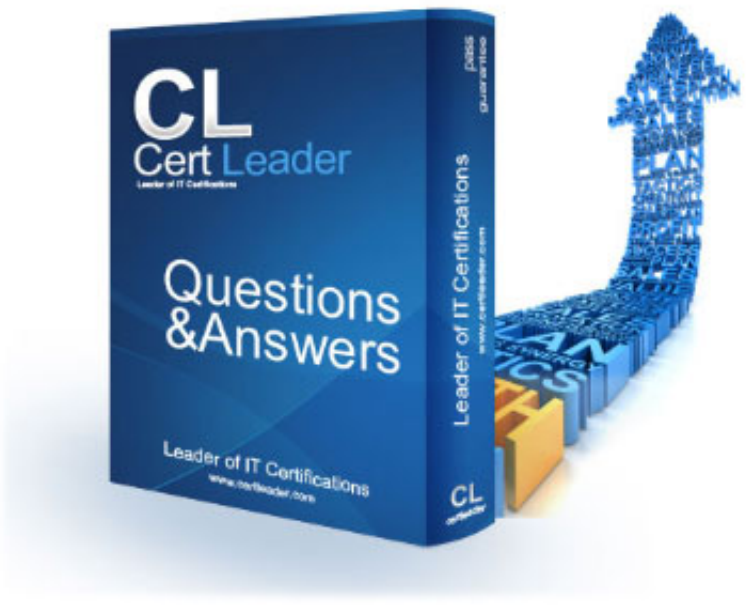
N10-009 Dumps

CompTIA Network+ Exam

https://www.certleader.com/N10-009-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
An IT director is setting up new disaster and HA policies for a company. Limited downtime is critical to operations. To meet corporate requirements, the director set up two different datacenters across the country that will stay current on data and applications. In the event of an outage, the company can immediately switch from one datacenter to another. Which of the following does this BEST describe?

A. A warm site
B. Data mirroring
C. Multipathing
D. Load balancing
E. A hot site

Answer: E

Explanation:
A hot site is a fully redundant site that can take over operations immediately if the primary site goes down. In this scenario, the company has set up two different datacenters across the country that are current on data and applications, and they can immediately switch from one datacenter to another in case of an outage.
References:
- Network+ N10-008 Objectives: 1.5 Compare and contrast disaster recovery concepts and methodologies.

NEW QUESTION 2
- (Exam Topic 1)
An administrator is writing a script to periodically log the IPv6 and MAC addresses of all the devices on a network segment. Which of the following switch features will MOST likely be used to assist with this task?

A. Spanning Tree Protocol
B. Neighbor Discovery Protocol
C. Link Aggregation Control Protocol
D. Address Resolution Protocol

Answer: B

Explanation:
Short explanation
The switch feature that is most likely to be used to assist with logging IPv6 and MAC addresses of devices on a network segment is Neighbor Discovery Protocol (NDP). NDP is used by IPv6 to discover and maintain information about other nodes on the network, including their IPv6 and MAC addresses. By periodically querying NDP, the administrator can log this information for auditing purposes.
References:
- CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.1: Compare and contrast TCP and UDP ports, protocols, and their purposes.

NEW QUESTION 3
- (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 4
- (Exam Topic 1)
Which of the following DNS records works as an alias to another record?

A. AAAA
B. CNAME
C. MX
D. SOA

Answer: B

Explanation:
The DNS record that works as an alias to another record is called CNAME (Canonical Name). CNAME records are used to create an alias for a domain name that points to another domain name.
References:
- CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a scenario, implement and configure the
appropriate addressing schema.

NEW QUESTION 5
- (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 6
- (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 7
- (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 8
- (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 9
- (Exam Topic 1)
A network administrator is configuring a load balancer for two systems. Which of the following must the administrator configure to ensure connectivity during a failover?

A. VIP
B. NAT
C. APIPA
D. IPv6 tunneling
E. Broadcast IP

Answer: A

Explanation:
A virtual IP (VIP) address must be configured to ensure connectivity during a failover. A VIP address is a single IP address that is assigned to a group of servers or network devices. When one device fails, traffic is automatically rerouted to the remaining devices, and the VIP address is reassigned to the backup device, allowing clients to continue to access the service without interruption.
References:
- CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 6: Network Servers, p. 300

NEW QUESTION 10
- (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 10
- (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 12
- (Exam Topic 1)
After the A record of a public website was updated, some visitors were unable to access the website. Which of the following should be adjusted to address the issue?

A. TTL
B. MX
C. TXT
D. SOA

Answer: A

Explanation:
TTL (Time To Live) should be adjusted to address the issue of some visitors being unable to access the website after the A record was updated. TTL is a value that specifies how long a DNS record should be cached by DNS servers and clients before it expires and needs to be refreshed. If the TTL is too high, some DNS servers and clients may still use the old A record that points to the previous IP address of the website, resulting in connection failures. By lowering the TTL, the DNS servers and clients will update their cache more frequently and use the new A record that points to the current IP address of the website. References:
https://www.cloudflare.com/learning/dns/dns-records/dns-ttl/

NEW QUESTION 16
- (Exam Topic 1)
A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds that jitter at the office is greater than 10ms on the only WAN connection available. Which of the following would be MOST affected by this statistic?

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

Answer: A

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

NEW QUESTION 17
- (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 22
- (Exam Topic 1)
A network engineer is investigating reports of poor network performance. Upon reviewing a device configuration, the engineer finds that duplex settings are mismatched on both ends. Which of the following would be the MOST likely result of this finding?

A. Increased CRC errors
B. Increased giants and runts
C. Increased switching loops
D. Increased device temperature

Answer: A

Explanation:
Mismatched duplex settings can cause an increase in CRC errors, which are errors in data transmission that can result in corrupted data. References: CompTIA Network+ Certification Study Guide, Chapter 4: Infrastructure.

NEW QUESTION 27
- (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 32
- (Exam Topic 1)
A technician is deploying a new switch model and would like to add it to the existing network monitoring software. The technician wants to know what metrics can be gathered from a given switch. Which of the following should the technician utilize for the switch?

A. MIB
B. Trap
C. Syslog
D. Audit log

Answer: A

Explanation:
To determine what metrics can be gathered from a given switch, a technician should utilize the Management Information Base (MIB). The MIB is a database of network management information that is used to manage and monitor network devices. It contains information about device configuration, status, and performance. References: Network+ Certification Study Guide, Chapter 5: Network Security

NEW QUESTION 36
- (Exam Topic 1)
Which of the following would need to be configured to ensure a device with a specific MAC address is always assigned the same IP address from DHCP?

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

Answer: B

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

NEW QUESTION 40
- (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 42
- (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 44
- (Exam Topic 1)
A technician needs to configure a Linux computer for network monitoring. The technician has the following information:
Linux computer details:

Interface	IP address	MAC address
eth0	10.1.2.24	A1:B2:C3:F4:E5:D6

Switch mirror port details:

Interface	IP address	MAC address
eth1	10.1.2.3	A1:B2:C3:D4:E5:F6

After connecting the Linux computer to the mirror port on the switch, which of the following commands should the technician run on the Linux computer?

A. ifconfig ecth0 promisc
B. ifconfig eth1 up
C. ifconfig eth0 10.1.2.3
D. ifconfig eth1 hw ether A1:B2:C3:D4:E5:F6

Answer: A

Explanation:
The ifconfig eth0 promisc command should be run on the Linux computer to enable promiscuous mode, which allows the computer to capture all network traffic passing through the switch mirror port. References: CompTIA Network+ Certification Study Guide, Chapter 7: Network Devices.

NEW QUESTION 47
- (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 51
- (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 54
- (Exam Topic 1)
Which of the following is the physical topology for an Ethernet LAN?

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

Answer: D

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

NEW QUESTION 58
- (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

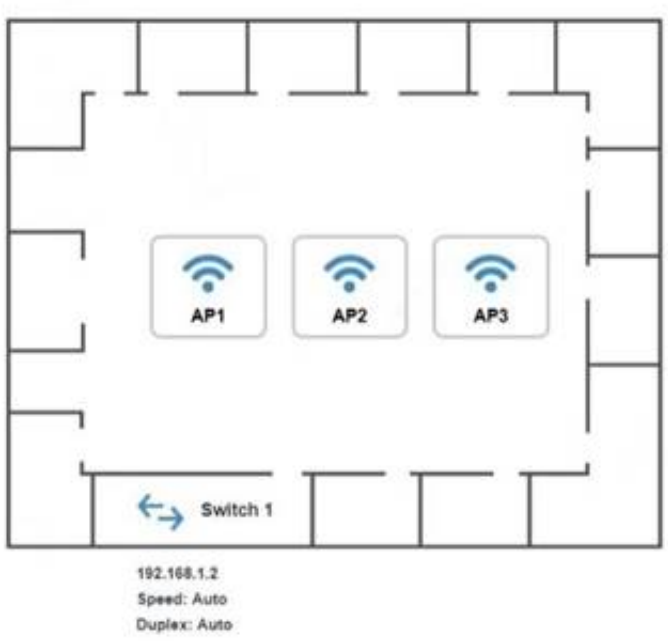
NEW QUESTION 61
- (Exam Topic 1)
A website administrator is concerned the company's static website could be defaced by hacktivists or used as a pivot point to attack internal systems. Which of the following should a network security administrator recommend to assist with detecting these activities?

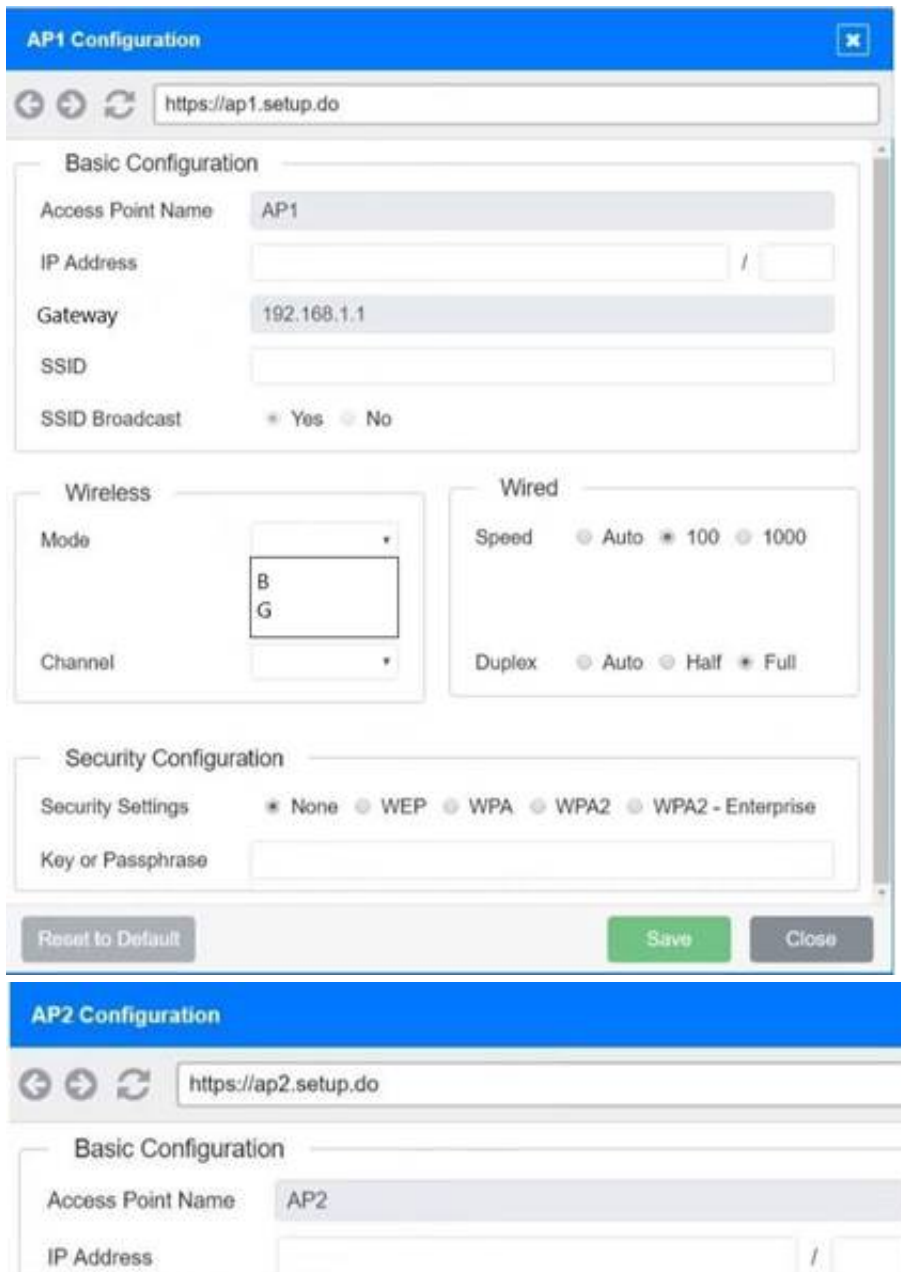
A. Implement file integrity monitoring.
B. Change the default credentials.
C. Use SSL encryption.
D. Update the web-server software.

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 63
- (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.



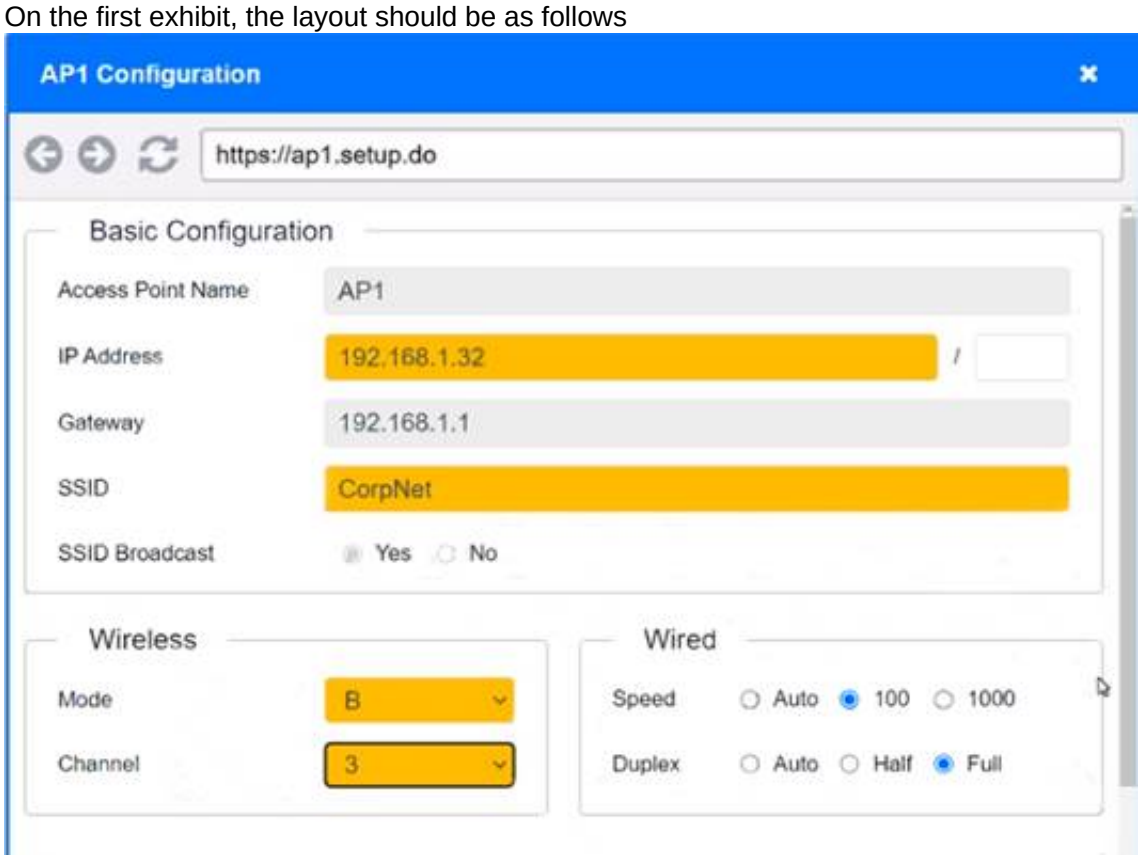

AP1 Configuration
https://ap1.setup.do
Basic Configuration
Access Point Name
AP1
IP Address
Gateway
192.168.1.1
SSID
SSID Broadcast
Yes
No
Wireless
Mode
B
G
Channel
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase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

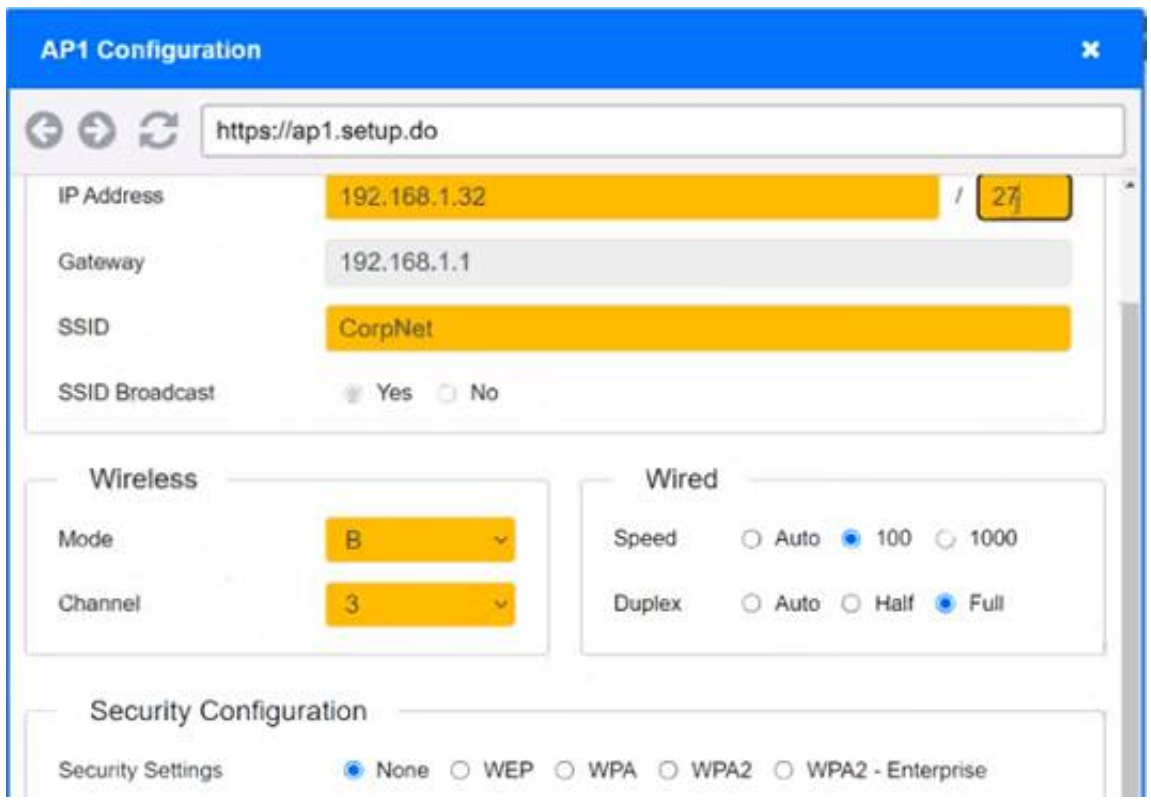
Answer: A

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

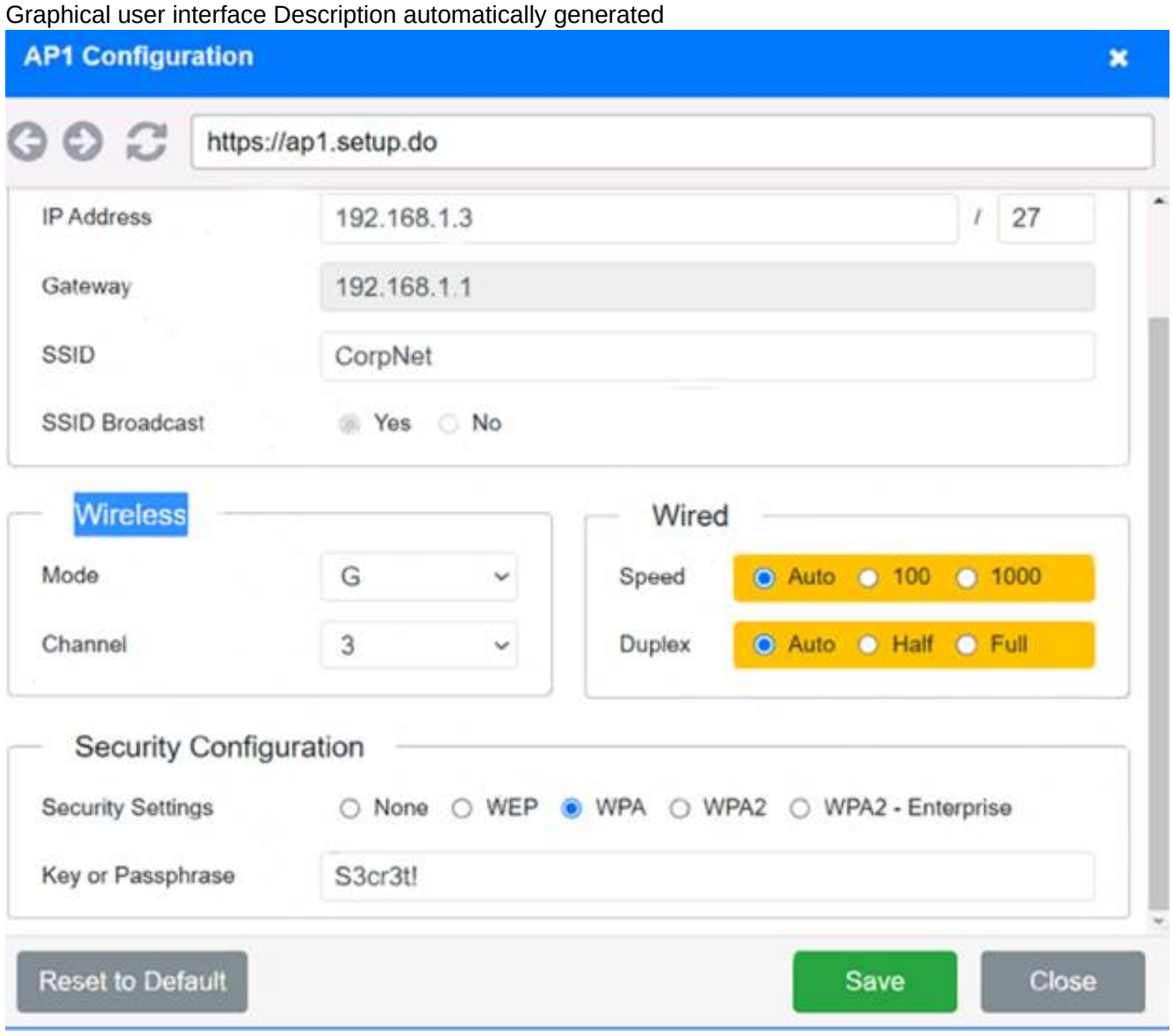
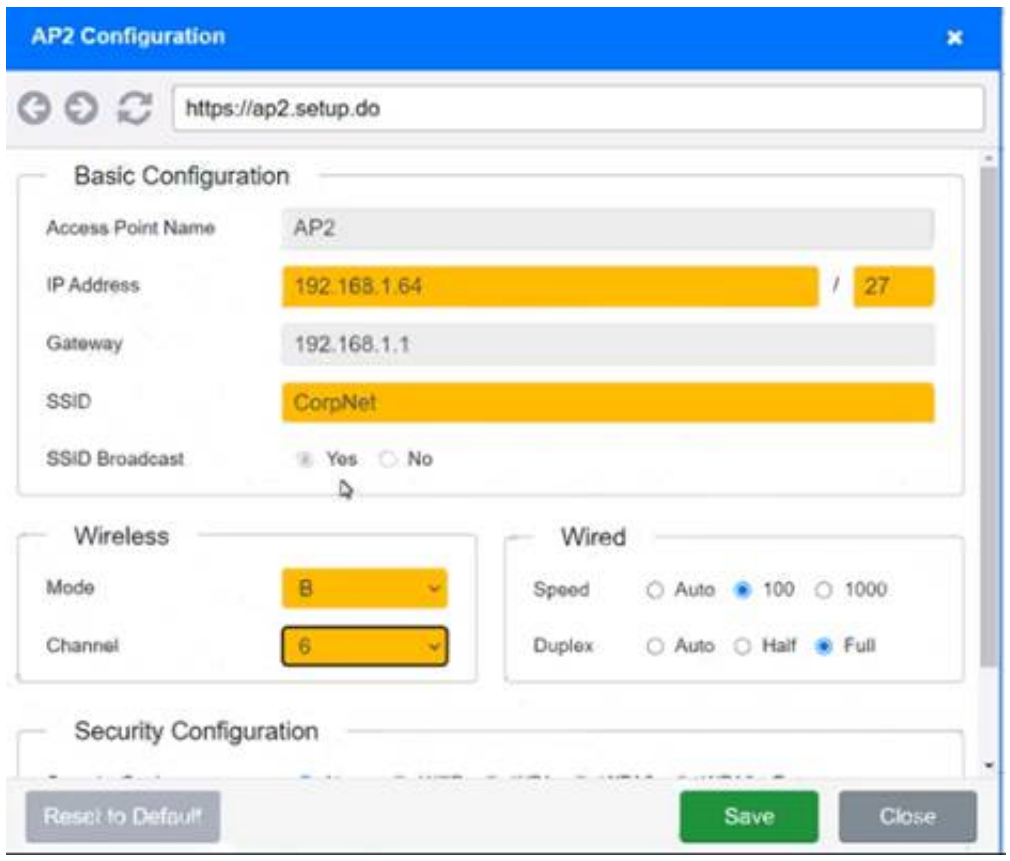


Exhibit 2 as follows Access Point Name AP2
Graphical user interface Description automatically generated



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

Graphical user interface Description automatically generated

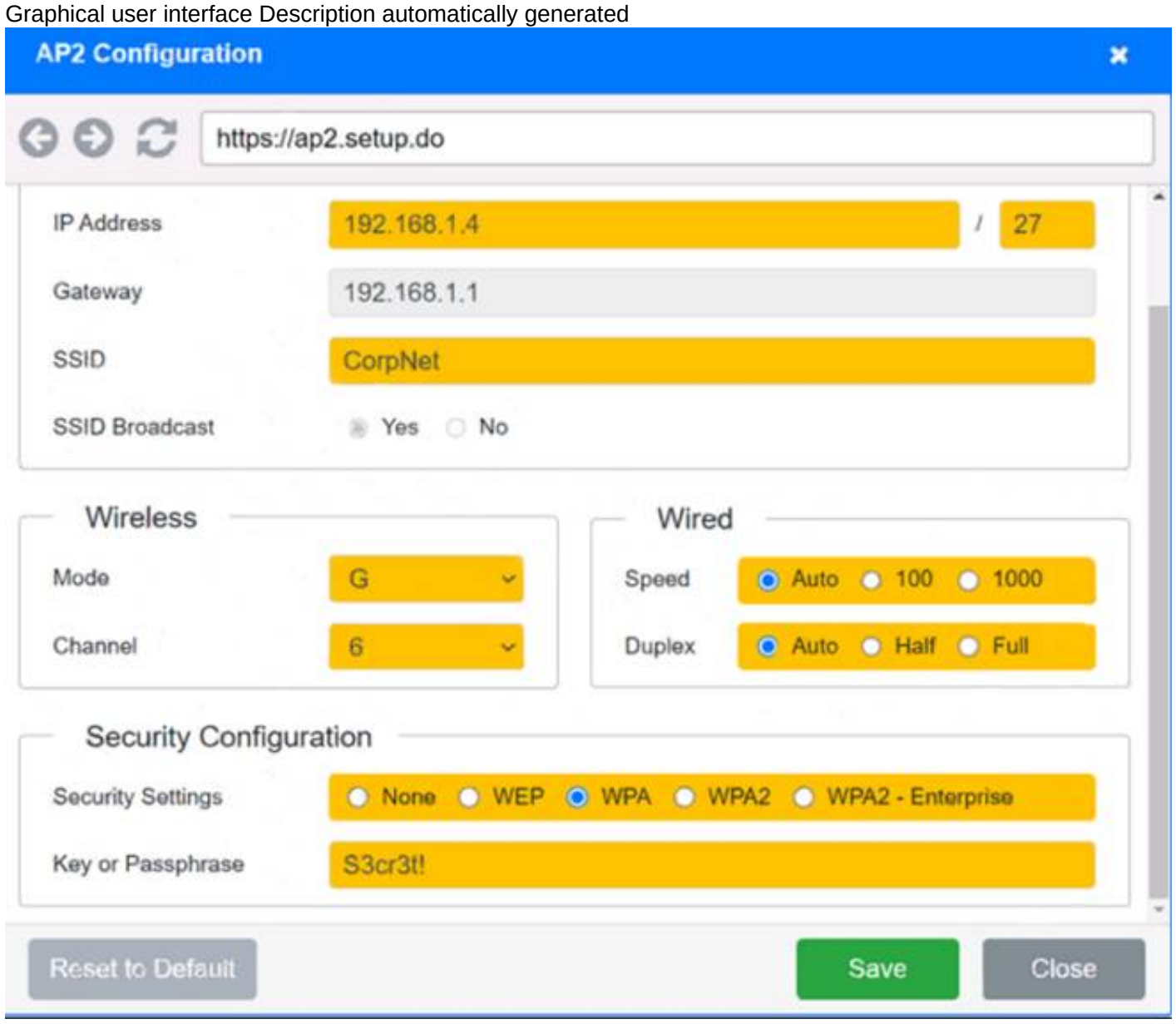
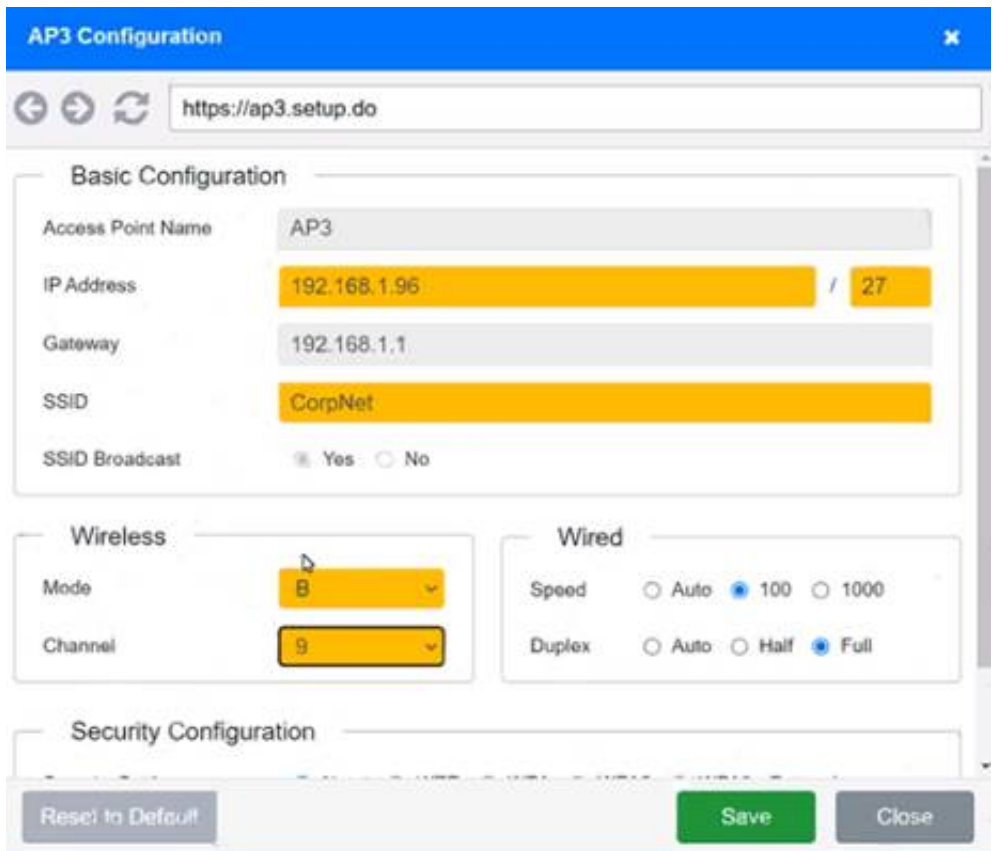
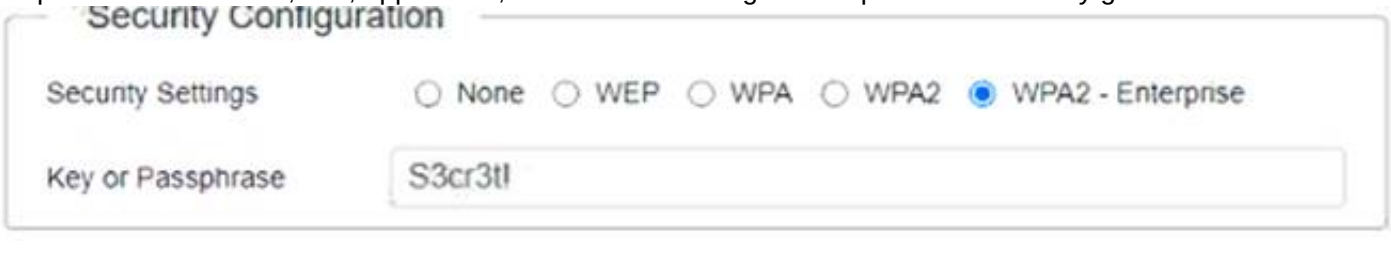


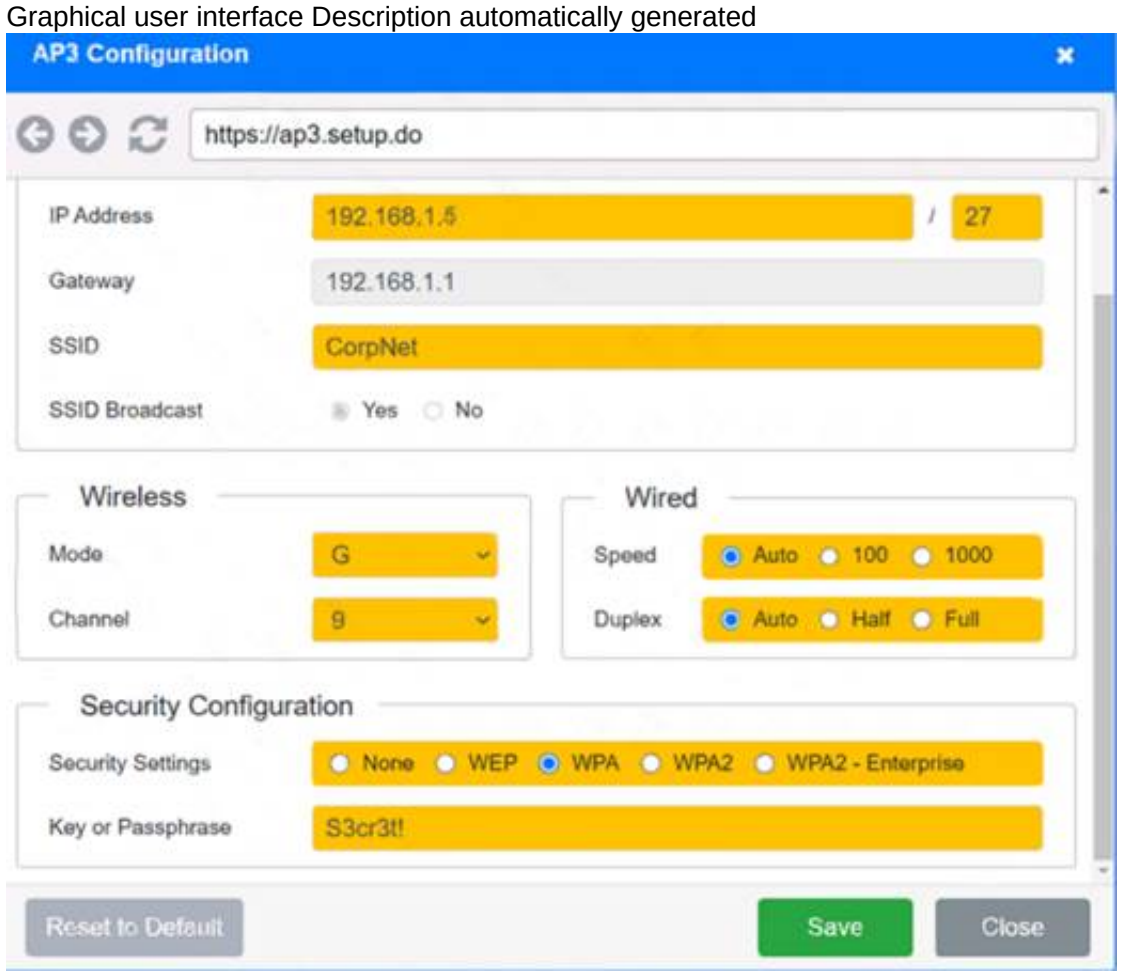
Exhibit 3 as follows Access Point Name AP3
Graphical user interface Description automatically generated



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



Graphical user interface Description automatically generated



NEW QUESTION 68
- (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 70

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

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

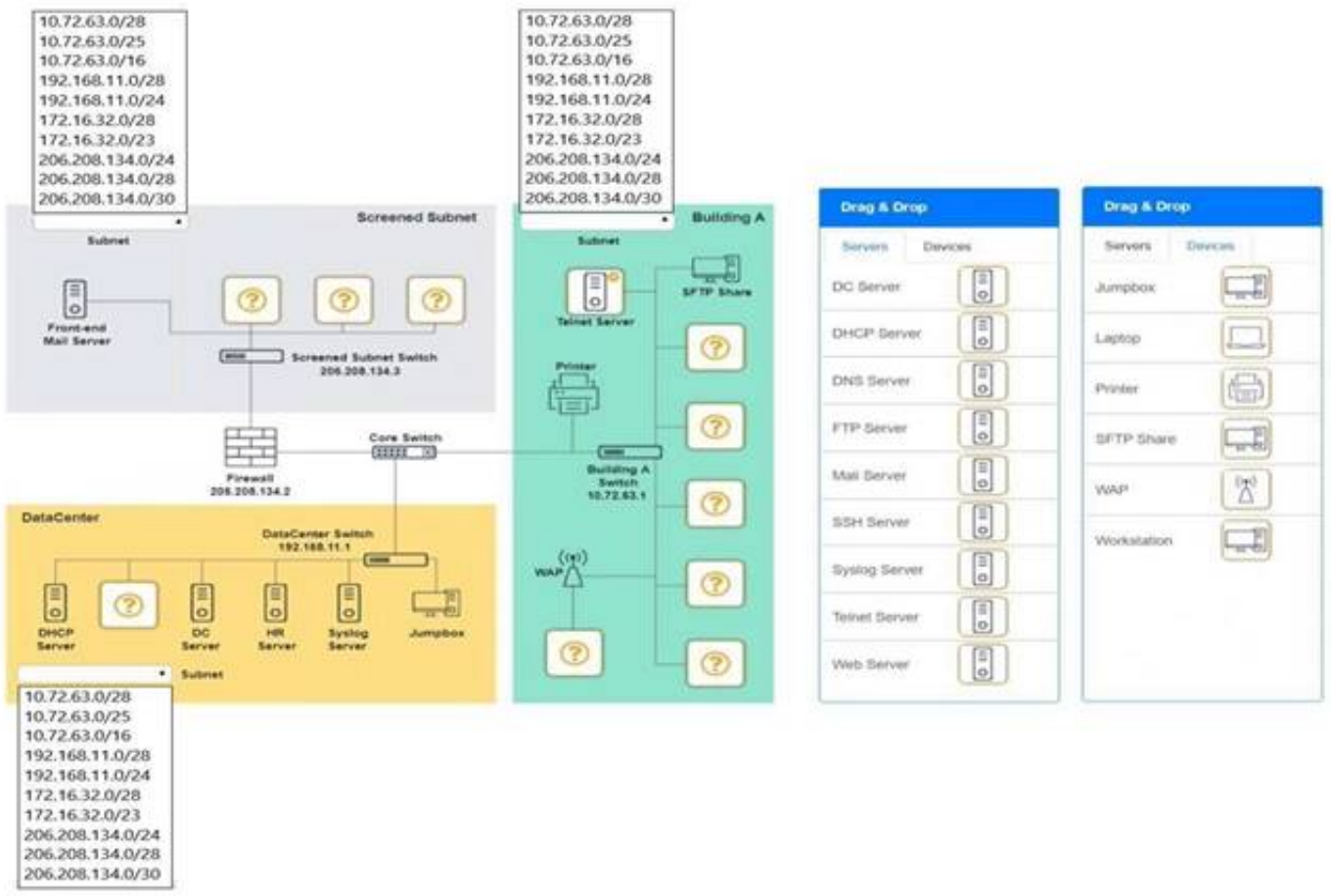
The network engineer observes that all users have lost Internet connectivity. Which of the following describes the issue?

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

Answer: C

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

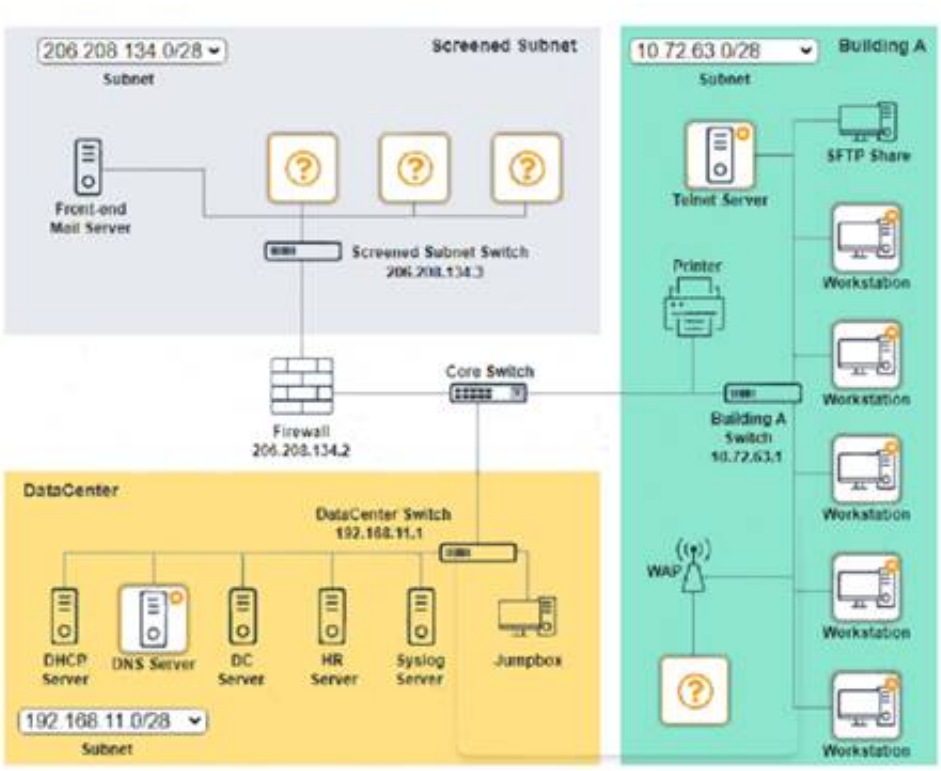
NEW QUESTION 74
- (Exam Topic 1)
You are tasked with verifying the following requirements are met in order to ensure network security. Requirements:
Datacenter
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage
Provide a dedicated server to resolve 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.

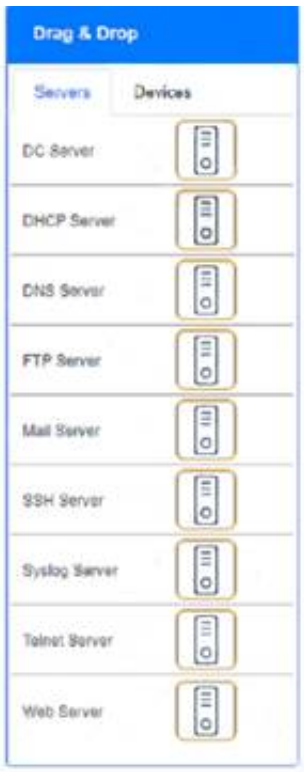


A. Mastered
B. Not Mastered

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 78
- (Exam Topic 1)
Which of the following technologies provides a failover mechanism for the default gateway?

A. FHRP
B. LACP
C. OSPF
D. STP

Answer: A

Explanation:
First Hop Redundancy Protocol (FHRP) provides a failover mechanism for the default gateway, allowing a backup gateway to take over if the primary gateway fails. References: CompTIA Network+ Certification Study Guide, Chapter 4: Infrastructure.

NEW QUESTION 79
- (Exam Topic 2)
Which of the following uses the destination IP address to forward packets?

A. A bridge
B. A Layer 2 switch
C. A router
D. A repeater

Answer: C

Explanation:
A router is a device that uses the destination IP address to forward packets between different networks. A bridge and a Layer 2 switch operate at the data link layer and use MAC addresses to forward frames within the same network. A repeater is a device that amplifies or regenerates signals at the physical layer.

NEW QUESTION 81
- (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 86
- (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 90
- (Exam Topic 2)
A technician is troubleshooting a previously encountered issue. Which of the following should the technician reference to find what solution was implemented to resolve the issue?

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

Answer: D

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

NEW QUESTION 91
- (Exam Topic 2)
There are two managed legacy switches running that cannot be replaced or upgraded. These switches do not support cryptographic functions, but they are password protected. Which of the following should a network administrator configure to BEST prevent unauthorized access?

A. Enable a management access list
B. Disable access to unnecessary services.
C. Configure a stronger password for access
D. Disable access to remote management
E. Use an out-of-band access method.

Answer: E

Explanation:
Using an out-of-band access method is the best way to prevent unauthorized access to the legacy switches that do not support cryptographic functions. Out-of-band access is a method of accessing a network device through a dedicated channel that is separate from the main network traffic. Out-of-band access can use physical connections such as serial console ports or dial-up modems, or logical connections such as VPNs or firewalls. Out-of-band access provides more security and reliability than in-band access, which uses the same network as the data traffic and may be vulnerable to attacks or failures. References: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book/

NEW QUESTION 96
- (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 99
- (Exam Topic 2)
Which of the following protocol types describes secure communication on port 443?

A. ICMP
B. UDP
C. TCP
D. IP

Answer: C

Explanation:
TCP is the protocol type that describes secure communication on port 443. TCP (Transmission Control Protocol) is a connection-oriented protocol that provides reliable and ordered delivery of data packets over an IP network. TCP uses port numbers to identify different applications or services on a device. Port 443 is the default port for HTTPS (Hypertext Transfer Protocol Secure), which is an extension of HTTP that uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) encryption to protect data in transit between a web server and a web browser. References:
https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

NEW QUESTION 102
- (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 104
- (Exam Topic 2)
A Chief Information Officer (CIO) wants to improve the availability of a company's SQL database Which of the following technologies should be utilized to achieve maximum availability?

A. Clustering
B. Port aggregation
C. NIC teaming
D. Snapshots

Answer: A

Explanation:
Clustering is a technique that involves grouping multiple servers or instances together to provide high
availability and fault tolerance for a database. Clustering can help improve the availability of a SQL database by allowing automatic failover and load balancing between the cluster nodes. If one node fails or becomes overloaded, another node can take over the database operations without disrupting the service.
References: https://www.educba.com/sql-cluster/

NEW QUESTION 105
- (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 107
- (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 111
- (Exam Topic 2)
Given the following output:

```
192.168.22.1     00-13-5d-00-c6-23
192.168.22.15    00-15-88-00-58-00
192.168.22.10    00-13-5d-00-c6-23
192.168.22.100   00-13-5d-00-c6-23
```

Which of the following attacks is this MOST likely an example of?

A. ARP poisoning
B. VLAN hopping
C. Rogue access point
D. Amplified DoS

Answer: A

Explanation:
The output is most likely an example of an ARP poisoning attack. ARP poisoning, also known as ARP spoofing, is a type of attack that exploits the ARP protocol to associate a malicious device's MAC address with a legitimate IP address on a local area network. This allows the attacker to intercept, modify, or redirect network traffic between two devices without their knowledge. The output shows that there are multiple entries for the same IP address (192.168.1.1) with different MAC addresses in the ARP cache of the device. This indicates that an attacker has sent fake ARP replies to trick the device into believing that its MAC address is associated with the IP address of another device (such as the default gateway). References: https://www.cisco.com/c/en/us/about/security-center/arp-spoofing.html

NEW QUESTION 114
- (Exam Topic 2)
An organization with one core and five distribution switches is transitioning from a star to a full-mesh topology Which of the following is the number of additional network connections needed?

A. 5
B. 7
C. 10
D. 15

Answer: C

Explanation:
10 additional network connections are needed to transition from a star to a full-mesh topology. A star topology is a network topology where each device is connected to a central device, such as a switch or a hub. A full-mesh topology is a network topology where each device is directly connected to every other device. The number of connections needed for a full-mesh topology can be calculated by the formula n(n-1)/2, where n is the number of devices. In this case, there are six devices (one core and five distribution switches), so the number of connections needed for a full-mesh topology is 6(6-1)/2 = 15. Since there are already five connections in the star topology (one from each distribution switch to the core switch), the number of additional connections needed is 15 - 5 = 10. References: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

NEW QUESTION 118
- (Exam Topic 2)
A network administrator wants to improve the security of the management console on the company's switches and ensure configuration changes made can be correlated to the administrator who conformed them Which of the following should the network administrator implement?

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

Answer: C

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

NEW QUESTION 121
- (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 122
- (Exam Topic 2)
A company requires a disaster recovery site to have equipment ready to go in the event of a disaster at its main datacenter. The company does not have the budget to mirror all the live data to the disaster recovery site. Which of the following concepts should the company select?

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

Answer: C

Explanation:
A warm site is a type of disaster recovery site that has equipment ready to go in the event of a disaster at the main datacenter, but does not have live data or applications. A warm site requires some time and effort to restore the data and services from backups, but it is less expensive than a hot site that has live data and applications. A cold site is a disaster recovery site that has no equipment or data, and requires a lot of time and money to set up after a disaster. A cloud site is a disaster recovery site that uses cloud computing resources to provide data and services, but it may have issues with bandwidth, latency, security, and cost.
References: https://www.comptia.org/blog/what-is-a-warm-site

NEW QUESTION 127
- (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 132
- (Exam Topic 2)
An IT technician suspects a break in one of the uplinks that provides connectivity to the core switch. Which of the following command-line tools should the technician use to determine where the incident is occurring?

A. nslookup
B. show config
C. netstat
D. show interface
E. show counters

Answer: D

Explanation:
show interface is a command-line tool that displays information about the status, configuration, and statistics of an interface on a network device. A technician can use show interface to determine where the incident is occurring in a network by checking the uplink status, speed, duplex mode, errors, collisions, and other parameters of each interface. References: https://www.comptia.org/blog/what-is-show-interface

NEW QUESTION 134
- (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 135
- (Exam Topic 2)
During the security audit of a financial firm the Chief Executive Officer (CEO) questions why there are three employees who perform very distinct functions on the server. There is an administrator for creating users another for assigning the users lo groups and a third who is the only administrator to perform file rights assignment Which of the following mitigation techniques is being applied'

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

Answer: B

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

NEW QUESTION 136
- (Exam Topic 2)
A client moving into a new office wants the IP network set up to accommodate 412 network-connected devices that are all on the same subnet. The subnet needs to be as small as possible. Which of the following subnet masks should be used to achieve the required result?

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

Answer: B

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

NEW QUESTION 137
- (Exam Topic 2)
A small, family-run business uses a single SOHO router to provide Internet and WiFi to its employees At the start of a new week, employees come in and find their usual WiFi network is no longer available, and there is a new wireless network to which they cannot connect. Given that information, which of the following should have been done to avoid this situation'

A. The device firmware should have been kept current.
B. Unsecure protocols should have been disabled.
C. Parental controls should have been enabled
D. The default credentials should have been changed

Answer: D

Explanation:
The default credentials are the username and password that come with a device or service when it is first installed or configured. They are often easy to guess or find online, which makes them vulnerable to unauthorized access or attacks. The default credentials should be changed to something unique and strong as soon as possible to avoid this situation. If the default credentials were not changed, someone could have accessed the SOHO router and changed the WiFi settings without the employees' knowledge. References: https://www.comptia.org/blog/network-security-basics-6-easy-ways-to-protect-your-network

NEW QUESTION 140
- (Exam Topic 2)
A company wants to implement a large number of WAPs throughout its building and allow users to be able to move around the building without dropping their connections Which of the following pieces of equipment would be able to handle this requirement?

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

Answer: C

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

NEW QUESTION 145
- (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 148
- (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 149
- (Exam Topic 3)
A company is reviewing ways to cut the overall cost of Its IT budget. A network technician suggests removing various computer programs from the IT budget and only providing these programs on an as-needed basis. Which of the following models would meet this requirement?

A. Multitinency
B. laaS
C. SaaS
D. VPN

Answer: C

Explanation:
SaaS stands for Software as a Service and is a cloud computing model where software applications are hosted and delivered over the internet by a service provider. SaaS can help the company cut the overall cost of its IT budget by eliminating the need to purchase, install, update, and maintain various computer programs on its own devices. The company can access the programs on an as-needed basis and pay only for what it uses. Multitenancy is a feature of cloud computing where multiple customers share the same physical or virtual resources. IaaS stands for Infrastructure as a Service and is a cloud computing model where computing resources such as servers, storage, and networking are provided over the internet by a service provider. VPN stands for Virtual Private Network and is a technology that creates a secure and encrypted connection over a public network.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 1.9: Compare and contrast common network service types.

NEW QUESTION 151
- (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 156
- (Exam Topic 3)

Which of the following has the capability to centrally manage configuration, logging, and firmware versioning for distributed devices?

A. WLAN controller
B. Load balancer
C. SIEM solution
D. Syslog server

Answer: A

Explanation:
A WLAN controller is a device that manages and controls multiple wireless access points (WAPs) in a wireless LAN (WLAN). A WLAN controller has the capability to centrally manage configuration, logging, and firmware versioning for distributed WAPs. A WLAN controller can also provide load balancing, security, and quality of service (QoS) for the WLAN.
References: Network+ Study Guide Objective 3.1: Explain the purposes and use cases for advanced networking devices.

NEW QUESTION 159
- (Exam Topic 3)
A network is experiencing extreme latency when accessing a particular website. Which of the following commands will BEST help identify the issue?

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

Answer: C

NEW QUESTION 164
- (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 169
- (Exam Topic 3)
Due to a surge in business, a company is onboarding an unusually high number of salespeople. The salespeople are assigned desktops that are wired to the network. The last few salespeople to be onboarded are able to access corporate materials on the network but not sales-specific resources. Which of the following is MOST likely the cause?

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

Answer: D

NEW QUESTION 174
- (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

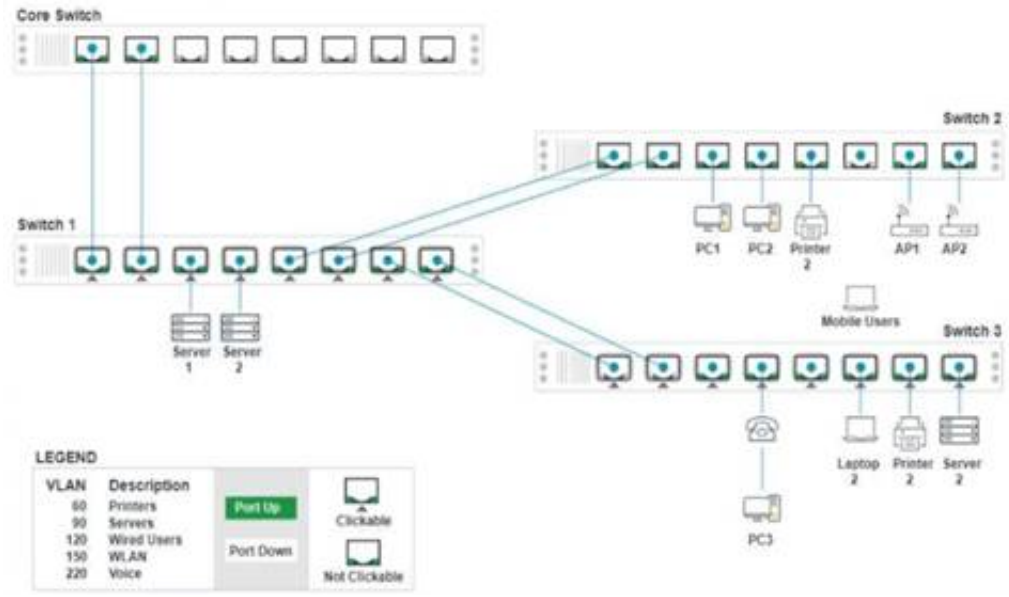
NEW QUESTION 179
- (Exam Topic 3)
Which of the following commands can be used to display the IP address, subnet address, gateway address, and DNS address on a Windows computer?

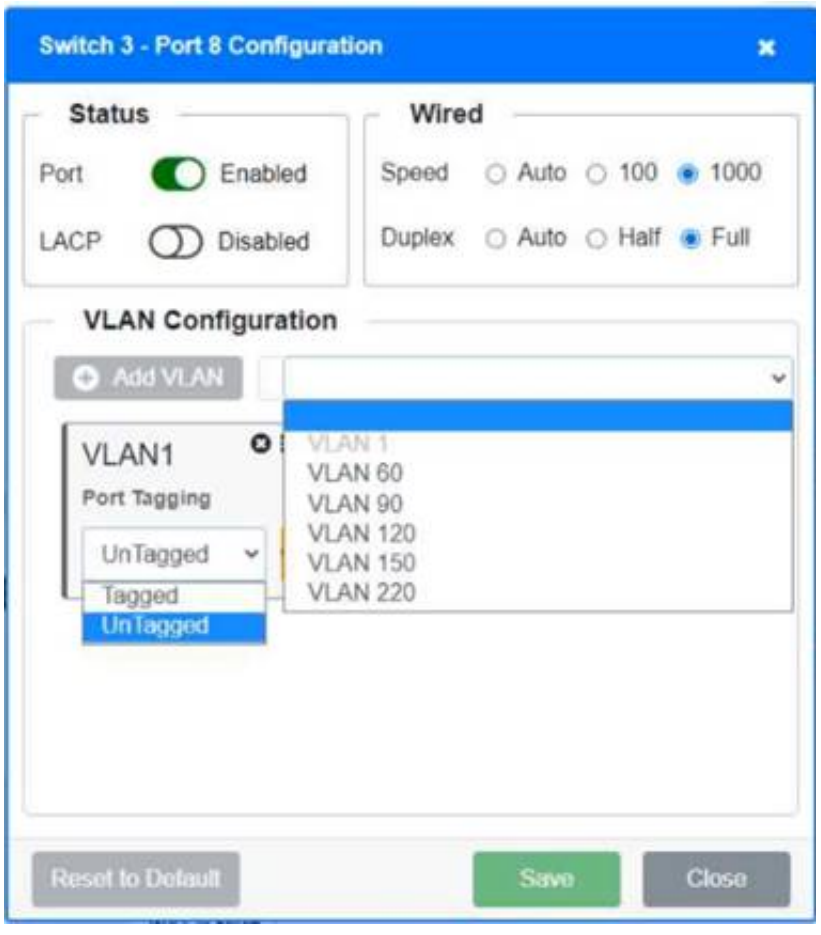
A. netstat -a
B. ifconfig
C. ip addr
D. ipconfig /all

Answer: D

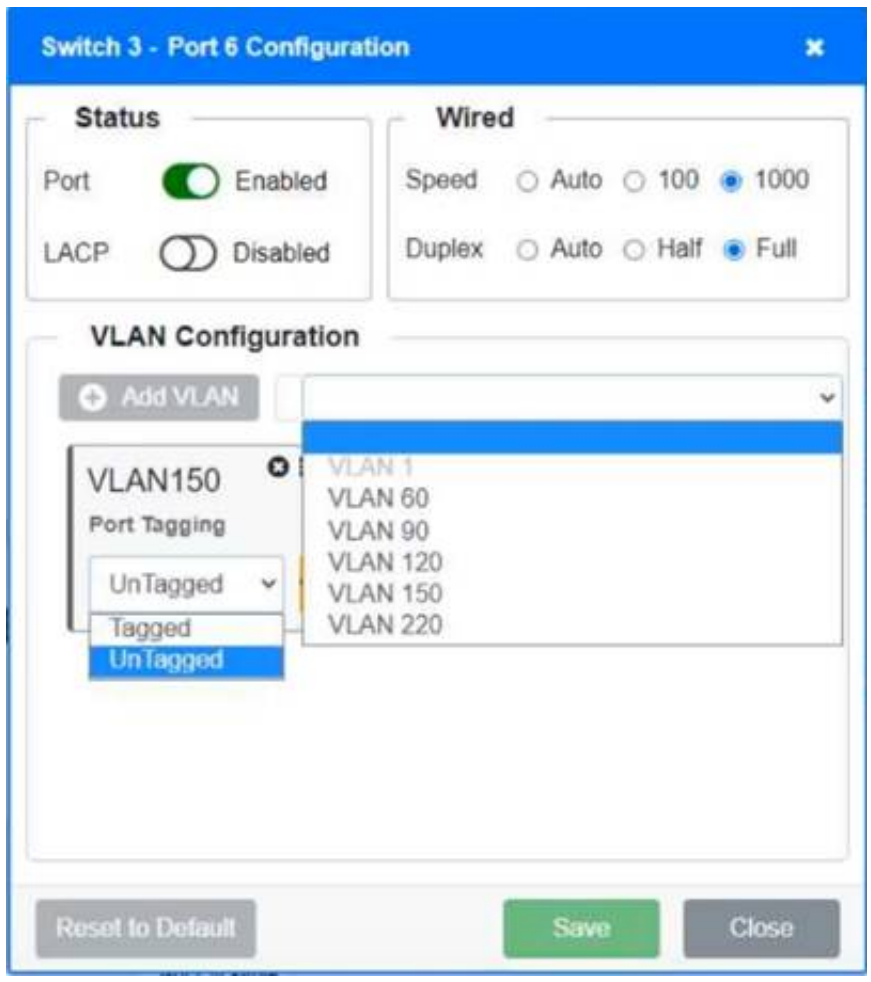
Explanation:
The ipconfig command is a utility that allows you to view and modify the network configuration of a Windows computer. By running the command "ipconfig /all", you can view detailed information about the network configuration of your computer, including the IP address, subnet mask, default 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.

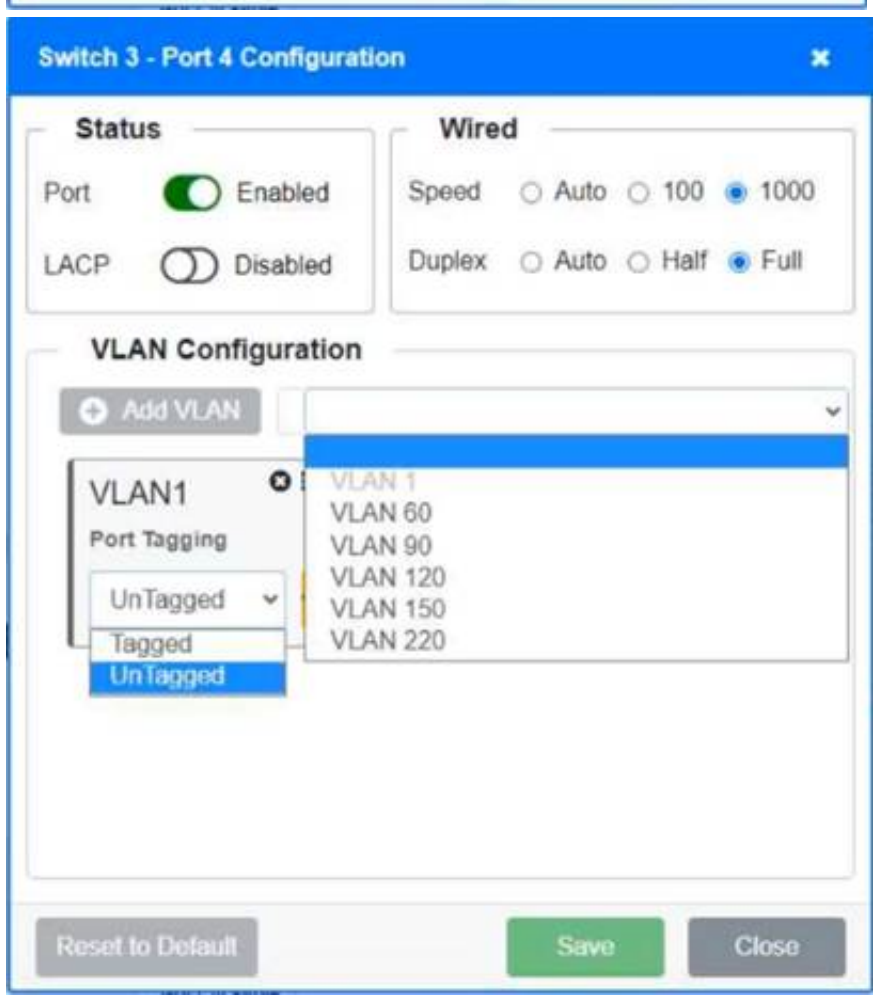
NEW QUESTION 182
- (Exam Topic 3)
SIMULATION
A network technician replaced a switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.
INSTRUCTIONS
Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings:
• Ensure 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.



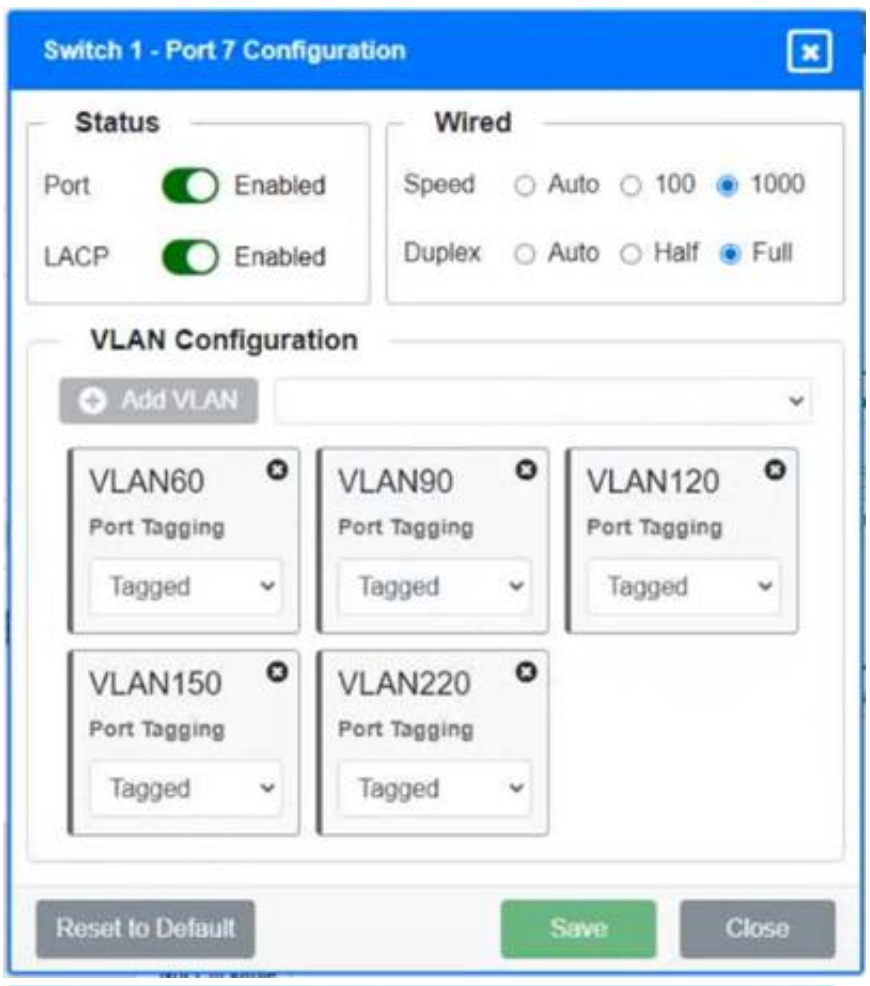


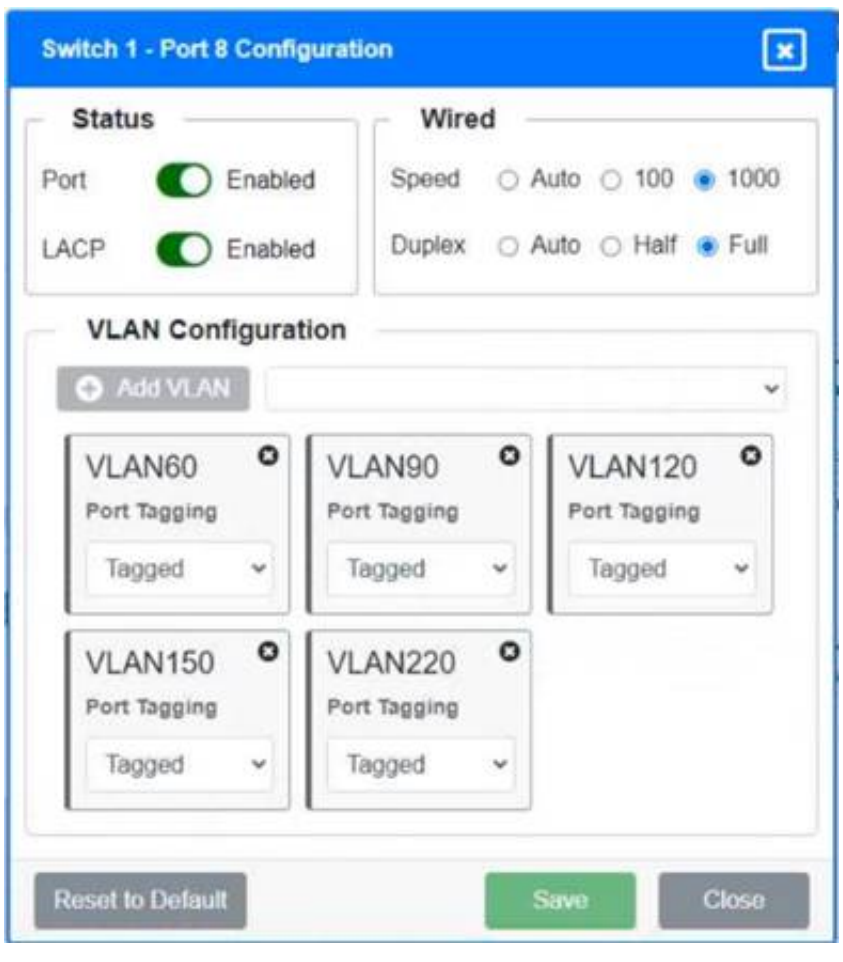
Switch 3 - Port 7 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close


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

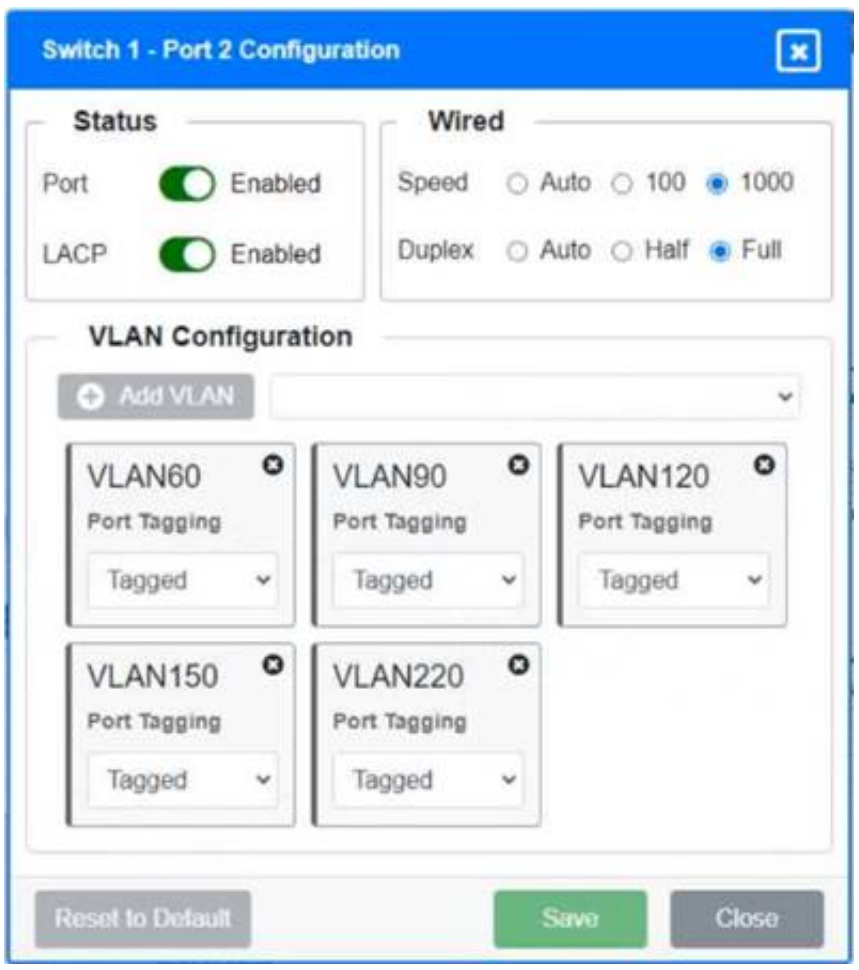

Switch 3 - Port 4 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

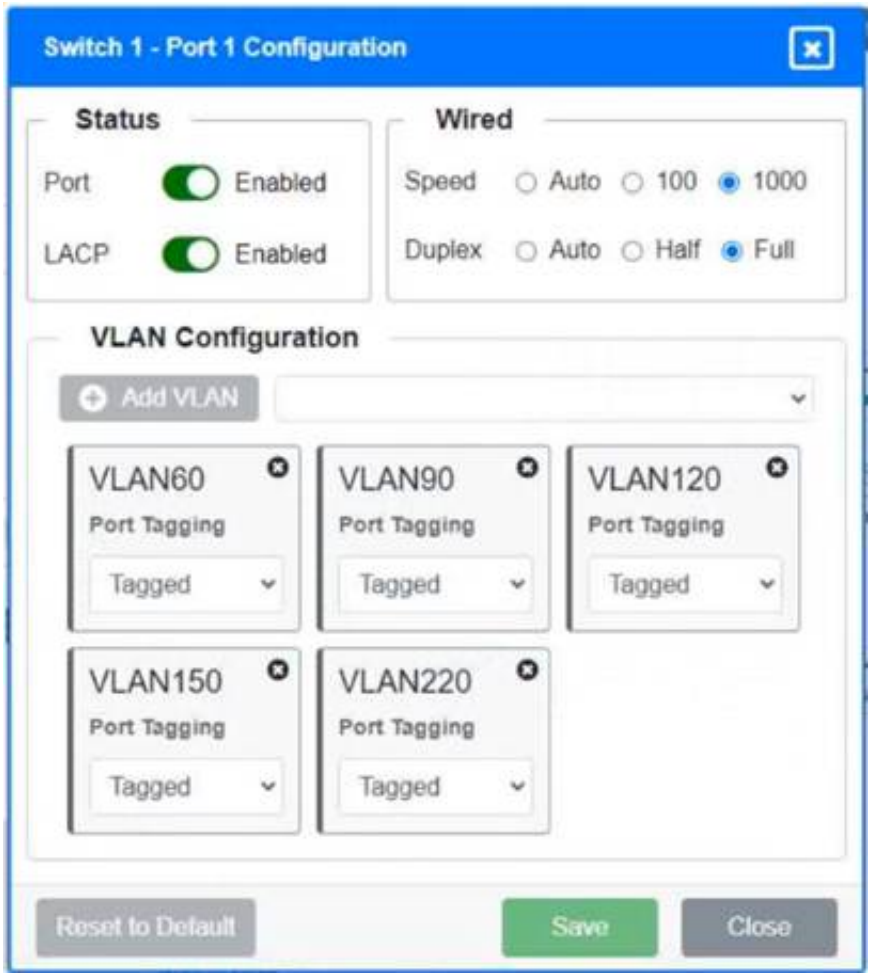
Switch 3 - Port 1 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close


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

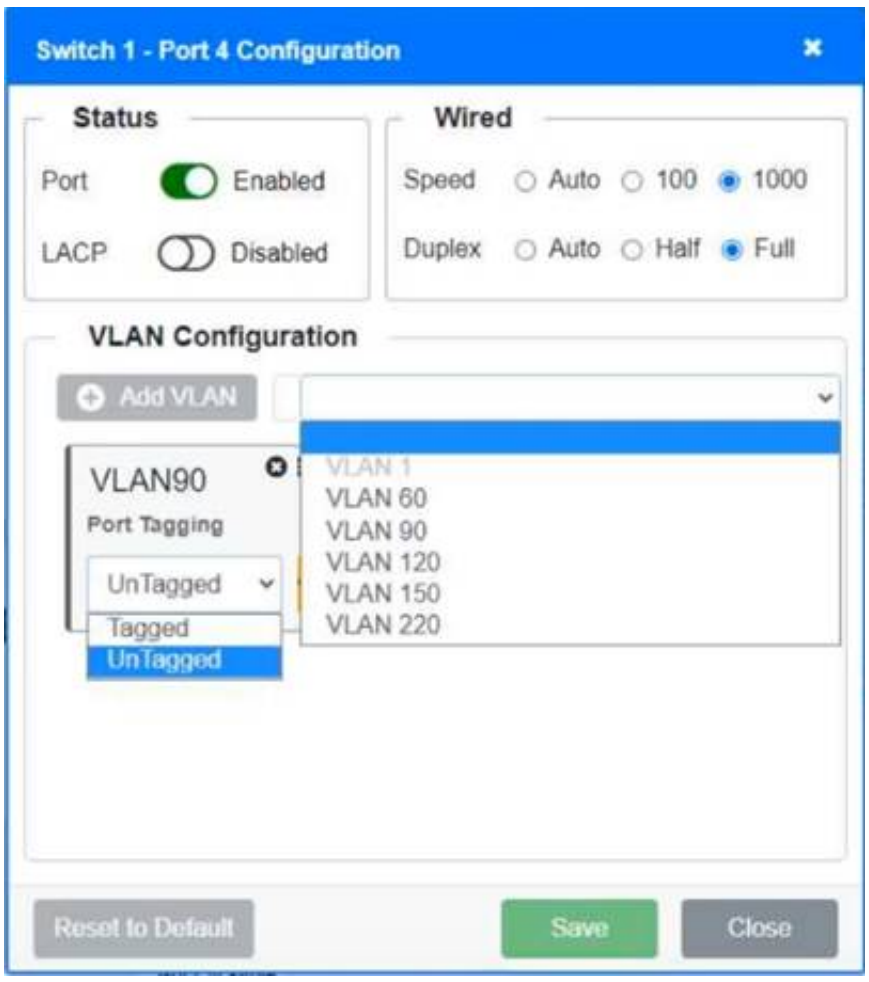

Switch 1 - Port 8 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save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

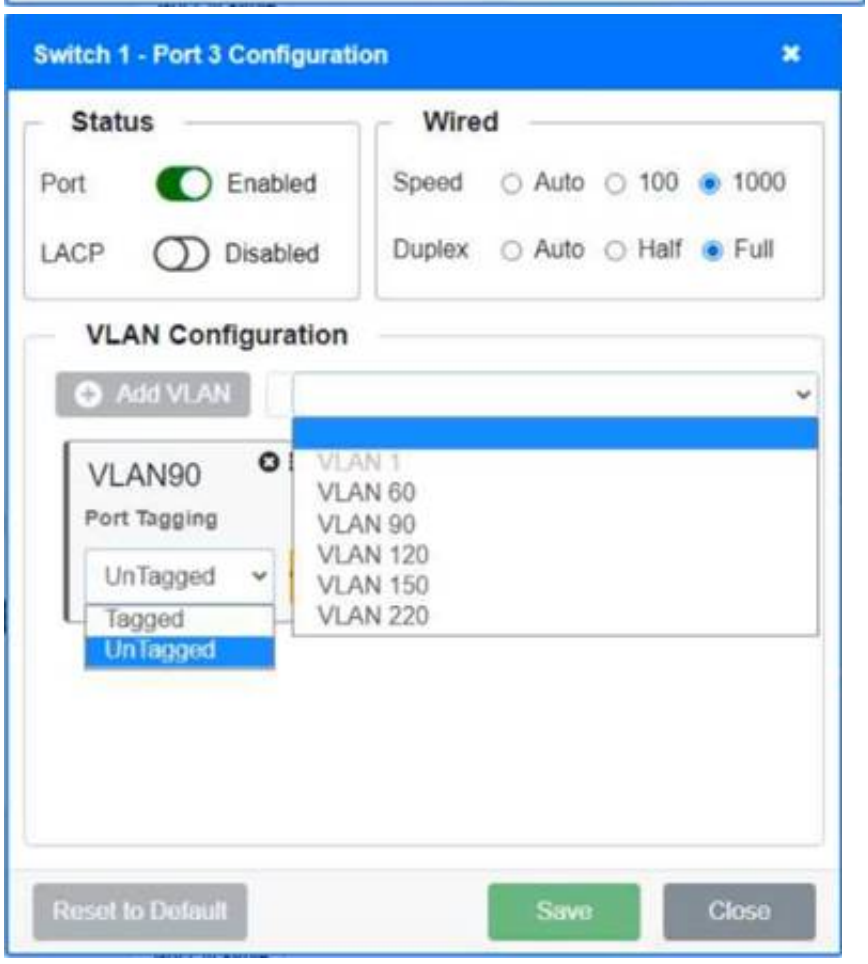
Switch 1 - Port 6 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
Reset to Default
Save
Close

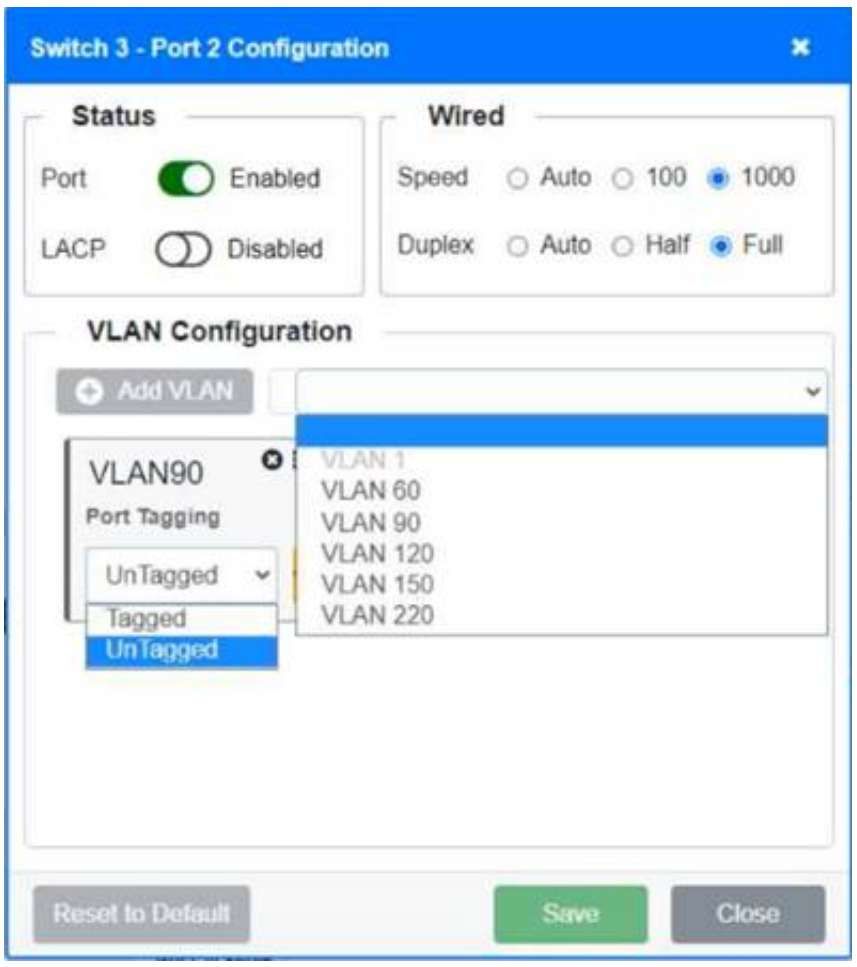

Switch 1 - Port 2 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
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 186
- (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 190
- (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 193
- (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 198
- (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 201
- (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 206
- (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 210
- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 214
- (Exam Topic 3)
A security administrator is trying to prevent incorrect IP addresses from being assigned to clients on the network. Which of the following would MOST likely prevent this and allow the network to continue to operate?

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

Answer: A

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

NEW QUESTION 219
- (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 221
- (Exam Topic 3)
A network technician needs to select an AP that will support at least 1.3Gbps and 5GHz only. Which of the following wireless standards must the AP support to meet the requirements?

A. B
B. AC
C. AX
D. N
E. G

Answer: B

Explanation:
Wireless AC is a wireless standard that supports up to 1.3Gbps data rate and operates in the 5GHz frequency band only. Wireless AC is also backward compatible with wireless A and N devices that use the 5GHz band. Wireless AC is suitable for high-performance applications such as HD video streaming and online gaming. References: Network+ Study Guide Objective 2.2: Explain the purposes and properties of routing and switching. Subobjective: Wireless standards and their characteristics.

NEW QUESTION 223
- (Exam Topic 3)
A company is undergoing expansion but does not have sufficient rack space in its data center. Which of the following would be BEST to allow the company to host its new equipment without a major investment in facilities?

A. Using a colocation service
B. Using available rack space in branch offices
C. Using a flat network topology
D. Reorganizing the network rack and installing top-of-rack switching

Answer: A

Explanation:
A colocation service is a service that provides rack space, power, cooling, security, and connectivity for a company's network equipment in a data center. A colocation service can be used when a company does not have sufficient rack space in its own data center and does not want to invest in building or expanding its own facilities. By using a colocation service, a company can host its new equipment in a professional and reliable environment without a major investment in facilities. References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 414)

NEW QUESTION 224
- (Exam Topic 3)
A technician is trying to determine whether an LACP bundle is fully operational. Which of the following commands will the technician MOST likely use?

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

Answer: A

Explanation:
https://www.cisco.com/c/en/us/td/docs/optical/cpt/r9_3/command/reference/cpt93_cr/cpt93_cr_chapter_01000.h

NEW QUESTION 225
- (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 230
- (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 233
- (Exam Topic 3)
A network administrator is investigating reports about network performance and finds high utilization on a switch uplink. The administrator is unsure whether this is an anomaly or normal behavior that will require an upgrade to resolve. Which Of the following should the administrator reference to gain historical perspective?

A. Device configuration review
B. ARP table export
C. Service-level agreement
D. Network performance baseline

Answer: D

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

NEW QUESTION 238
- (Exam Topic 3)
An ISP is unable to provide services to a user in a remote area through cable and DSL. Which of the following is the NEXT best solution to provide services

without adding external infrastructure?

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

Answer: C

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

NEW QUESTION 241
- (Exam Topic 3)
A building was recently remodeled in order to expand the front lobby. Some mobile users have been unable to connect to the available network jacks within the new lobby, while others have had no issues. Which of the following is the MOST likely cause of the connectivity issues?

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

Answer: B

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

NEW QUESTION 246
- (Exam Topic 3)
Which of the following BEST describes a spirt-tunnel client-to-server VPN connection?

A. The client sends an network traffic down the VPN tunnel
B. The client has two different IP addresses that can be connected to a remote site from two different ISPs to ensure availability
C. The client sends some network traffic down the VPN tunnel and other traffic to the local gateway.
D. The client connects to multiple remote sites at the same time

Answer: C

Explanation:
In a split-tunnel VPN, the client can access both the local network and the remote network simultaneously, with some network traffic sent through the VPN tunnel and other traffic sent to the local gateway. This approach allows for more efficient use of bandwidth and reduces the load on the VPN server. It also allows the client to continue accessing local resources while connected to the remote network.

NEW QUESTION 247
- (Exam Topic 3)
A technician is installing the Wi-Fi infrastructure for legacy industrial machinery at a warehouse. The equipment only supports 802.11a and 802.11b standards. Speed of transmission is the top business requirement. Which of the following is the correct maximum speed for this scenario?

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

Answer: B

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

NEW QUESTION 249
- (Exam Topic 3)
Which of the following topologies is designed to fully support applications hosted in on-premises data centers, public or private clouds, and SaaS services?

A. SDWAN
B. MAN
C. PAN
D. MPLS

Answer: A

NEW QUESTION 250

- (Exam Topic 3)
A switch is connected to another switch. Incompatible hardware causes a surge in traffic on both switches. Which of the following configurations will cause traffic to pause, allowing the switches to drain buffers?

A. Speed
B. Flow control
C. 802.1Q
D. Duplex

Answer: B

Explanation:
Flow control is a mechanism that allows a network device to regulate the amount of traffic it can receive or send. Flow control can help prevent congestion and buffer overflow by sending pause frames or signals to the sender when the receiver's buffer is full or nearly full. Flow control can cause traffic to pause, allowing the switches to drain buffers and resume normal operation. Speed is a parameter that determines the data transfer rate of a network link. 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 254
- (Exam Topic 3)
An auditor assessing network best practices was able to connect a rogue switch into a network Jack and get network connectivity. Which of the following controls would BEST address this risk?

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

Answer: A

NEW QUESTION 256
- (Exam Topic 3)
Which of the following options represents the participating computers in a network?

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

Answer: A

NEW QUESTION 261
- (Exam Topic 3)
A desktop support department has observed slow wireless speeds for a new line of laptops using the organization's standard image. No other devices have experienced the same issue. Which of the following should the network administrator recommend troubleshooting FIRST to resolve this issue?

A. Increasing wireless signal power
B. Installing a new WAP
C. Changing the protocol associated to the SSID
D. Updating the device wireless drivers

Answer: D

Explanation:
Wireless drivers can affect the performance and compatibility of your wireless connection5. If only a new line of laptops using the organization's standard image has experienced slow wireless speeds, it could be that their wireless drivers are outdated or incompatible with the network. Updating the device wireless drivers could resolve this issue.
Wireless drivers play an important role in the performance of a wireless connection, as they control how the device interacts with the wireless network. If the laptops in question are using an outdated version of the wireless driver, it could be causing the slow speeds. The network administrator should recommend updating the device wireless drivers first to see if this resolves the issue.

NEW QUESTION 265
- (Exam Topic 3)
A newly installed VoIP phone is not getting the DHCP IP address it needs to connect to the phone system. Which of the following tasks needs to be completed to allow the phone to operate correctly?

A. Assign the phone's switchport to the correct VLAN
B. Statically assign the phone's gateway address.
C. Configure a route on the VoIP network router.
D. Implement a VoIP gateway

Answer: A

NEW QUESTION 270
- (Exam Topic 3)

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

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

Answer: D

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

NEW QUESTION 271
- (Exam Topic 3)
A network technician is performing tests on a potentially faulty network card that is installed in a server. Which of the following addresses will MOST likely be used during traffic diagnostic tests?

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

Answer: B

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

NEW QUESTION 272
- (Exam Topic 3)
A technician is configuring a static IP address on a new device in a newly created subnet. The work order specifies the following requirements:
• The IP address should use the highest address available in the subnet.
• The default gateway needs to be set to 172.28.85.94.
• The subnet mask needs to be 255.255.255.224.
Which of the following addresses should the engineer apply to the device?

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

Answer: A

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

NEW QUESTION 274
- (Exam Topic 3)
A network technician 13 troubleshooting a specific port on a switch. Which of the following commands should the technician use to see the port configuration?

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

Answer: B

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

NEW QUESTION 279
- (Exam Topic 3)
A network security engineer locates an unapproved wireless bridge connected to the corporate LAN that is broadcasting a hidden SSID, providing unauthenticated access to internal resources. Which of the following types of attacks BEST describes this finding?

A. Rogue access point Most Voted
B. Evil twin
C. ARP spoofing
D. VLAN hopping

Answer: A

Explanation:
A rogue access point is an illegitimate access point plugged into a network to create a bypass from outside into the legitimate network. By contrast, an evil twin is a copy of a legitimate access point.

NEW QUESTION 284
- (Exam Topic 3)
A client who shares office space and an IT closet with another company recently reported connectivity issues throughout the network. Multiple third-party vendors regularly perform on-site maintenance in the shared IT closet. Which of the following security techniques would BEST secure the physical networking equipment?

A. Disabling unneeded switchports
B. Implementing role-based access
C. Changing the default passwords
D. Configuring an access control list

Answer: B

Explanation:
Role-based access is a security technique that assigns permissions and privileges to users or groups based on their roles or functions within an organization. Role-based access can help secure the physical networking equipment by limiting who can access, modify, or manage the devices in the shared IT closet. Only authorized personnel with a valid role and credentials should be able to access the networking equipment. Disabling unneeded switchports is a security technique that prevents unauthorized devices from connecting to the network by turning off unused ports on a switch. Changing the default passwords is a security technique that prevents unauthorized access to network devices by replacing the factory-set passwords with strong and unique ones. Configuring an access control list is a security technique that filters network traffic by allowing or denying packets based on criteria such as source and destination IP addresses, ports, or protocols.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.2: Given a scenario, use appropriate network hardening techniques.

NEW QUESTION 286
- (Exam Topic 3)
Which of the following compromises internet-connected devices and makes them vulnerable to becoming part of a botnet? (Select TWO)

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

Answer: BF

NEW QUESTION 289
- (Exam Topic 3)
A PC user who is on a local network reports very slow speeds when accessing files on the network server The user's PC Is connecting, but file downloads are very slow when compared to other users' download speeds The PC's NIC should be capable of Gigabit Ethernet. Which of the following will MOST likely fix the issue?

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

Answer: B

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

NEW QUESTION 290
- (Exam Topic 3)
A technician is troubleshooting reports that a networked printer is unavailable. The printer's IP address is configured with a DHCP reservation, but the address cannot be pinged from the print server in the same subnet. Which of the following is MOST likely the cause of me connectivity failure?

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

Answer: D

NEW QUESTION 295
- (Exam Topic 3)
Which of the following would be BEST suited for use at the access layer in a three-tier architecture system?

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

Answer: C

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

NEW QUESTION 297
- (Exam Topic 3)
A network engineer is investigating reports of poor network performance. Upon reviewing a report, the engineer finds hundreds of CRC errors on an interface. Which of the following is the MOST likely cause of these errors?

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

Answer: A

NEW QUESTION 301
- (Exam Topic 3)
Which of the following would be the MOST likely attack used to bypass an access control vestibule?

A. Tailgating
B. Phishing
C. Evil twin
D. Brute-force

Answer: A

Explanation:
Tailgating is when someone follows an authorized person into a restricted area without having the proper credentials. This is usually done by pretending to be with the authorized person, or by offering assistance. Tailgating is a social engineering attack and does not require any technical skill.

NEW QUESTION 303
- (Exam Topic 3)
A network resource was accessed by an outsider as a result of a successful phishing campaign. Which of the following strategies should be employed to mitigate the effects of phishing?

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

Answer: A

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

NEW QUESTION 308
- (Exam Topic 3)
A company is designing a SAN and would like to use STP as its medium for communication. Which of the following protocols would BEST suit me company's needs?

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

Answer: B

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

NEW QUESTION 311
- (Exam Topic 3)
A technician is investigating packet loss to a device that has varying data bursts throughout the day. Which of the following will the technician MOST likely configure to resolve the issue?

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

Answer: A

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

NEW QUESTION 313
- (Exam Topic 3)
An organization is interested in purchasing a backup solution that supports the organization's goals. Which of the following concepts would specify the maximum duration that a given service can be down before impacting operations?

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

Answer: B

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

NEW QUESTION 317
- (Exam Topic 3)
Which of the following can be used to store various types of devices and provide contactless delivery to users?

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

Answer: C

NEW QUESTION 322
- (Exam Topic 3)
A network engineer needs to reduce the overhead of file transfers. Which of the following configuration changes would accomplish that goal?

A. Link aggregation
B. Jumbo frames
C. Port security
D. Flow control
E. Lower FTP port

Answer: A

NEW QUESTION 325
- (Exam Topic 3)
An engineer recently decided to upgrade the firmware on a router. During the upgrade, the help desk received calls about a network outage, and a critical ticket was opened. The network manager would like to create a policy to prevent this from happening in the future. Which of the following documents should the manager create?

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

Answer: A

NEW QUESTION 329
- (Exam Topic 3)
Network traffic is being compromised by DNS poisoning every time a company's router is connected to the internet. The network team detects a non-authorized

DNS server being assigned to the network clients and remediates the incident by setting a trusted DNS server, but the issue occurs again after internet exposure. Which of the following best practices should be implemented on the router?

A. Change the device's default password.
B. Disable router advertisement guard.
C. Activate control plane policing.
D. Disable unneeded network services.

Answer: A

NEW QUESTION 331
- (Exam Topic 3)
A malicious user is using special software 10 perform an on-path attack. Which of the following best practices should be configured to mitigate this threat?

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

Answer: A

NEW QUESTION 335
- (Exam Topic 3)
A company is moving to a new building designed with a guest waiting area that has existing network ports. Which of the following practices would BEST secure the network?

A. Ensure all guests sign an NDA.
B. Disable unneeded switchports in the area.
C. Lower the radio strength to reduce Wi-Fi coverage in the waiting area.
D. Enable MAC filtering to block unknown hardware addresses.

Answer: B

Explanation:
One of the best practices to secure the network would be to disable unneeded switchports in the guest waiting area. This will prevent unauthorized users from connecting to the network through these ports. It's important to identify which switchports are not in use and disable them, as this will prevent unauthorized access to the network.
Other practices such as ensuring all guests sign an NDA, lowering the radio strength to reduce Wi-Fi coverage in the waiting area and enabling MAC filtering to block unknown hardware addresses are not as effective in securing the network as disabling unneeded switchports. Enforcing an NDA with guests may not stop a malicious user from attempting to access the network, reducing the radio strength only limits the Wi-Fi coverage, and MAC filtering can be easily bypassed by hackers.

NEW QUESTION 338
- (Exam Topic 3)
Classification using labels according to information sensitivity and impact in case of unauthorized access or leakage is a mandatory component of:

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

Answer: C

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

NEW QUESTION 341
- (Exam Topic 3)
A network client is trying to connect to the wrong TCP port. Which of the following responses would the client MOST likely receive?

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

Answer: A

NEW QUESTION 346
- (Exam Topic 3)
A company's data center is hosted at its corporate office to ensure greater control over the security of sensitive data. During times when there are increased workloads, some of the company’s non-sensitive data is shifted to an external cloud provider. Which of the following cloud deployment models does this describe?

A. Hybrid
B. Community
C. Public

D. Private

Answer: A

NEW QUESTION 350
- (Exam Topic 3)
A technician removes an old PC from the network and replaces it with a new PC that is unable to connect to the LAN. Which of the Mowing is MOST likely the cause of the issue?

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

Answer: A

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

NEW QUESTION 353
- (Exam Topic 3)
A corporate client is experiencing global system outages. The IT team has identified multiple potential underlying causes throughout the enterprise Each team member has been assigned an area to trouble shoot. Which of the following approaches is being used?

A. Divide-and-conquer
B. Top-to-bottom
C. Bottom-to-top
D. Determine if anything changed

Answer: A

NEW QUESTION 355
- (Exam Topic 3)
A network administrator is decommissioning a server. Which of the following will the network administrator MOST likely consult?

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

Answer: D

NEW QUESTION 356
- (Exam Topic 3)
A company joins a bank's financial network and establishes a connection to the clearinghouse servers in the range 192 168.124.0/27. An IT technician then realizes the range exists within the VM pool at the data center. Which of the following is the BEST way for the technician to connect to the bank's servers?

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

Answer: A

NEW QUESTION 358
- (Exam Topic 3)
A network technician is hired to review all the devices within a network and make recommendations to improve network efficiency. Which of the following should the technician do FIRST before reviewing and making any recommendations?

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

Answer: A

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

NEW QUESTION 362
- (Exam Topic 3)

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

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

Answer: A

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

NEW QUESTION 366
- (Exam Topic 3)
Which of the following connectors and terminations are required to make a Cat 6 cable that connects from a PC to a non-capable MDIX switch? (Select TWO).

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

Answer: AD

NEW QUESTION 369
- (Exam Topic 3)
Which of the following describes the BEST device to configure as a DHCP relay?

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

Answer: B

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

NEW QUESTION 370
- (Exam Topic 3)
Which of the following must be functioning properly in order for a network administrator to create an accurate timeline during a troubleshooting process?

A. NTP
B. IP helper
C. Syslog
D. MySQL

Answer: A

NEW QUESTION 371
- (Exam Topic 3)
Which of the following ports should be used to securely receive mail that is synchronized across multiple devices?

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

Answer: D

NEW QUESTION 372
- (Exam Topic 3)
A network administrator is investigating a performance issue on a dual-link connection—VPN and MPLS—to a partner network. The MPLS is the primary path, and the VPN is used as a backup. While communicating, the delay is measured at 18ms, which is higher than the 6ms expected when the MPLS link is operational but lower than the 30ms expected tor the VPN connection. Which of the following will MOST likely point to the root cause of the Issue?

A. Checking the routing tables on both sides to ensure there is no asymmetric routing
B. Checking on the partner network for a missing route pointing to the VPN connection

C. Running iPerf on both sides to confirm the delay that Is measured is accurate
D. Checking for an incorrect VLAN assignment affecting the MPLS traffic

Answer: A

Explanation:
Asymmetric routing can occur when two routers have different paths for the same two hosts, resulting in increased latency and possible packet loss. According to the CompTIA Network+ Study Manual, “If the path from the source to the destination is not the same in both directions, the packets will take different routes and the latency can increase significantly.” To confirm this, the network administrator should check the routing tables on both sides of the connection and ensure that the same path is used in both directions.

NEW QUESTION 374
- (Exam Topic 3)
A network attack caused a network outage by wiping the configuration and logs of the border firewall. Which of the following sources, in an investigation to determine how the firewall was compromised, can provide the MOST detailed data?

A. Syslog server messages
B. MIB of the attacked firewall
C. Network baseline reports
D. NetFlow aggregate data

Answer: A

NEW QUESTION 377
- (Exam Topic 3)
An organization set up its offices so that a desktop is connected to the network through a VoIP phone. The VoIP vendor requested that voice traffic be segmented separately from non-voice traffic. Which of the following would allow the organization to configure multiple devices with network isolation on a single switch port?

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

Answer: A

NEW QUESTION 381
- (Exam Topic 3)
An IT technician is working on a support ticket regarding an unreachable web-site. The technician has utilized the ping command to the website, but the site is still unreachable. Which of the following tools should the technician use NEXT?

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

Answer: B

Explanation:
tracert is a command-line tool that can trace the route of a packet from the source to the destination. It can show the number of hops, the IP address and hostname of each router, and the round-trip time for each hop. tracert can help the technician troubleshoot the unreachable website by identifying where the packet is dropped or delayed along the path. ipconfig is a command-line tool that can display and configure the IP settings of a network interface. arp is a command-line tool that can display and manipulate the Address Resolution Protocol (ARP) cache, which maps IP addresses to MAC addresses. netstat is a command-line tool that can display network connections, routing tables, and statistics.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.4: Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

NEW QUESTION 385
- (Exam Topic 3)
A technician notices that equipment is being moved around and misplaced in the server room, even though the room has locked doors and cabinets. Which of the following would be the BEST solution to identify who is responsible?

A. Install motion detection
B. Install cameras.
C. Install tamper detection.
D. Hire a security guard.

Answer: B

Explanation:
Installing cameras in the server room is the best solution to identify who is responsible for the equipment being moved and misplaced. Cameras provide a way to monitor the server room in real time and can be used to identify suspicious activity. Additionally, they provide a way to review past activity and allow you to review footage to determine who may be responsible for the misplacement of equipment.

NEW QUESTION 386
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your N10-009 Exam with Our Prep Materials Via below:

https://www.certleader.com/N10-009-dumps.html