CompTIA

Exam Questions N10-009

CompTIA Network+ Exam

NEW QUESTION 1
- (Exam Topic 1)
Which of the following devices would be used to manage a corporate WLAN?

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

Answer: D

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

NEW QUESTION 2
- (Exam Topic 1)
Which of the following would be BEST to use to detect a MAC spoofing attack?

A. Internet Control Message Protocol
B. Reverse Address Resolution Protocol
C. Dynamic Host Configuration Protocol
D. Internet Message Access Protocol

Answer: B

Explanation:
Reverse Address Resolution Protocol (RARP) is a protocol that allows a device to obtain its MAC address from its IP address. A MAC spoofing attack is an attack where a device pretends to have a different MAC address than its actual one. RARP can be used to detect a MAC spoofing attack by comparing the MAC address obtained from RARP with the MAC address obtained from other sources, such as ARP or DHCP. References:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.techopedia.com/definition/25597/reverse-address-resolution-protocol-rarp

NEW QUESTION 3
- (Exam Topic 1)
A technician is writing documentation regarding a company's server farm. The technician needs to confirm the server name for all Linux servers. Which of the following commands should the technician run?

A. ipconfig
B. nslookup
C. arp
D. route

Answer: B

Explanation:
The nslookup command should be run to confirm the server name for all Linux servers. Nslookup is a tool that queries DNS servers to resolve hostnames to IP addresses or vice versa. It can also provide other information about DNS records, such as MX, NS, SOA, etc. By running nslookup with the IP address of a Linux server, the technician can obtain its hostname. References:
https://www.howtogeek.com/663056/how-to-use-the-nslookup-command-on-linux/

NEW QUESTION 4
- (Exam Topic 1)
A technician is installing a new fiber connection to a network device in a datacenter. The connection from the device to the switch also traverses a patch panel connection. The chain of connections is in the following order:
Device
LC/LC patch cable Patch panel
Cross-connect fiber cable Patch panel
LC/LC patch cable Switch
The connection is not working. The technician has changed both patch cables with known working patch cables. The device had been tested and was working properly before being installed. Which of the following is the MOST likely cause of the issue?

A. TX/RX is reversed
B. An incorrect cable was used
C. The device failed during installation
D. Attenuation is occurring

Answer: A

Explanation:
The most likely cause of the issue where the fiber connection from a device to a switch is not working is that the TX/RX (transmit/receive) is reversed. When connecting fiber optic cables, it is important to ensure that the TX of one device is connected to the RX of the other device and vice versa. If the TX/RX is reversed, data cannot be transmitted successfully.
References:
CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 5: Network Operations, Objective 5.1: Given a scenario, use appropriate documentation and diagrams to manage the network.

NEW QUESTION 5
- (Exam Topic 1)
A technician is configuring a network switch to be used in a publicly accessible location. Which of the following should the technician configure on the switch to prevent unintended connections?

A. DHCP snooping
B. Geofencing
C. Port security
D. Secure SNMP

Answer: C

Explanation:
Port security is a feature that restricts input to a switch port by limiting and identifying MAC addresses of the devices allowed to access the port. This prevents unintended connections from unauthorized devices or spoofed MAC addresses. Port security can also be configured to take actions such as shutting down the port or sending an alert when a violation occurs. References:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0),
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-10/configuration_guide/se

NEW QUESTION 6
- (Exam Topic 1)
Which of the following transceiver types can support up to 40Gbps?

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

Answer: B

Explanation:
QSFP+ is a transceiver type that can support up to 40Gbps. It stands for Quad Small Form-factor Pluggable Plus and uses four lanes of data to achieve high-speed transmission. It is commonly used for data center and high-performance computing applications. References:
https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/data_sheet_c78-6600

NEW QUESTION 7
- (Exam Topic 1)
A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds that jitter at the office is greater than 10ms on the only WAN connection available. Which of the following would be MOST affected by this statistic?

A. A VoIP sales call with a customer
B. An in-office video call with a coworker
C. Routing table from the ISP
D. Firewall CPU processing time

Answer: A

Explanation:
A VoIP sales call with a customer would be most affected by jitter greater than 10ms on the WAN connection. Jitter is the variation in delay of packets arriving at the destination. It can cause choppy or distorted audio quality for VoIP applications, especially over WAN links that have limited bandwidth and high latency. The recommended jitter for VoIP is less than 10ms. References: https://www.voip-info.org/voip-jitter/

NEW QUESTION 8
- (Exam Topic 1)
A technician is installing a cable modem in a SOHO. Which of the following cable types will the technician MOST likely use to connect a modem to the ISP?

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

Answer: A

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

NEW QUESTION 9
- (Exam Topic 1)
According to troubleshooting methodology, which of the following should the technician do NEXT after determining the most likely probable cause of an issue?

A. Establish a plan of action to resolve the issue and identify potential effects
B. Verify full system functionality and, if applicable, implement preventive measures
C. Implement the solution or escalate as necessary
D. Test the theory to determine the cause

Answer: A

Explanation:
According to troubleshooting methodology, after determining the most likely probable cause of an issue, the next step is to establish a plan of action to resolve the issue and identify potential effects. This step involves defining the steps needed to implement a solution, considering the possible consequences of each step, and obtaining approval from relevant stakeholders if necessary. References: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.comptia.org/blog/the-comptia-guide-to-it-troubleshooting

NEW QUESTION 10
- (Exam Topic 1)
Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

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

Answer: B

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

NEW QUESTION 10
- (Exam Topic 1)
A network technician is reviewing the interface counters on a router interface. The technician is attempting to confirm a cable issue. Given the following information:

Metric	Value
Last cleared	7 minutes, 34 seconds
# of packets output	6915
# of packets input	270
CRCs	183
Giants	0
Runts	0
Multicasts	14

Which of the following metrics confirms there is a cabling issue?

A. Last cleared
B. Number of packets output
C. CRCs
D. Giants
E. Multicasts

Answer: C

Explanation:
CRC stands for Cyclic Redundancy Check, and it is a type of error-detecting code used to detect accidental changes to raw data. If the CRC count is increasing on a particular interface, it indicates that there might be an issue with the cabling, which is causing data corruption. References:
Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

NEW QUESTION 14
- (Exam Topic 1)
A company hired a technician to find all the devices connected within a network. Which of the following software tools would BEST assist the technician in completing this task?

A. IP scanner
B. Terminal emulator
C. NetFlow analyzer
D. Port scanner

Answer: A

Explanation:
To find all devices connected within a network, a technician can use an IP scanner. An IP scanner sends a ping request to all IP addresses within a specified range and then identifies the active devices that respond to the request.

NEW QUESTION 19
- (Exam Topic 1)
A network is experiencing a number of CRC errors during normal network communication. At which of the following layers of the OSI model will the administrator MOST likely start to troubleshoot?

A. Layer 1
B. Layer 2

C. Layer 3
D. Layer 4
E. Layer 5
F. Layer 6
G. Layer 7

Answer: A

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

NEW QUESTION 21
- (Exam Topic 1)
Which of the following is the physical topology for an Ethernet LAN?

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

Answer: D

Explanation:
In a star topology, all devices on a network connect to a central hub or switch, which acts as a common connection point. Ethernet LANs typically use a star topology, with each device connected to a central switch. References:
Network+ N10-008 Objectives: 2.2 Explain common logical network topologies and their characteristics.

NEW QUESTION 22
- (Exam Topic 1)
Which of the following provides redundancy on a file server to ensure the server is still connected to a LAN even in the event of a port failure on a switch?

A. NIC teaming
B. Load balancer
C. RAID array
D. PDUs

Answer: A

Explanation:
NIC teaming, also known as network interface card teaming or link aggregation, allows multiple network interface cards to be grouped together to provide redundancy and increased throughput. In the event of a port failure on a switch, NIC teaming ensures that the file server remains connected to the LAN by automatically switching to another network interface card.
References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

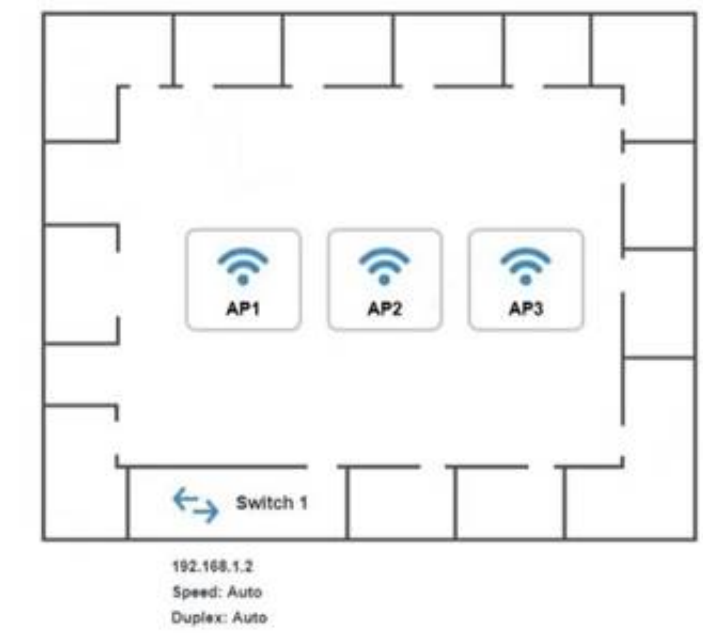
NEW QUESTION 25
- (Exam Topic 1)
A website administrator is concerned the company's static website could be defaced by hacktivists or used as a pivot point to attack internal systems. Which of the following should a network security administrator recommend to assist with detecting these activities?

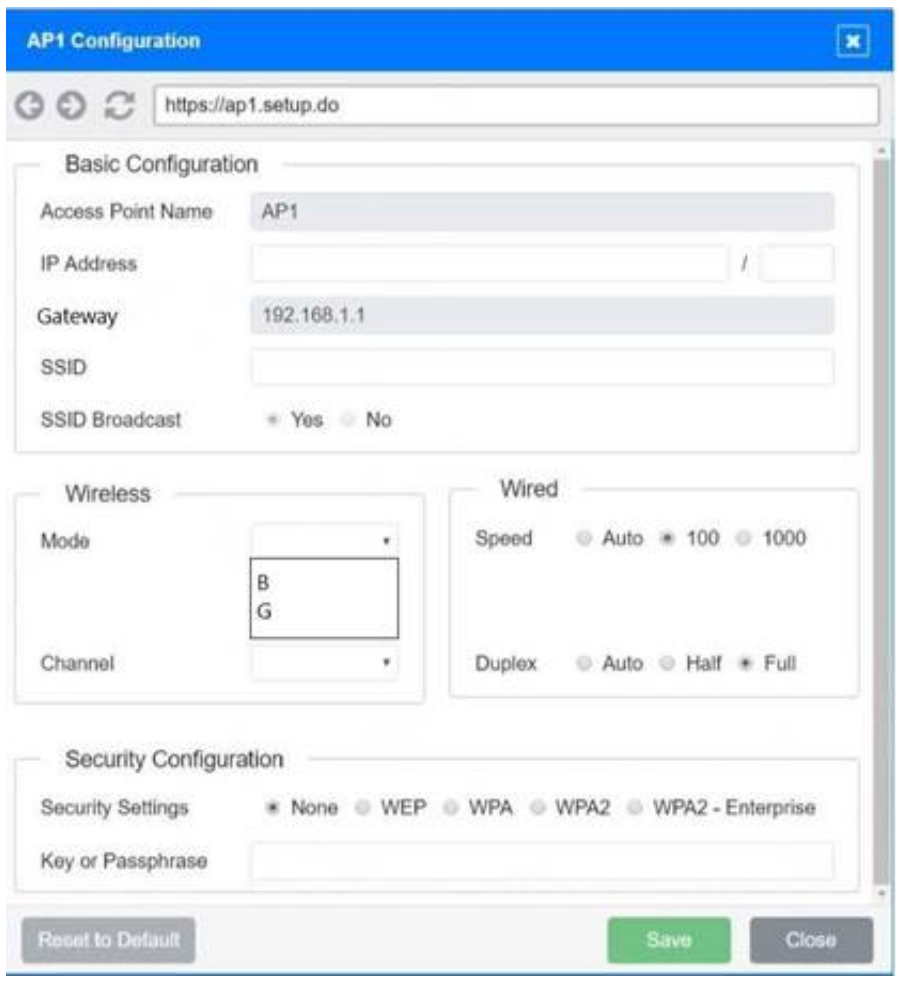
A. Implement file integrity monitoring.
B. Change the default credentials.
C. Use SSL encryption.
D. Update the web-server software.

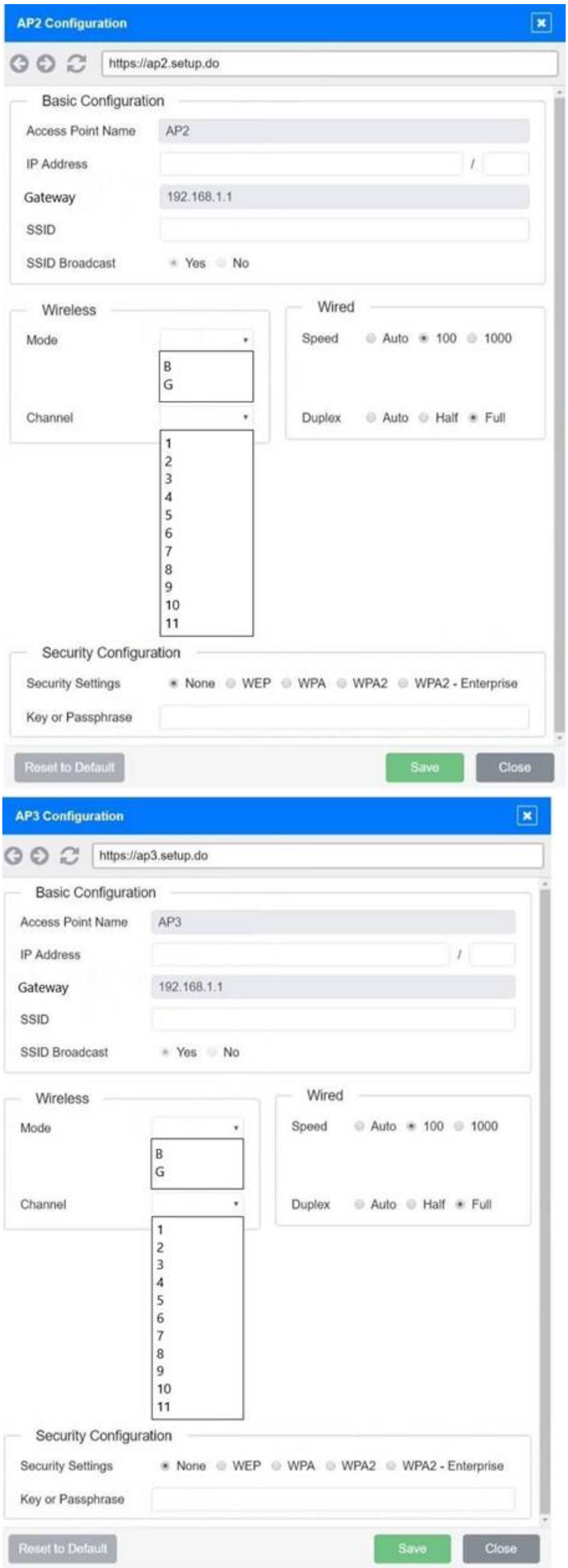
Answer: A

Explanation:
Implementing file integrity monitoring (FIM) would assist with detecting activities such as website defacement or internal system attacks. FIM is a process that monitors and alerts on changes to files or directories that are critical for security or functionality. FIM can help detect unauthorized modifications, malware infections, data breaches, or configuration errors. FIM can also help with compliance and auditing requirements. References:
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/what-is-file-integrity-monitor

NEW QUESTION 30
- (Exam Topic 1)
SIMULATION
You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:
The SSIDs need to be configured as CorpNet with a key of S3cr3t! The wireless signals should not interfere with each other
The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTONS
Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


AP1
AP2
AP3
Switch 1
192.168.1.2
Speed: Auto
Duplex: Auto

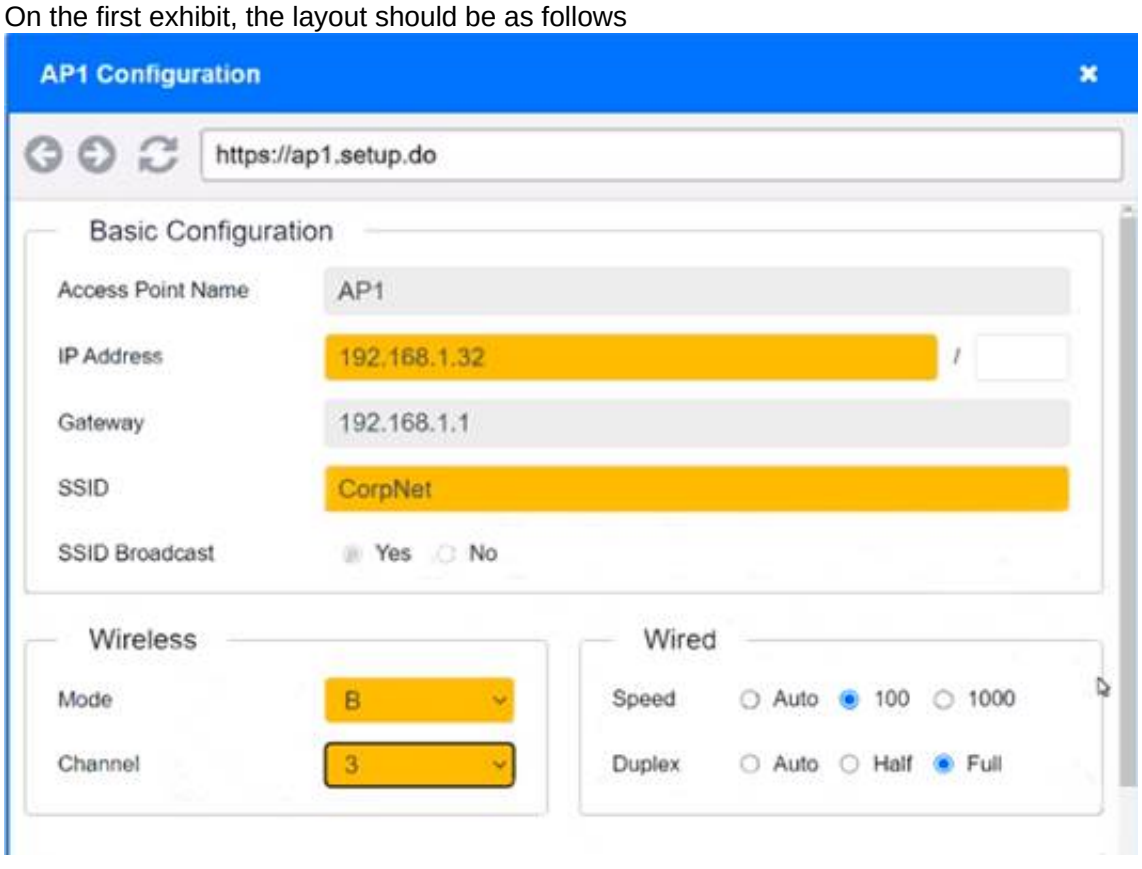

AP1 Configuration
https://ap1.setup.do
Basic Configuration
Access Point Name
AP1
IP Address
Gateway
192.168.1.1
SSID
SSID Broadcast
Yes
No
Wireless
Mode
B
G
Channel
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase
Reset to Default
Save
Close



A. Mastered
B. Not Mastered

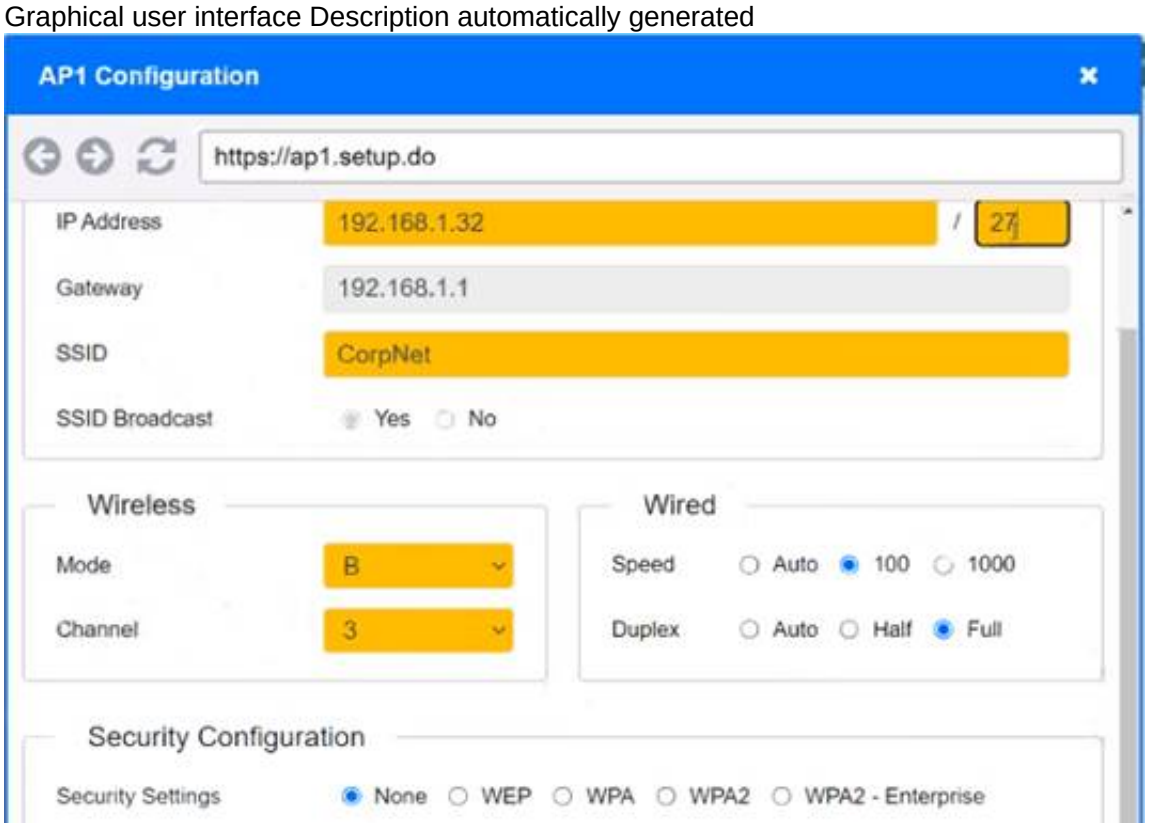
Answer: A

Explanation:
On the first exhibit, the layout should be as follows



Graphical user interface, text, application, chat or text message Description automatically generated

Graphical user interface Description automatically generated



Graphical user interface, text, application, chat or text message Description automatically generated

Graphical user interface Description automatically generated

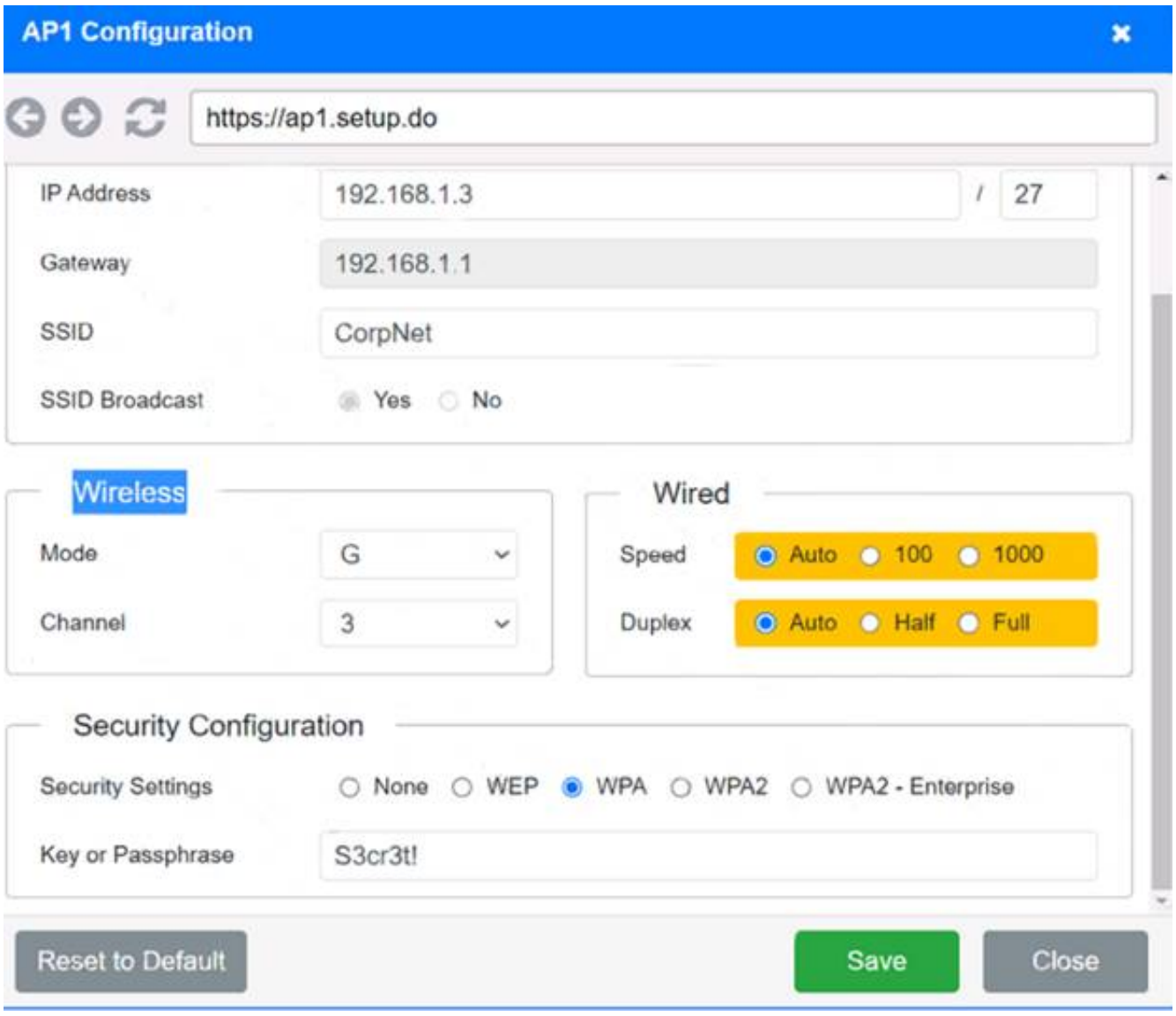
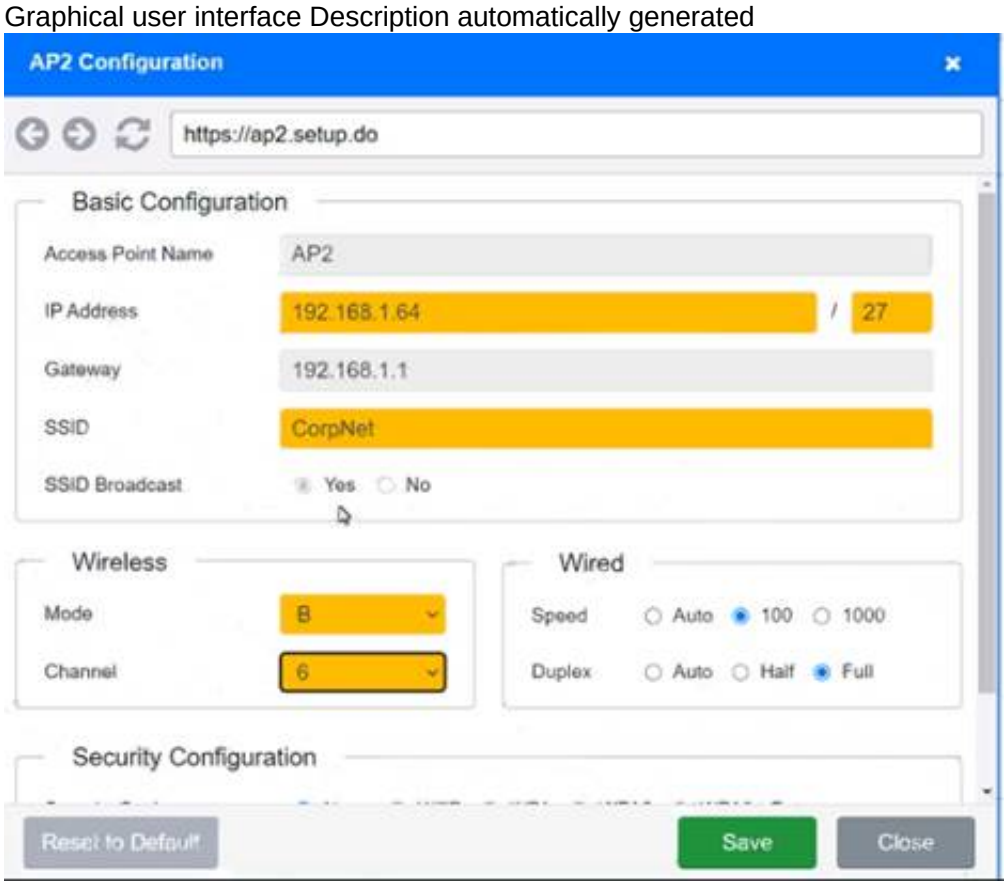


Exhibit 2 as follows Access Point Name AP2
Graphical user interface Description automatically generated



Graphical user interface, text, application, chat or text message Description automatically generated

Graphical user interface Description automatically generated

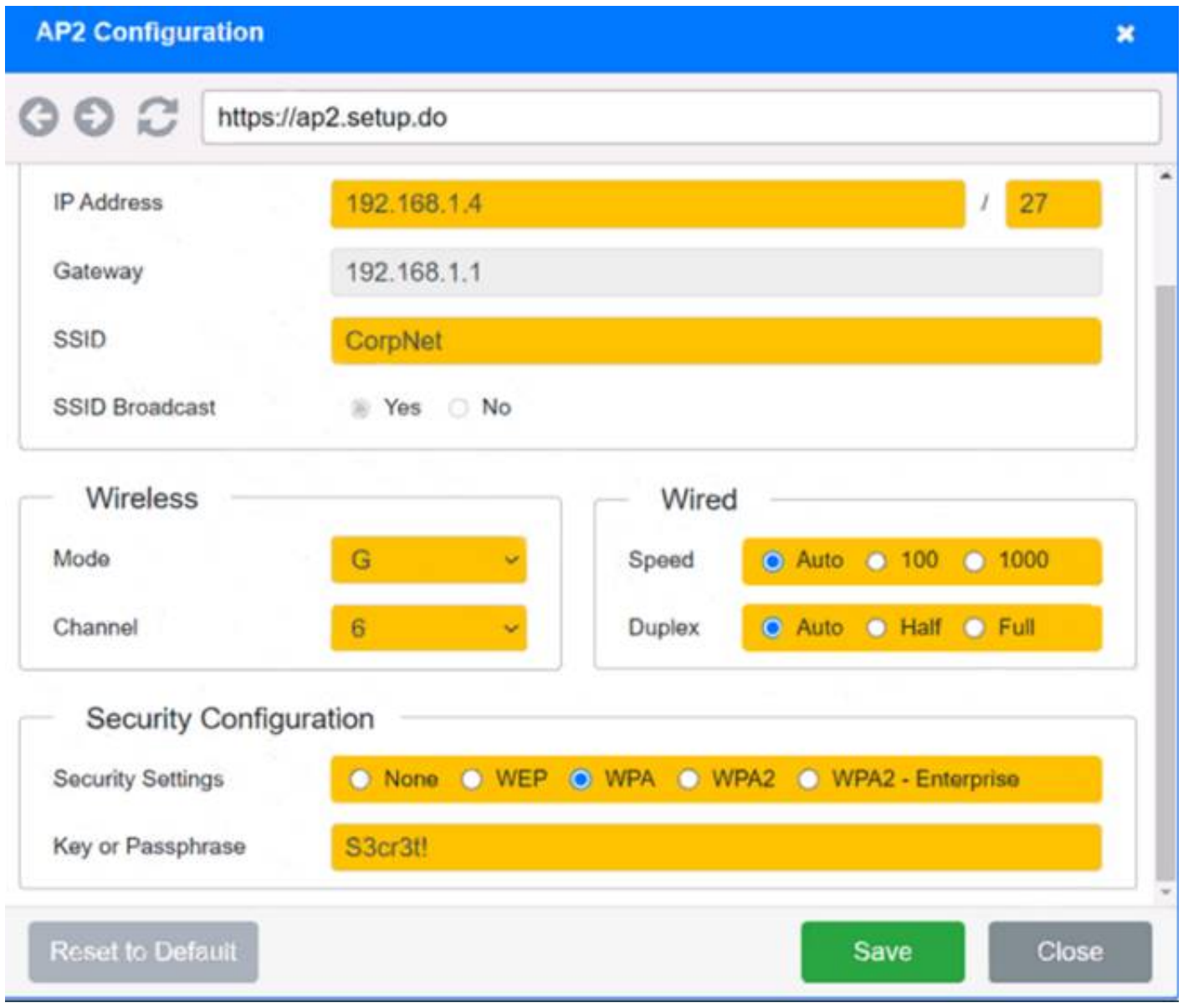
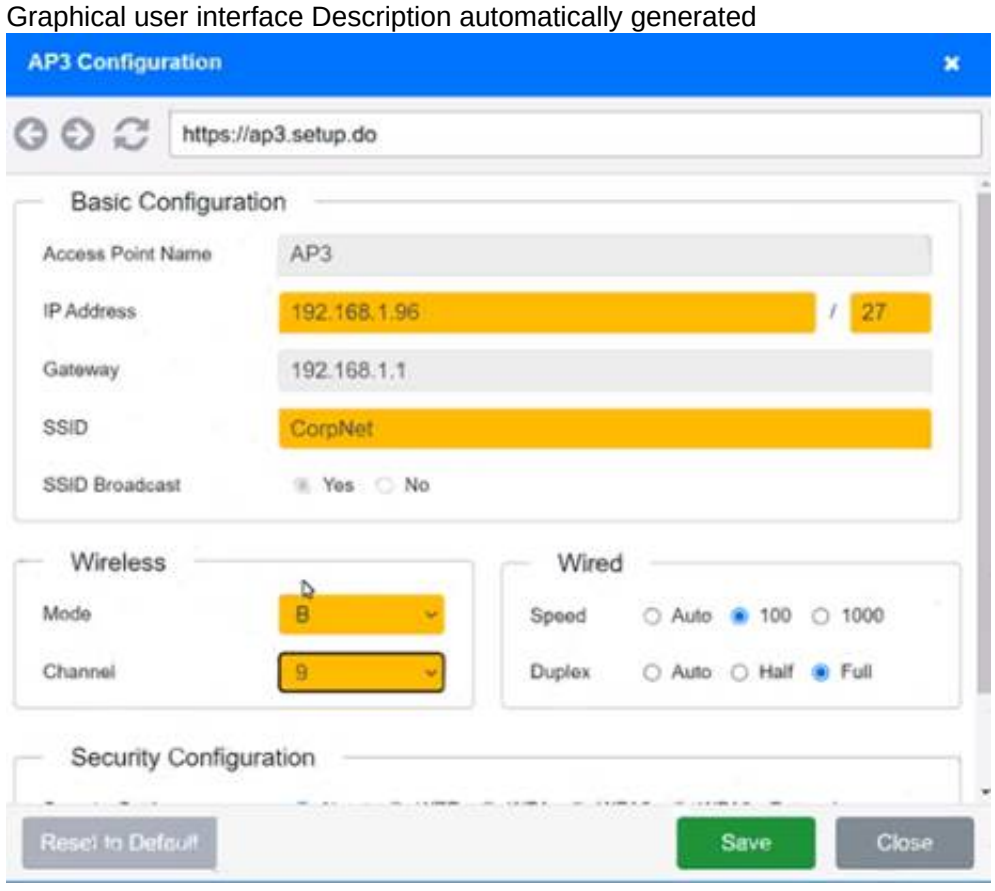
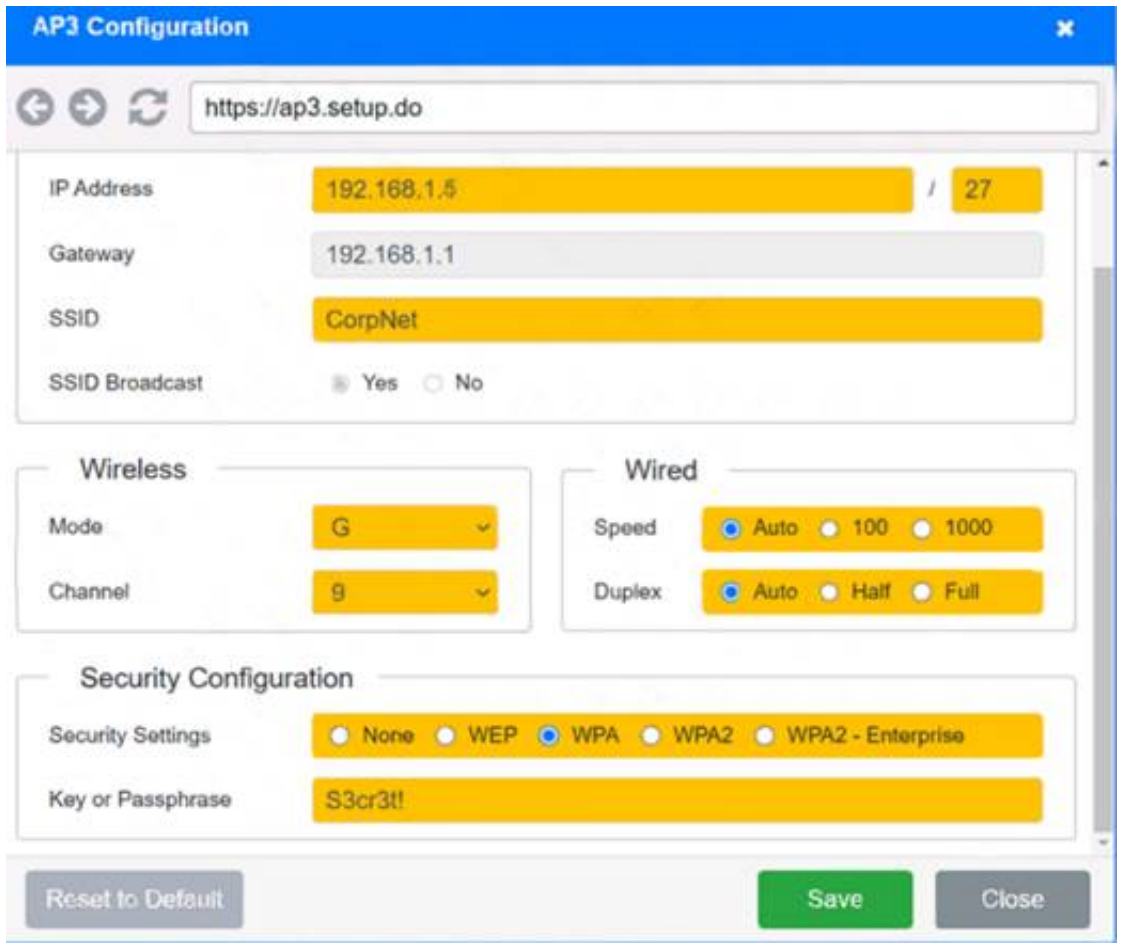


Exhibit 3 as follows Access Point Name AP3
Graphical user interface Description automatically generated



Graphical user interface, text, application, chat or text message Description automatically generated

Graphical user interface Description automatically generated



NEW QUESTION 31
- (Exam Topic 1)
A network administrator walks into a datacenter and notices an unknown person is following closely. The administrator stops and directs the person to the security desk. Which of the following attacks did the network administrator prevent?

A. Evil twin
B. Tailgating
C. Piggybacking
D. Shoulder surfing

Answer: B

Explanation:
:
Tailgating is a physical security attack where an unauthorized person follows an authorized person into a restricted area without proper identification or authorization. The network administrator prevented this attack by stopping and directing the person to the security desk. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 3.0 Network Security, Objective 3.1 Compare and contrast risk-related concepts.

NEW QUESTION 35
- (Exam Topic 1)
A user reports being unable to access network resources after making some changes in the office. Which of the following should a network technician do FIRST?

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

Answer: D

Explanation:
When a user reports being unable to access network resources after making some changes, the network technician should first ask the user what changes were made. This information can help the technician identify the cause of the issue and determine the appropriate course of action.
References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 37
- (Exam Topic 1)
Client devices cannot enter a network, and the network administrator determines the DHCP scope is exhausted. The administrator wants to avoid creating a new DHCP pool. Which of the following can the administrator perform to resolve the issue?

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

Answer: D

Explanation:
To resolve the issue of DHCP scope exhaustion without creating a new DHCP pool, the administrator can reduce the lease time. By decreasing the lease time, the IP addresses assigned by DHCP will be released back to the DHCP scope more quickly, allowing them to be assigned to new devices.
References:
- CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a

scenario, implement and configure the appropriate addressing schema.
- https://www.networkcomputing.com/data-centers/10-tips-optimizing-dhcp-performance

NEW QUESTION 41
- (Exam Topic 1)
Which of the following is MOST likely to generate significant East-West traffic in a datacenter?

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

Answer: B

Explanation:
East-West traffic refers to data flows between servers or devices within the same datacenter. When a hosted virtual server is duplicated to another physical server for redundancy, it generates significant East-West traffic as the data is replicated between the two servers. References:
- Network+ N10-008 Objectives: 3.3 Given a scenario, implement secure network architecture concepts.

NEW QUESTION 46
- (Exam Topic 1)
A branch of a company recently switched to a new ISP. The network engineer was given a new IP range to assign. The ISP assigned 196.26.4.0/26, and the branch gateway router now has the following configurations on the interface that peers to the ISP:

```
IP address:          196.26.4.30
Subnet mask:         255.255.255.224
Gateway:             196.24.4.1
```

The network engineer observes that all users have lost Internet connectivity. Which of the following describes the issue?

A. The incorrect subnet mask was configured
B. The incorrect gateway was configured
C. The incorrect IP address was configured
D. The incorrect interface was configured

Answer: C

Explanation:
The IP address configured on the router interface is 196.26.4.1/26, which belongs to the IP range assigned by the ISP (196.26.4.0/26). However, this IP address is not valid for this interface because it is the network address of the subnet, which cannot be assigned to any host device. The network address is the first address of a subnet that identifies the subnet itself. The valid IP addresses for this subnet are from 196.26.4.1 to 196.26.4.62, excluding the network address (196.26.4.0) and the broadcast address (196.26.4.63). The router interface should be configured with a valid IP address within this range to restore Internet connectivity for all users. References:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.techopedia.com/definition/24136/network-address

NEW QUESTION 51
- (Exam Topic 2)
A network technician was troubleshooting an issue for a user who was being directed to cloned websites that were stealing credentials. The URLs were correct for the websites but an incorrect IP address was revealed when the technician used ping on the user's PC After checking the is setting, the technician found the DNS server address was incorrect Which of the following describes the issue?

A. Rogue DHCP server
B. Misconfigured HSRP
C. DNS poisoning
D. Exhausted IP scope

Answer: C

Explanation:
DNS poisoning is a type of attack that modifies the DNS records of a domain name to point to a malicious IP address instead of the legitimate one. This can result in users being directed to cloned websites that are stealing credentials, even if they enter the correct URL for the website. The incorrect DNS server address on the user’s PC could be a sign of DNS poisoning, as the attacker could have compromised the DNS server or spoofed its response to redirect the user’s queries. References: https://www.comptia.org/blog/what-is-dns-poisoning

NEW QUESTION 56
- (Exam Topic 2)
A technician is troubleshooting a previously encountered issue. Which of the following should the technician reference to find what solution was implemented to resolve the issue?

A. Standard operating procedures
B. Configuration baseline documents
C. Work instructions
D. Change management documentation

Answer: D

Explanation:
Change management documentation is a record of the changes that have been made to a system or process, including the reason, date, time, and impact of each change. A technician can reference this documentation to find what solution was implemented to resolve a previously encountered issue, as well as any potential side effects or dependencies of the change. References: https://www.comptia.org/blog/what-is-change-management

NEW QUESTION 60
- (Exam Topic 2)
A corporation has a critical system that would cause unrecoverable damage to the brand if it was taken offline. Which of the following disaster recovery solutions should the corporation implement?

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

Answer: C

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

NEW QUESTION 61
- (Exam Topic 2)
Which of the following is used to provide networking capability for VMs at Layer 2 of the OSI model?

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

Answer: C

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

NEW QUESTION 64
- (Exam Topic 2)
A user is having difficulty with video conferencing and is looking for assistance. Which of the following would BEST improve performance?

A. Packet shaping
B. Quality of service
C. Port mirroring
D. Load balancing

Answer: B

Explanation:
Quality of service (QoS) is a mechanism that prioritizes network traffic based on different criteria, such as application type, source and destination address, port number, etc., and allocates bandwidth and resources accordingly. QoS would best improve performance for video conferencing, as it would ensure that video traffic gets higher priority and lower latency than other types of traffic on the network. Packet shaping is a
technique that controls the rate or volume of network traffic by delaying or dropping packets that exceed certain thresholds or violate certain policies, which may not improve performance for video conferencing if it causes packet loss or jitter. Port mirroring is a technique that copies traffic from one port to another port on a switch for monitoring or analysis purposes, which does not improve performance for video conferencing at all. Load balancing is a technique that distributes network traffic across multiple servers or devices for improved availability and scalability, which does not

NEW QUESTION 67
- (Exam Topic 2)
A technician wants to install a WAP in the center of a room that provides service in a radius surrounding a radio. Which of the following antenna types should the AP utilize?

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

Answer: A

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

NEW QUESTION 72
- (Exam Topic 2)
An organization wants to implement a method of centrally managing logins to network services. Which of the following protocols should the organization use to allow for authentication, authorization and auditing?

A. MS-CHAP
B. RADIUS
C. LDAPS
D. RSTP

Answer: B

Explanation:
RADIUS (Remote Authentication Dial-In User Service) is a protocol that should be used by the organization to allow for authentication, authorization, and auditing of network services. RADIUS is an AAA (Authentication, Authorization, and Accounting) protocol that manages network access by verifying user credentials, granting access permissions, and logging user activities. RADIUS uses a client-server model where a RADIUS client (such as a router, switch, or VPN server) sends user information to a RADIUS server (such as an authentication server) for verification and authorization. The RADIUS server can also send accounting information to another server for billing or reporting purposes. References:
https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838

NEW QUESTION 75
- (Exam Topic 2)
A technician is implementing a new wireless network to serve guests at a local office. The network needs to provide Internet access but disallow associated stations from communicating with each other. Which of the following would BEST accomplish this requirement?

A. Wireless client isolation
B. Port security
C. Device geofencing
D. DHCP snooping

Answer: A

Explanation:
Wireless client isolation is a feature on wireless routers that limits the connectivity between wireless devices connected to the same network. It prevents them from accessing resources on other wireless or wired devices, as a security measure to reduce attacks and threats. This feature can be useful for guest and BYOD SSIDs, but it can also be disabled on the router's settings. References:
https://www.howtogeek.com/179089/lock-down-your-wi-fi-network-with-your-routers-wireless-isolation-option

NEW QUESTION 78
- (Exam Topic 2)
Which of the following is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines?

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

Answer: B

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

NEW QUESTION 83
- (Exam Topic 2)
Which of the following attacks encrypts user data and requires a proper backup implementation to recover?

A. DDoS
B. Phishing
C. Ransomware
D. MAC spoofing

Answer: C

Explanation:
Ransomware is a type of malware that encrypts user data and demands a ransom for its decryption. Ransomware can prevent users from accessing their files and applications, and cause data loss or corruption. A proper backup implementation is essential to recover from a ransomware attack, as it can help restore the encrypted data without paying the ransom or relying on the attackers' decryption key. References: https://www.comptia.org/blog/what-is-ransomware

NEW QUESTION 88
- (Exam Topic 2)
A network field technician is installing and configuring a secure wireless network. The technician performs a site survey. Which of the following documents would MOST likely be created as a result of the site survey?

A. Physical diagram

B. Heat map
C. Asset list
D. Device map

Answer: B

Explanation:
A heat map would most likely be created as a result of the site survey. A heat map is a graphical representation of the wireless signal strength and coverage in a given area. It can show the location of APs, antennas, walls, obstacles, interference sources, and dead zones. It can help with planning, optimizing, and troubleshooting wireless networks. References: https://www.netspotapp.com/what-is-a-wifi-heatmap.html

NEW QUESTION 91
- (Exam Topic 2)
A network administrator wants to improve the security of the management console on the company's switches and ensure configuration changes made can be correlated to the administrator who conformed them Which of the following should the network administrator implement?

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

Answer: C

Explanation:
TACACS+ is a protocol that provides centralized authentication, authorization, and accounting (AAA) for network devices and users. TACACS+ can help improve the security of the management console on the company's switches by verifying the identity and credentials of the administrators, enforcing granular access policies and permissions, and logging the configuration changes made by each administrator. This way, the network administrator can ensure only authorized and authenticated users can access and modify the switch settings, and also track and correlate the changes made by each user. References: https://www.comptia.org/blog/what-is-tacacs

NEW QUESTION 96
- (Exam Topic 2)
During the security audit of a financial firm the Chief Executive Officer (CEO) questions why there are three employees who perform very distinct functions on the server. There is an administrator for creating users another for assigning the users lo groups and a third who is the only administrator to perform file rights assignment Which of the following mitigation techniques is being applied'

A. Privileged user accounts
B. Role separation
C. Container administration
D. Job rotation

Answer: B

Explanation:
Role separation is a security principle that involves dividing the tasks and privileges for a specific business process among multiple users. This reduces the risk of fraud and errors, as no one user has complete control over the process. In the scenario, there are three employees who perform very distinct functions on the server, which is an example of role separation. References: https://hyperproof.io/resource/segregation-of-duties/

NEW QUESTION 99
- (Exam Topic 2)
A technician is connecting DSL for a new customer. After installing and connecting the on-premises equipment, the technician verifies DSL synchronization. When connecting to a workstation, however, the link LEDs on the workstation and modem do not light up. Which of the following should the technician perform during troubleshooting?

A. Identify the switching loops between the modem and the workstation.
B. Check for asymmetrical routing on the modem.
C. Look for a rogue DHCP server on the network.
D. Replace the cable connecting the modem and the workstation.

Answer: D

Explanation:
If the link LEDs on the workstation and modem do not light up when connecting to a workstation, it could indicate a problem with the cable connecting them. The cable could be damaged, defective, or incompatible with the devices. A technician should replace the cable with a known good one and check if the link LEDs light up. If not, the problem could be with the network interface cards (NICs) on the workstation or modem. References: https://www.comptia.org/blog/what-is-link-light

NEW QUESTION 100
- (Exam Topic 2)
A client moving into a new office wants the IP network set up to accommodate 412 network-connected devices that are all on the same subnet. The subnet needs to be as small as possible. Which of the following subnet masks should be used to achieve the required result?

A. 255.255.0.0
B. 255.255.252.0
C. 255.255.254.0
D. 255.255.255.0

Answer: B

Explanation:

* 255.255.252.1 is a subnet mask that allows for 1022 network-connected devices on the same subnet, which is the smallest subnet that can accommodate 412 devices. The subnet mask determines how many bits are used for the network portion and how many bits are used for the host portion of an IP address. A smaller subnet mask means more bits are used for the network portion and less bits are used for the host portion, which reduces the number of available hosts on the subnet. 255.255.0.0 allows for 65534 hosts on the same subnet, which is too large. 255.255.254.0 allows for 510 hosts on the same subnet, which is also too large. 255.255.255.0 allows for 254 hosts on the same subnet, which is too small.

NEW QUESTION 103
- (Exam Topic 2)
Which of the following is MOST commonly used to address CVEs on network equipment and/or operating systems?

A. Vulnerability assessment
B. Factory reset
C. Firmware update
D. Screened subnet

Answer: C

Explanation:
Firmware is a type of software that controls the low-level functions of a hardware device, such as a router, switch, printer, or camera. Firmware updates are patches or upgrades that fix bugs, improve performance, add features, or address security vulnerabilities in firmware. Firmware updates are commonly used to address CVEs (Common Vulnerabilities and Exposures) on network equipment and operating systems, as CVEs are publicly known flaws that can be exploited by attackers. References:
https://www.comptia.org/blog/what-is-firmware

NEW QUESTION 104
- (Exam Topic 2)
A user recently made changes to a PC that caused it to be unable to access websites by both FQDN and IP Local resources, such as the file server remain accessible. Which of the following settings did the user MOST likely misconfigure?

A. Static IP
B. Default gateway
C. DNS entries
D. Local host file

Answer: B

Explanation:
The default gateway is the setting that the user most likely misconfigured on the PC that caused it to be unable to access websites by both FQDN and IP. The default gateway is a device, usually a router or a firewall, that connects a local network to other networks such as the Internet. It acts as an intermediary between devices on different networks and forwards packets based on their destination IP addresses. If the default gateway is not configured correctly on a PC, it will not be able to communicate with devices outside its local network, such as web servers or DNS servers. References:
https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/16448-default-gateway.html

NEW QUESTION 108
- (Exam Topic 2)
A company wants to implement a large number of WAPs throughout its building and allow users to be able to move around the building without dropping their connections Which of the following pieces of equipment would be able to handle this requirement?

A. A VPN concentrator
B. A load balancer
C. A wireless controller
D. A RADIUS server

Answer: C

Explanation:
A wireless controller would be able to handle the requirement of implementing a large number of WAPs throughout the building and allowing users to move around without dropping their connections. A wireless controller is a device that centrally manages and configures multiple wireless access points (WAPs) on a network. It can provide features such as load balancing, roaming, security, QoS, and monitoring for the wireless network. A wireless controller can also support wireless mesh networks, where some WAPs act as relays for other WAPs to extend the wireless coverage. References: https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/index.html

NEW QUESTION 111
- (Exam Topic 3)
A technician is investigating a misconfiguration on a Layer 3 switch. When the technician logs in and runs a command, the following data is shown:
Which of the following commands generated this output?

A. show route
B. show config
C. show interface
D. tcpdump
E. netstat —s

Answer: C

Explanation:
The output shown in the image is from the show interface command, which displays information about the status and configuration of a network interface on a switch or router. The output includes the interface name, description, MAC address, IP address, speed, duplex mode, status, and statistics. The show route command displays the routing table of the device. The show config command displays the current configuration of the device. The tcpdump command captures

and analyzes network traffic. The netstat -s command displays statistics for each protocol.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.4: Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

NEW QUESTION 115
- (Exam 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 117
- (Exam Topic 3)
A technician is consolidating a topology with multiple SSIDs into one unique SSID deployment. Which of the following features will be possible after this new configuration?

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

Answer: A

NEW QUESTION 122
- (Exam Topic 3)
An administrator is investigating reports of network slowness in a building. While looking at the uplink interface statistics In the switch's CLI, the administrator discovers the uplink Is at 100% utilization However, the administrator is unsure how to Identify what traffic is causing the saturation. Which of the following tools should the administrator utilize to identify the source and destination addresses of the traffic?

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

Answer: D

Explanation:
To identify the source and destination addresses of the traffic causing network saturation, the network administrator should use a network protocol analyzer that supports the NetFlow protocol. NetFlow is a network protocol that collects IP traffic information as it enters or exits an interface and sends it to a NetFlow collector for analysis. This data includes the source and destination addresses of the traffic, the ports used, and the number of bytes and packets transferred.
Therefore, the correct answer is option D, NetFlow.
Reference: CompTIA Network+ Study Guide, Exam N10-007, Fourth Edition, by Todd Lammle (Chapter 6: Network Devices)

NEW QUESTION 125
- (Exam Topic 3)
A company needs a redundant link to provide a channel to the management network in an incident response scenario. Which of the following remote access methods provides the BEST solution?

A. Out-of-band access
B. Split-tunnel connections
C. Virtual network computing
D. Remote desktop gateways

Answer: A

Explanation:
Out-of-band access is a remote access method that provides a separate, independent channel for accessing network devices and systems. Out-of-band access uses a dedicated network connection or a separate communication channel, such as a dial-up or cellular connection, to provide access to network devices and systems. This allows an administrator to access the management network even if the primary network connection is unavailable or impaired. Out-of-band access is a good solution for providing a redundant link to the management network in an incident response scenario because it can be used to access the network even if the primary connection is unavailable or impaired.

NEW QUESTION 129
- (Exam Topic 3)
A network device needs to discover a server that can provide it with an IPv4 address. Which of the following does the device need to send the request to?

A. Default gateway

B. Broadcast address
C. Unicast address
D. Link local address

Answer: B

Explanation:
The DHCP client sends broadcast request packets to the network; the DHCP servers respond with broadcast packets that offer IP parameters, such as an IP address for the client. After the client chooses the IP parameters, communication between the client and server is by unicast packets.
"When a DHCP client boots up, it automatically sends out a DHCP Discover UDP datagram to the broadcast address, 255.255.255.255. This DHCP Discover message asks “Are there any DHCP servers out there?” The client can’t send unicast traffic yet, as it doesn’t have a valid IP address that can be used."

NEW QUESTION 130
- (Exam Topic 3)
A technician is checking network devices to look for opportunities to improve security Which of the following toots would BEST accomplish this task?

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

Answer: B

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

NEW QUESTION 135
- (Exam 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 140
- (Exam Topic 3)
A network administrator is installing a new server in the data center. The administrator is concerned the amount of traffic generated will exceed 1GB. and higher-throughput NiCs are not available for installation. Which of the following is the BEST solution for this issue?

A. Install an additional NIC and configure LACP.
B. Remove some of the applications from the server.
C. Configure the NIC to use fun duplex
D. Configure port mirroring to send traffic to another server.
E. Install a SSD to decrease data processing time.

Answer: A

NEW QUESTION 143
- (Exam Topic 3)
A technician manages a DHCP scope but needs to allocate a portion of the scope’s subnet for statically assigned devices. Which of the following DHCP concepts would be BEST to use to prevent IP address conflicts?

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

Answer: B

Explanation:
To prevent IP address conflicts when allocating a portion of a DHCP scope's subnet for statically assigned devices, it is recommended to use the concept of DHCP exclusion ranges. DHCP exclusion ranges allow a DHCP administrator to specify a range of IP addresses within the scope that should not be assigned to DHCP clients. This can be useful in situations where some devices on the network need to be assigned static IP addresses, as it ensures that the statically assigned addresses do not overlap with addresses assigned by the DHCP server. To set up a DHCP exclusion range, the administrator needs to specify the start and end IP addresses of the range, as well as the subnet mask. The DHCP server will then exclude the specified range of addresses from its pool of available addresses, and will not assign them to DHCP clients. By using DHCP exclusion ranges, the technician can ensure that the statically assigned addresses do not conflict with addresses assigned by the DHCP server, and can prevent IP address conflicts on the network.
Anthony Sequeira
"Another frequent configuration you might make in a DHCP implementation is to configure an exclusion range. This is a portion of the address pool that you never want leased out to clients in the network. Perhaps you have numbered your servers 192.168.1.1–192.168.1.10. Because the servers are statically configured with

these addresses, you exclude these addresses from the 192.168.1.0/24 pool of addresses."
Mike Meyers
"Exclusion ranges represent an IP address or range of IP addresses from the pool of addresses that are not to be given out by the DHCP server. Exclusions should be made for the static addresses manually configured on servers and router interfaces, so these IP addresses won't be offered to DHCP clients."

NEW QUESTION 146
- (Exam 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 148
- (Exam Topic 3)
A company has wireless APS that were deployed with 802.11g. A network engineer has noticed more frequent reports of wireless performance issues during the lunch hour in comparison to the rest of the day. The engineer thinks bandwidth consumption will increase while users are on their breaks, but network utilization logs do not show increased bandwidth numbers. Which Of the following would MOST likely resolve this issue?

A. Adding more wireless APS
B. Increasing power settings to expand coverage
C. Configuring the APS to be compatible with 802.1la
D. Changing the wireless channel used

Answer: C

Explanation:
* 802.11 g is an older wireless standard that operates in the 2.4 GHz frequency band and has a maximum data rate of 54 Mbps. 802.11a is a newer wireless standard that operates in the 5 GHz frequency band and has a maximum data rate of 54 Mbps. By configuring the APS to be compatible with 802.11a, the network engineer can reduce interference and congestion in the 2.4 GHz band and improve wireless performance.
References: Network+ Study Guide Objective 2.5: Implement network troubleshooting methodologies

NEW QUESTION 153
- (Exam Topic 3)
A non-employee was able to enter a server room. Which of the following could have prevented this from happening?

A. A security camera
B. A biometric reader
C. OTP key fob
D. Employee training

Answer: B

Explanation:
A biometric reader is a device that scans a person's physical characteristics, such as fingerprints, iris, or face, and compares them to a database of authorized users. A biometric reader can be used to restrict access to a server room and prevent unauthorized entry. A biometric reader provides a high level of security and cannot be easily bypassed or duplicated.
References: Network+ Study Guide Objective 5.1: Summarize the importance of physical security controls.

NEW QUESTION 155
- (Exam Topic 3)
Which of the following would MOST likely utilize PoE?

A. A camera
B. A printer
C. A hub
D. A modem

Answer: A

Explanation:
A camera is most likely to utilize PoE (Power over Ethernet). PoE is a technology that allows electrical power to be delivered over Ethernet cables. It is used to power a variety of devices, such as cameras, phones, access points, and other networking equipment.Cameras are particularly well-suited for PoE because they are often installed in locations where it is difficult or impossible to run electrical power. By using PoE, cameras can be powered directly over the Ethernet cable, eliminating the need for separate power cables and outlets.Other devices, such as printers, hubs, and modems, are less likely to utilize PoE because they typically do not need to be powered over Ethernet. These devices are usually powered by AC (alternating current) power and are typically connected to a power outlet rather than an Ethernet cable.

NEW QUESTION 159
- (Exam Topic 3)
Which of the following OSI model layers would allow a user to access and download files from a remote computer?

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

Answer: D

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

NEW QUESTION 163
- (Exam Topic 3)
A security vendor needs to add a note to the DNS to validate the ownership of a company domain before services begin. Which of the following records did the security company MOST likely ask the company to configure?

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

Answer: A

Explanation:
TXT stands for Text and is a type of DNS record that can store arbitrary text data associated with a domain name. TXT records can be used for various purposes, such as verifying the ownership of a domain, providing information about a domain, or implementing security mechanisms such as SPF (Sender Policy Framework) or DKIM (DomainKeys Identified Mail). In this scenario, the security company most likely asked the company to configure a TXT record with a specific value that can prove the ownership of the domain. AAAA stands for IPv6 Address and is a type of DNS record that maps a domain name to an IPv6 address. CNAME stands for Canonical Name and is a type of DNS record that maps an alias name to another name. SRV stands for Service and is a type of DNS record that specifies the location of a service on a network.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.8: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 164
- (Exam Topic 3)
Which of the following devices Is used to configure and centrally manage access points Installed at different locations?

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

Answer: A

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

NEW QUESTION 166
- (Exam 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 169
- (Exam Topic 3)
Which of the following can be used to limit the ability of devices to perform only HTTPS connections to an internet update server without exposing the devices to the public internet?

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

Answer: A

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

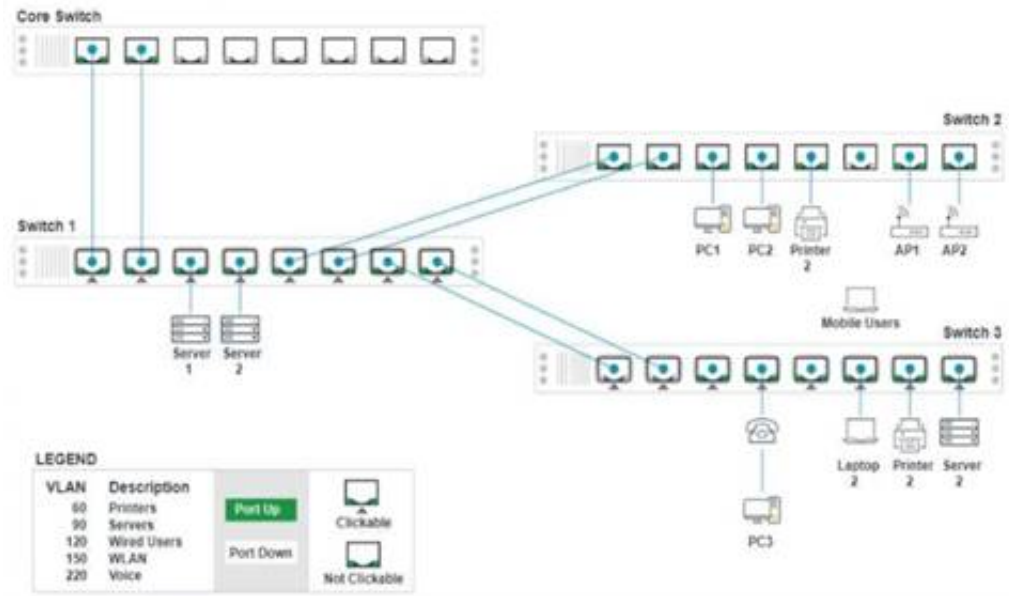
NEW QUESTION 173
- (Exam Topic 3)
Which of the following commands can be used to display the IP address, subnet address, gateway address, and DNS address on a Windows computer?

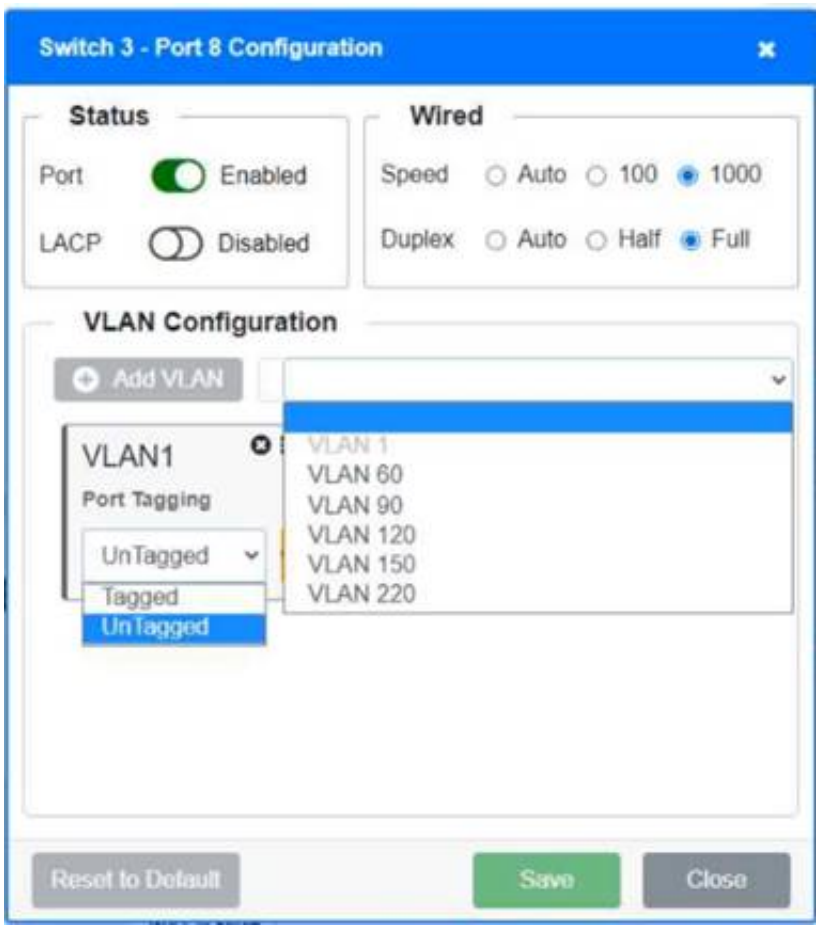
A. netstat -a
B. ifconfig
C. ip addr
D. ipconfig /all

Answer: D

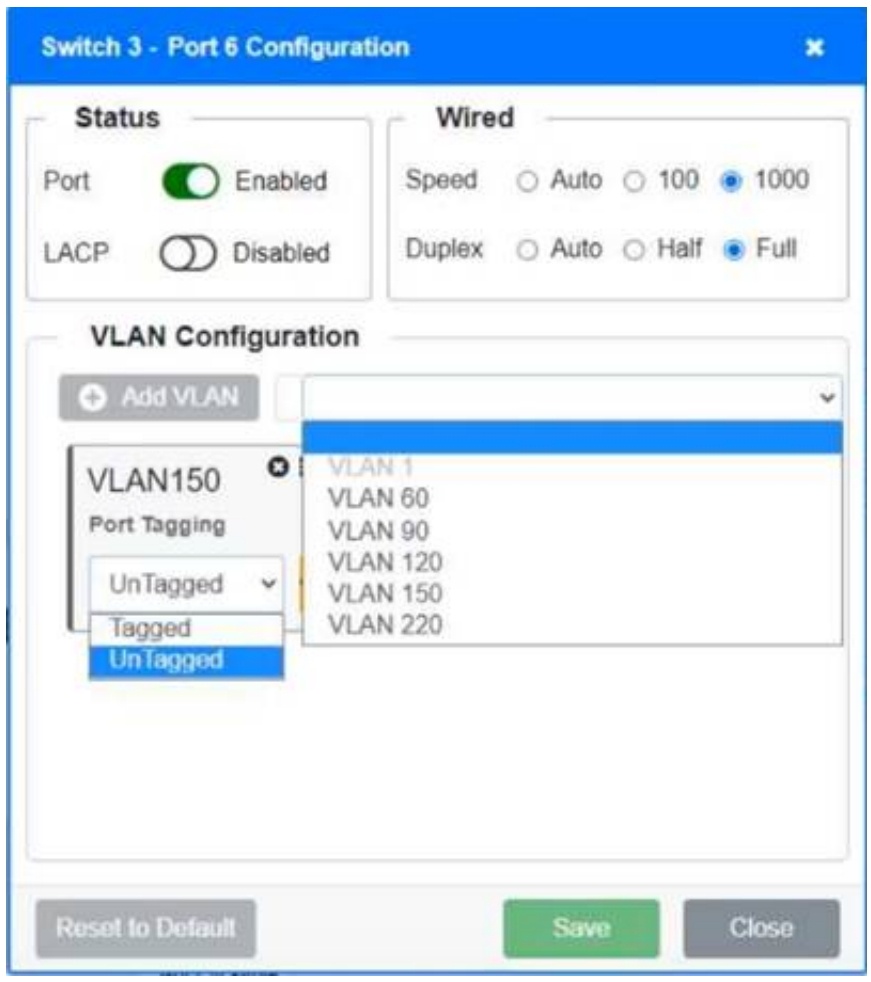
Explanation:
The ipconfig command is a utility that allows you to view and modify the network configuration of a Windows computer. By running the command "ipconfig /all", you can view detailed information about the network configuration of your computer, including the IP address, subnet mask, default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

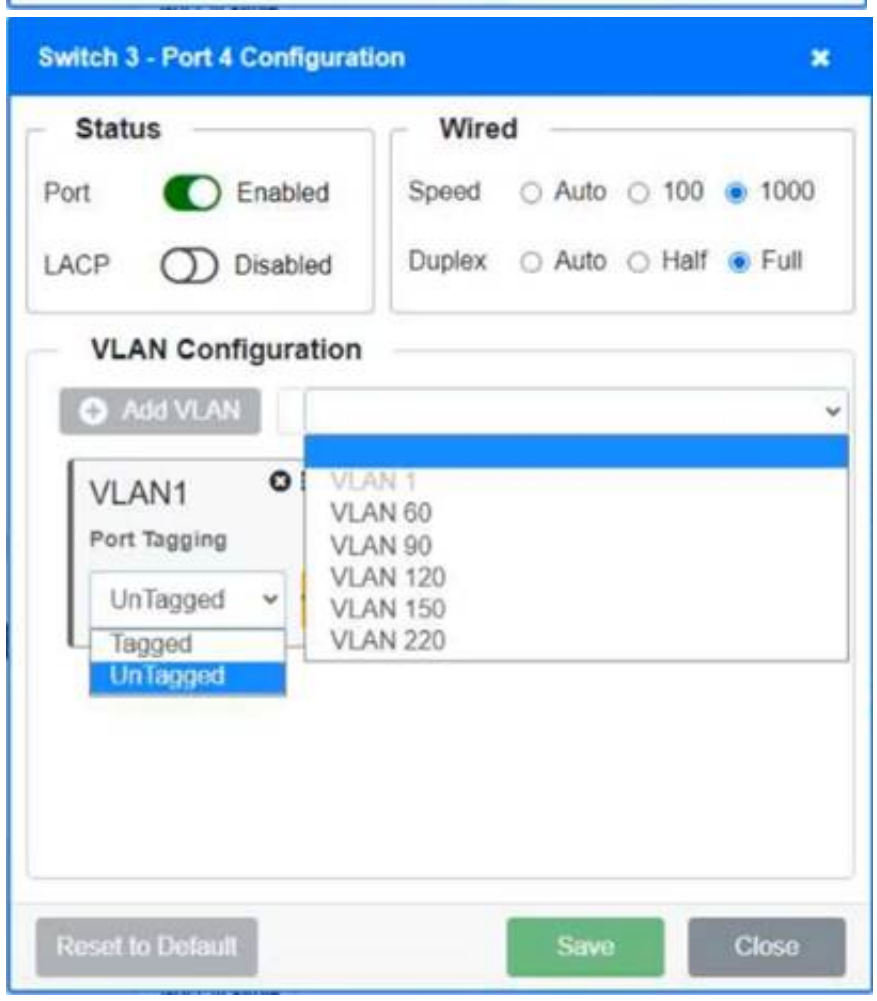
NEW QUESTION 175
- (Exam Topic 3)
SIMULATION
A network technician replaced a switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.
INSTRUCTIONS
Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings:
• Ensure each device accesses only its correctly associated network
• Disable all unused switch ports
• Require fault-tolerant connections between the switches
• Only make necessary changes to complete the above requirements
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

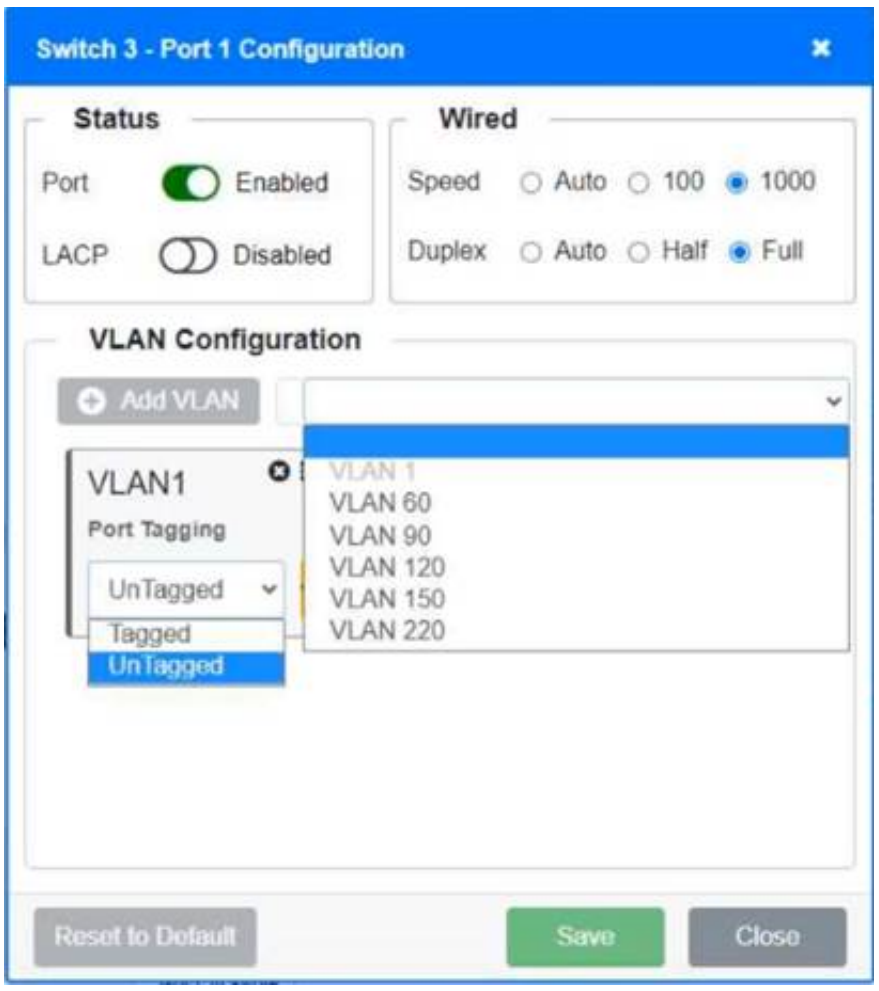


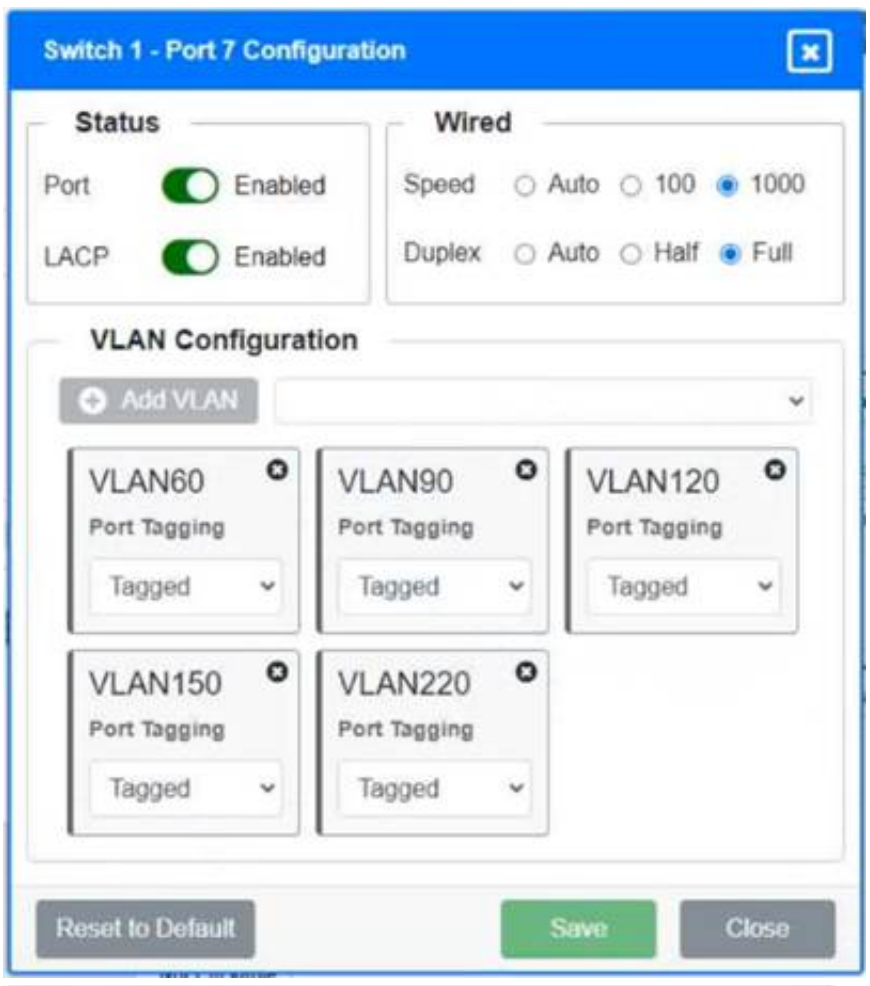


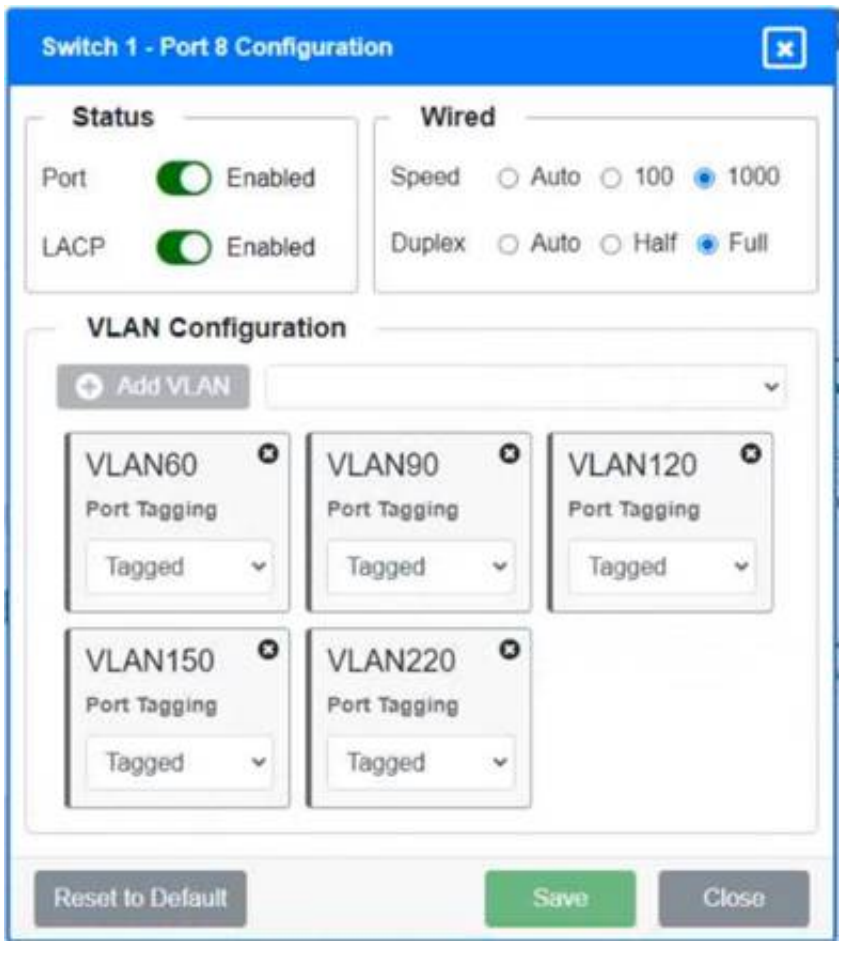
Switch 3 - Port 7 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close


Switch 3 - Port 6 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN150
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close


Switch 3 - Port 4 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

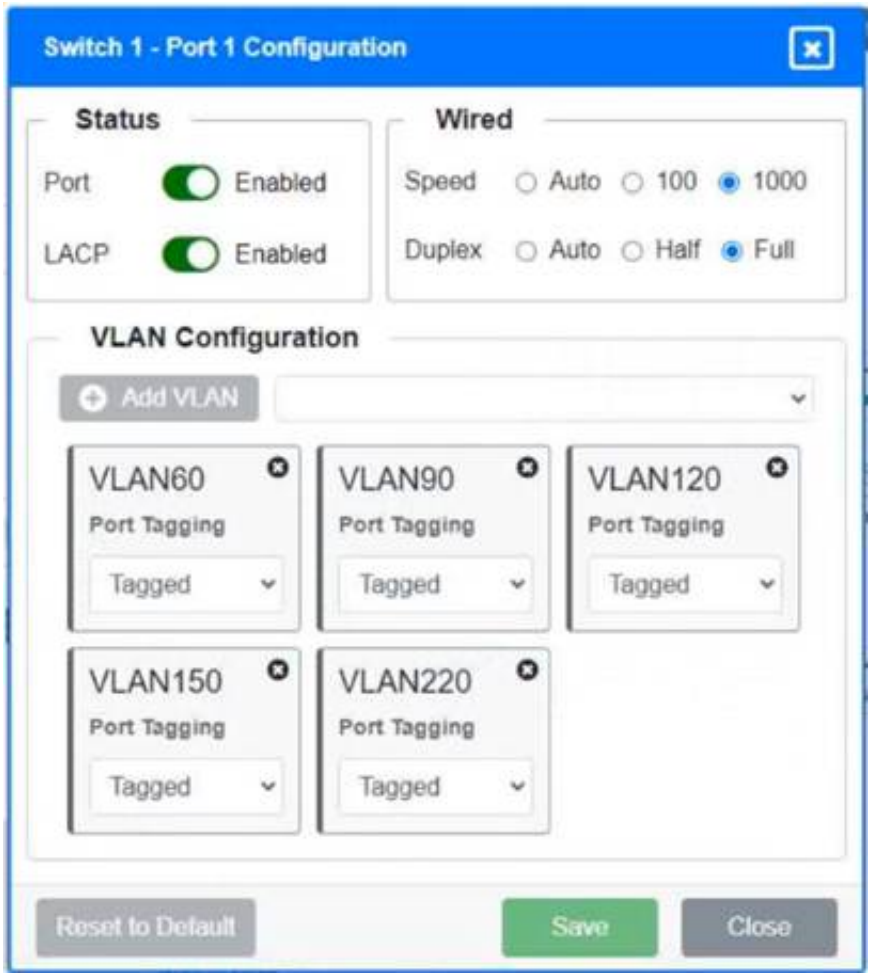

Switch 3 - Port 1 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close


Switch 1 - Port 7 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
Close

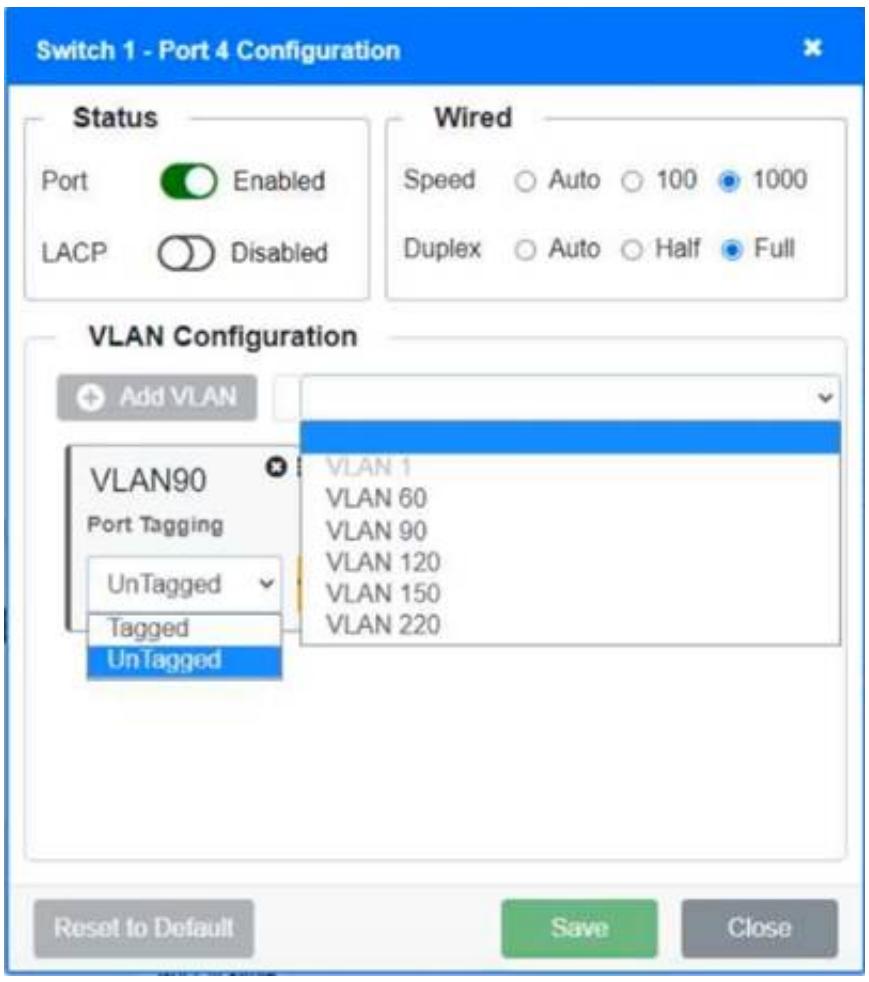

Switch 1 - Port 8 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
Close

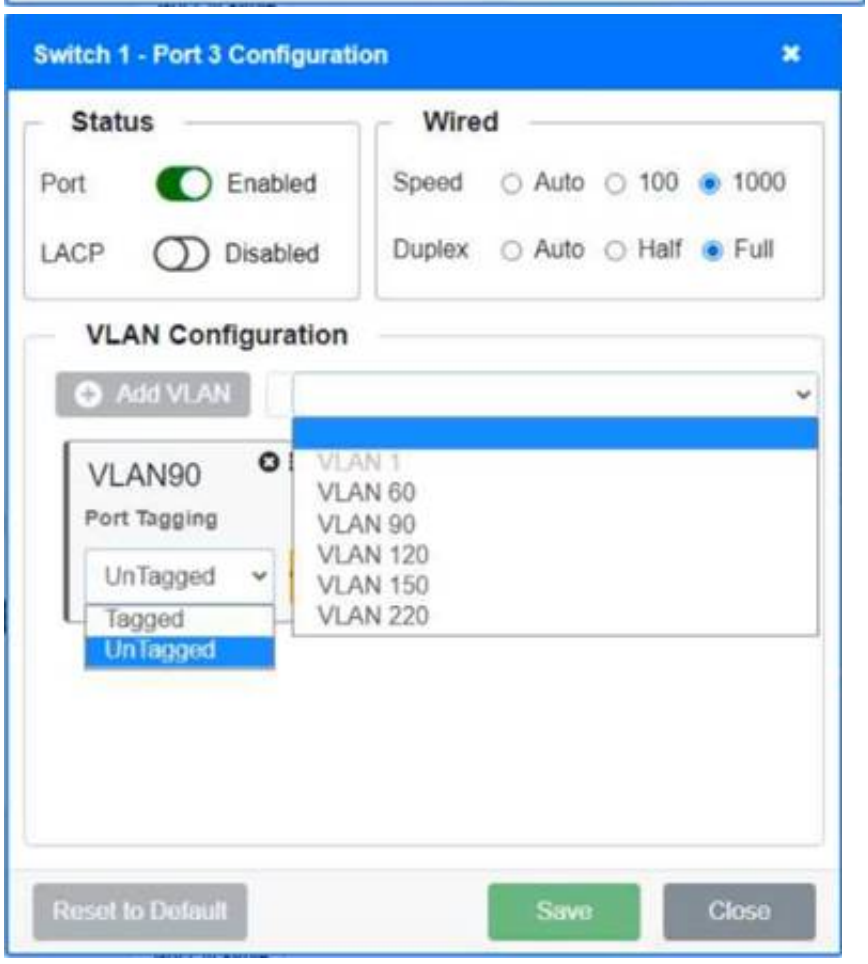
Switch 1 - Port 6 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
Reset to Default
Save
Close

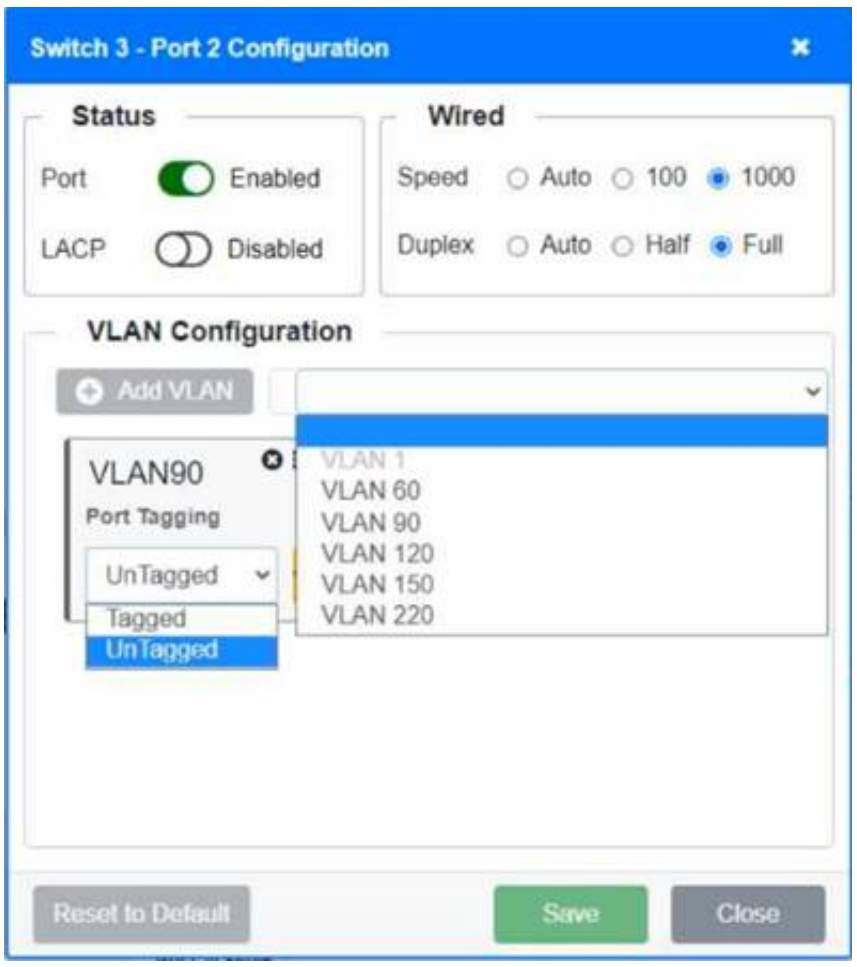
Switch 1 - Port 2 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
Close


Switch 1 - Port 1 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
Close

Switch 1 - Port 5 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
Reset to Default
Save
Close


Switch 1 - Port 4 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN90
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close


Switch 1 - Port 3 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN90
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Switch 1 and Switch 2 is the only two switches that can be configured. Only switches linked together with there switch ports needs to be "tagged" and "LACP" needs to be enabled. The other ports must be untagged with no LACP enabled. You only need to assign the correct vlan via each port. 'Speed and Duplex' needs to be Speed=1000 and Duplex=Full, with is by default.
https://resources.infosecinstitute.com/topic/what-are-tagged-and-untagged-ports/

NEW QUESTION 178
- (Exam Topic 3)
An engineer is gathering data to determine the effectiveness of UPSs in use at remote retail locations. Which of the following statistics can the engineer use to determine the availability of the remote network equipment?

A. Uptime
B. NetFlow baseline
C. SNMP traps
D. Interface statistics

Answer: A

Explanation:
Uptime is a statistic that can be used to determine the availability of the remote network equipment. Uptime is the amount of time that a device or system has been running without experiencing any failures or disruptions. It is commonly expressed as a percentage of total time, such as 99.99% uptime. By measuring the uptime of the network equipment at the remote retail locations, the engineer can determine how reliable and available the equipment is.

NEW QUESTION 179
- (Exam Topic 3)
Which of the following would be the MOST cost-effective recovery solution for a company's lower-priority applications?

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

Answer: C

NEW QUESTION 181
- (Exam Topic 3)
A public, wireless ISP mounts its access points on top of traffic signal poles. Fiber-optic cables are installed from a fiber switch through the ground and up the pole to a fiber-copper media converter, and then connected to the AP. In one location, the switchport is showing sporadic link loss to the attached AP. A similar link loss is not seen at the AP interface. The fiber-optic cable is moved to another unused switchport with a similar result. Which of the following steps should the assigned technician complete NEXT?

A. Disable and enable the switchport.
B. Clean the fiber-optic cable ends.
C. Replace the media converter.
D. Replace the copper patch cord.

Answer: B

Explanation:
Fiber-optic cables are cables that use light signals to transmit data over long distances at high speeds.
Fiber-optic cables are sensitive to dirt, dust, moisture, or other contaminants that can interfere with the light signals and cause link loss or signal degradation. To troubleshoot link loss issues with fiber-optic cables, one of the steps that should be completed next is to clean the fiber-optic cable ends with a lint-free cloth or a specialized cleaning tool. Cleaning the fiber-optic cable ends can remove any dirt or debris that may be blocking or reflecting the light signals and restore the link quality.

NEW QUESTION 186
- (Exam Topic 3)
Users within a corporate network need to connect to the Internet, but corporate network policy does not allow direct connections. Which of the following is MOST likely to be used?

A. Proxy server
B. VPN client
C. Bridge
D. VLAN

Answer: A

NEW QUESTION 190
- (Exam Topic 3)
A technician knows the MAC address of a device and is attempting to find the device's IP address. Which of the following should the technician look at to find the IP address? (Select TWO).

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

Answer: BE

NEW QUESTION 193
- (Exam Topic 3)
A company is opening a new building on the other side of its campus. The distance from the closest building to the new building is 1,804ft (550m). The company needs to connect the networking equipment in the new building to the Other buildings on the campus without using a repeater. Which Of the following transceivers should the company use?

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

Answer: B

Explanation:
10GBASE-LR is a standard for 10 Gbps Ethernet over single-mode fiber optic cable. It can support a maximum distance of 6.2 miles (10 km), which is much longer than the distance between the buildings. 10GBASE-SW, 10GBASE-LX4, and 10GBASE-SR are all standards for 10 Gbps Ethernet over multimode fiber optic cable, which have shorter maximum distances ranging from 984ft (300m) to 1,312ft (400m).
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5: Compare and contrast network cabling types, standards and speeds.

NEW QUESTION 198
- (Exam Topic 3)
Which of the following describes the ability of a corporate IT department to expand its cloud-hosted VM environment with minimal effort?

A. Scalability
B. Load balancing
C. Multitenancy
D. Geo-redundancy

Answer: A

Explanation:
Scalability is the ability of a corporate IT department to expand its cloud-hosted virtual machine (VM) environment with minimal effort. This allows IT departments to quickly and easily scale up their cloud environment to meet increased demand. Scalability also allows for the efficient use of resources, as IT departments can quickly and easily scale up or down as needed.

NEW QUESTION 200
- (Exam Topic 3)
A network administrator is getting reports of some internal users who cannot connect to network resources. The users slate they were able to connect last week, but not today. No changes have been configured on the network devices or server during the last few weeks. Which of the following is the MOST likely cause of the issue?

A. The client DHCP scope is fully utilized

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

Answer: A

NEW QUESTION 202
- (Exam Topic 3)
A security administrator is trying to prevent incorrect IP addresses from being assigned to clients on the network. Which of the following would MOST likely prevent this and allow the network to continue to operate?

A. Configuring DHCP snooping on the switch
B. Preventing broadcast messages leaving the client network
C. Blocking ports 67/68 on the client network
D. Enabling port security on access ports

Answer: A

Explanation:
To prevent incorrect IP addresses from being assigned to clients on the network and allow the network to continue to operate, the security administrator should consider configuring DHCP (Dynamic Host Configuration Protocol) snooping on the switch. DHCP snooping is a security feature that is used to prevent unauthorized DHCP servers from operating on a network. It works by allowing the switch to monitor and validate DHCP traffic on the network, ensuring that only legitimate DHCP messages are forwarded to clients. This can help to prevent incorrect IP addresses from being assigned to clients, as it ensures that only authorized DHCP servers are able to provide IP addresses to clients on the network.

NEW QUESTION 204
- (Exam Topic 3)
A network technician receives a report about a performance issue on a client PC that is connected to port 1/3 on a network switch. The technician observes the following configuration output from the switch:

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

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

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

Answer: A

NEW QUESTION 209
- (Exam 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 210
- (Exam Topic 3)
A network technician is attempting to increase throughput by configuring link port aggregation between a Gigabit Ethernet distribution switch and a Fast Ethernet access switch. Which of the following is the BEST choice concerning speed and duplex for all interfaces that are participating in the link aggregation?

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

Answer: B

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

NEW QUESTION 215
- (Exam Topic 3)
Which of the following layers of the OSI model receives data from the application layer and converts it into syntax that is readable by other devices on the network?

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

Answer: C

NEW QUESTION 217
- (Exam Topic 3)
A network technician is having issues connecting an IoT 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 218
- (Exam Topic 3)
Which of the following can be used to decrease latency during periods of high utilization of a firewall?

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

Answer: B

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

NEW QUESTION 220
- (Exam Topic 3)
While waking from the parking lot lo an access-controlled door an employee sees an authorized user open the door. Then the employee notices that another person catches the door before It closes and goes inside Which of the following attacks Is taking place?

A. Tailgating
B. Pipgybacking
C. Shoulder surfing
D. Phisning

Answer: A

Explanation:
The difference between piggybacking and tailgaiting is that with piggybacking, the person is willfully and intentionally letting you in. In this particular case, the person caught the door before it closed, so it is tailgating.
Tailgating is a physical security attack that occurs when an unauthorized person follows an authorized person through a secured door or gate without their knowledge or consent. Tailgating can allow an attacker to bypass access control mechanisms and gain entry to restricted areas or resources. Tailgating can also pose a safety risk for the authorized person and other occupants of the facility.
Piggybacking is a physical security attack that occurs when an unauthorized person follows an authorized person through a secured door or gate with their knowledge or consent. Piggybacking can also allow an attacker to bypass access control mechanisms and gain entry to restricted areas or resources. Piggybacking can also violate security policies and compromise the accountability of the authorized person.
Shoulder surfing is a physical security attack that occurs when an unauthorized person observes or records an authorized person’s confidential information, such as passwords, PINs, or credit card numbers. Shoulder surfing can allow an attacker to steal credentials and access sensitive data or systems. Shoulder surfing can also violate privacy and confidentiality rights of the authorized person.
Phishing is a cyber security attack that occurs when an unauthorized person sends fraudulent emails or messages that appear to come from legitimate sources, such as banks, companies, or government agencies. Phishing can trick recipients into clicking on malicious links, opening malicious attachments, or providing personal or financial information. Phishing can allow an attacker to install malware, steal credentials, or perform identity theft. Phishing does not involve physical access to secured doors or gates.

NEW QUESTION 221
- (Exam Topic 3)
A network administrator is investigating reports about network performance and finds high utilization on a switch uplink. The administrator is unsure whether this is an anomaly or normal behavior that will require an upgrade to resolve. Which Of the following should the administrator reference to gain historical perspective?

A. Device configuration review

B. ARP table export
C. Service-level agreement
D. Network performance baseline

Answer: D

Explanation:
A network performance baseline is a set of metrics that represents the normal or expected behavior of a network under various conditions and scenarios. A network performance baseline can help a network administrator to investigate reports about network performance by comparing the current metrics with the historical metrics and identifying any deviations or anomalies. A network performance baseline can also help to plan and justify network upgrades by showing the trends and patterns of network utilization and performance over time.
A device configuration review is a process that involves checking and verifying the settings and parameters of a network device, such as a switch, router, firewall, or server. A device configuration review can help a network administrator to troubleshoot network issues by finding and fixing any errors, inconsistencies, or vulnerabilities in the device configuration. A device configuration review can also help to ensure compliance with security policies and best practices by applying the latest updates and patches to the device.
An ARP table export is a file that contains the contents of the ARP (Address Resolution Protocol) table of a network device. The ARP table is a data structure that maps IP addresses to MAC addresses on a local network. An ARP table export can help a network administrator to monitor and manage the network devices on a local network by showing their IP addresses and MAC addresses. An ARP table export can also help to detect and prevent ARP spoofing attacks by identifying any duplicate or malicious entries in the ARP table.
A service-level agreement (SLA) is a contract that defines the expectations and responsibilities of both parties in terms of service quality, availability, performance, and response time. An SLA can help a network administrator to provide and maintain a satisfactory level of service to the customers or users of the network by setting and measuring specific goals and metrics. An SLA can also help to resolve any disputes or issues that may arise between the service provider and the service consumer by establishing clear terms and conditions for the service delivery.

NEW QUESTION 226
- (Exam Topic 3)
An engineer needs to restrict the database servers that are in the same subnet from communicating with each other. The database servers will still need to communicate with the application servers in a different subnet. In some cases, the database servers will be clustered, and the servers will need to communicate with other cluster members. Which of the following technologies will be BEST to use to implement this filtering without creating rules?

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

Answer: A

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

NEW QUESTION 230
- (Exam Topic 3)
A computer engineer needs to ensure that only a specific workstation can connect to port 1 on a switch. Which of the following features should the engineer configure on the switch interface?

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

Answer: B

Explanation:
Port security is a feature that can be configured on a switch interface to limit and identify the MAC addresses of workstations that are allowed to connect to that specific port. This can help ensure that only a specific workstation (or workstations) can connect to the interface. According to the CompTIA Network+ Study Manual, “Port security can be used to specify which MAC addresses are allowed to connect to a particular switch port. If a port security violation is detected, the switch can take a number of different actions, such as shutting down the port, sending an SNMP trap, or sending an email alert.”

NEW QUESTION 235
- (Exam 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 236
- (Exam Topic 3)

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

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

Answer: AC

Explanation:
To achieve this, you should do two things:
- Tag the three VLANs across the uplink port that connects to another switch or router. This will allow data packets from different VLANs to cross over into other networks.
- Untag an individual VLAN per device port that connects to an end device. This will assign each device to its expected network without additional connections.

NEW QUESTION 240
- (Exam Topic 3)
After rebooting an AP a user is no longer able to conned to me enterprise LAN A technician plugs a laptop In to the same network jack and receives the IP 169.254 0 200. Which of the following is MOST likely causing the issue?

A. DHCP scope exhaustion
B. Signal attenuation
C. Channel overlap
D. Improper DNS configuration

Answer: A

Explanation:
DHCP scope exhaustion occurs when the number of available IP addresses to be leased from a DHCP server have been used up. This could be caused by a large number of clients on the network, or a misconfigured DHCP scope. When this happens, clients will be assigned an IP address from the APIPA range (169.254.0.0 to 169.254.255.255). To resolve this issue, the DHCP scope needs to be expanded or adjusted to accommodate the number of clients on the network.

NEW QUESTION 244
- (Exam Topic 3)
A Wi-Fi network was recently deployed in a new, multilevel budding. Several issues are now being reported related to latency and drops in coverage. Which of the following is the FIRST step to troubleshoot the issues?

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

Answer: A

NEW QUESTION 245
- (Exam Topic 3)
An auditor assessing network best practices was able to connect a rogue switch into a network Jack and get network connectivity. Which of the following controls would BEST address this risk?

A. Activate port security on the switchports providing end user access.
B. Deactivate Spanning Tree Protocol on network interfaces that are facing public areas.
C. Disable Neighbor Resolution Protocol in the Layer 2 devices.
D. Ensure port tagging is in place for network interfaces in guest areas

Answer: A

NEW QUESTION 247
- (Exam Topic 3)
Which of the following options represents the participating computers in a network?

A. Nodes
B. CPUs
C. Servers
D. Clients

Answer: A

NEW QUESTION 248
- (Exam Topic 3)
A new office space is being designed. The network switches are up. but no services are running yet A network engineer plugs in a laptop configured as a DHCP client to a switch Which ol the following IP addresses should be assigned to the laptop?

A. 10.1.1.1

B. 169.254.1.128
C. 172 16 128 128
D. 192 168.0.1

Answer: B

Explanation:
When a DHCP client is connected to a network and no DHCP server is available, the client can automatically configure a link-local address in the 169.254.0.0/16 range using the Automatic Private IP Addressing (APIPA) feature. So, the correct answer is option B, 169.254.1.128. This is also known as an APIPA address.
Reference: CompTIA Network+ Study Guide, Exam N10-007, Fourth Edition, by Todd Lammle (Chapter 4: IP Addressing)

NEW QUESTION 250
- (Exam Topic 3)
An engineer needs to verity the external record tor SMTP traffic. The engineer logged in to the server and entered the nslookup command. Which of the following commands should the engineer send before entering the DNS name?

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

Answer: D

NEW QUESTION 252
- (Exam Topic 3)
A network technician is planning a network scope. The web server needs to be within 12.31 69.1 to 12.31.69.29. Which of the following would meet this requirement?

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

Answer: A

NEW QUESTION 255
- (Exam 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 260
- (Exam Topic 3)
A network technician is performing tests on a potentially faulty network card that is installed in a server. Which of the following addresses will MOST likely be used during traffic diagnostic tests?

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

Answer: B

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

NEW QUESTION 263
- (Exam Topic 3)
A corporation is looking for a method to secure all traffic between a branch office and its data center in order to provide a zero-touch experience for all staff members who work there. Which of the following would BEST meet this requirement?

A. Site-to-site VPN
B. VNC
C. Remote desktop gateway

D. Virtual LANs

Answer: A

Explanation:
A site-to-site VPN is a method that creates a secure and encrypted connection between two internet gateways, such as routers or firewalls, that belong to different networks1. A site-to-site VPN can secure all traffic between a branch office and its data center by creating a virtual tunnel that protects the data from interception or tampering. A site-to-site VPN can also provide a zero-touch experience for all staff members who work there, as they do not need to install any software or configure any settings on their devices to access the data center resources. They can simply use their local network as if they were physically connected to the data center network.
VNC (Virtual Network Computing) is a method that allows remote access and control of a computer's desktop from another device over a network2. VNC can enable staff members to work remotely by accessing their office computers from their home computers or mobile devices. However, VNC does not secure all traffic between a branch office and its data center, as it only works at the application layer and does not encrypt the network layer. VNC also does not provide a zero-touch experience for staff members, as they need to install software and configure settings on both the host and the client devices.
Remote desktop gateway is a method that allows remote access and control of a computer's desktop from another device over a network using the Remote Desktop Protocol (RDP). Remote desktop gateway can also enable staff members to work remotely by accessing their office computers from their home computers or mobile devices. However, remote desktop gateway does not secure all traffic between a branch office and its data center, as it only works at the application layer and does not encrypt the network layer. Remote desktop gateway also does not provide a zero-touch experience for staff members, as they need to install software and configure settings on both the host and the client devices.
Virtual LANs (VLANs) are methods that create logical subdivisions of a physical network based on criteria such as function, department, or security level. VLANs can improve network performance, security, and management by reducing broadcast domains, isolating traffic, and enforcing policies. However, VLANs do not secure all traffic between a branch office and its data center, as they only work at the data link layer and do not encrypt the network layer. VLANs also do not provide a zero-touch experience for staff members, as they need to configure settings on their network devices to join or leave a VLAN.

NEW QUESTION 264
- (Exam Topic 3)
In which of the following components do routing protocols belong in a software-defined network?

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

Answer: B

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

NEW QUESTION 265
- (Exam Topic 3)
A user in a branch office reports that access to all files has been lost after receiving a new PC. All other users in the branch can access fileshares. The IT engineer who is troubleshooting this incident is able to ping the workstation from the branch router, but the machine cannot ping the router. Which of the following is MOST likely the cause of the incident?

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

Answer: A

NEW QUESTION 267
- (Exam 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 268
- (Exam 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: BF

NEW QUESTION 273
- (Exam Topic 3)
Which of the following would be BEST suited for use at the access layer in a three-tier architecture system?

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

Answer: C

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

NEW QUESTION 275
- (Exam Topic 3)
Which of the following can be used to validate domain ownership by verifying the presence of pre-agreed content contained in a DNS record?

A. SOA
B. SRV
C. AAA
D. TXT

Answer: D

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

NEW QUESTION 279
- (Exam Topic 3)
A network technician is configuring a wireless access point and wants to only allow company-owned devices to associate with the network. The access point uses PSKs,
and a network authentication system does not exist on the network. Which of the following should the technician implement?

A. Captive portal
B. Guest network isolation
C. MAC filtering
D. Geofencing

Answer: C

Explanation:
MAC filtering is a method of allowing only company-owned devices to associate with the network by using their MAC addresses as identifiers. A MAC address is a unique identifier assigned to each network interface card (NIC) by the manufacturer. MAC filtering can be configured on the wireless access point to allow or deny access based on the MAC address of the device. This way, only devices with known MAC addresses can connect to the network. References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 323)

NEW QUESTION 280
- (Exam Topic 3)
A technician is configuring a wireless network and needs to ensure users agree to an AUP before connecting. Which of the following should be implemented to achieve this goal?

A. Captive portal
B. Geofencing
C. Wireless client isolation
D. Role-based access

Answer: A

NEW QUESTION 282

- (Exam Topic 3)
A security engineer is trying to determine whether an internal server was accessed by hosts on the internet. The internal server was shut down during the investigation Which of the following will the engineer review to determine whether the internal server had an unauthorized access attempt?

A. The server's syslog
B. The NetFlow statistics
C. The firewall logs
D. The audit logs on the core switch

Answer: A

NEW QUESTION 283
- (Exam Topic 3)
Which of the following uses the link-state routing algorithm and operates within a single autonomous system?

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

Answer: B

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

NEW QUESTION 287
- (Exam Topic 3)
Two network technicians are installing a fiber-optic link between routers. The technicians used a light meter to verify the correct fibers However, when they connect the fibers to the router interface the link does not connect. Which of the following would explain the issue? (Select TWO).

A. They used the wrong type of fiber transceiver.
B. Incorrect TX/RX polarity exists on the link
C. The connection has duplexing configuration issues.
D. Halogen light fixtures are causing interference.
E. One of the technicians installed a loopback adapter.
F. The RSSI was not strong enough on the link

Answer: AB

NEW QUESTION 292
- (Exam Topic 3)
A network administrator is troubleshooting a connectivity performance issue. As part of the troubleshooting process, the administrator performs a traceout from the client to the server, and also from the server to the client. While comparing the outputs, the administrator notes they show different hops between the hosts. Which of the following BEST explains these findings?

A. Asymmetric routing
B. A routing loop
C. A switch loop
D. An incorrect gateway

Answer: C

NEW QUESTION 296
- (Exam 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 299
- (Exam 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 301
- (Exam Topic 3)
A company wants to invest in new hardware for the core network infrastructure. The management team requires that the infrastructure be capable of being repaired in less than 60 minutes if any major part fails. Which of the following metrics is MOST likely associated with this requirement?

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

Answer: B

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

NEW QUESTION 306
- (Exam Topic 3)
A cafeteria is lacing lawsuits related to criminal internet access that was made over its guest network. The marketing team, however, insists on keeping the cafeteria phone number as the wireless passphrase. Which of the following actions would Improve wireless security while accommodating the marketing team and accepting the terms of use?

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

Answer: B

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

NEW QUESTION 309
- (Exam Topic 3)
At which of the following OSI model layers does routing occur?

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

Answer: D

NEW QUESTION 311
- (Exam Topic 3)
A company streams video to multiple devices across a campus. When this happens, several users report a degradation of network performance. Which of the following would MOST likely address this issue?

A. Enable IGMP snooping on the switches.
B. Implement another DHCP server.
C. Reconfigure port tagging for the video traffic.
D. Change the SSID of the APs

Answer: A

NEW QUESTION 313
- (Exam Topic 3)
A technician is tasked with setting up a mail server and a DNS server. The mail port should be secured and have the ability to transfer large files. Which of the following ports should be opened? (Select TWO).

A. 22
B. 53
C. 110
D. 389
E. 995
F. 3389

Answer: BE

Explanation:
Port 53 is used for DNS, which is a service that translates domain names into IP addresses. Port 995 is used for POP3S, which is a protocol for receiving email messages securely. POP3S supports large file transfers and encryption. Therefore, these two ports should be opened for the mail server and the DNS server project

NEW QUESTION 318
- (Exam Topic 3)
A PC and a network server have no network connectivity, and a help desk technician is attempting to resolve the issue. The technician plans to run a constant ping command from a Windows workstation while testing various possible reasons for the connectivity issue. Which of the following should the technician use?

A. ping —w
B. ping -i
C. ping —s
D. ping —t

Answer: D

Explanation:
ping -t is an option for the ping command in Windows that allows the user to send continuous ping requests to a target until stopped by pressing Ctrl-C. This can help the technician run a constant ping command while testing various possible reasons for the connectivity issue. ping -w is an option for the ping command in Windows that allows the user to specify a timeout value in milliseconds for each ping request. ping -i is an option for the ping command in Linux that allows the user to specify the time interval in seconds between each ping request. ping -s is an option for the ping command in Linux that allows the user to specify the size of the data payload in bytes for each ping request.
References: How to Use the Ping Command in Windows - Lifewire (https://www.lifewire.com/ping-command-2618099)

NEW QUESTION 320
- (Exam Topic 3)
After a critical power issue, the network team was not receiving UPS status notifications. The network team would like to be alerted on these status changes. Which of the following would be BEST to use tor these notifications?

A. Traps
B. MB
C. NetFlow
D. Syslog

Answer: A

NEW QUESTION 325
- (Exam Topic 3)
Which of the following can be used to store various types of devices and provide contactless delivery to users?

A. Asset tags
B. Biometrics
C. Access control vestibules
D. Smart lockers

Answer: C

NEW QUESTION 327
- (Exam Topic 3)
A network administrator responds to a support ticket that was submitted by a customer who is having issues connecting to a website inside of the company network The administrator verities that the customer could not connect to a website using a URL Which of the following troubleshooting steps would be BEST for the administrator to take?

A. Check for certificate issues
B. Contact the ISP
C. Attempt to connect to the site via IP address
D. Check the NTP configuration.

Answer: C

Explanation:
The best option for the administrator to take would be to attempt to connect to the site via IP address. This will help to determine if the issue is related to the website's DNS address or if the site itself is not accessible. Checking for certificate issues may be necessary, but this should be done after the administrator has attempted to connect to the site via IP address. Contacting the ISP is unnecessary since the issue is related to the website inside of the company network, and

checking the NTP configuration is not relevant to this issue.
When a customer is having issues connecting to a website using a URL, one of the first troubleshooting steps a network administrator should take is attempting to connect to the site using the IP address of the website. This will help to determine if the issue is related to a DNS resolution problem or a connectivity problem. If the administrator is able to connect to the website using the IP address, then the issue may be related to a DNS problem. However, if the administrator is still unable to connect, then the issue may be related to a connectivity problem. In either case, further troubleshooting steps will be necessary. Checking for certificate issues or NTP configuration, and contacting the ISP would not be the BEST initial steps in this scenario.

NEW QUESTION 332
- (Exam 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%20n "To summarize this general best practice guide, you should NOT enable jumbo frame feature as a general home user."

NEW QUESTION 337
- (Exam Topic 3)
A malicious user is using special software 10 perform an on-path attack. Which of the following best practices should be configured to mitigate this threat?

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

Answer: A

NEW QUESTION 341
- (Exam Topic 3)
Which of the following protocols would enable a company to upgrade its internet connection by acquiring its own public IP prefixes and autonomous system number?

A. EIGRP
B. BGP
C. IPv6
D. MPLS

Answer: B

Explanation:
BGP is a routing protocol that is used to exchange routing information between different autonomous systems (ASes) on the internet. An autonomous system is a network or group of networks that is under the same administrative control and uses a common routing protocol. By acquiring its own public IP prefixes and autonomous system number, a company can use BGP to advertise these prefixes to other ASes and establish its own internet connection. This would enable the company to have more control over its internet connection and potentially improve its connectivity.EIGRP (Enhanced Interior Gateway Routing Protocol) is a routing protocol used within a single autonomous system, so it would not be used to establish a connection to the internet. IPv6 is a version of the Internet Protocol (IP) used to identify devices on a network. It is not a routing protocol and would not be used to establish an internet connection.MPLS (Multi-Protocol Label Switching) is a networking technology that is used to route packets between different networks. It is not a routing protocol and would not be used to establish an internet connection.

NEW QUESTION 346
- (Exam Topic 3)
A technician uses a badge to enter a security checkpoint on a corporate campus. An unknown individual quickly walks in behind the technician without speaking. Which of the following types of attacks did the technician experience?

A. Tailgating
B. Evil twin
C. On-path
D. Piggybacking

Answer: A

Explanation:
Tailgating is a type of physical security attack where an unauthorized person follows an authorized person into a restricted area without their consent or knowledge. Tailgating can allow an attacker to bypass security measures and gain access to sensitive information or resources. In this scenario, the technician experienced tailgating when the unknown individual walked in behind the technician without speaking. Piggybacking is similar to tailgating, but it involves the

consent or cooperation of the authorized person. Evil twin is a type of wireless network attack where an attacker sets up a rogue access point that mimics a legitimate one. On-path is a type of network attack where an attacker intercepts and modifies traffic between two parties.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.2: Given a scenario, use appropriate network hardening techniques.

NEW QUESTION 349
- (Exam Topic 3)
Classification using labels according to information sensitivity and impact in case of unauthorized access or leakage is a mandatory component of:

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

Answer: C

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

NEW QUESTION 352
- (Exam 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 354
- (Exam Topic 3)
A company's data center is hosted at its corporate office to ensure greater control over the security of sensitive data. During times when there are increased workloads, some of the company’s non-sensitive data is shifted to an external cloud provider. Which of the following cloud deployment models does this describe?

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

Answer: A

NEW QUESTION 359
- (Exam Topic 3)
A network engineer is designing a wireless network that has the following requirements:
• Network speed must be higher than 100Mbps
• Must use the 2.4GHz and 5GHz bands
Which of the following 802.11 standards should the engineer select?

A. 802. lla
B. 802.11b
C. 802. 11g
D. 802.11 n

Answer: D

Explanation:
* 802.11 n is a wireless standard that supports up to 600 Mbps data rate and operates in both the 2.4 GHz and 5 GHz frequency bands. 802.11n uses multiple-input multiple-output (MIMO) technology to increase the number of spatial streams and improve the wireless performance and range. 802.11n meets the requirements of the wireless network design.
References: Network+ Study Guide Objective 1.6: Explain the functions of network services.

NEW QUESTION 363
- (Exam Topic 3)
A network technician is troubleshooting a new web server connectivity issue. The network technician discovers the following on the support ticket
• The server's IP address can be pinged from the client PCs,
• Access to the web resource works correctly when on the server's console.
• No clients can access the servers data via URL.
• The server does not have a firewall configured
• No ACLs are preventing connectivity from the client's network.
• All services on the server are operating normally, which was confirmed by the server team. Which of the following actions will resolve the issue?

A. Reset port security on the switchport connecting the server.
B. Adjust the web server's NTP settings to match the client settings.
C. Configure A records for the web server.

D. Install the correct MIB on the web server

Answer: C

Explanation:
The problem is likely related to DNS resolution, as the clients are able to ping the server's IP address but not access the web resource via URL. The other answers do not address this issue. Configuring A records for the web server will ensure that clients are able to access the web resource via its domain name.

NEW QUESTION 364
- (Exam Topic 3)
A network administrator is creating a subnet for a remote office that has 53 network devices. An additional requirement is to use the most efficient subnet. Which of the following CIDR notations indicates the appropriate number of IP addresses with the LEAST amount of unused addresses? (Choose Correct option and give explanation directly from CompTIA Network+ Study guide or documents)

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

Answer: B

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

NEW QUESTION 367
- (Exam Topic 3)
At which of the following OSI model layers does a MAC filter list for a wireless infrastructure operate?

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

Answer: D

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

NEW QUESTION 370
- (Exam 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 373
- (Exam Topic 3)
A company is deploying a SAN at headquarters and a branch office 1, 000ml (1,609km) away that w« access small amounts of data. Which of the following types of connections would be MOST cost effective to implement?

A. ISCSI
B. FCoE
C. Ethernet
D. FC

Answer: A

Explanation:
Mike Meyers
"Internet Small Computer Systems Interface (iSCSI) is built on top of TCP/IP, enabling devices that use the SCSI protocol to communicate across existing networks using cheap, readily available hardware."
Jason Dion "iSCSI (IP Small Computer System Interface)
- Lower cost, built using Ethernet switches (<10 Gbps)
- Relies on configuration allowing jumbo frames over the network"

NEW QUESTION 377
- (Exam Topic 3)
While setting up a new workstation, a technician discovers that the network connection is only 100 full duplex (FD), although it is connected to a gigabit switch. While reviewing the interface information in the switch CLI, the technician notes the port is operating at IOOFD but Shows many RX and TX errors. The technician moves the computer to another switchport and experiences the same issues.
Which of the following is MOST likely the cause of the low data rate and port errors?

A. Bad switch ports
B. Duplex issues
C. Cable length
D. Incorrect pinout

Answer: B

NEW QUESTION 381
- (Exam Topic 3)
A company joins a bank's financial network and establishes a connection to the clearinghouse servers in the range 192 168.124.0/27. An IT technician then realizes the range exists within the VM pool at the data center. Which of the following is the BEST way for the technician to connect to the bank's servers?

A. NAT
B. PAT
C. CIDR
D. SLAAC

Answer: A

NEW QUESTION 383
- (Exam Topic 3)
A company needs to virtualize a replica of its internal physical network without changing the logical topology and the way that devices behave and are managed. Which of the following technologies meets this requirement?

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

Answer: A

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

NEW QUESTION 384
- (Exam Topic 3)
A network technician is hired to review all the devices within a network and make recommendations to improve network efficiency. Which of the following should the technician do FIRST before reviewing and making any recommendations?

A. Capture a network baseline
B. Perform an environmental review.
C. Read the network logs
D. Run a bandwidth test

Answer: A

Explanation:
Before making any recommendations, a network technician should first capture a network baseline, which is a snapshot of the current performance of the network. This will give the technician a baseline to compare against after any changes are made. According to the CompTIA Network+ Study Manual, the technician should "capture the state of the network before making any changes and then compare the performance after the changes have been made. This will provide an accurate baseline to compare the performance of the network before and after the changes have been made."

NEW QUESTION 387
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

N10-009 Practice Exam Features:

* N10-009 Questions and Answers Updated Frequently

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

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

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