are associated with each VLAN. An SVI is a logical interface that represents a VLAN on a switch and has an IP address that belongs to the VLAN subnet. The switch then performs inter-VLAN routing by forwarding packets between the SVIs based on their destination IP addresses.
VLAN trunking is a method that allows traffic from multiple VLANs to be carried over a single link between switches or routers. VLAN trunking requires the use of a tagging protocol, such as 802.1Q, that adds a header to each frame that identifies its VLAN ID. VLAN trunking does not require sub-interfaces to be configured on the switches or routers; instead, it uses trunk ports that are configured to allow or deny traffic from specific VLANs. The switches or routers then forward packets between the trunk ports based on their VLAN IDs.
* 802.1Q is a standard that defines how VLAN tagging and trunking are performed on Ethernet networks.
* 802.1Q adds a 4-byte header to each frame that contains a 12-bit field for the VLAN ID and a 3-bit field for the priority level. 802.1Q does not require sub-interfaces to be configured on the switches or routers; instead, it uses trunk ports that are configured to support 802.1Q tagging and untagging. The switches or routers then forward packets between the trunk ports based on their VLAN IDs and priority levels.

NEW QUESTION 216
SIMULATION - (Topic 3)
After a recent power outage, users are reporting performance issues accessing the application servers. Wireless users are also reporting intermittent Internet issues.
INSTRUCTIONS
Click on each tab at the top of the screen. Select a widget to view information, then
use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

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

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

A screenshot of a computer
Description automatically generated

NEW QUESTION 221
- (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 222
- (Topic 3)
An ISP is unable to provide services to a user in a remote area through cable and DSL. Which of the following is the NEXT best solution to provide services without adding external infrastructure?

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

Answer: C

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

NEW QUESTION 227
- (Topic 3)
Which of the following describes a network in which users and devices need to mutually authenticate before any network resource can be accessed?

A. Least privilege
B. Local authentication
C. Zero trust
D. Need to know

Answer: C

Explanation:
A zero trust network is a network in which users and devices need to mutually authenticate before any network resource can be accessed. A zero trust network assumes that no one and nothing can be trusted by default, even if they were previously verified or are within the network perimeter. A zero trust network uses various technologies and practices, such as data and log aggregation, cybersecurity analytics, continuous diagnostics and mitigation, user behavior analytics, microsegmentation, and identity and access management, to enforce granular and dynamic policies based on the context and behavior of the users and devices123.
References:
? What is Zero Trust? | Internet of Things | CompTIA3
? The Death of the Perimeter: Zero Trust is (Almost) Here to Stay | Cybersecurity | CompTIA2
? CompTIA Network+ Certification Exam N10-008 Practice Test 17 -
ExamCompass1

NEW QUESTION 230
- (Topic 3)
Which of the following steps of the troubleshooting methodology would most likely include checking through each level of the OSI model after the problem has been identified?

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

Answer: C

Explanation:
Creating a plan of action is the step of the troubleshooting methodology that would most likely include checking through each level of the OSI model after the problem has been identified. According to the web search results, the troubleshooting methodology consists of the following steps: 12
? Define the problem: Identify the symptoms and scope of the problem, and gather relevant information from users, devices, and logs.
? Establish a theory: Based on the information collected, hypothesize one or more possible causes of the problem, and rank them in order of probability.
? Test the theory: Test the most probable cause first, and if it is not confirmed, eliminate it and test the next one. Repeat this process until the root cause is found or a new theory is needed.
? Create a plan of action: Based on the confirmed cause, devise a solution that can resolve the problem with minimal impact and risk. The solution may involve checking through each level of the OSI model to ensure that all layers are functioning properly and that there are no configuration errors, physical damages, or logical inconsistencies34

? Implement the solution: Execute the plan of action, and monitor the results. If the problem is not solved, revert to the previous state and create a new plan of action.
? Verify functionality: Confirm that the problem is fully resolved and that the network is restored to normal operation. Perform preventive measures if possible to avoid recurrence of the problem.
? Document the findings: Record the problem description, the solution, and the outcome. Update any relevant documentation, such as network diagrams, policies, or procedures.
References1: Troubleshooting Methods for Cisco IP Networks 2: Troubleshooting Methodologies - CBT IT Certification Training 3: How to use the OSI Model to Troubleshoot Networks 4: How is the OSI model used in troubleshooting? – Sage-Answer

NEW QUESTION 232
- (Topic 3)
Which of the following describes when an active exploit is used to gain access to a network?

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

Answer: A

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

NEW QUESTION 235
- (Topic 3)
Which of the following is most likely responsible for the security and handling of personal data in Europe?

A. GDPR
B. SCADA
C. SAML
D. PCI DSS

Answer: A

Explanation:
GDPR stands for General Data Protection Regulation, which is a European Union
regulation on information privacy and security. It applies to any organization that collects or processes personal data of individuals in the EU, and it sets out rules and requirements for data protection, consent, breach notification, and enforcement1
References1: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

NEW QUESTION 238
- (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 242
- (Topic 3)
A network security administrator needs to monitor the contents of data sent between a secure network and the rest of the company. Which of the following monitoring methods will accomplish this task?

A. Port mirroring
B. Flow data
C. Syslog entries
D. SNMP traps

Answer: A

Explanation:
Port mirroring is a method of monitoring network traffic by copying the data packets from one port to another port on the same switch or router. This allows the network security administrator to analyze the contents of the data sent between different networks without affecting the performance or security of the original traffic. Port mirroring can be configured to capture all traffic or only specific types of traffic, such as VLANs, protocols, or IP addresses.
References:
? Port Mirroring - CompTIA Network+ N10-008 Domain 3.1 - YouTube1
? CompTIA Network+ Certification Exam Objectives, page 142

NEW QUESTION 244
- (Topic 3)
A network technician 13 troubleshooting a network issue for employees who have reported Issues with speed when accessing a server in another subnet. The server is in another building that is 410ft (125m) away from the employees' building. The 10GBASE-T connection between the two buildings uses Cat 5e. Which of the following BEST explains the speed issue?

A. The connection type is not rated for that distance
B. A broadcast storm is occurring on the subnet.
C. The cable run has interference on it
D. The connection should be made using a Cat 6 cable

Answer: D

Explanation:
The 10GBASE-T connection between the two buildings uses Cat 5e, which is not rated for a distance of 410ft (125m). According to the CompTIA Network+ Study Manual, for 10GBASE-T connections, "Cat 5e is rated for up to 55m, Cat 6a is rated for 100m, and Cat 7 is rated for 150m." Therefore, the speed issue is likely due to the fact that the connection type is not rated for the distance between the two buildings. To resolve the issue, the technician should consider using a Cat 6a or Cat 7 cable to increase the distance the connection is rated for.

NEW QUESTION 245
- (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 250
- (Topic 3)
A network technician receives a report about a performance issue on a client PC that is connected to port 1/3 on a network switch. The technician observes the following configuration output from the switch:

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

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

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

Answer: A

NEW QUESTION 253
- (Topic 3)
After a company installed a new IPS, the network is experiencing speed degradation. A network administrator is troubleshooting the issue and runs a speed test. The results from the different network locations are as follows:
Which of the following is the most likely issue?

A. Packet loss
B. Bottlenecking
C. Channel overlap
D. Network congestion

Answer: B

Explanation:
The most likely issue is bottlenecking. Bottlenecking occurs when a component or device limits the performance or capacity of the network. In this case, the IPS (intrusion prevention system) may be causing a bottleneck by inspecting and filtering the incoming and outgoing traffic, which reduces the speed and bandwidth available for the network devices12
To confirm this issue, the network administrator can compare the speed test results before and after installing the IPS, and check the IPS configuration and logs for any errors or warnings. The network administrator can also try to bypass the IPS temporarily and run the speed test again to see if there is any improvement3
If the IPS is indeed the cause of the bottleneck, the network administrator can try to optimize the IPS settings, such as adjusting the inspection rules, thresholds,

and priorities, to reduce the processing overhead and latency. Alternatively, the network administrator can upgrade the IPS hardware or software, or add more IPS devices to balance the load and increase the throughput45
1: What is Network Congestion? Common Causes and How to Fix Them? -
GeeksforGeeks 2: Network congestion - Wikipedia 3: How to Fix Packet Loss - Lifewire 4: How to Optimize Your IPS Performance - Cisco 5: How to Avoid Network Bottlenecks - TechRepublic

NEW QUESTION 255
- (Topic 3)
Which of the following fouling protocols is generally used by major ISPs for handing large- scale internet traffic?

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

Answer: D

NEW QUESTION 256
- (Topic 3)
A large metropolitan city is looking to standardize the ability tor police department laptops to connect to the city government's VPN The city would like a wireless solution that provides the largest coverage across the city with a minimal number of transmission towers Latency and overall bandwidth needs are not high priorities. Which of the following would BEST meet the city's needs?

A. 5G
B. LTE
C. Wi-Fi 4
D. Wi-Fi 5
E. Wi-Fi 6

Answer: B

NEW QUESTION 259
- (Topic 3)
A PC user who is on a local network reports very slow speeds when accessing files on the network server The user's PC Is connecting, but file downloads are very slow when compared to other users' download speeds The PC's NIC should be capable of Gigabit Ethernet. Which of the following will MOST likely fix the issue?

A. Releasing and renewing the PC's IP address
B. Replacing the patch cable
C. Reseating the NIC inside the PC
D. Flushing the DNS cache

Answer: B

Explanation:
A slow download speed can be caused by a faulty patch cable, which is the cable used to connect the user's PC to the network server. If the patch cable is damaged, the connection will be slower than expected, resulting in slow download speeds. Replacing the patch cable is the most likely solution to this issue, as it will provide a new, reliable connection that should allow for faster download speeds.

NEW QUESTION 260
- (Topic 3)
A customer has an attached USB printer that needs to be shared with other users. The desktop team set up printer sharing. Now, the network technician needs to obtain the necessary information about the PC and share it with other users so they can connect to the printer. Which of the following commands should the technician use to get the required information? (Select TWO).

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

Answer: EF

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

NEW QUESTION 261
- (Topic 3)
An AP uses a 98ft (30m) Cat 6 cable to connect to an access switch. The cable is wired through a duct close to a three-phase motor installation. Anytime the three-phase is turned on, all users connected to the switch experience high latency on the network. Which Of the following is MOST likely the cause Of the issue?

A. Interference
B. Attenuation
C. Open circuit

D. Short circuit

Answer: A

Explanation:
Interference is a phenomenon that occurs when unwanted signals or noise affect the transmission or reception of data signals on a network. Interference can cause network issues such as high latency, low throughput, packet loss, or errors. Interference can be caused by various sources, such as electromagnetic fields, radio waves, power lines, or electrical devices. In this scenario, the three-phase motor installation is a source of interference that affects the Cat 6 cable that connects the AP to the access switch. The cable is wired through a duct close to the motor installation, which exposes it to the electromagnetic fields generated by the motor. Anytime the motor is turned on, the interference causes high latency for all users connected to the switch.

NEW QUESTION 266
- (Topic 3)
A user reports that a crucial fileshare is unreachable following a network upgrade that was completed the night before. A network technician confirms the problem exists. Which of the following
troubleshooting Steps should the network technician perform NEXT?

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

Answer: A

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

NEW QUESTION 267
- (Topic 3)
A company realizes that only half of its employees work in the office, and the employees who work from home no longer need a computer at the office. Which of the following security measures should the network administrator implement when removing a computer from a cubicle?

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

Answer: D

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

NEW QUESTION 272
- (Topic 3)
A junior network engineer is trying to change the native network ID to a non-default value that can then be applied consistently throughout the network environment. Which of the following
issues is the engineer attempting to prevent?

A. DDoS
B. ARP spoofing
C. VLAN hopping
D. Rogue DHCP

Answer: C

Explanation:

VLAN hopping is a type of network attack where an attacker can send or receive traffic from a VLAN that they are not supposed to access. VLAN hopping can allow an attacker to bypass security policies, access sensitive data, or launch other attacks on the network. VLAN hopping can be performed using two methods: double tagging and switch spoofing1.
Double tagging is where the attacker sends a frame with two VLAN tags, one for the native VLAN and one for the target VLAN. The native VLAN is the VLAN that is used for untagged traffic on a trunk port. If the attacker's access port is in the same VLAN as the native VLAN, the switch will accept the frame and forward it on the trunk port. The switch will remove the first tag, which is the native VLAN, and send the frame with the second tag, which is the target VLAN. The frame will then reach the target VLAN and be processed by the devices in that VLAN.
Switch spoofing is where the attacker sends Dynamic Trunking Protocol (DTP) packets and tries to negotiate a trunk with the switch. DTP is a Cisco protocol that allows switches to automatically form trunks between them. If the switch's port is configured with the default dynamic auto or dynamic desirable mode, it will accept the DTP packets and form a trunk with the attacker. The attacker will then have access to all VLANs on the trunk.
To prevent VLAN hopping, the junior network engineer is trying to change the native network ID to a non-default value that can then be applied consistently throughout the network environment. This means that the engineer is changing the VLAN that is used for untagged traffic on the trunk ports to a different VLAN than the default VLAN 1. This will prevent double tagging attacks, as the attacker's access port will not be in the same VLAN as the native VLAN, and the switch will not accept the frames with two tags. The engineer should also disable DTP on the trunk ports and use the switchport nonegotiate command to prevent switch spoofing attacks2.
ReferencesVLAN Hopping - NetworkLessons.comVLAN Hopping on Native VLAN - Cisco Community

NEW QUESTION 277
- (Topic 3)
Users report they cannot reach any websites on the internet. An on-site network engineer is able to duplicate the issue on a different PC. The network engineer then tries to ping a website and receives the following message:
Ping request could not find host www.google.com. Please check the name and try again. Which of the following is the next step the engineer should take?
A. Ping 127. 0. 0. 1 to test local hardware.
B. Test the website from outside the company.
C. Ping internal name server functionality.
D. Check internet firewall logs for blocked DNS traffi

Answer: C

Explanation:

The error message "Ping request could not find host www.google.com" indicates that the network engineer's PC cannot resolve the hostname www.google.com to its corresponding IP address. This means that there is a problem with the DNS (Domain Name System) service, which is responsible for translating hostnames to IP addresses and vice versa. The DNS service can be provided by internal or external name servers, depending on the network configuration.
The next step the engineer should take is to ping the internal name server functionality, which means to test if the PC can communicate with the name server that is configured in its network settings, and if the name server can resolve internal hostnames, such as those of the company's servers or devices. To do this, the engineer can use the following commands:
? To find out the IP address of the name server, use ipconfig /all and look for the DNS Servers entry.
? To ping the name server, use ping <name server IP address> and check if the packets are sent and received successfully.
? To test the name resolution, use nslookup <internal hostname> and check if the name server returns the correct IP address.
If the ping or the nslookup commands fail, it means that the internal name server is not working properly, and the engineer should troubleshoot the name server configuration or connectivity. If the ping and the nslookup commands succeed, it means that the internal name server is working properly, but there is a problem with the external name resolution, and the engineer should check the internet firewall logs for blocked DNS traffic, or test the website from outside the company.
ReferencesWindows 10 can't resolve hostnames - ping with IP works but not with hostnamePing request could not find host xyz.local. Please check the name and try againDNS problem, nslookup works, ping doesn't Users are connected to a switch on an Ethernet interface of a campus router. The service provider is connected to the serial 1 interface on the router. The output of the interfaces is:
E1/0: 192.168.8.1/24 S1: 192.168.7.252/30

NEW QUESTION 278
- (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 282

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

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

Answer: A

Explanation:

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

NEW QUESTION 284
- (Topic 3)
An administrator needs to ensure an access switch is sending the appropriate logs to the network monitoring server. Which of the following logging levels is most appropriate for the access layer switch?

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

Answer: C

Explanation:

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

NEW QUESTION 288
- (Topic 3)
A network engineer has added a new route on a border router and is trying to determine if traffic is using the new route. Which of the following commands should the engineer use?

A. ping
B. arp
C. tracert
D. route

Answer: C

Explanation:

The tracert command is a network diagnostic tool that traces the route of packets from the source host to the destination host. It displays the IP addresses and hostnames of the routers along the path, as well as the time taken for each hop. The tracert command can be used to determine if traffic is using the new route by comparing the output before and after adding the route. If the new route is effective, the tracert command should show a different or shorter path to the destination host.
ReferencesNetworking Commands For Troubleshooting Windows - GeeksforGeeksNine Switch Commands Every Cisco Network Engineer Needs to Know

NEW QUESTION 290
- (Topic 3)
Which of the following passwords would provide the best defense against a brute-force attack?

A. ThislsMyPasswordForWork
B. Qwerty!@#$
C. Password! 1
D. T5!8j5

Answer: D

Explanation:

A brute-force attack is a method of guessing passwords by trying every possible combination of characters until the correct one is found. The longer and more complex the password, the harder it is to crack by brute-force. A password that provides the best defense against a brute-force attack should have a combination of uppercase and lowercase letters, numbers, and special characters, and should be as long as possible. The password T5!8j5 meets these criteria, while the other options are either too short, too simple, or too common.
References:
? Password Attacks – N10-008 CompTIA Network+ : 4.21
? CompTIA Network+ Cert Guide: Security Concepts and Tools, page 25 https://www.pearsonitcertification.com/articles/article.aspx?p=3021579&seqNum=2

NEW QUESTION 293
- (Topic 3)
Which of the following ports should a network administrator enable for encrypted log-in to a network switch?

A. 22
B. 23
C. 80
D. 123

Answer: A

Explanation:
Port 22 is used by Secure Shell (SSH), which is a protocol that provides a secure and encrypted method for remote access to hosts by using public-key cryptography and challenge-response authentication. SSH can be used to log in to a network switch and configure it without exposing the credentials or commands to eavesdropping or tampering. Port 23 is used by Telnet, which is an insecure and plaintext protocol for remote access. Port 80 is used by HTTP, which is a protocol for web communication. Port 123 is used by NTP, which is a protocol for time synchronization

NEW QUESTION 297
- (Topic 3)
A medical building offers patients Wi-Fi in the waiting room. Which of the following security
features would be the BEST solution to provide secure connections and keep the medical data protected?

A. Isolating the guest network
B. Securing SNMP
C. MAC filtering
D. Disabling unneeded switchports

Answer: A

NEW QUESTION 299
- (Topic 3)
A network administrator is deploying a new switch and wants to make sure that the default priority value was set for a spanning tree. Which of the following values would the network administrator expect to see?

A. 4096
B. 8192
C. 32768
D. 36684

Answer: C

Explanation:
The default priority value for spanning tree is 32768, regardless of the STP version (legacy STP, RSTP, MSTP, Per-VLAN STP, Per-VLAN RSTP). This value can be modified by the network administrator to influence the root bridge election. The priority value must be set in increments of 4096, which is the minimum unit of change for the priority value. https://community.cisco.com/t5/switching/spanning-tree-default-priorities/td-p/3304365

NEW QUESTION 300
- (Topic 3)
A technician is installing the Wi-Fi infrastructure for legacy industrial machinery at a warehouse. The equipment only supports 802.11a and 802.11b standards. Speed of transmission is the top business requirement. Which of the following is the correct maximum speed for this scenario?

A. 11Mbps
B. 54Mbps
C. 128Mbps
D. 144Mbps

Answer: B

Explanation:
802.11b (Wi-Fi 1) 11 Mbps
100 meter maximum effective range 802.11a (Wi-Fi 2)
54 Mbps
50 meter maximum effective range

NEW QUESTION 303
- (Topic 3)
A technician needs to configure a routing protocol for an internet-facing edge router. Which of the following routing protocols will the technician MOST likely use?

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

Answer: A

NEW QUESTION 306
- (Topic 3)
An international company is transferring its IT assets including a number of WAPs from the United States to an office in Europe for deployment. Which of the following considerations should the company research before Implementing the wireless hardware?

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

Answer: B

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

NEW QUESTION 309
- (Topic 3)
A company is utilizing multifactor authentication for data center access. Which of the following is the MOST effective security mechanism against physical intrusions due to stolen credentials?

A. Biometrics security hardware
B. Access card readers
C. Access control vestibule
D. Motion detection cameras

Answer: C

NEW QUESTION 311
- (Topic 3)
A customer needs to distribute Ethernet to multiple computers in an office. The customer would like to use non-proprietary standards. Which of the following blocks does the technician need to install?
? 110
? 66

A. BiX
B. Krone

Answer: A

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

NEW QUESTION 313
- (Topic 3)
A network administrator is reviewing north-south traffic to determine whether a security threat exists. Which of the following explains the type of traffic the administrator is reviewing?

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

Answer: C

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

NEW QUESTION 315
- (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 317
.....

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/