CompTIA

Exam Questions N10-009

CompTIA Network+ Exam

NEW QUESTION 1
- (Exam Topic 1)
A network technician is installing new software on a Windows-based server in a different geographical location. Which of the following would be BEST for the technician to use to perform this task?

A. RDP
B. SSH
C. FTP
D. DNS

Answer: A

Explanation:
RDP (Remote Desktop Protocol) is the best option for a network technician to use when installing new
software on a Windows-based server in a different geographical location. This protocol allows the technician to connect to the server remotely and control it as if they were physically present.
References:
Network+ N10-007 Certification Exam Objectives, Objective 2.2: Given a scenario, implement the appropriate network-based security and troubleshoot common connectivity issues.

NEW QUESTION 2
- (Exam Topic 1)
A company built a new building at its headquarters location. The new building is connected to the company's LAN via fiber-optic cable. Multiple users in the new building are unable to access the company's intranet site via their web browser, but they are able to access internet sites. Which of the following describes how the network administrator can resolve this issue?

A. Correct the DNS server entries in the DHCP scope
B. Correct the external firewall gateway address
C. Correct the NTP server settings on the clients
D. Correct a TFTP Issue on the company's server

Answer: A

Explanation:
If multiple users in a new building are unable to access the company's intranet site via their web browser but are able to access internet sites, the network administrator can resolve this issue by correcting the DNS server entries in the DHCP scope. The DHCP scope is responsible for assigning IP addresses and DNS server addresses to clients. If the DNS server entries are incorrect, clients will not be able to access intranet sites.
References:
CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 4: Network Implementations, Objective 4.4: Explain the purpose and properties of DHCP.

NEW QUESTION 3
- (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 4
- (Exam Topic 1)
A technician is installing a high-density wireless network and wants to use an available frequency that supports the maximum number of channels to reduce interference. Which of the following standard 802.11 frequency ranges should the technician look for while reviewing WAP specifications?

A. 2.4GHz
B. 5GHz
C. 6GHz
D. 900MHz

Answer: B

Explanation:
* 802.11 a/b/g/n/ac wireless networks operate in two frequency ranges: 2.4 GHz and 5 GHz. The 5 GHz frequency range supports more channels than the 2.4 GHz frequency range, making it a better choice for high-density wireless networks.
References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 5
- (Exam Topic 1)
Wireless users are reporting intermittent internet connectivity. Connectivity is restored when the users disconnect and reconnect, utilizing the web authentication

process each time. The network administrator can see the devices connected to the APs at all times. Which of the following steps will MOST likely determine the cause of the issue?

A. Verify the session time-out configuration on the captive portal settings
B. Check for encryption protocol mismatch on the client's wireless settings
C. Confirm that a valid passphrase is being used during the web authentication
D. Investigate for a client's disassociation caused by an evil twin AP

Answer: A

Explanation:
A captive portal is a web page that requires users to authenticate before they can access the internet. If the session time-out configuration is too short, users may experience intermittent internet connectivity and have to reconnect using the web authentication process each time. The network administrator can verify the session time-out configuration on the captive portal settings and adjust it if needed. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 1.0 Network Architecture, Objective 1.8 Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 6
- (Exam Topic 1)
At which of the following OSI model layers would a technician find an IP header?

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 4

Answer: C

Explanation:
An IP header can be found at the third layer of the OSI model, also known as the network layer. This layer is responsible for logical addressing, routing, and forwarding of data packets.
References:
- CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: Network Models, p. 82

NEW QUESTION 7
- (Exam Topic 1)
An attacker is attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt. Which of the following attack types BEST describes this action?

A. Pass-the-hash attack
B. Rainbow table attack
C. Brute-force attack
D. Dictionary attack

Answer: D

Explanation:
The attacker attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt is using a dictionary attack.
References: CompTIA Network+ Certification Study Guide, Chapter 6: Network Attacks and Mitigation.

NEW QUESTION 8
- (Exam Topic 1)
A workstation is configured with the following network details:

IP address	Subnet mask	Default gateway
10.1.2.23	10.1.2.0/27	10.1.2.1

Software on the workstation needs to send a query to the local subnet broadcast address. To which of the following addresses should the software be configured to send the query?

A. 10.1.2.0
B. 10.1.2.1
C. 10.1.2.23
D. 10.1.2.255
E. 10.1.2.31

Answer: D

Explanation:
The software on the workstation should be configured to send the query to 10.1.2.255, which is the local subnet broadcast address. A broadcast address is a special address that allows a device to send a message to all devices on the same subnet. It is usually derived by setting all the host bits to 1 in the network address. In this case, the network address is 10.1.2.0/27, which has 27 network bits and 5 host bits. By setting all the host bits to 1, we get 10.1.2.31 as the broadcast address in decimal notation, or 10.1.2.255 in dotted decimal notation. References: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

NEW QUESTION 9
- (Exam Topic 1)
A network administrator is installing a wireless network at a client's office. Which of the following IEEE 802.11 standards would be BEST to use for multiple simultaneous client access?

A. CDMA
B. CSMA/CD
C. CSMA/CA
D. GSM

Answer: C

Explanation:
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is an IEEE 802.11 standard that would be best to use for multiple simultaneous client access on a wireless network. CSMA/CA is a media access control method that allows multiple devices to share the same wireless channel without causing collisions or interference. It works by having each device sense the channel before transmitting data and waiting for an acknowledgment from the receiver after each transmission. If the channel is busy or no acknowledgment is received, the device will back off and retry later with a random delay. References: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-csma-ca.html

NEW QUESTION 10
- (Exam Topic 1)
A network administrator discovers that users in an adjacent building are connecting to the company's guest wireless network to download inappropriate material. Which of the following can the administrator do to MOST easily mitigate this issue?

A. Reduce the wireless power levels
B. Adjust the wireless channels
C. Enable wireless client isolation
D. Enable wireless port security

Answer: A

Explanation:
Reducing the wireless power levels can limit the range of the guest wireless network and prevent users in an adjacent building from connecting to it. Adjusting the wireless channels or enabling wireless client isolation will not affect the signal strength or coverage of the guest network. Enabling wireless port security will not work on a guest network that does not use authentication or MAC address filtering. References: CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006), Domain 2.0 Network Operations, Objective 2.5 Given a scenario, implement appropriate wireless configuration settings; Guest WiFi Security - Cisco Umbrella

NEW QUESTION 10
- (Exam Topic 1)
The management team needs to ensure unnecessary modifications to the corporate network are not permitted and version control is maintained. Which of the following documents would BEST support this?

A. An incident response plan
B. A business continuity plan
C. A change management policy
D. An acceptable use policy

Answer: C

Explanation:
A change management policy is a document that outlines the procedures and guidelines for making changes to a network or system, including how changes are approved, tested, and implemented. By following a change management policy, organizations can ensure that unnecessary modifications to the network are not permitted and version control is maintained. References:
> Network+ N10-008 Objectives: 1.6 Given a scenario, implement network configuration and change management best practices.

NEW QUESTION 15
- (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 19

- (Exam Topic 1)
A network engineer performs the following tasks to increase server bandwidth: Connects two network cables from the server to a switch stack
Configure LACP on the switchports
Verifies the correct configurations on the switch interfaces Which of the following needs to be configured on the server?

A. Load balancing
B. Multipathing
C. NIC teaming
D. Clustering

Answer: C

Explanation:
NIC teaming is a technique that combines two or more network interface cards (NICs) on a server into a single logical interface that can increase bandwidth, provide redundancy, and balance traffic. NIC teaming can be configured with different modes and algorithms depending on the desired outcome. Link Aggregation Control Protocol (LACP) is a protocol that enables NIC teaming by dynamically bundling multiple links between two devices into one logical link. References: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming/nic-teaming

NEW QUESTION 20
- (Exam Topic 1)
Several WIFI users are reporting the inability to connect to the network. WLAN users on the guest network are able to access all network resources without any performance issues. The following table summarizes the findings after a site survey of the area in question:

Location	AP 1	AP 2	AP 3	AP 4
SSID	Corp1	Corp1	Corp1/Guest	Corp1/Guest
Channel	2	1	5	11
RSSI	-81dBm	-82dBm	-44dBm	-41dBm
Antenna type	Omni	Omni	Directional	Directional

Which of the following should a wireless technician do NEXT to troubleshoot this issue?

A. Reconfigure the channels to reduce overlap
B. Replace the omni antennas with directional antennas
C. Update the SSIDs on all the APs
D. Decrease power in AP 3 and AP 4

Answer: A

Explanation:
Based on the site survey table, we can see that AP 2, AP 3, and AP 4 are all broadcasting on the same channel, which can cause interference and affect performance. Therefore, the next step a wireless technician should take to troubleshoot this issue is to reconfigure the channels to reduce overlap. This will help to improve network performance and eliminate any interference.
References:
- Network+ N10-007 Certification Exam Objectives, Objective 2.8: Given a scenario, troubleshoot common wireless problems and perform site surveys.

NEW QUESTION 25
- (Exam Topic 1)
Given the following information:

Protocol	Local address	Foreign address	State
TCP	127.0.0.1:57779	Desktop-Open:57780	Established
TCP	127.0.0.1:57780	Desktop-Open:57779	Established

Which of the following command-line tools would generate this output?

A. netstat
B. arp
C. dig
D. tracert

Answer: D

Explanation:
Tracert is a command-line tool that traces the route of a packet from a source to a destination and displays the number of hops and the round-trip time for each hop. The output shown in the question is an example of a tracert output, which shows five hops with their IP addresses and hostnames (if available) and three latency measurements for each hop in milliseconds. References:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.lumen.com/help/en-us/network/traceroute/understanding-the-traceroute-output.html

NEW QUESTION 26
- (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 29
- (Exam Topic 1)
Which of the following types of devices can provide content filtering and threat protection, and manage multiple IPSec site-to-site connections?

A. Layer 3 switch
B. VPN headend
C. Next-generation firewall
D. Proxy server
E. Intrusion prevention

Answer: C

Explanation:
Next-generation firewalls can provide content filtering and threat protection, and can manage multiple IPSec site-to-site connections. References: CompTIA Network+ Certification Study Guide, Chapter 5: Network Security.

NEW QUESTION 30
- (Exam Topic 1)
Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

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

Answer: B

Explanation:
TACACS+ (Terminal Access Controller Access Control System Plus) can be used to centrally manage credentials for various types of administrative privileges on configured network devices. This protocol separates authentication, authorization, and accounting (AAA) functions, providing more granular control over access to network resources.
References:
- Network+ N10-007 Certification Exam Objectives, Objective 4.2: Given a scenario, implement secure network administration principles.

NEW QUESTION 34
- (Exam Topic 1)
Which of the following is used to track and document various types of known vulnerabilities?

A. CVE
B. Penetration testing
C. Zero-day
D. SIEM
E. Least privilege

Answer: A

Explanation:
CVE stands for Common Vulnerabilities and Exposures, which is a list of publicly disclosed cybersecurity vulnerabilities that is free to search, use, and incorporate into products and services. CVE provides a standardized identifier and description for each vulnerability, as well as references to related sources of information. CVE helps to track and document various types of known vulnerabilities and facilitates communication and coordination among security professionals. References: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://cve.mitre.org/cve/

NEW QUESTION 37
- (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 40
- (Exam Topic 1)
A new cabling certification is being requested every time a network technician rebuilds one end of a Cat 6 (vendor-certified) cable to create a crossover connection that is used to connect switches. Which of the following would address this issue by allowing the use of the original cable?

A. CSMA/CD
B. LACP
C. PoE+
D. MDIX

Answer: D

Explanation:
MDIX (medium-dependent interface crossover) is a feature that allows network devices to automatically detect and configure the appropriate cabling type, eliminating the need for crossover cables. By enabling
MDIX on the switches, a technician can use the original Cat 6 cable to create a crossover connection. References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 41
- (Exam Topic 1)
Within the realm of network security, Zero Trust:

A. prevents attackers from moving laterally through a system.
B. allows a server to communicate with outside networks without a firewall.
C. block malicious software that is too new to be found in virus definitions.
D. stops infected files from being downloaded via websites.

Answer: A

Explanation:
Zero Trust is a security framework that requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust prevents attackers from moving laterally through a system by applying granular policies and controls based on the principle of least privilege and by segmenting and encrypting data flows across the network. References: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

NEW QUESTION 43
- (Exam Topic 1)
A technician receives feedback that some users are experiencing high amounts of jitter while using the wireless network. While troubleshooting the network, the technician uses the ping command with the IP address of the default gateway and verifies large variations in latency. The technician thinks the issue may be interference from other networks and non-802.11 devices. Which of the following tools should the technician use to troubleshoot the issue?

A. NetFlow analyzer
B. Bandwidth analyzer
C. Protocol analyzer
D. Spectrum analyzer

Answer: D

Explanation:
A spectrum analyzer is a tool that measures the frequency and amplitude of signals in a wireless network. It can be used to troubleshoot issues related to interference from other networks and non-802.11 devices, such as microwave ovens or cordless phones, by identifying the sources and levels of interference in the wireless spectrum. A spectrum analyzer can also help to optimize the channel selection and placement of wireless access points. References: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.flukenetworks.com/blog/cabling-chronicles/what-spectrum-analyzer-and-how-do-you-use-it

NEW QUESTION 46
- (Exam Topic 1)
Which of the following is the LARGEST MTU for a standard Ethernet frame?

A. 1452
B. 1492
C. 1500
D. 2304

Answer: C

Explanation:
The maximum transmission unit (MTU) is the largest size of a data packet that can be transmitted over a network. A standard Ethernet frame supports an MTU of 1500 bytes, which is the default value for most Ethernet networks. Larger MTUs are possible with jumbo frames, but they are not widely supported and may cause fragmentation or compatibility issues. References:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0),
https://en.wikipedia.org/wiki/Maximum_transmission_unit

NEW QUESTION 51
- (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 55
- (Exam Topic 1)
A network device is configured to send critical events to a syslog server; however, the following alerts are not being received:
Severity 5 LINK-UPDOWN: Interface 1/1, changed state to down Severity 5 LINK-UPDOWN: Interface 1/3, changed state to down
Which of the following describes the reason why the events are not being received?

A. The network device is not configured to log that level to the syslog server
B. The network device was down and could not send the event
C. The syslog server is not compatible with the network device
D. The syslog server did not have the correct MIB loaded to receive the message

Answer: A

Explanation:
The reason why the alerts are not being received is that the network device is not configured to log that level to the syslog server. The severity level for the events may need to be adjusted in order for them to be sent to the syslog server. References: Network+ Certification Study Guide, Chapter 8: Network Troubleshooting

NEW QUESTION 60
- (Exam Topic 1)
The network administrator is informed that a user's email password is frequently hacked by brute-force programs. Which of the following policies should the network administrator implements to BEST mitigate this issue? (Choose two.)

A. Captive portal
B. Two-factor authentication
C. Complex passwords
D. Geofencing
E. Role-based access
F. Explicit deny

Answer: BC

Explanation:
Two-factor authentication (2FA) is a method of verifying a user's identity by requiring two pieces of evidence, such as something the user knows (e.g., a password) and something the user has (e.g., a token or a smartphone). 2FA adds an extra layer of security that makes it harder for hackers to access a user's account by brute-force programs. Complex passwords are passwords that are long, random, and use a combination of uppercase and lowercase letters, numbers, and symbols. Complex passwords are more resistant to brute-force attacks than simple or common passwords. References: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0),https://www.csoonline.com/article/3225913/what-is-two-factor-authentication-2fa-how-to-enable-it-and-why-yo https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/

NEW QUESTION 64
- (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 69
- (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

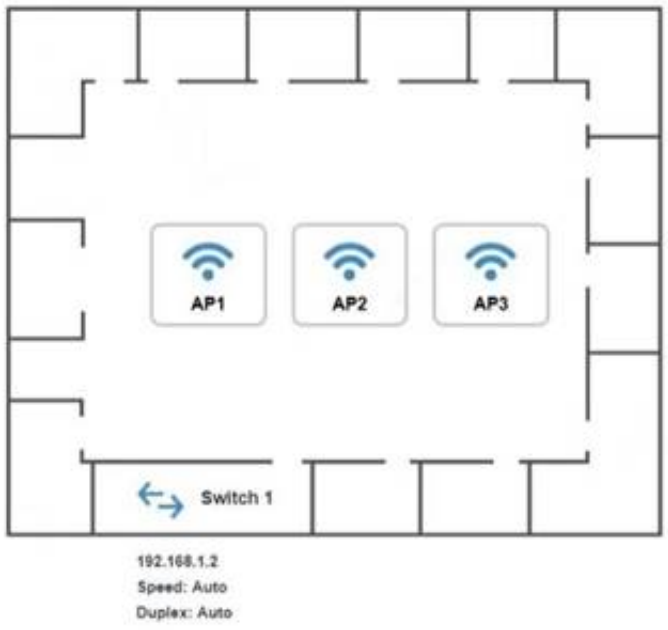
NEW QUESTION 74
- (Exam Topic 1)
A website administrator is concerned the company's static website could be defaced by hacktivists or used as a pivot point to attack internal systems. Which of the following should a network security administrator recommend to assist with detecting these activities?

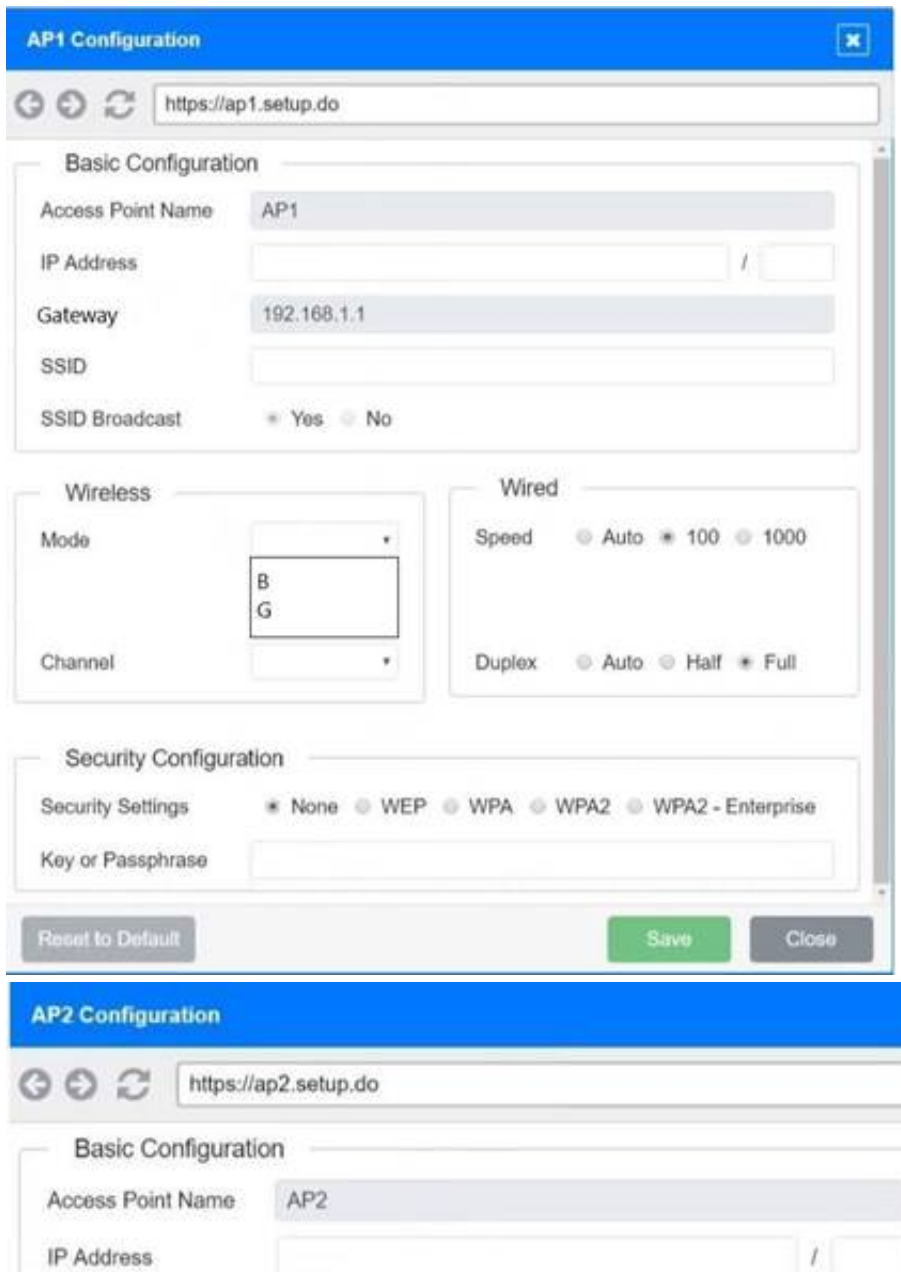
A. Implement file integrity monitoring.
B. Change the default credentials.
C. Use SSL encryption.
D. Update the web-server software.

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 75
- (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.



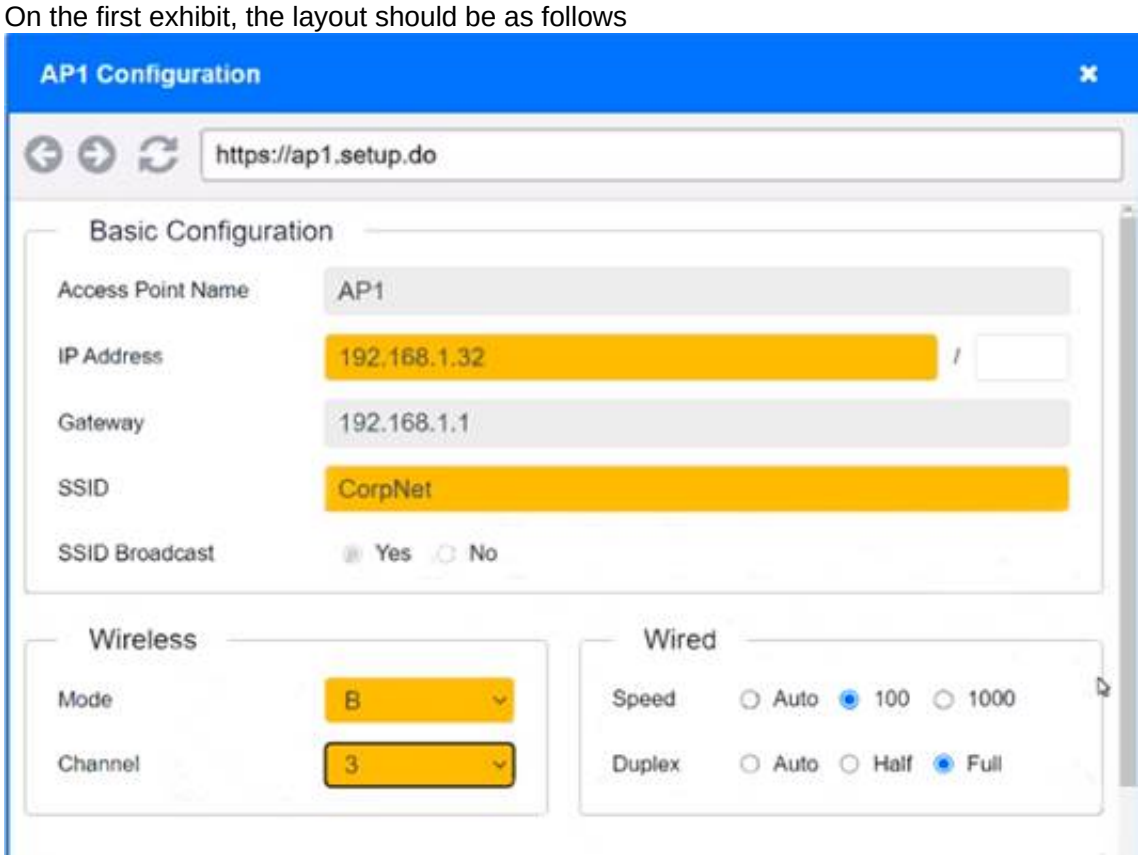

AP1 Configuration
https://ap1.setup.do
Basic Configuration
Access Point Name
AP1
IP Address
Gateway
192.168.1.1
SSID
SSID Broadcast
Yes
No
Wireless
Mode
B
G
Channel
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase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


AP2 Configuration
https://ap2.setup.do
Basic Configuration
Access Point Name
AP2
IP Address
Gateway
192.168.1.1
SSID
SSID Broadcast
Yes
No
Wireless
Mode
B
G
Channel
1
2
3
4
5
6
7
8
9
10
11
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

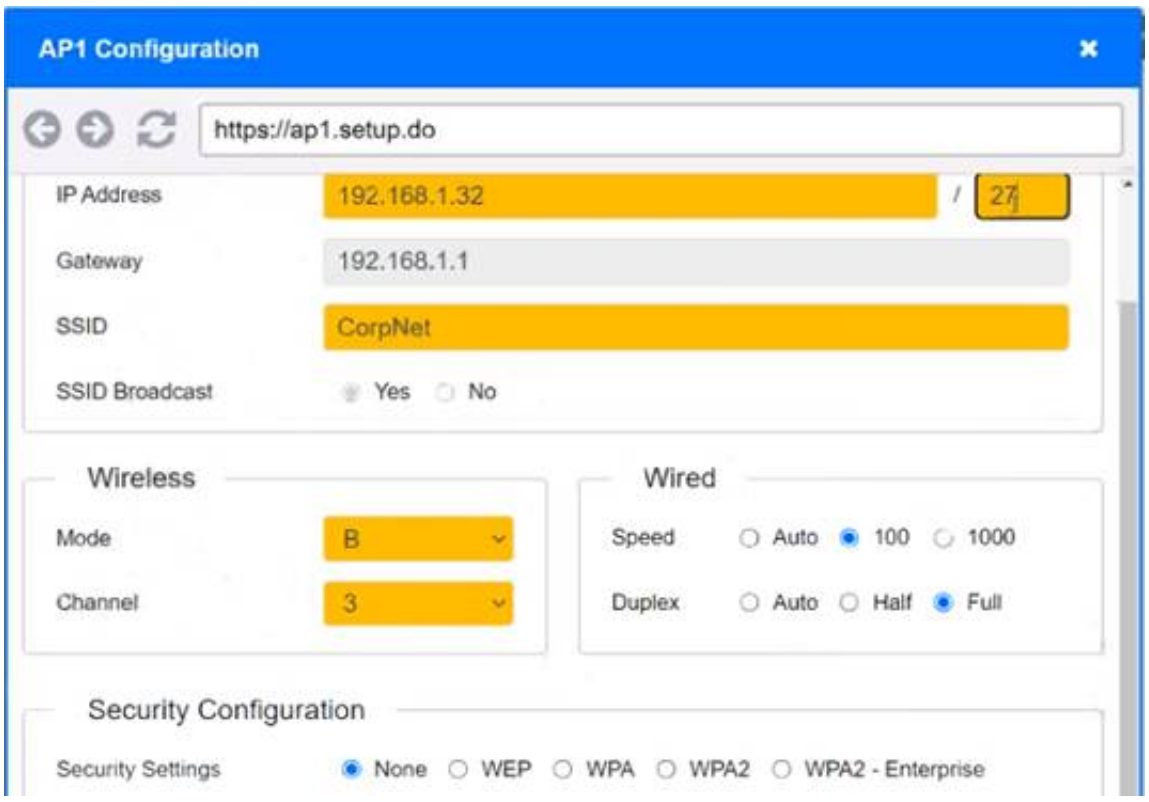
Answer: A

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

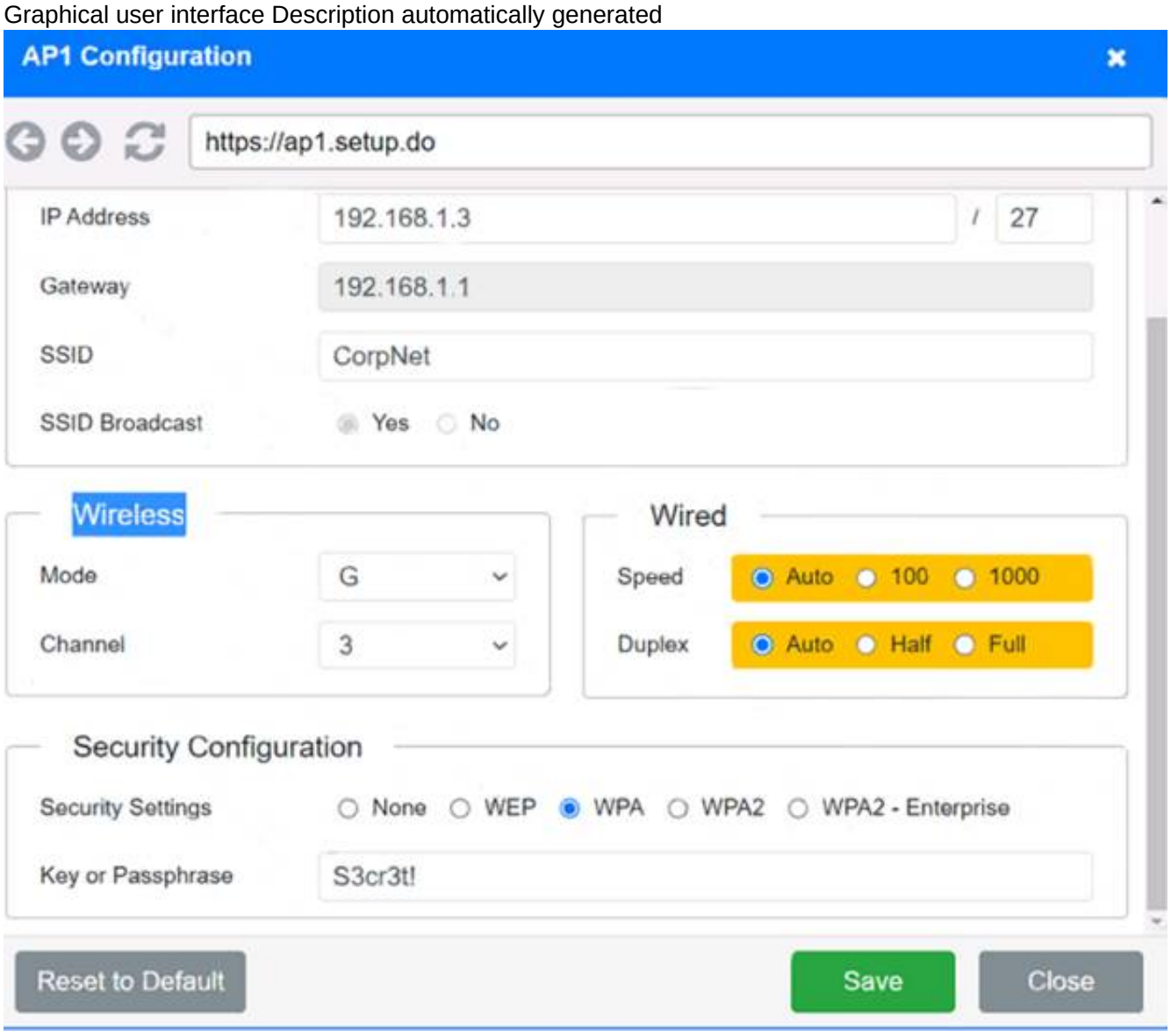
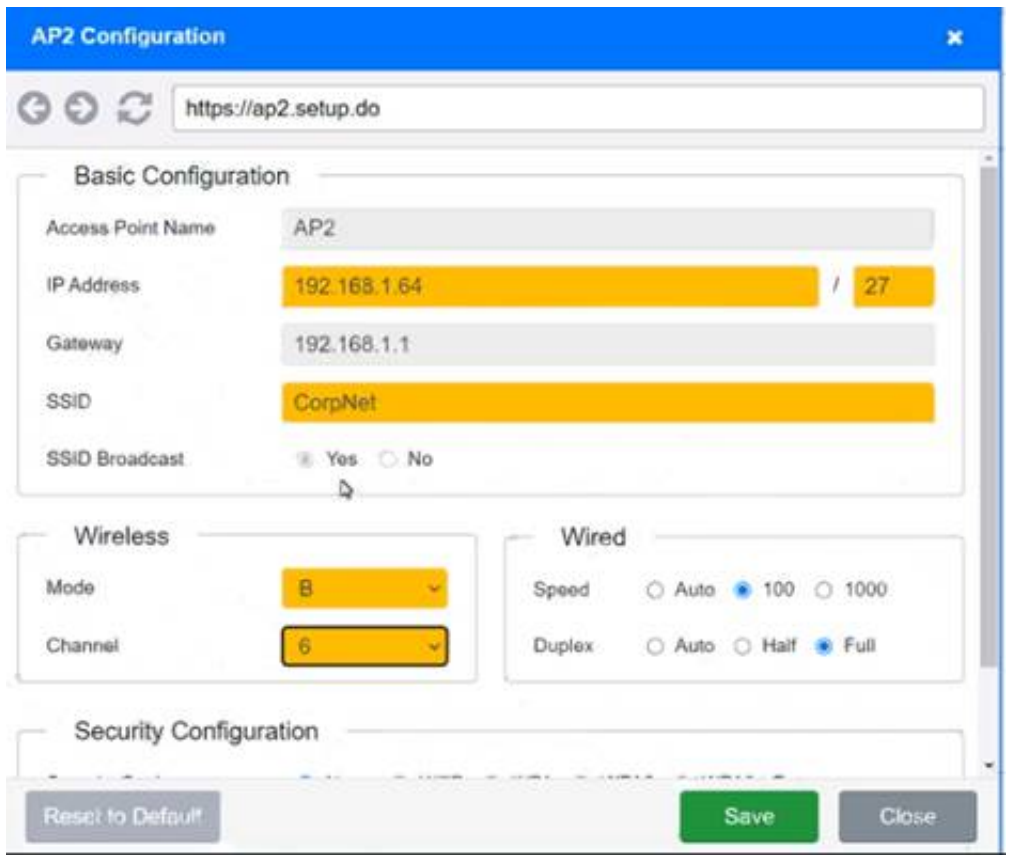


Exhibit 2 as follows Access Point Name AP2
Graphical user interface Description automatically generated



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

Graphical user interface Description automatically generated

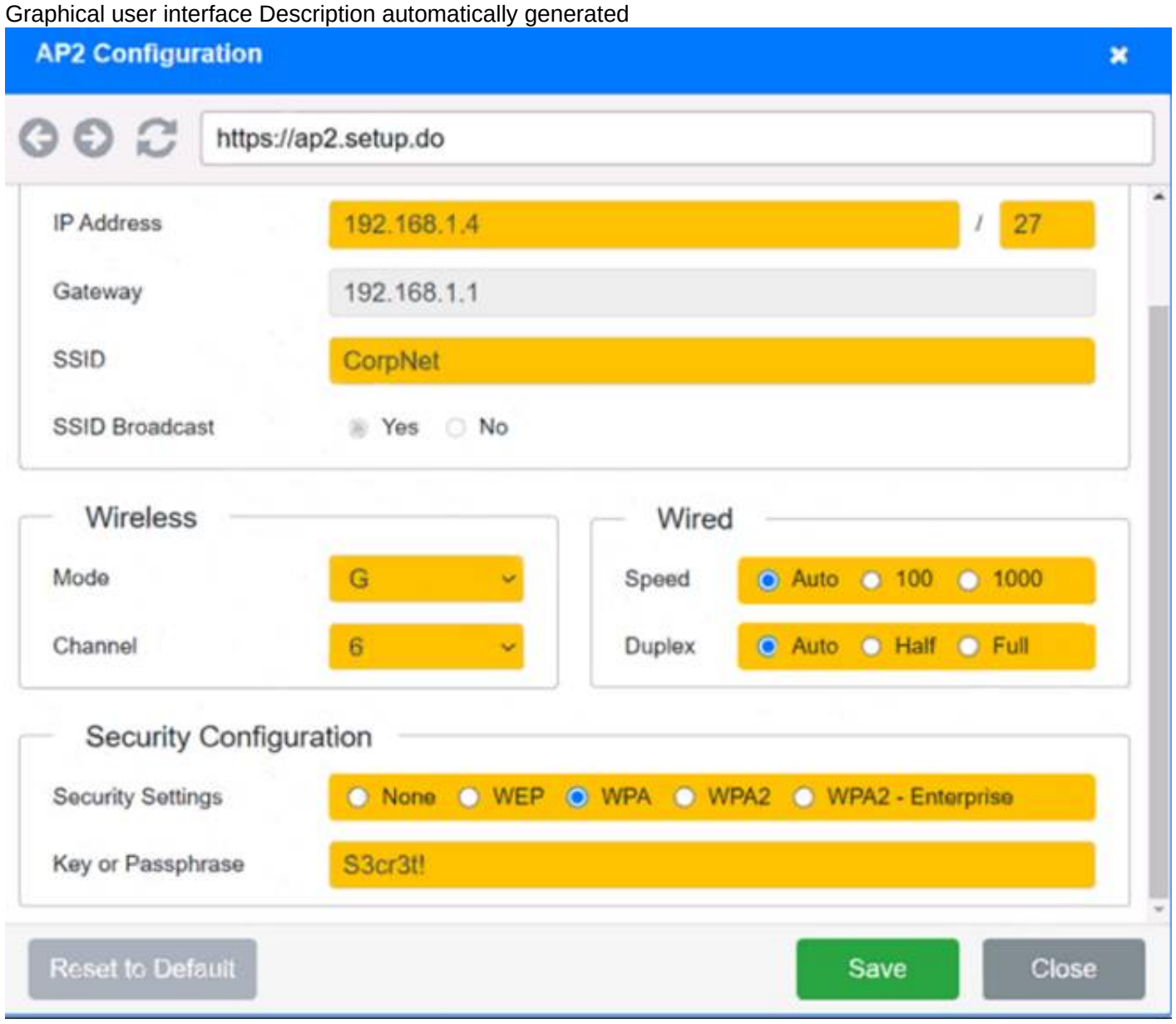
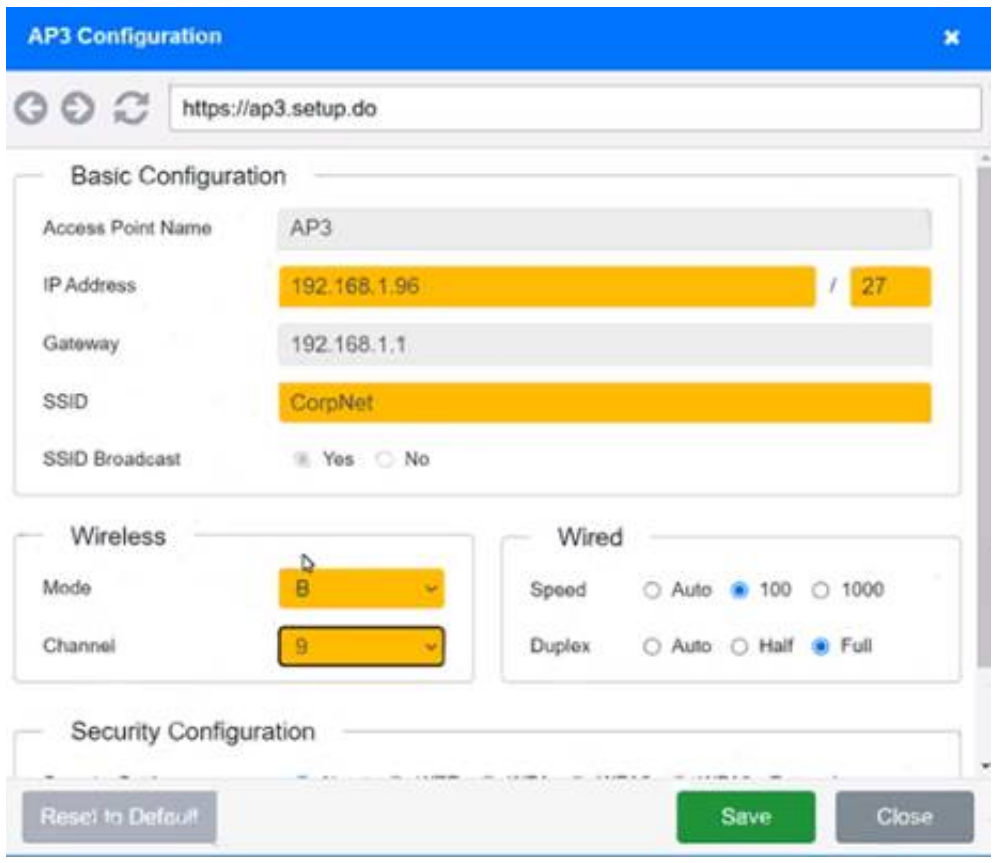
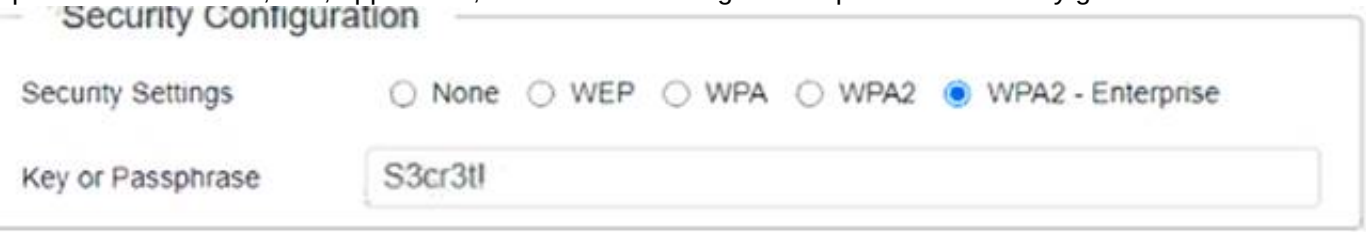


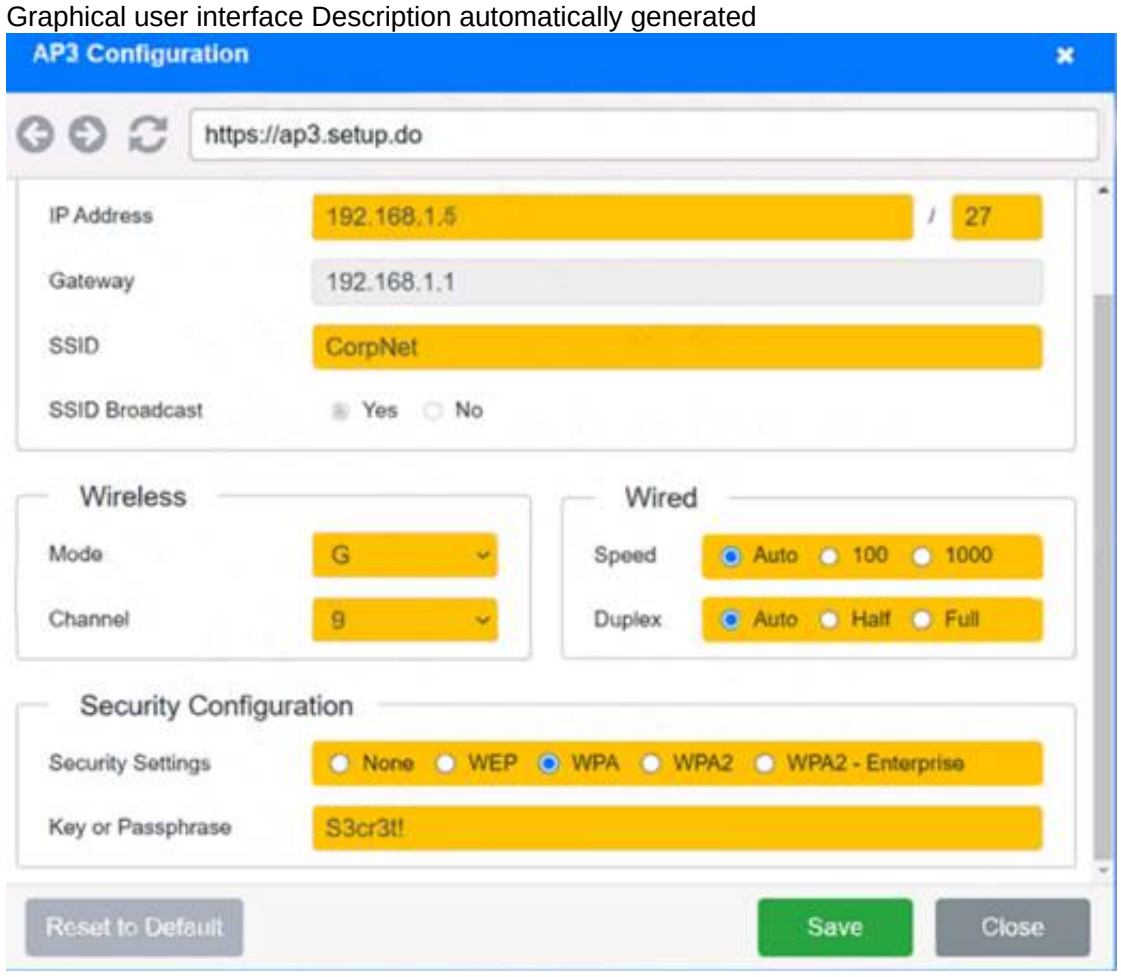
Exhibit 3 as follows Access Point Name AP3
Graphical user interface Description automatically generated



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



Graphical user interface Description automatically generated



NEW QUESTION 78
- (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 79
- (Exam Topic 1)
Which of the following factors should be considered when evaluating a firewall to protect a datacenter's east-west traffic?

A. Replication traffic between an on-premises server and a remote backup facility
B. Traffic between VMs running on different hosts
C. Concurrent connections generated by Internet DDoS attacks
D. VPN traffic from remote offices to the datacenter's VMs

Answer: B

Explanation:
When evaluating a firewall to protect a datacenter's east-west traffic, it is important to consider traffic between VMs running on different hosts. This type of traffic is referred to as east-west traffic and is often protected by internal firewalls. By implementing firewalls, an organization can protect their internal network against threats such as lateral movement, which can be caused by attackers who have breached a perimeter firewall. References: Network+ Certification Study Guide, Chapter 5: Network Security

NEW QUESTION 82
- (Exam Topic 1)
An IT organization needs to optimize speeds for global content distribution and wants to reduce latency in high-density user locations. Which of the following technologies BEST meets the organization's requirements?

A. Load balancing
B. Geofencing
C. Public cloud
D. Content delivery network
E. Infrastructure as a service

Answer: D

Explanation:
A content delivery network (CDN) is a distributed network of servers that delivers web content to users based on their geographic location. By replicating content across multiple servers in various locations, a CDN can optimize speed and reduce latency in high-density user locations.

NEW QUESTION 87
- (Exam Topic 1)
A technician is assisting a user who cannot connect to a network resource. The technician first checks for a link light. According to troubleshooting methodology, this is an example of:

A. using a bottom-to-top approach.
B. establishing a plan of action.
C. documenting a finding.
D. questioning the obvious.

Answer: A

Explanation:
Using a bottom-to-top approach means starting from the physical layer and moving up the OSI model to troubleshoot a network problem. Checking for a link light is a physical layer check that verifies the connectivity of the network cable and device. References:
https://www.professormesser.com/network-plus/n10-007/troubleshooting-methodologies-2/

NEW QUESTION 89
- (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 94
- (Exam Topic 1)
Which of the following service models would MOST likely be used to replace on-premises servers with a cloud solution?

A. PaaS
B. IaaS
C. SaaS
D. Disaster recovery as a Service (DRaaS)

Answer: B

Explanation:
IaaS stands for Infrastructure as a Service, which is a cloud service model that provides virtualized computing resources over the Internet, such as servers, storage, networking, and operating systems. IaaS allows customers to replace their on-premises servers with cloud servers that can be scaled up or down on demand and pay only for what they use. PaaS stands for Platform as a Service, which provides customers with a cloud-based platform for developing, testing, and deploying applications without managing the underlying infrastructure. SaaS stands for Software as a Service, which provides customers with access to cloud-based software applications over the Internet without installing or maintaining them on their devices. Disaster recovery as a Service (DRaaS) is a type of cloud service that provides customers with backup and recovery solutions for their data and applications in case of a disaster.

NEW QUESTION 99
- (Exam Topic 1)
Which of the following BEST describes a network appliance that warns of unapproved devices that are accessing the network?

A. Firewall
B. AP
C. Proxy server
D. IDS

Answer: D

Explanation:
IDS stands for intrusion detection system, which is a network appliance that monitors network traffic and alerts administrators of any suspicious or malicious activity. An IDS can warn of unapproved devices that are accessing the network by detecting anomalies, signatures, or behaviors that indicate unauthorized access attempts or attacks. References:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.cisco.com/c/en/us/products/security/what-is-an-intrusion-detection-system-ids.html

NEW QUESTION 102
- (Exam Topic 1)
A network technician needs to ensure outside users are unable to telnet into any of the servers at the datacenter. Which of the following ports should be blocked when checking firewall configuration?

A. 22
B. 23
C. 80
D. 3389
E. 8080

Answer: B

Explanation:
Port 23 should be blocked when checking firewall configuration to prevent outside users from telnetting into any of the servers at the datacenter. Port 23 is the default port for Telnet, which is an insecure protocol that allows remote access to servers and network devices. Telnet sends data in clear text, which can be easily intercepted and compromised by attackers. A more secure alternative is SSH, which uses port 22 and encrypts data. References:
https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

NEW QUESTION 103
- (Exam Topic 1)
You are tasked with verifying the following requirements are met in order to ensure network security. Requirements:
Datacenter
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic Building A
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
Provide devices to support 5 additional different office users
Add an additional mobile user
Replace the Telnet server with a more secure solution Screened subnet
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
Provide a server to handle external 80/443 traffic Provide a server to handle port 20/21 traffic INSTRUCTIONS
Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.
Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Screened Subnet devices – Web server, FTP server
Building A devices – SSH server top left, workstations on all 5 on the right, laptop on bottom left DataCenter devices – DNS server.

NEW QUESTION 106
- (Exam Topic 1)
Which of the following would MOST likely be used to review previous upgrades to a system?

A. Business continuity plan
B. Change management
C. System life cycle
D. Standard operating procedures

Answer: B

Explanation:
Change management is the process of reviewing previous upgrades to a system. It is a systematic approach to managing changes to an organization's IT systems and infrastructure. Change management involves the assessment of potential risks associated with a change, as well as the identification of any necessary resources required to implement the change. References: Network+ Certification Study Guide, Chapter 8: Network Troubleshooting

NEW QUESTION 109
- (Exam Topic 1)
A network technician is manually configuring the network settings for a new device and is told the network block is 192.168.0.0/20. Which of the following subnets should the technician use?

A. 255.255.128.0
B. 255.255.192.0
C. 255.255.240.0
D. 255.255.248.0

Answer: C

Explanation:
A subnet mask is a binary number that indicates which bits of an IP address belong to the network portion and which bits belong to the host portion. A slash notation (/n) indicates how many bits are used for the network portion. A /20 notation means that 20 bits are used for the network portion and 12 bits are used for the host portion. To convert /20 to a dotted decimal notation, we need to write 20 ones followed by 12 zeros in binary and then divide them into four octets separated by dots. This gives us 11111111.11111111.11110000.00000000 or 255.255.240.0 in decimal. References: https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0), https://www.techopedia.com/definition/950/subnet-mask

NEW QUESTION 111
- (Exam Topic 2)
A network technician needs to correlate security events to analyze a suspected intrusion. Which of the following should the technician use?

A. SNMP
B. Log review
C. Vulnerability scanning
D. SIEM

Answer: D

Explanation:
SIEM stands for Security Information and Event Management, which is a tool that collects, analyzes, and correlates data from various network devices and sources to provide alerts and reports on security incidents and events. A network technician can use SIEM to correlate security events to analyze a suspected intrusion, as SIEM can help identify the source, target, method, and impact of an attack, as well as provide recommendations for remediation. References: https://www.comptia.org/blog/what-is-siem

NEW QUESTION 112
- (Exam Topic 2)
Which of the following services can provide data storage, hardware options, and scalability to a third-party company that cannot afford new devices?

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

Answer: B

Explanation:
IaaS stands for Infrastructure as a Service, which is a cloud computing model that provides virtualized computing resources such as servers, storage, and networking over the Internet. IaaS can provide data storage, hardware options, and scalability to a third-party company that cannot afford new devices by allowing them to rent or lease the infrastructure they need from a cloud provider. The company can pay only for what they use and scale up or down as needed. References: https://www.comptia.org/blog/what-is-iaas

NEW QUESTION 113
- (Exam Topic 2)
A SaaS provider has decided to leave an unpatched VM available via a public DMZ port. With which of the following concepts is this technique MOST closely associated?

A. Insider threat
B. War driving
C. Evil twin
D. Honeypot

Answer: D

Explanation:
A honeypot is a decoy system that is intentionally left vulnerable or exposed to attract attackers and divert them from the real targets. A honeypot can also be used to collect information about the attackers' techniques and motives. In the scenario, the SaaS provider has left an unpatched VM available via a public DMZ port, which could be a honeypot technique to lure attackers and monitor their activities. References: https://www.comptia.org/blog/what-is-a-honeypot

NEW QUESTION 115
- (Exam Topic 2)
A network technician is observing the behavior of an unmanaged switch when a new device is added to the network and transmits data. Which of the following BEST describes how the switch processes this information?

A. The data is flooded out of every por
B. including the one on which it came in.
C. The data is flooded out of every port but only in the VLAN where it is located.
D. The data is flooded out of every port, except the one on which it came in
E. The data is flooded out of every port, excluding the VLAN where it is located

Answer: C

Explanation:
The switch processes the data by flooding it out of every port, except the one on which it came in. Flooding is a process where a switch sends a data frame to all ports except the source port when it does not have an entry for the destination MAC address in its MAC address table. Flooding allows the switch to learn the MAC addresses of the devices connected to its ports and update its MAC address table accordingly. Flooding also ensures that the data frame reaches its intended destination, even if the switch does not know its location. References: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10556-16.html

NEW QUESTION 117
- (Exam Topic 2)
A network administrator wants to analyze attacks directed toward the company's network. Which of the following must the network administrator implement to assist in this goal?

A. A honeypot
B. Network segmentation
C. Antivirus
D. A screened subnet

Answer: A

Explanation:
A honeypot is a decoy system that is intentionally left vulnerable or exposed to attract attackers and divert them from the real targets. A honeypot can also be used to collect information about the attackers' techniques and motives. A network administrator can implement a honeypot to analyze attacks directed toward the company's network, as a honeypot can help identify the source, target, method, and impact of an attack, as well as provide recommendations for remediation. References:
https://www.comptia.org/blog/what-is-a-honeypot

NEW QUESTION 121
- (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 125
- (Exam Topic 2)
A lab environment hosts Internet-facing web servers and other experimental machines, which technicians use for various tasks A technician installs software on one of the web servers to allow communication to the company's file server, but it is unable to connect to it Other machines in the building are able to retrieve files from the file server. Which of the following is the MOST likely reason the web server cannot retrieve the files, and what should be done to resolve the problem?

A. The lab environment's IDS is blocking the network traffic 1 he technician can whitelist the new application in the IDS
B. The lab environment is located in the DM2, and traffic to the LAN zone is denied by defaul
C. The technician can move the computer to another zone or request an exception from the administrator.
D. The lab environment has lost connectivity to the company router, and the switch needs to be rebooted.The technician can get the key to the wiring closet and manually restart the switch
E. The lab environment is currently set up with hubs instead of switches, and the requests are getting bounced back The technician can submit a request for upgraded equipment to management.

Answer: B

Explanation:
The lab environment is located in the DMZ, and traffic to the LAN zone is denied by default. This is the most likely reason why the web server cannot retrieve files from the file server, and the technician can either move the computer to another zone or request an exception from the administrator to resolve the problem. A DMZ (Demilitarized Zone) is a network segment that separates the internal network (LAN) from the external network (Internet). It usually hosts public-facing servers such as web servers, email servers, or FTP servers that need to be accessed by both internal and external users. A firewall is used to control the traffic between the DMZ and the LAN zones, and usually denies traffic from the DMZ to the LAN by default for security reasons. Therefore, if a web server in the DMZ needs to communicate with a file server in the LAN, it would need a special rule or permission from the firewall administrator. References:
https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

NEW QUESTION 128
- (Exam Topic 2)
Two remote offices need to be connected securely over an untrustworthy MAN. Each office needs to access network shares at the other site. Which of the following will BEST provide this functionality?

A. Client-to-site VPN
B. Third-party VPN service
C. Site-to-site VPN
D. Split-tunnel VPN

Answer: C

Explanation:
A site-to-site VPN is a type of VPN that connects two or more remote offices securely over an untrustworthy network, such as the Internet. A site-to-site VPN allows each office to access network shares and resources at the other site, as if they were on the same local network. A site-to-site VPN encrypts and tunnels the traffic between the offices, ensuring privacy and integrity of the data. References: https://www.comptia.org/blog/what-is-a-site-to-site-vpn

NEW QUESTION 132
- (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 135
- (Exam Topic 2)
A network technician has multimode fiber optic cable available in an existing IDF. Which of the following Ethernet standards should the technician use to connect the network switch to the existing fiber?

A. 10GBaseT
B. 1000BaseT
C. 1000BaseSX
D. 1000BaseLX

Answer: C

Explanation:
1000BaseSX is an Ethernet standard that should be used to connect the network switch to the existing multimode fiber optic cable. 1000BaseSX is a Gigabit Ethernet standard that uses short-wavelength laser (850 nm) over multimode fiber optic cable. It can support distances up to 550 meters depending on the cable type and quality. It is suitable for short-range network segments such as campus or building backbone networks. References:
https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/produc

NEW QUESTION 136
- (Exam Topic 2)
A network administrator is talking to different vendors about acquiring technology to support a new project for a large company. Which of the following documents will MOST likely need to be signed before information about the project is shared?

A. BYOD policy
B. NDA
C. SLA
D. MOU

Answer: B

Explanation:
NDA stands for Non-Disclosure Agreement, which is a legal contract between two or more parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by others. A network administrator may need to sign an NDA before sharing information about a new project with different vendors, as the project may involve sensitive or proprietary data that the company wants to protect from competitors or unauthorized use. References: https://www.adobe.com/sign/esignature-resources/sign-nda.html

NEW QUESTION 140
- (Exam Topic 2)
A network technician is installing an analog desk phone for a new receptionist After running a new phone line, the technician now needs to cnmp on a new connector. Which of the following connectors would MOST likely be used in this case?

A. DB9
B. RJ11
C. RJ45
D. DB25

Answer: B

Explanation:
RJ11 is a type of connector that is commonly used for analog phone lines. RJ11 has four wires and six positions, but only two or four of them are used. A technician can crimp an RJ11 connector to a new phone line to install an analog desk phone for a new receptionist. References:

https://www.comptia.org/blog/what-is-rj11

NEW QUESTION 141
- (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 143
- (Exam Topic 2)
Which of the following protocols will a security appliance that is correlating network events from multiple devices MOST likely rely on to receive event messages?

A. Syslog
B. Session Initiation Protocol
C. Secure File Transfer Protocol
D. Server Message Block

Answer: A

Explanation:
Syslog is a protocol that provides a standard way for network devices and applications to send event messages to a logging server or a security appliance. Syslog messages can contain information about security incidents, errors, warnings, system status, configuration changes, and other events. A security appliance that is correlating network events from multiple devices can rely on Syslog to receive event messages from different sources and formats. References: https://www.comptia.org/blog/what-is-syslog

NEW QUESTION 145
- (Exam Topic 2)
A local firm has hired a consulting company to clean up its IT infrastructure. The consulting company notices remote printing is accomplished by port forwarding via publicly accessible IPs through the firm's firewall Which of the following would be the MOST appropriate way to enable secure remote printing?

A. SSH
B. VPN
C. Telnet
D. SSL

Answer: B

Explanation:
VPN (Virtual Private Network) is the most appropriate way to enable secure remote printing. VPN is a technology that creates a secure and encrypted tunnel over a public network such as the Internet. It allows remote users or sites to access a private network as if they were directly connected to it. VPN can be used for various purposes such as accessing corporate resources, bypassing geo-restrictions, or enhancing privacy and security. VPN can also be used for remote printing by allowing users to connect to a printer on the private network and send print jobs securely over the VPN tunnel. References: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-work

NEW QUESTION 147
- (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 148
- (Exam Topic 2)
A technician is troubleshooting a workstation's network connectivity and wants to confirm which switchport corresponds to the wall jack the PC is using Which of the following concepts would BEST help the technician?

A. Consistent labeling
B. Change management

C. Standard work instructions
D. Inventory management
E. Network baseline

Answer: A

Explanation:
Consistent labeling would be the concept that would best help the technician to confirm which switchport corresponds to the wall jack the PC is using. Consistent labeling is a practice of using standardized and descriptive labels for network devices, ports, cables, jacks, and other components. It can help with identifying, locating, and troubleshooting network issues. For example, a technician can use consistent labeling to trace a cable from a PC to a wall jack, and then from a patch panel to a switchport. References: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/DC_Infra2_5/DCInfra_6.html

NEW QUESTION 152
- (Exam Topic 2)
A company is being acquired by a large corporation. As part of the acquisition process, the company's address should now redirect clients to the corporate organization page. Which of the following DNS records needs to be created?

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

Answer: C

Explanation:
Reference:
https://www.namecheap.com/support/knowledgebase/article.aspx/9604/2237/types-of-domain-redirects-301-302
CNAME (Canonical Name) is a type of DNS record that maps an alias name to another name, which can be either another alias or the canonical name of a host or domain. A CNAME record can be used to redirect clients from one domain name to another domain name, such as from the company’s address to the corporate organization page. SOA (Start of Authority) is a type of DNS record that specifies authoritative information about a DNS zone, such as the primary name server, contact email address, serial number, refresh interval, etc., which does not redirect clients to another domain name. NS (Name Server) is a type of DNS record that specifies which name server is authoritative for a domain or subdomain, which does not redirect clients to another domain name. TXT (Text) is a type of DNS record that provides arbitrary text information about a domain or subdomain, such as SPF (Sender Policy Framework) records or DKIM (DomainKeys Identified Mail) records, which does not redirect clients to another domain name.

NEW QUESTION 155
- (Exam Topic 2)
A network administrator decided to use SLAAC in an extensive IPv6 deployment to alleviate IP address management. The devices were properly connected into the LAN but autoconfiguration of the IP address did not occur as expected. Which of the following should the network administrator verify?

A. The network gateway is configured to send router advertisements.
B. A DHCP server is present on the same broadcast domain as the clients.
C. The devices support dual stack on the network layer.
D. The local gateway supports anycast routing.

Answer: A

Explanation:
SLAAC (Stateless Address Autoconfiguration) is a method for IPv6 devices to automatically configure their IP addresses based on the network prefix advertised by a router. The router sends periodic router advertisements (RAs) that contain the network prefix and other parameters for the devices to use. If the network gateway is not configured to send RAs, then SLAAC will not work. A DHCP server is not needed for SLAAC, as the devices generate their own addresses without relying on a server. Dual stack and anycast routing are not related to SLAAC.

NEW QUESTION 156
- (Exam Topic 2)
An IDS was installed behind the edge firewall after a network was breached. The network was then breached again even though the IDS logged the attack. Which of the following should be used in place of these devices to prevent future attacks?

A. A network tap
B. A proxy server
C. A UTM appliance
D. A content filter

Answer: C

Explanation:
A UTM appliance stands for Unified Threat Management appliance, which is a device that combines multiple security functions into one solution. A UTM appliance can provide firewall, IDS/IPS, antivirus, VPN, web filtering, and other security features. A network technician can use a UTM appliance in place of an edge firewall and an IDS to prevent future attacks, as a UTM appliance can block malicious traffic and detect and respond to intrusions more effectively. References: https://www.comptia.org/blog/what-is-utm

NEW QUESTION 161
- (Exam Topic 2)
A network technician is configuring a new firewall for a company with the necessary access requirements to be allowed through the firewall. Which of the following would normally be applied as the LAST rule in the firewall?

A. Secure SNMP
B. Port security
C. Implicit deny

D. DHCP snooping

Answer: C

Explanation:
Implicit deny is a firewall rule that blocks all traffic that is not explicitly allowed by other rules. Implicit deny is usually applied as the last rule in the firewall to ensure that only the necessary access requirements are allowed through the firewall and that any unwanted or malicious traffic is rejected. Implicit deny can also provide a default security policy and a baseline for auditing and logging purposes.
Secure SNMP is a protocol that allows network devices to send event messages to a centralized server or console for logging and analysis. Secure SNMP can be used to monitor and manage the status, performance, and configuration of network devices. Secure SNMP can also help to detect and respond to potential problems or faults on the network. However, secure SNMP is not a firewall rule; it is a network management protocol.
Port security is a feature that allows a switch to restrict the devices that can connect to a specific port based on their MAC addresses. Port security can help to prevent unauthorized access, spoofing, or MAC flooding attacks on the switch. However, port security is not a firewall rule; it is a switch feature.
DHCP snooping is a feature that allows a switch to filter DHCP messages and prevent rogue DHCP servers from assigning IP addresses to devices on the network. DHCP snooping can help to prevent IP address conflicts, spoofing, or denial-of-service attacks on the network. However, DHCP snooping is not a firewall rule; it is a switch feature.

NEW QUESTION 163
- (Exam Topic 2)
The following instructions were published about the proper network configuration for a videoconferencing device:
"Configure a valid static RFC1918 address for your network. Check the option to use a connection over NAT." Which of the following is a valid IP address configuration for the device?

A. FE80::1
B. 100.64.0.1
C. 169.254.1.2
D. 172.19.0.2
E. 224.0.0.12

Answer: D

Explanation:
* 172.19.0.2 is a valid IP address configuration for the device that uses a static RFC1918 address for the network and allows for a connection over NAT (Network Address Translation). RFC1918 addresses are private IP addresses that are not routable on the public Internet and are used for internal networks. The RFC1918 address ranges are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. NAT is a technique that translates private IP addresses to public IP addresses when communicating with external networks, such as the Internet. FE80::1 is an IPv6 link-local address that is not a static RFC1918 address and does not allow for a connection over NAT. 100.64.1.1 is an IPv4 address that belongs to the shared address space range (100.64.0.0/10) that is used for carrier-grade NAT (CGN) between service providers and subscribers, which is not a static RFC1918 address and does not allow for a connection over NAT. 169.254.1.2 is an IPv4 link-local address that is automatically assigned by a device when it cannot obtain an IP address from a DHCP server or manual configuration, which is not a static RFC1918 address and does not allow for a connection over NAT. 224.0.0.12 is an IPv4 multicast address that is used for VRRP (Virtual Router Redundancy Protocol), which is not a static RFC1918 address and does not allow for a connection over NAT.

NEW QUESTION 168
- (Exam Topic 2)
A network requirement calls for segmenting departments into different networks. The campus network is set up with users of each department in multiple buildings. Which of the following should be configured to keep the design simple and efficient?

A. MDIX
B. Jumbo frames
C. Port tagging
D. Flow control

Answer: C

Explanation:
Port tagging is a technique that involves adding a tag or identifier to the frames or packets that belong to a certain VLAN. A VLAN is a logical segment of a network that isolates traffic between different groups of devices. Port tagging allows devices on different physical ports or switches to communicate with each other as if they were on the same port or switch. Port tagging can help keep the design simple and efficient by reducing the number of physical ports and switches needed to segment departments into different networks. References: https://www.comptia.org/blog/what-is-port-tagging

NEW QUESTION 171
- (Exam Topic 2)
Which of the following OSI model layers is where conversations between applications are established, coordinated, and terminated?

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

Answer: A

Explanation:
Reference: https://www.techtarget.com/searchnetworking/definition/OSI#:~:text=The%20session%20layer,and%20termina
The session layer is where conversations between applications are established, coordinated, and terminated. It is responsible for creating, maintaining, and ending sessions between different devices or processes. The physical layer deals with the transmission of bits over a medium. The presentation layer formats and translates data for different applications. The data link layer provides reliable and error-free delivery of frames within a network.

NEW QUESTION 176
- (Exam Topic 2)

Which of the following technologies allows traffic to be sent through two different ISPs to increase performance?

A. Fault tolerance
B. Quality of service
C. Load balancing
D. Port aggregation

Answer: C

Explanation:
Load balancing is a technology that allows traffic to be sent through two different ISPs to increase performance. Load balancing is a process of distributing network traffic across multiple servers or links to optimize resource utilization, throughput, latency, and reliability. Load balancing can be implemented at different layers of the OSI model, such as layer 4 (transport) or layer 7 (application). Load balancing can also be used for outbound traffic by using multiple ISPs and routing protocols such as BGP (Border Gateway Protocol) to select the best path for each packet. References:
https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/border-gateway-protocol-bgp/prod_white_

NEW QUESTION 179
- (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 182
- (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 186
- (Exam Topic 2)
A network administrator is configuring a database server and would like to ensure the database engine is listening on a certain port. Which of the following commands should the administrator use to accomplish this goal?

A. nslookup
B. netstat -a
C. ipconfig /a
D. arp -a

Answer: B

Explanation:
netstat -a is a command that displays information about active TCP connections and listening ports on a system. A network administrator can use netstat -a to check if the database engine is listening on a certain port, as well as verify if there are any connections established to or from that port. References:
https://www.comptia.org/blog/what-is-netstat

NEW QUESTION 187
- (Exam Topic 2)
A customer wants to segregate the traffic between guests on a hypervisor. Which of the following does a technician need to configure to meet the requirement?

A. Virtual switches
B. OSPF routing
C. Load balancers
D. NIC teaming
E. Fibre Channel

Answer: A

Explanation:
A virtual switch is a software-based switch that connects virtual machines on a hypervisor. A virtual switch can create and manage VLANs, which are logical segments of a network that isolate traffic between different groups of devices. A customer can use virtual switches to segregate the traffic between guests on a hypervisor by creating a separate VLAN for each guest and assigning it to a virtual switch port. References: https://www.comptia.org/blog/what-is-a-virtual-switch

NEW QUESTION 189
- (Exam Topic 2)
A network administrator is setting up several loT devices on a new VLAN and wants to accomplish the following
* 1. Reduce manual configuration on each system
* 2. Assign a specific IP address to each system
* 3. Allow devices to move to different switchports on the same VLAN
Which of the following should the network administrator do to accomplish these requirements?

A. Set up a reservation for each device
B. Configure a static IP on each device
C. Implement private VLANs for each device
D. Use DHCP exclusions to address each device

Answer: A

Explanation:
A reservation is a feature of DHCP that assigns a specific 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, regardless of its location or connection time. A network administrator can set up a reservation for each loT device to accomplish the requirements of reducing manual configuration, assigning a specific IP address, and allowing devices to move to different switchports on the same VLAN.
References: https://www.comptia.org/blog/what-is-dhcp

NEW QUESTION 193
- (Exam Topic 3)
A technician is consolidating a topology with multiple SSlDs 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 195
- (Exam Topic 3)
Which of the following devices have the capability to allow communication between two different subnetworks? (Select TWO).

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

Answer: DE

NEW QUESTION 200
- (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 204
- (Exam Topic 3)
A technician performed a manual reconfiguration of a firewall, and network connectivity was reestablished. Some connection events that were previously sent to a syslog server are no longer being generated by the flrewal Which of Vie following should the technician perform to fix the Issue?

A. Adjust the proper logging level on the new firewall.
B. Tune the filter for logging the severity level on the syslog server.
C. Activate NetFlow traffic between the syslog server and the firewall
D. Restart the SNMP service running on the syslog server.

Answer: A

Explanation:
Logging level is a setting that determines what types of events are recorded by a device and sent to a syslog server. Different logging levels have different severity levels, ranging from emergency to debug. If the technician performed a manual reconfiguration of the firewall, it is possible that the logging level was changed or reset to a lower level that does not include the connection events that were previously sent to the syslog server. To fix the issue, the technician should adjust the proper logging level on the new firewall to match the desired level of detail and severity for the connection events. References: Network+ Study Guide Objective 3.4: Explain common scanning, monitoring and patching processes and summarize their expected outputs. Subobjective: Syslog.

NEW QUESTION 205
- (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 210
- (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 211
- (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 214
- (Exam Topic 3)
A network administrator notices excessive wireless traffic occurring on an access point after normal business hours. The access point is located on an exterior wall. Which of the following should the administrator do to limit wireless access outside the building?

A. Set up a private VLAN.
B. Disable roaming on the WAP.
C. Change to a directional antenna.
D. Stop broadcasting of the SSID.

Answer: C

Explanation:
A directional antenna is a type of antenna that radiates or receives radio waves in a specific direction. This can help limit wireless access outside the building by

focusing the signal towards the intended area and reducing the signal strength in other directions. A private VLAN is a feature that isolates network devices within a VLAN. Disabling roaming on the WAP prevents wireless clients from switching to another WAP when the signal is weak. Stopping broadcasting of the SSID hides the network name from wireless clients, but does not prevent them from connecting if they know the SSID.
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 218
- (Exam Topic 3)
A network technician needs to ensure that all files on a company's network can be moved in a safe and protected manner without interception from someone who is not the intended recipient. Which of the following would allow the network technician to meet these requirements?

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

Answer: D

NEW QUESTION 222
- (Exam Topic 3)
Which of the following layers of the OSI model has new protocols activated when a user moves from a wireless to a wired connection?

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

Answer: A

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

NEW QUESTION 225
- (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 228
- (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 233
- (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 237
- (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 241
- (Exam Topic 3)
Which of the following is an example of on-demand scalable hardware that is typically housed in the vendor's data center?

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

Answer: B

NEW QUESTION 242
- (Exam Topic 3)
A large number of PCs are obtaining an APIPA IP address, and a number of new computers were added to the network. Which of the following is MOST likely causing the PCs to obtain an APIPA address?

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

Answer: D

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

NEW QUESTION 245
- (Exam Topic 3)
A technician thinks one of the router ports is flapping. Which of the following available resources should the technician use in order to determine if the router is flapping?

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

Answer: C

Explanation:
Syslog is a protocol that allows network devices to send event messages to a centralized server or console for logging and analysis1. Syslog can help a technician to determine if a router port is flapping by providing timestamps, severity levels, and descriptions of the events that occur on the router, such as interface up or down, link state change, or error messages. Syslog can also help to identify the cause and frequency of the port flapping and troubleshoot the issue.
Audit logs are records of actions or events that occur on a system or network, such as user login, file access, configuration change, or policy violation. Audit logs can help to monitor and verify the activities and behaviors of users, devices, or applications on a system or network. Audit logs can also help to detect and investigate security incidents, compliance issues, or performance problems. However, audit logs do not provide detailed information about router port flapping.

NetFlow is a protocol that collects and analyzes network traffic data for monitoring and troubleshooting purposes2. NetFlow can help to identify the sources, destinations, volumes, and types of traffic on a network. NetFlow can also help to optimize network performance, security, and capacity planning. However, NetFlow does not provide detailed information about router port flapping.
Traffic logs are records of network traffic that pass through a device or application, such as a firewall, proxy, or web server. Traffic logs can help to monitor and filter the network traffic based on rules or policies. Traffic logs can also help to detect and prevent malicious traffic, such as malware, attacks, or unauthorized access. However, traffic logs do not provide detailed information about router port flapping.

NEW QUESTION 248
- (Exam Topic 3)
A technician installed an 8-port switch in a user's office. The user needs to add a second computer in the office, so the technician connects both PCs to the switch and connects the switch to the wall jack. However, the new PC cannot connect to network resources. The technician then observes the following:
• The new computer does not get an IP address on the client's VLAN.
• Both computers have a link light on their NICs.
• The new PC appears to be operating normally except for the network issue.
• The existing computer operates normally.
Which of the following should the technician do NEXT to address the situation?

A. Contact the network team to resolve the port security issue.
B. Contact the server team to have a record created in DNS for the new PC.
C. Contact the security team to review the logs on the company's SIEM.
D. Contact the application team to check NetFlow data from the connected switch.

Answer: A

NEW QUESTION 252
- (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 254
- (Exam Topic 3)
A systems operator is granted access to a monitoring application, configuration application, and timekeeping application. The operator is denied access to the financial and project management applications by the system's security configuration. Which of the following BEST describes the security principle in use?

A. Network access control
B. Least privilege
C. Multifactor authentication
D. Separation of duties

Answer: D

NEW QUESTION 258
- (Exam Topic 3)
A network manager is configuring switches in IDFs to ensure unauthorized client computers are not connecting to a secure wired network. Which of the following is the network manager MOST likely performing?

A. Disabling unneeded switchports
B. Changing the default VLAN
C. Configuring DHCP snooping
D. Writing ACLs to prevent access to the switch

Answer: C

NEW QUESTION 259
- (Exam Topic 3)
Several end users viewing a training video report seeing pixelated images while watching. A network administrator reviews the core switch and is unable to find an immediate cause. Which of the following BEST explains what is occurring?

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

Answer: A

Explanation:

"Jitter is the loss of packets due to an overworked WAP. Jitter shows up as choppy conversations over a video call, strange jumps in the middle of an online game—pretty much anything that feels like the network has missed some data. Latency is when data stops moving for a moment due to a WAP being unable to do the work. This manifests as a Word document that stops loading, for example, or an online file that stops downloading."

NEW QUESTION 262
- (Exam Topic 3)
Which of the following is the MOST cost-effective alternative that provides proper cabling and supports gigabit Ethernet devices?

A. Twisted cable with a minimum Cat 5e certification
B. Multimode fiber with an SC connector
C. Twinaxial cabling using an F-type connector
D. Cable termination using TIA/EIA-568-B

Answer: A

Explanation:
twisted cable with a minimum Cat 5e certification is the MOST cost-effective alternative that provides proper cabling and supports gigabit Ethernet devices.

NEW QUESTION 266
- (Exam Topic 3)
A user from a remote office is reporting slow file transfers. Which of the following tools will an engineer MOST likely use to get detailed measurement data?

A. Packet capture
B. IPerf
C. SIEM log review
D. Internet speed test

Answer: B

Explanation:
An engineer will most likely use IPerf to get detailed measurement data about the user's slow file transfers. IPerf is a tool used for measuring network performance and bandwidth, and it can be used to measure the speed and throughput of file transfers from the remote office. It can also provide detailed information about the latency and jitter of the connection, which can be used to troubleshoot the slow file transfers. Reference: CompTIA Network+ Study Manual (Chapter 10, Page 214).

NEW QUESTION 267
- (Exam Topic 3)
An administrator needs to connect two laptops directly to each other using 802.11ac but does not have an AP available. Which of the following describes this configuration?

A. Basic service set
B. Extended service set
C. Independent basic service set
D. MU-MIMO

Answer: C

NEW QUESTION 271
- (Exam Topic 3)
During a risk assessment which of the following should be considered when planning to mitigate high CPU utilization of a firewall?

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

Answer: D

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

NEW QUESTION 272
- (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?

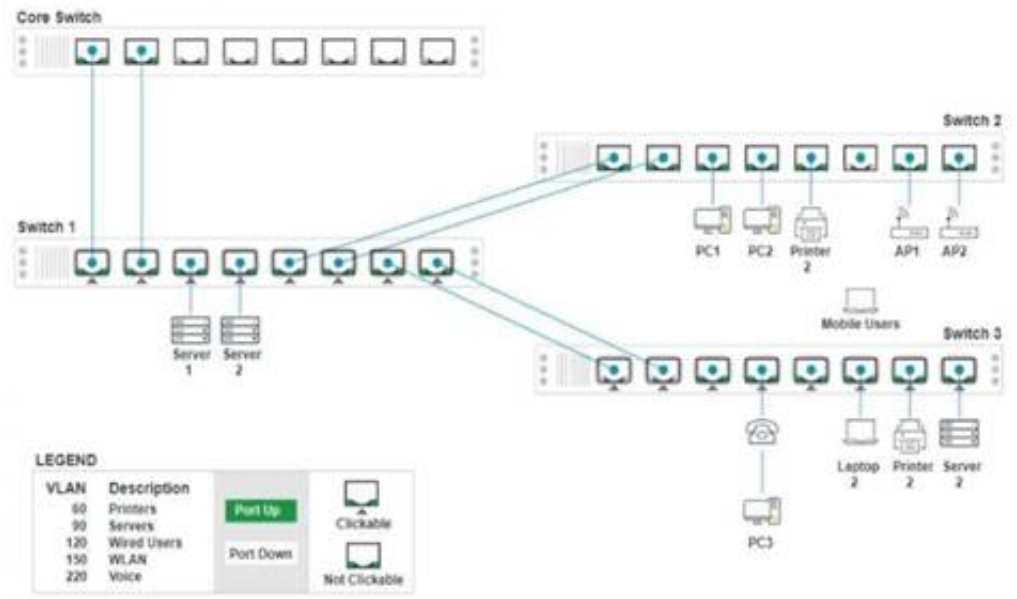
A. netstat -a
B. ifconfig
C. ip addr
D. ipconfig /all

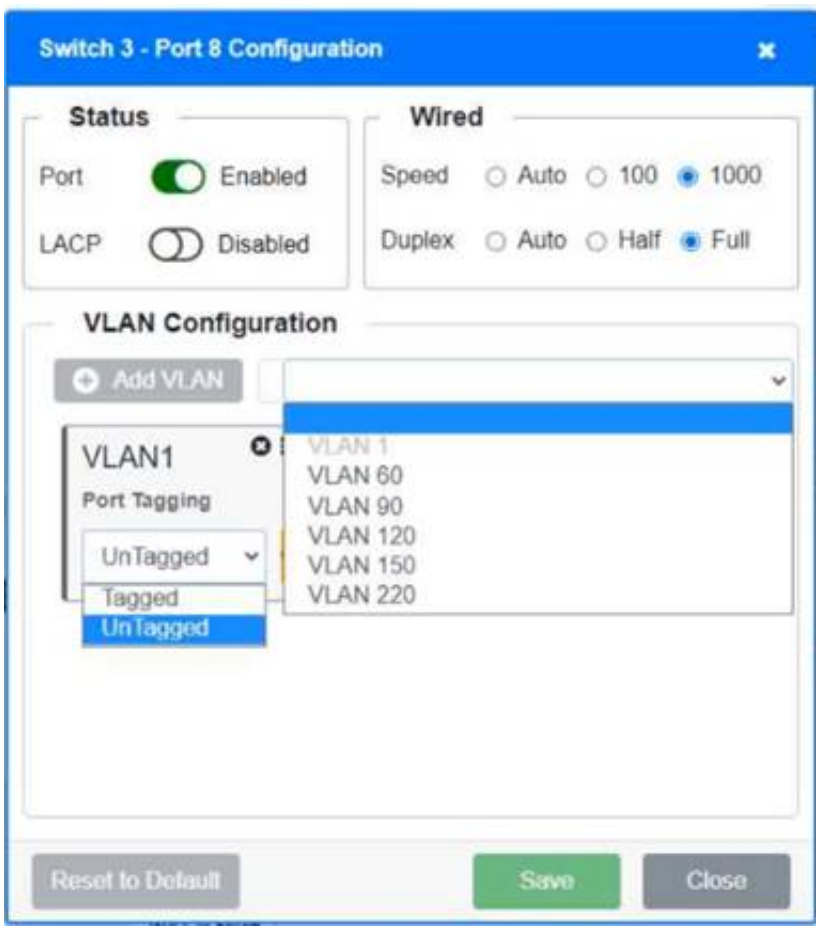
Answer: D

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

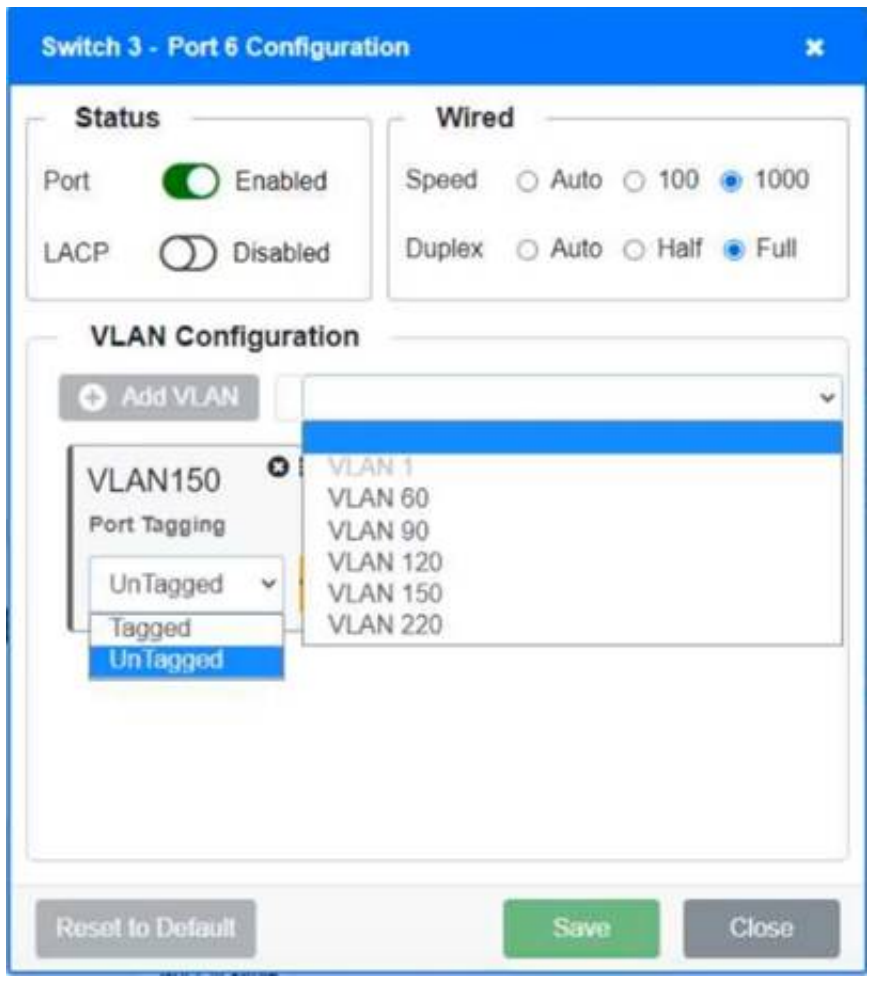
addresses.
Option A (netstat -a) is a command that displays active network connections and their status, but it does not display IP address or other network configuration information. Option B (ifconfig) is a command used on Linux and Unix systems to view and modify network configuration, but it is not 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.

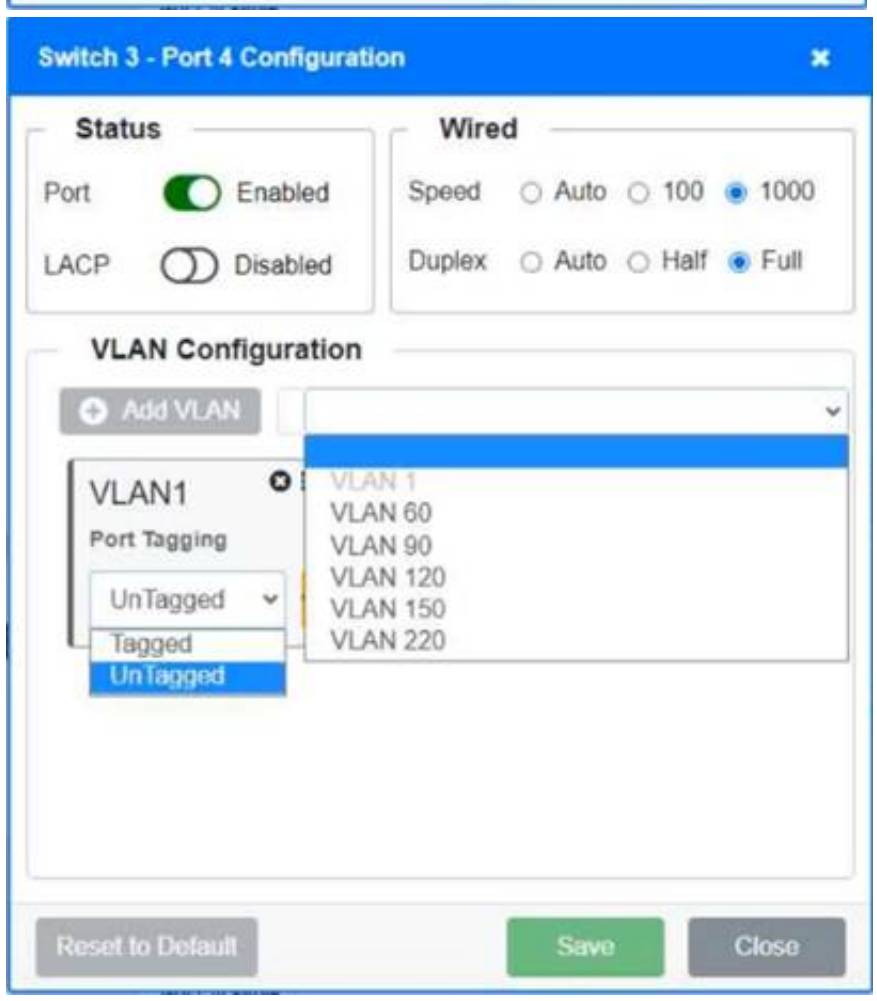
NEW QUESTION 276
- (Exam Topic 3)
SIMULATION
A network technician replaced a switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.
INSTRUCTIONS
Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings:
• Ensure 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.

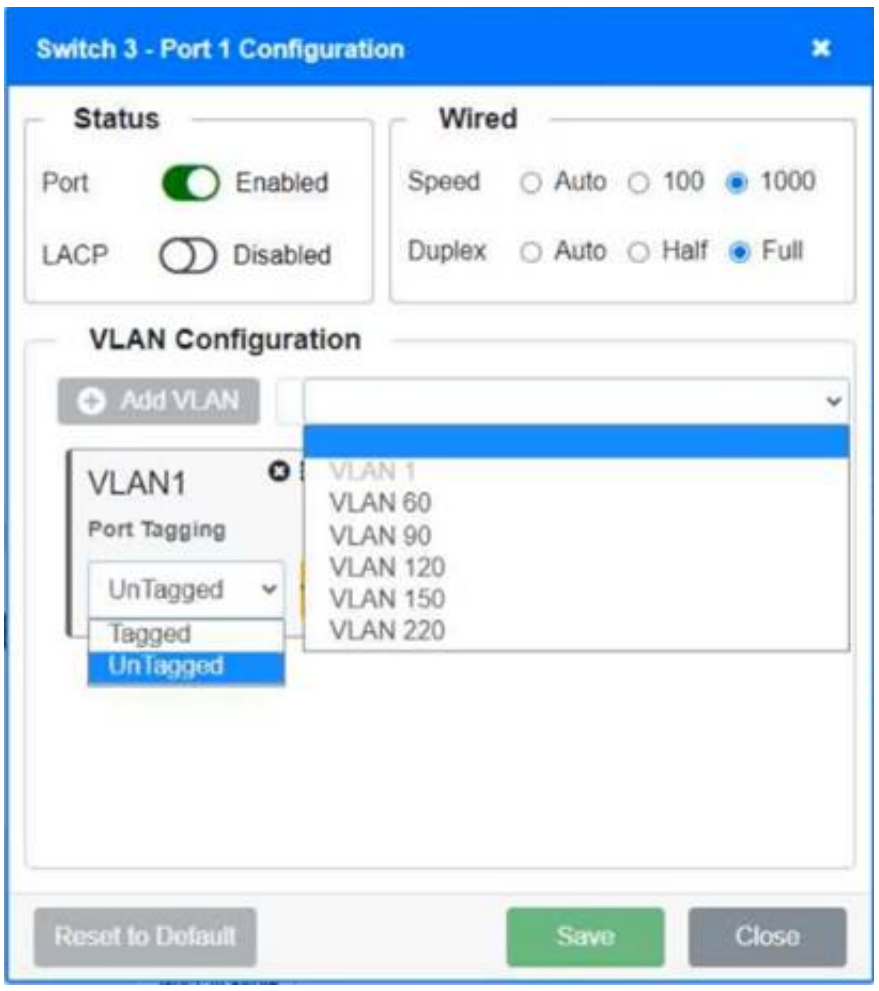


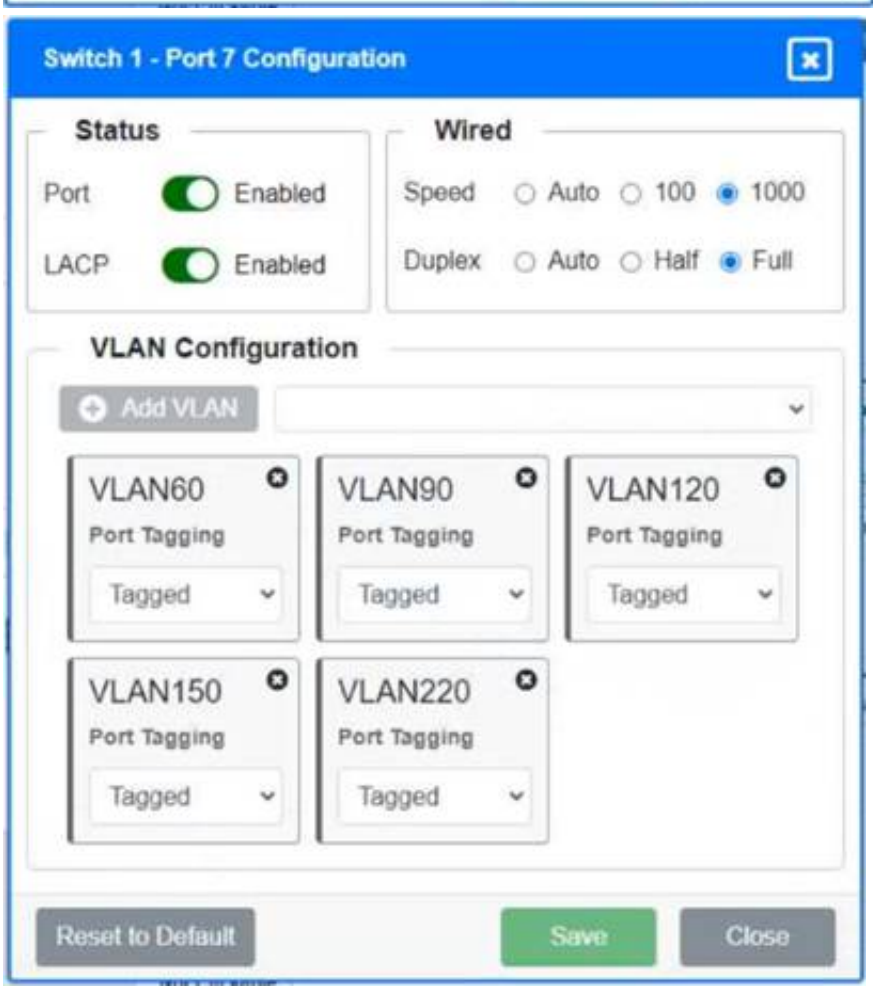


Switch 3 - Port 7 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close


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

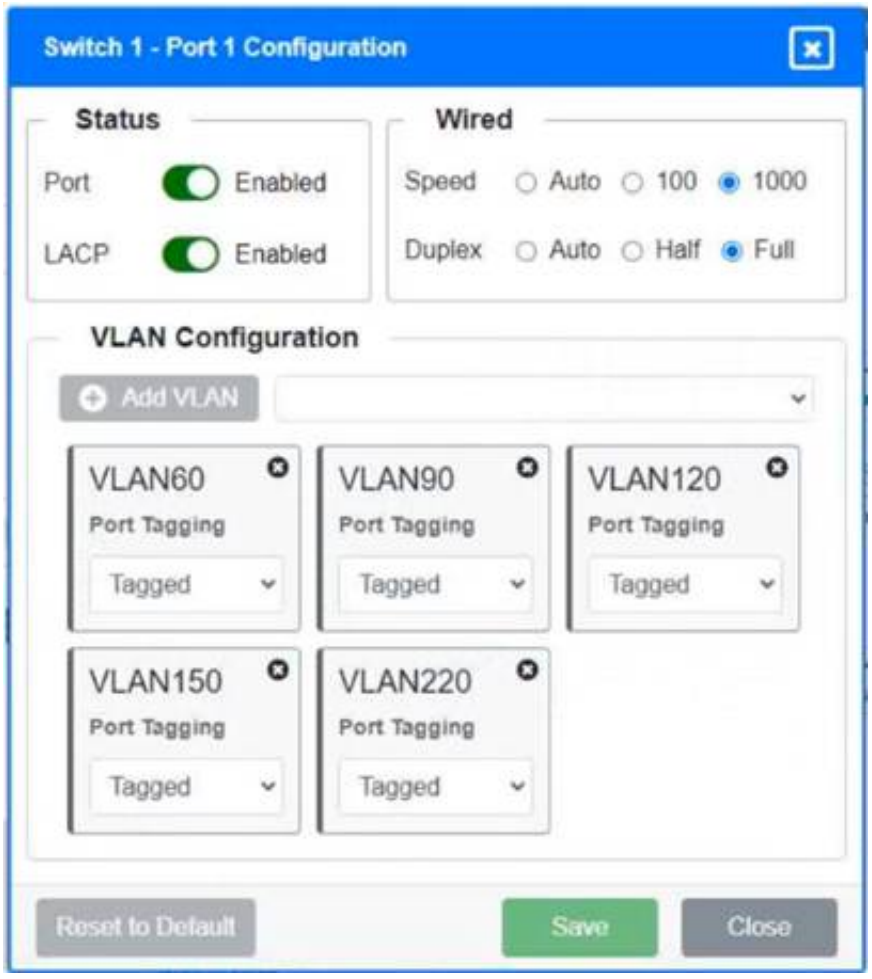

Switch 3 - Port 1 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

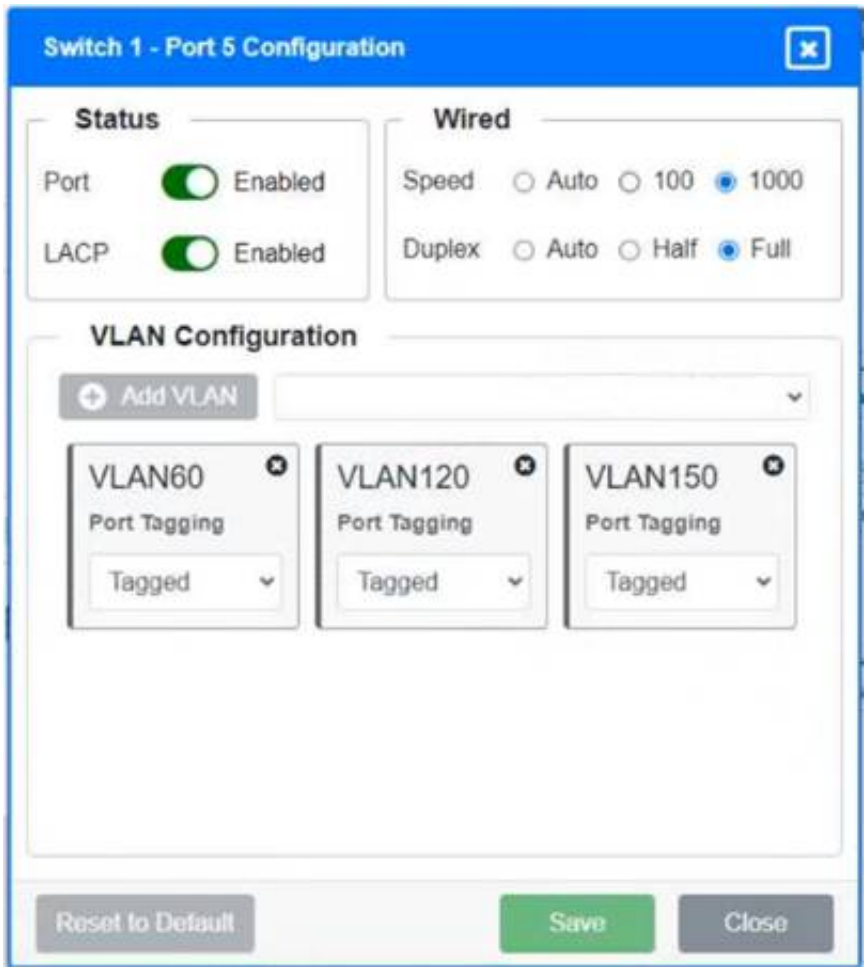

Switch 1 - Port 7 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save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

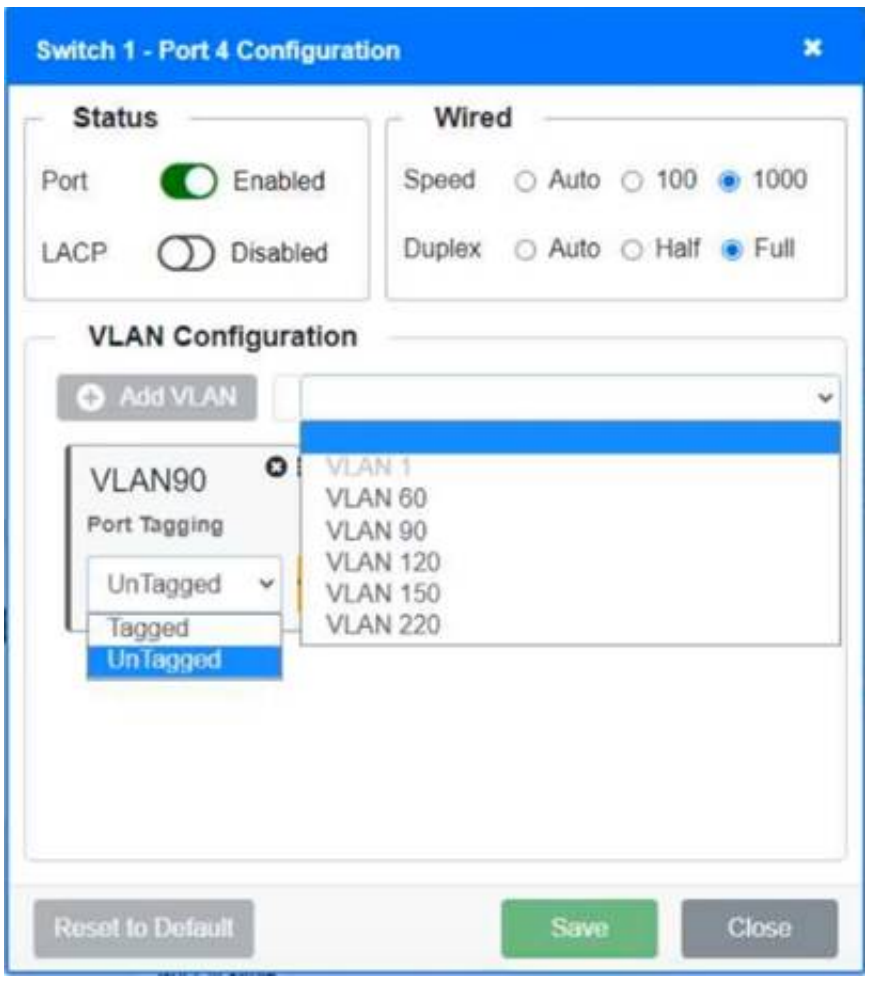
Switch 1 - Port 8 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save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

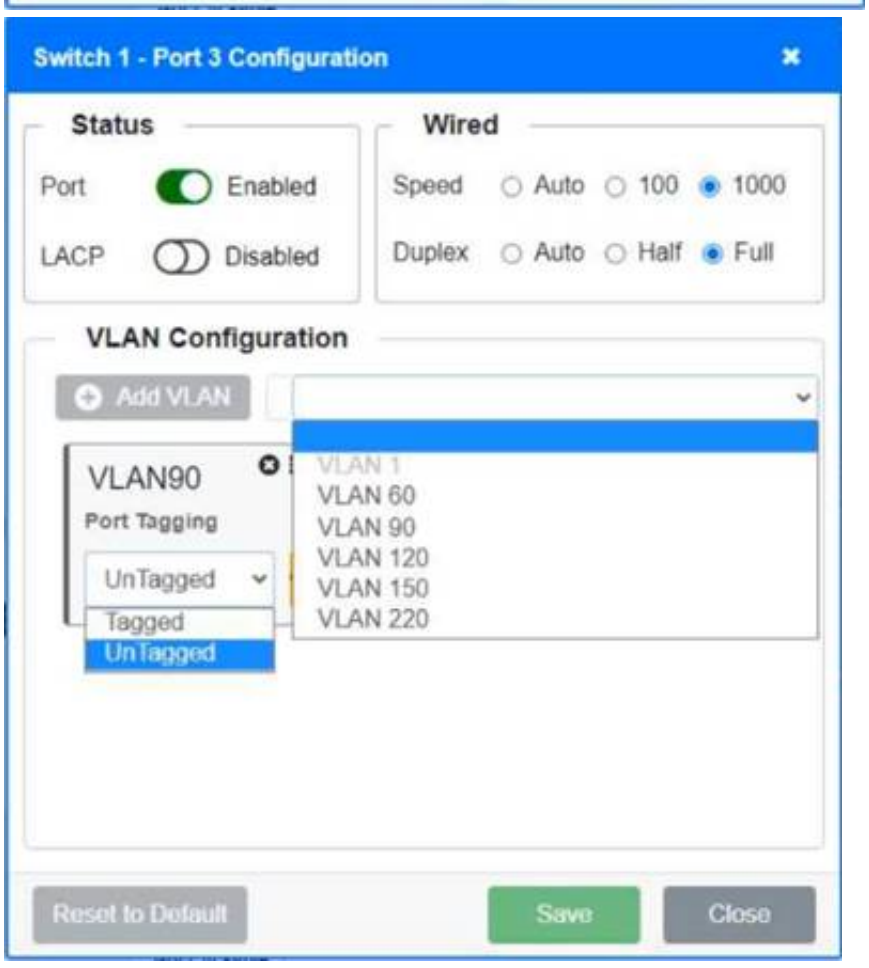
Switch 1 - Port 6 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
Reset to Default
Save
Close

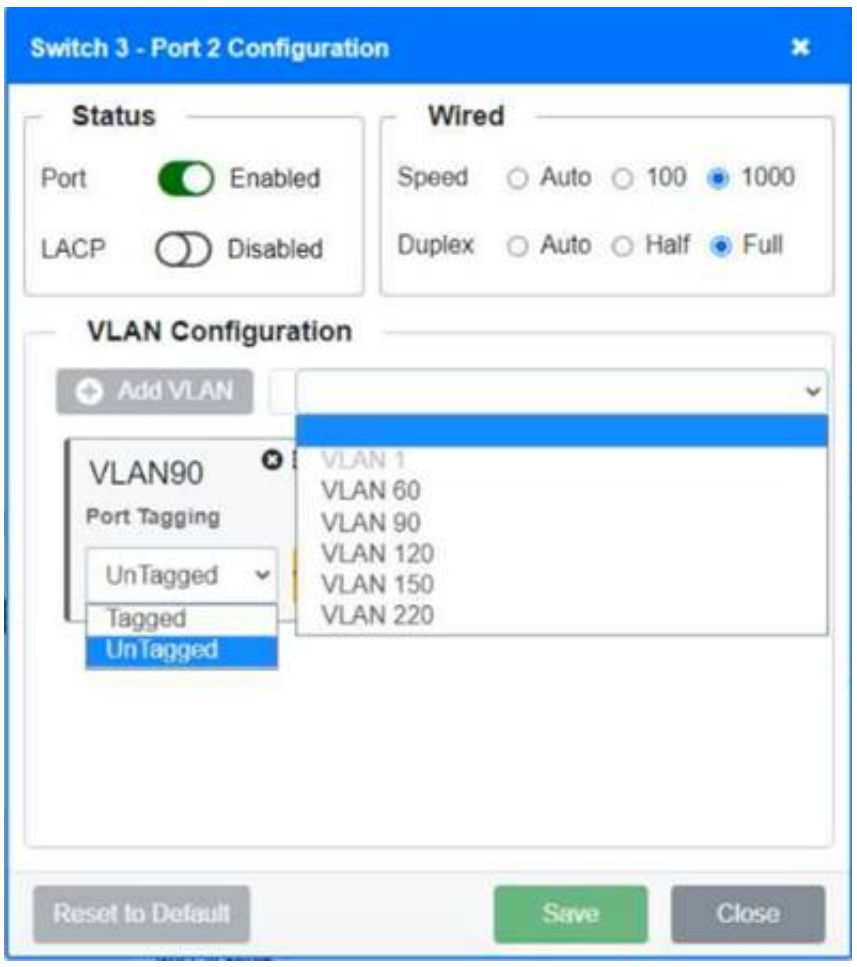
Switch 1 - Port 2 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
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 277
- (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 278
- (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 280
- (Exam Topic 3)
A network administrator installed an additional IDF during a building expansion project. Which of the following documents need to be updated to reflect the change? (Select TWO).

A. Data loss prevention policy
B. BYOD policy
C. Acceptable use policy
D. Non-disclosure agreement
E. Disaster recovery plan
F. Physical network diagram

Answer: BF

NEW QUESTION 281
- (Exam Topic 3)
A user reports that a new VoIP phone works properly but the computer that is connected to the phone cannot access any network resources. Which of the following MOST Likely needs to be configured correctly to provide network connectivity to the computer?

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

Answer: D

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

NEW QUESTION 282
- (Exam Topic 3)
An ISP is providing Internet to a retail store and has terminated its point of connection using a standard Cat 6 pin-out Which of me following terminations should the technician use when running a cable from the ISP's port lo the front desk?

A. F-type connector
B. TIA/E1A-56S-B
C. LC
D. SC

Answer: B

Explanation:
The termination that the technician should use when running a cable from the ISP’s port to the front desk is B. TIA/EIA-568-B. This is a standard pin-out for Cat 6 cables that is used for Ethernet and other network physical layers1. It specifies how to arrange the eight wires in an RJ45 connector, which is a common type of connector for network cables.

NEW QUESTION 284
- (Exam Topic 3)
A network administrator would like to purchase a device that provides access ports to endpoints and has the ability to route between networks. Which of the following would be BEST for the administrator to purchase?

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

Answer: B

NEW QUESTION 289
- (Exam Topic 3)
All packets arriving at an interface need to be fully analyzed. Which of me following features should be used to enable monitoring of the packets?

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

Answer: C

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

NEW QUESTION 293
- (Exam Topic 3)
A network technician is implementing a solution that will allow end users to gain access to multiple applications after logging on. Which of the following authentication methods would allow this type of access?

A. SSO
B. LDAP
C. EAP
D. TACACS+

Answer: A

NEW QUESTION 296
- (Exam Topic 3)
A help desk technician is concerned that a client's network cable issues may be causing intermittent connectivity. Which of the following would help the technician determine if this is the issue?

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

Answer: A

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

NEW QUESTION 297
- (Exam Topic 3)
Switch 3 was recently added lo an existing stack to extend connectivity to various parts of the network. After the update, new employees were not able to print to the main networked copiers from then workstations. Following are the port configurations for the switch stack in question:

Switch 1:

	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	60	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Active	Active	Active	Active

Switch 2:

	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	60	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Active	Shut down	Active	Active

Switch 3:

	Ports 1–12	Ports 13–24	Ports 25–36	Ports 37–44	Ports 45–48
Description	Workstations	Printers	Workstations	Wireless APs	Uplink
VLAN	20	80	20	80	20/60/80
Duplex	Full	Full	Full	Full	Full
Status	Active	Shut down	Shut down	Shut down	Active

Which of the following should be configured to resolve the issue? (Select TWO).

A. Enable the printer ports on Switch 3.
B. Reconfigure the duplex settings on the printer ports on Switch 3.
C. Reconfigure the VLAN on an printer ports to VLAN 20.
D. Enable all ports that are shut down on me stack.
E. Reconfigure me VLAN on the printer ports on Switch 3.
F. Enable wireless APs on Switch 3.

Answer: AE

NEW QUESTION 301
- (Exam Topic 3)
Which of the following allows for an devices within a network to share a highly reliable time source?

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

Answer: A

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

NEW QUESTION 305
- (Exam Topic 3)

When accessing corporate network resources, users are required to authenticate to each application they try to access. Which of the following concepts does this BEST represent?

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

Answer: B

NEW QUESTION 307
- (Exam Topic 3)
On a network with redundant switches, a network administrator replaced one of the switches but was unable to get a connection with another switch. Which of the following should the administrator chock after successfully testing the cable that was wired for TIA/EIA-568A on both ends?

A. If MDIX is enabled on the new switch
B. If PoE is enabled
C. If a plenum cable is being used
D. If STP is disabled on the switches

Answer: A

Explanation:
Auto-MDIX (or medium dependent interface crossover) is a feature that automatically detects the type of cable connection and configures the interface accordingly (i.e. straight-through or crossover). This ensures that the connection between the two switches is successful. This is referenced in the CompTIA Network+ Study Manual, page 519.

NEW QUESTION 311
- (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 315
- (Exam Topic 3)
A technician discovered that some information on the local database server was changed during a tile transfer to a remote server. Which of the following should concern the technician the MOST?

A. Confidentiality
B. Integrity
C. DDoS
D. On-path attack

Answer: B

Explanation:
The technician should be most concerned about data integrity and security. If information on the local database server was changed during a file transfer to a remote server, it could indicate that unauthorized access or modifications were made to the data. It could also indicate a failure in the file transfer process, which could result in data loss or corruption. The technician should investigate the cause of the changes and take steps to prevent it from happening again in the future. Additionally, they should verify the integrity of the data and restore it from a backup if necessary to ensure that the correct and complete data is available. The technician should also take appropriate actions such as notifying the system administrator and management of the incident, and following the incident management process to minimize the damage caused by the incident.

NEW QUESTION 316
- (Exam Topic 3)
A new company recently moved into an empty office space Within days, users in the next office began noticing increased latency and packet drops with their Wi-Fi-connected devices. Which of the following is the MOST likely reason for this issue?

A. Channel overlap
B. Distance from the AP
C. Bandwidth latency
D. RF attenuation
E. Network congestion

Answer: A

NEW QUESTION 320
- (Exam Topic 3)
An IT technician needs to increase bandwidth to a server. The server has multiple gigabit ports. Which of the following can be used to accomplish this without replacing hardware?

A. STP
B. 802. IQ
C. Duplex
D. LACP

Answer: D

Explanation:
LACP stands for Link Aggregation Control Protocol and is a protocol that allows multiple physical ports to be combined into a single logical port. This can increase bandwidth, redundancy, and load balancing for a server. LACP is part of the IEEE 802.3ad standard for link aggregation. STP stands for Spanning Tree Protocol and is a protocol that prevents loops in a network by blocking redundant links. 802.1Q is a standard for VLAN (Virtual Local Area Network) tagging, which allows multiple logical networks to share the same physical infrastructure. Duplex is a mode of communication that determines how data is transmitted and received on a link. Full duplex allows simultaneous transmission and reception, while half duplex allows only one direction at a time.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.5: Compare and contrast network cabling types, standards and speeds.

NEW QUESTION 322
- (Exam Topic 3)
Which of the following protocols is widely used in large-scale enterprise networks to support complex networks with multiple routers and balance traffic load on multiple links?

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

Answer: A

NEW QUESTION 325
- (Exam Topic 3)
Which of the following would be the BEST choice to connect branch sites to a main office securely?

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

Answer: A

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

NEW QUESTION 330
- (Exam Topic 3)
A company cell phone was stolen from a technician's vehicle. The cell phone has a passcode, but it contains sensitive information about clients and vendors. Which of the following should also be enabled?

A. Factory reset
B. Autolock
C. Encryption
D. Two-factor authentication

Answer: C

NEW QUESTION 334
- (Exam Topic 3)
Which of the following bandwidth management techniques uses buffers al the client side to prevent TCP retransmissions from occurring when the ISP starts to drop packets of specific types that exceed the agreed traffic rate?

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

Answer: D

NEW QUESTION 338
- (Exam Topic 3)
A Wi-Fi network was originally configured to be able to handle interference from a microwave oven. The microwave oven was recently removed from the office. Now the network administrator wants to optimize the system to maximize the range of the signal. The main sources of signal degradation are the numerous cubicles and wooden walls between the WAP and the intended destination. Which of the following actions should the administrator take?

A. Implement CDMA.
B. Change from omni to directional.
C. Change the SSID.
D. Change the frequency.

Answer: D

Explanation:
- the microwave was already removed from the office
- the signal is OK now
- Notice that the question mentions "numerous cubicles and wooden walls" - meaning the signal now won't have the interference as before
- KEY POINT: the admin wants to "maximize the range of the signal:"
Manually change the frequency to 2.4 GHz for more reliable speeds and range. While 5 GHz gives you a stronger signal, it doesn't travel through walls or ceilings as well, so it doesn't give you the best range.
"Microwave ovens: Older microwave ovens, which might not have sufficient shielding, can emit relatively high-powered signals in the 2.4GHz band, resulting in significant interference with WLAN devices operating in the 2.4GHz band."

NEW QUESTION 339
- (Exam Topic 3)
A network technician is selecting a replacement for a damaged fiber cable that goes directly to an SFP transceiver on a network switch. Which of the following cable connectors should be used?

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

Answer: C

NEW QUESTION 341
- (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 344
- (Exam Topic 3)
An IT technician successfully connects to the corporate wireless network at a hank. While performing some tests, the technician observes that the physical address of the DHCp server has changed even though the network connection has not been lost. Which of the following would BEST explain this change?

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

Answer: D

Explanation:
A rogue server is a DHCP server on a network that is not under the administrative control of the network staff 1. It may provide incorrect IP addresses or other network configuration information to devices on the network, causing them to lose connectivity or be vulnerable to attacks2. The physical address of the DHCP server may change if a rogue server takes over the role of assigning IP addresses to devices on the network. This can be detected by monitoring DHCP traffic or using tools such as RogueChecker2.

NEW QUESTION 348
- (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 349
- (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 353
- (Exam Topic 3)
The Chief Executive Officer of a company wants to ensure business operations are not disrupted in the event of a disaster. The solution must have fully redundant equipment, real-time synchronization, and zero data loss. Which Of the following should be prepared?

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

Answer: C

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

NEW QUESTION 357
- (Exam Topic 3)
Which of the following is considered a physical security detection device?

A. Cameras
B. Biometric readers
C. Access control vestibules
D. Locking racks

Answer: A

NEW QUESTION 359
- (Exam Topic 3)
An international company is transferring its IT assets including a number of WAPs from the United States to an office in Europe for deployment. Which of the following considerations should the company research
before Implementing the wireless hardware?

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

Answer: B

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

NEW QUESTION 364
- (Exam Topic 3)
An employee working in a warehouse facility is experiencing interruptions in mobile applications while walking around the facility. According to a recent site survey, the WLAN comprises autonomous APs that are directly connected to the internet, providing adequate signal coverage. Which of the following is the BEST solution to improve network stability?

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

Answer: A

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

broadcast area, they will change WAP connections seamlessly, a process called roaming."

NEW QUESTION 367

.....

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