Exam Questions N10-009

CompTIA Network+ Exam

https://www.2passeasy.com/dumps/N10-009/

NEW QUESTION 1
- (Exam Topic 1)
Which of the following TCP ports is used by the Windows OS for file sharing?

A. 53
B. 389
C. 445
D. 1433

Answer: C

Explanation:
TCP port 445 is used by the Windows OS for file sharing. It is also known as SMB (Server Message Block) or CIFS (Common Internet File System) and allows users to access files, printers, and other shared resources on a network. References:
https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smb

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

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

Answer: A

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

NEW QUESTION 3
- (Exam Topic 1)
Wireless users are reporting intermittent internet connectivity. Connectivity is restored when the users disconnect and reconnect, utilizing the web authentication process each time. The network administrator can see the devices connected to the APs at all times. Which of the following steps will MOST likely determine the cause of the issue?

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

Answer: A

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

NEW QUESTION 4
- (Exam Topic 1)
Which of the following would be BEST to use to detect a MAC spoofing attack?

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

Answer: B

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

NEW QUESTION 5
- (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 6
- (Exam Topic 1)
An attacker is attempting to find the password to a network by inputting common words and phrases in plaintext to the password prompt. Which of the following attack types BEST describes this action?

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

Answer: D

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

NEW QUESTION 7
- (Exam Topic 1)
A workstation is configured with the following network details:

IP address	Subnet mask	Default gateway
10.1.2.23	10.1.2.0/27	10.1.2.1

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

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

Answer: D

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

NEW QUESTION 8
- (Exam Topic 1)
A network administrator is installing a wireless network at a client's office. Which of the following IEEE 802.11 standards would be BEST to use for multiple simultaneous client access?

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

Answer: C

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

NEW QUESTION 9
- (Exam Topic 1)
A technician is connecting multiple switches to create a large network for a new office. The switches are unmanaged Layer 2 switches with multiple connections between each pair. The network is experiencing an extreme amount of latency. Which of the following is MOST likely occurring?

A. Ethernet collisions
B. A DDoS attack
C. A broadcast storm
D. Routing loops

Answer: C

Explanation:
A broadcast storm is most likely occurring when connecting multiple unmanaged Layer 2 switches with multiple connections between each pair. A broadcast storm is a situation where broadcast packets flood a network segment and consume all the available bandwidth. It can be caused by loops in the network topology, where broadcast packets are endlessly forwarded by switches without any loop prevention mechanism. Unmanaged switches do not support features such as Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) that can detect and block loops. References:
https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10556-16.html

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

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

Answer: A

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

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

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

Answer: C

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

NEW QUESTION 13
- (Exam Topic 1)
Given the following information:

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

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

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

Answer: D

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

NEW QUESTION 15
- (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 18
- (Exam Topic 1)
Which of the following can be used to centrally manage credentials for various types of administrative privileges on configured network devices?

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

Answer: B

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

NEW QUESTION 21
- (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 22
- (Exam Topic 1)
Which of the following transceiver types can support up to 40Gbps?

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

Answer: B

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

NEW QUESTION 26
- (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 31
- (Exam Topic 1)
A technician is searching for a device that is connected to the network and has the device's physical network address. Which of the following should the technician review on the switch to locate the device's network port?

A. IP route table
B. VLAN tag
C. MAC table
D. QoS tag

Answer: C

Explanation:
To locate a device's network port on a switch, a technician should review the switch's MAC address table. The MAC address table maintains a list of MAC addresses of devices connected to each port on the switch. By checking the MAC address of the device in question, the technician can identify the port to which the device is connected.
References: CompTIA Network+ Certification Study Guide, Sixth Edition by Glen E. Clarke

NEW QUESTION 36
- (Exam Topic 1)
A technician receives feedback that some users are experiencing high amounts of jitter while using the wireless network. While troubleshooting the network, the technician uses the ping command with the IP address of the default gateway and verifies large variations in latency. The technician thinks the issue may be interference from other networks and non-802.11 devices. Which of the following tools should the technician use to troubleshoot the issue?

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

Answer: D

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

NEW QUESTION 40
- (Exam Topic 1)
A client recently added 100 users who are using VMs. All users have since reported slow or unresponsive desktops. Reports show minimal network congestion, zero packet loss, and acceptable packet delay. Which of the following metrics will MOST accurately show the underlying performance issues? (Choose two.)

A. CPU usage
B. Memory
C. Temperature
D. Bandwidth
E. Latency
F. Jitter

Answer: AB

NEW QUESTION 44
- (Exam Topic 1)
A network administrator is designing a new datacenter in a different region that will need to communicate to the old datacenter with a secure connection. Which of the following access methods would provide the BEST security for this new datacenter?

A. Virtual network computing
B. Secure Socket Shell
C. In-band connection
D. Site-to-site VPN

Answer: D

Explanation:
Site-to-site VPN provides the best security for connecting a new datacenter to an old one because it creates a secure tunnel between the two locations, protecting data in transit. References: CompTIA Network+ Certification Study Guide, Chapter 5: Network Security.

NEW QUESTION 49
- (Exam Topic 1)
The network administrator is informed that a user's email password is frequently hacked by brute-force programs. Which of the following policies should the network administrator implements to BEST mitigate this issue? (Choose two.)

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

Answer: BC

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

NEW QUESTION 53
- (Exam Topic 1)
A company hired a technician to find all the devices connected within a network. Which of the following software tools would BEST assist the technician in completing this task?

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

Answer: A

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

NEW QUESTION 55
- (Exam Topic 1)
A technician is troubleshooting a network switch that seems to stop responding to requests intermittently whenever the logging level is set for debugging. Which of the following metrics should the technician check to begin troubleshooting the issue?

A. Audit logs
B. CPU utilization
C. CRC errors
D. Jitter

Answer: B

Explanation:
CPU utilization is a metric that measures the percentage of time a CPU spends executing instructions. When the logging level is set for debugging, the router may generate a large amount of logging data, which can increase CPU utilization and cause the router to stop responding to requests intermittently. References:
- Network+ N10-008 Objectives: 2.1 Given a scenario, troubleshoot common physical connectivity issues.

NEW QUESTION 57
- (Exam Topic 1)
An engineer is configuring redundant network links between switches. Which of the following should the engineer enable to prevent network stability issues?

A. 802.1Q
B. STP
C. Flow control
D. CSMA/CD

Answer: B

Explanation:
Spanning Tree Protocol (STP) should be enabled when configuring redundant network links between switches. STP ensures that only one active path is used at a time, preventing network loops and stability issues.
References:
- CompTIA Network+ Certification Study Guide

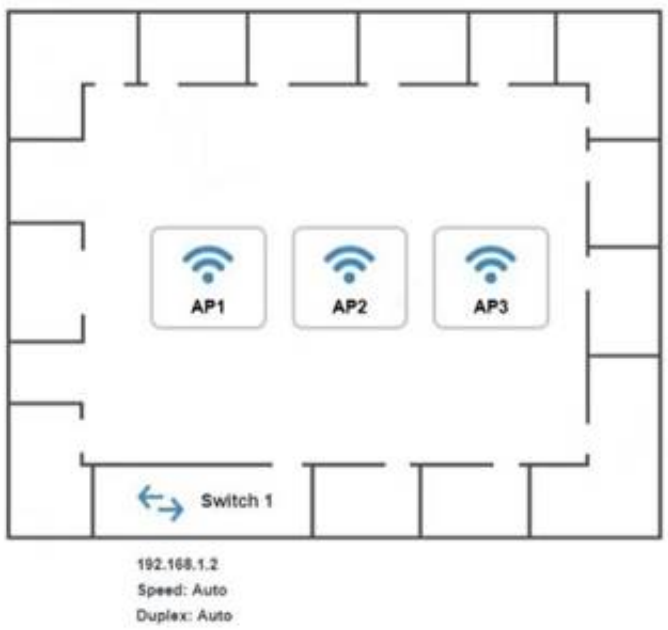
NEW QUESTION 62
- (Exam Topic 1)
Which of the following is the physical topology for an Ethernet LAN?

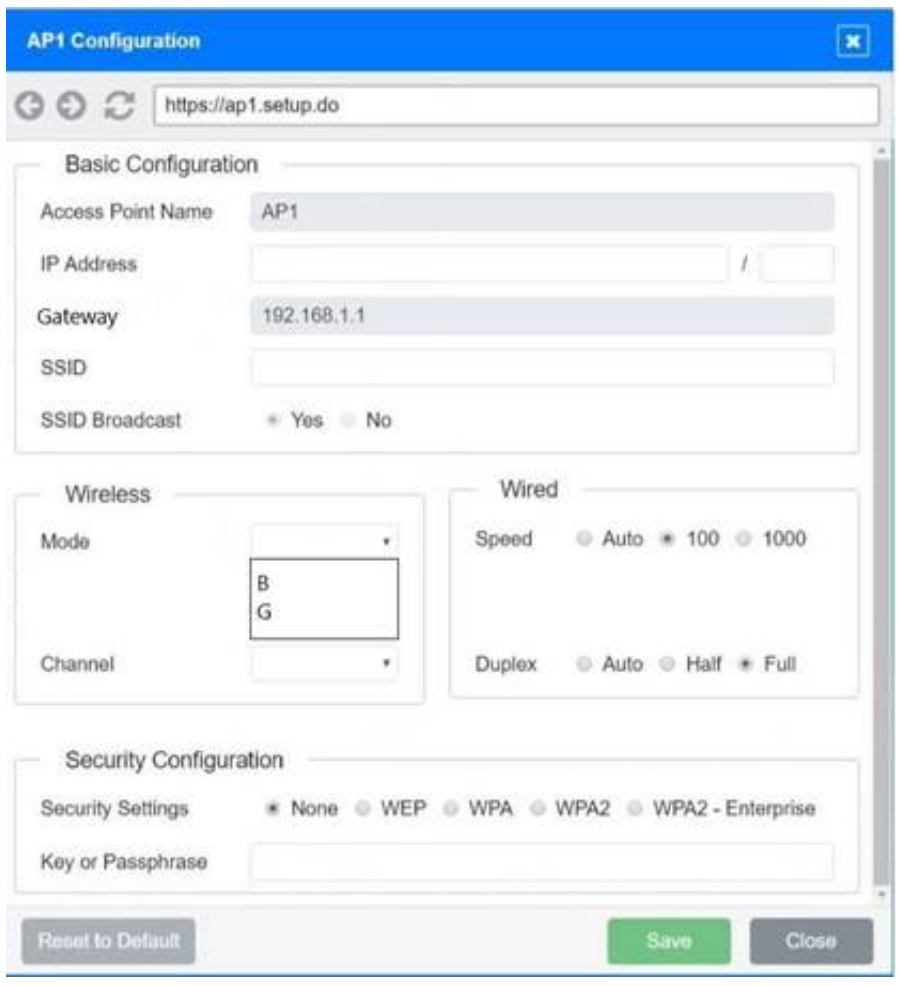
A. Bus
B. Ring
C. Mesh
D. Star

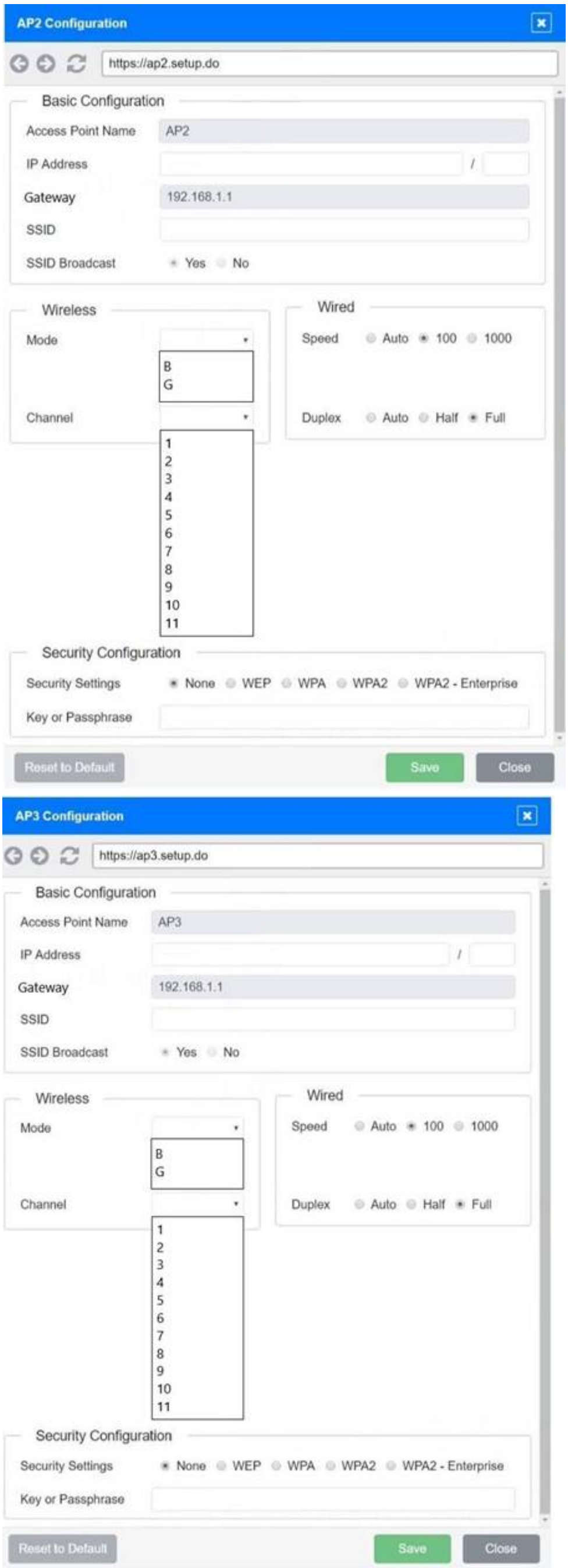
Answer: D

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 67
- (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.



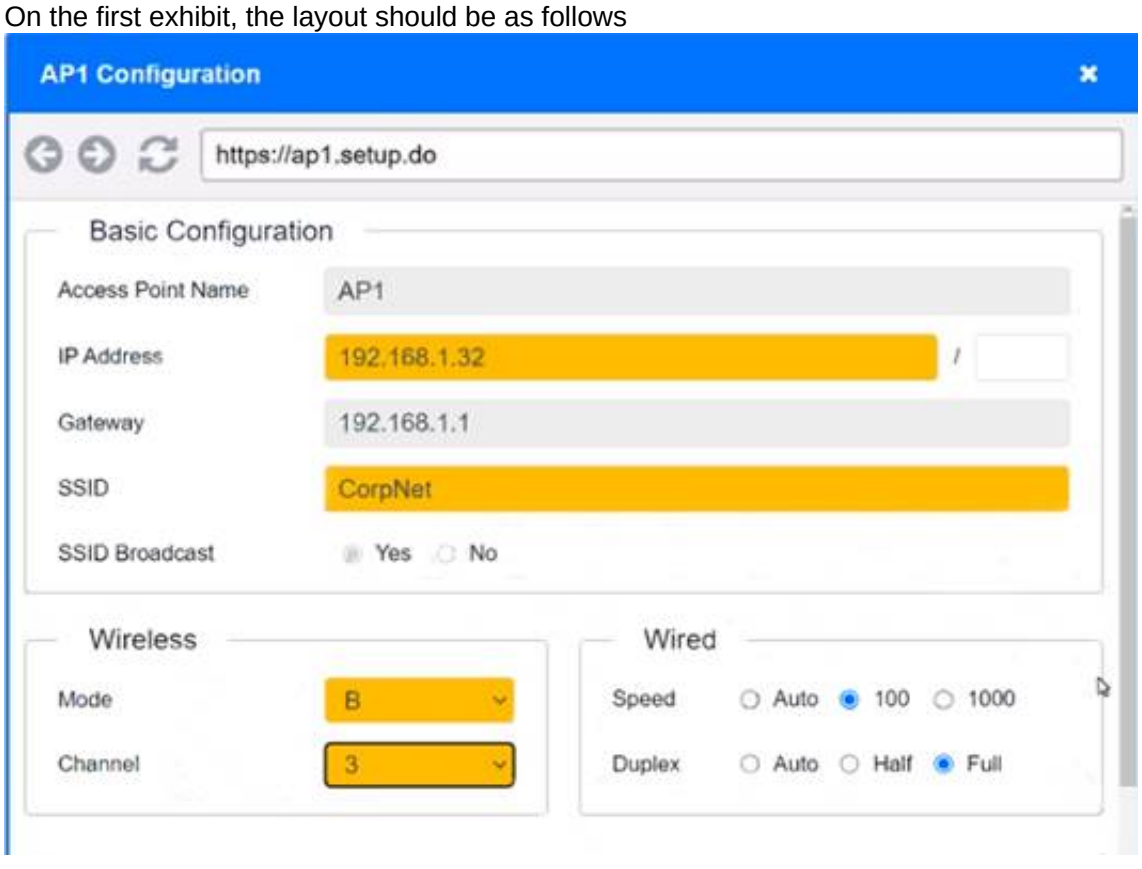




A. Mastered
B. Not Mastered

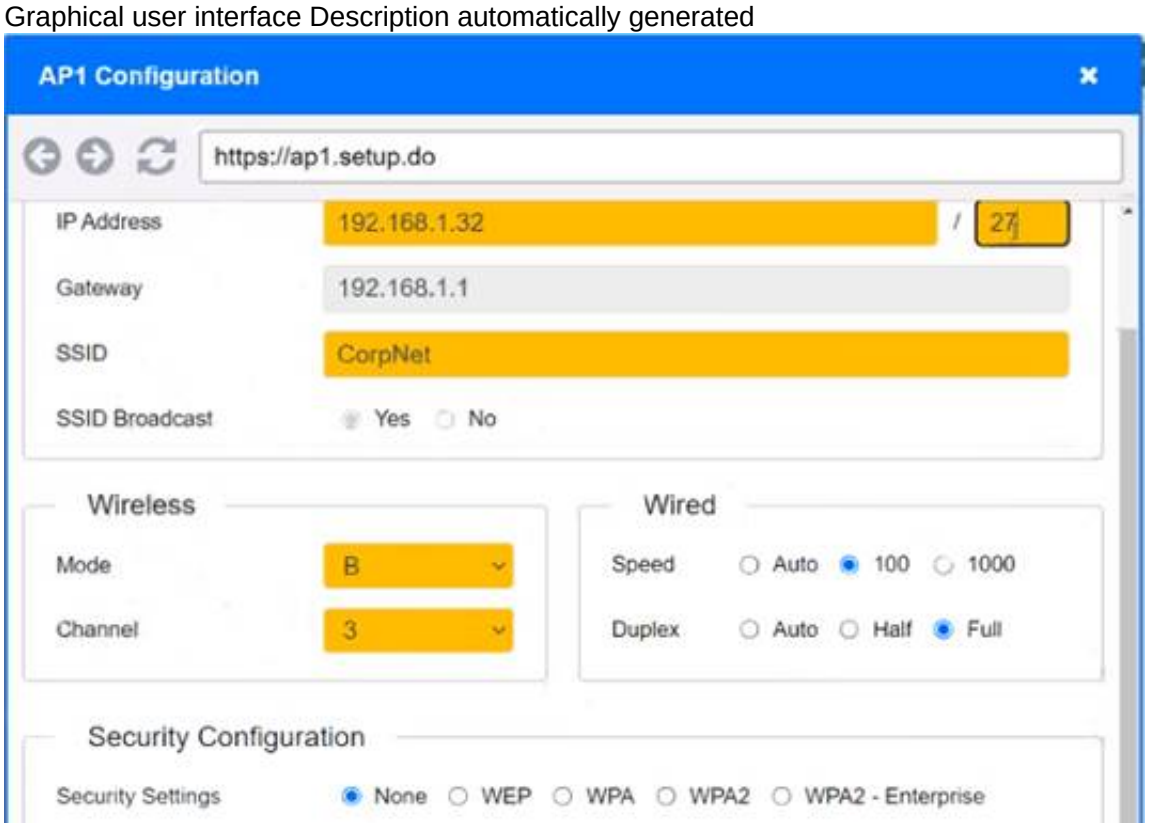
Answer: A

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

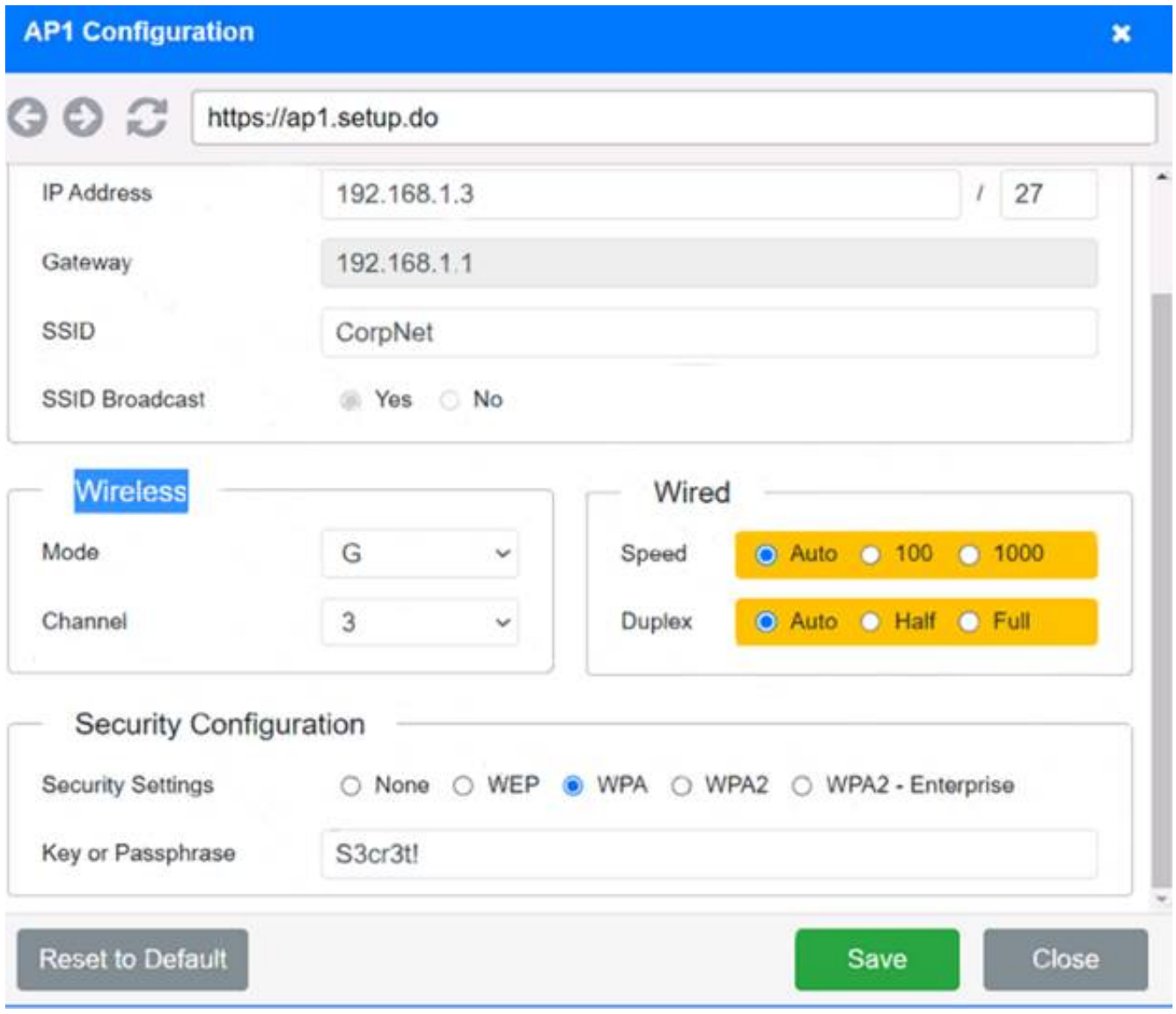
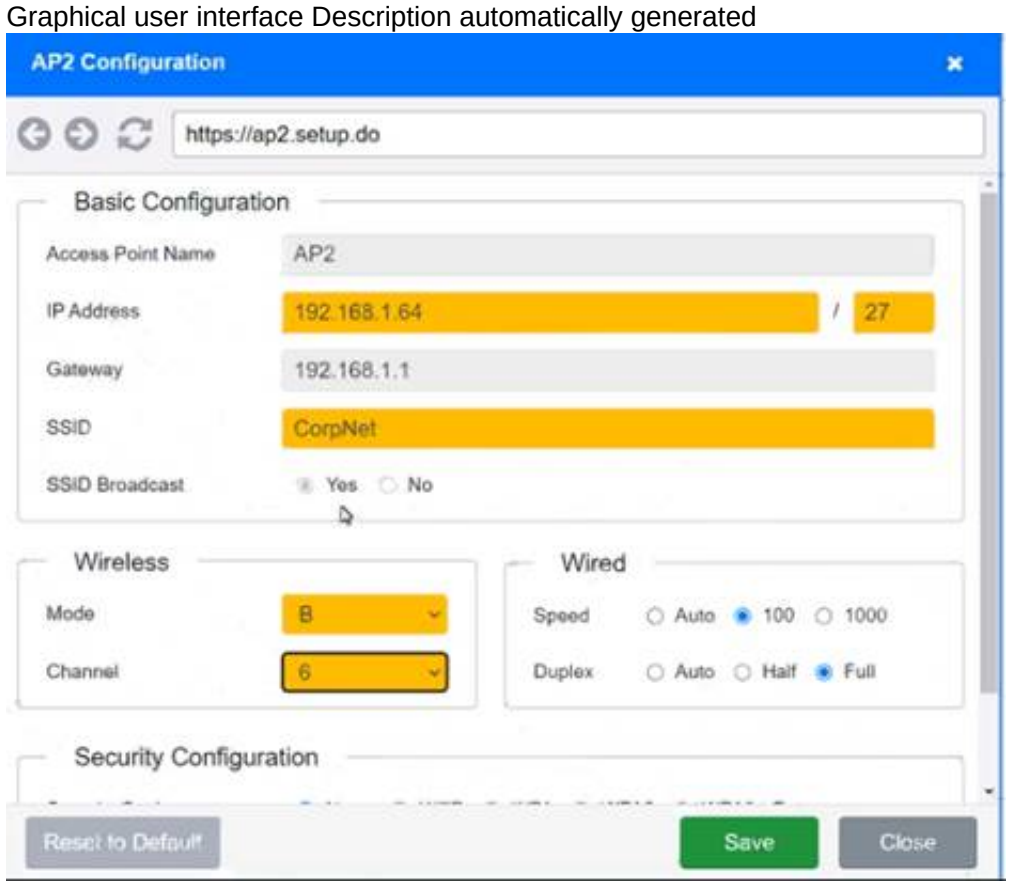


Exhibit 2 as follows Access Point Name AP2
Graphical user interface Description automatically generated



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

Graphical user interface Description automatically generated

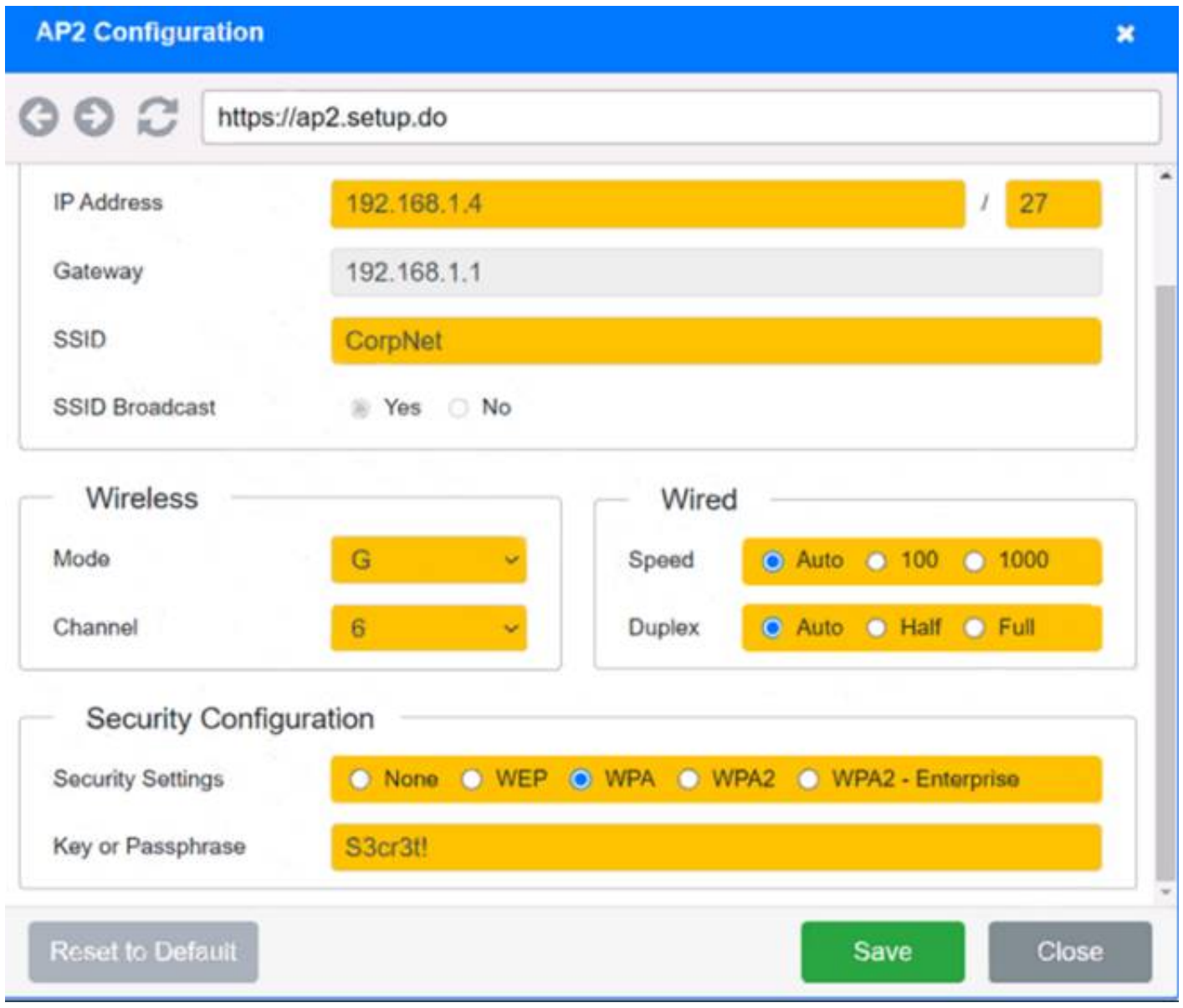
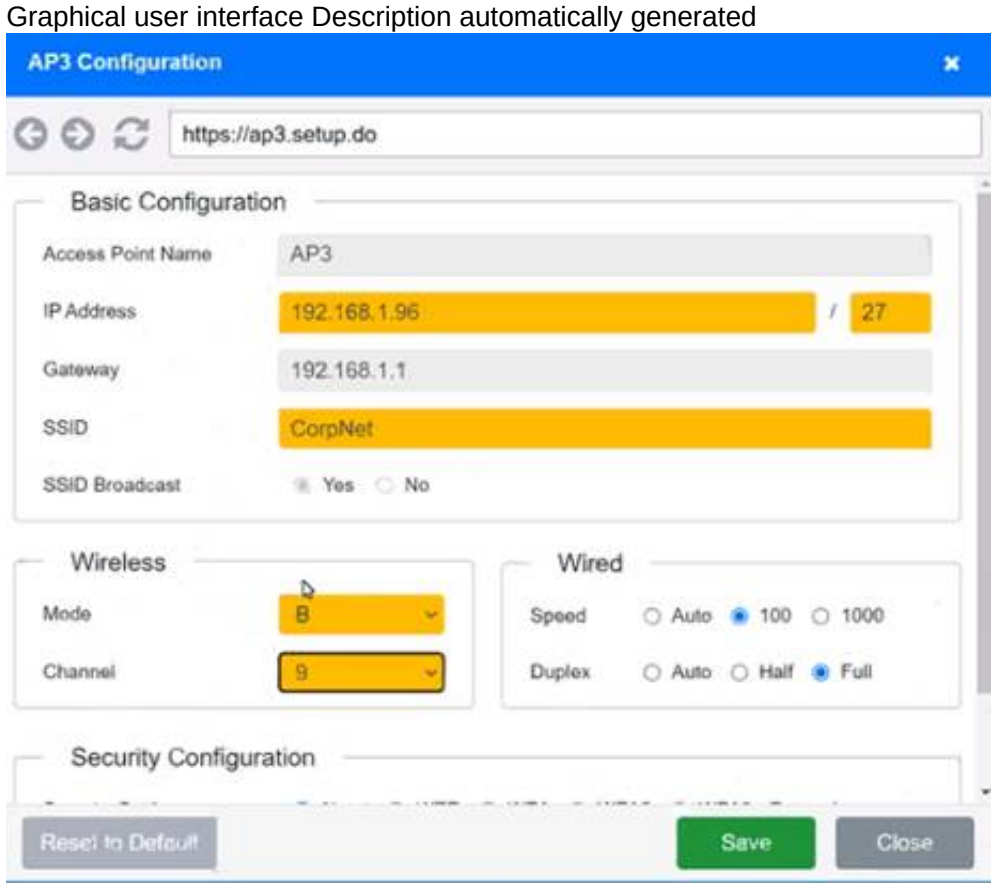
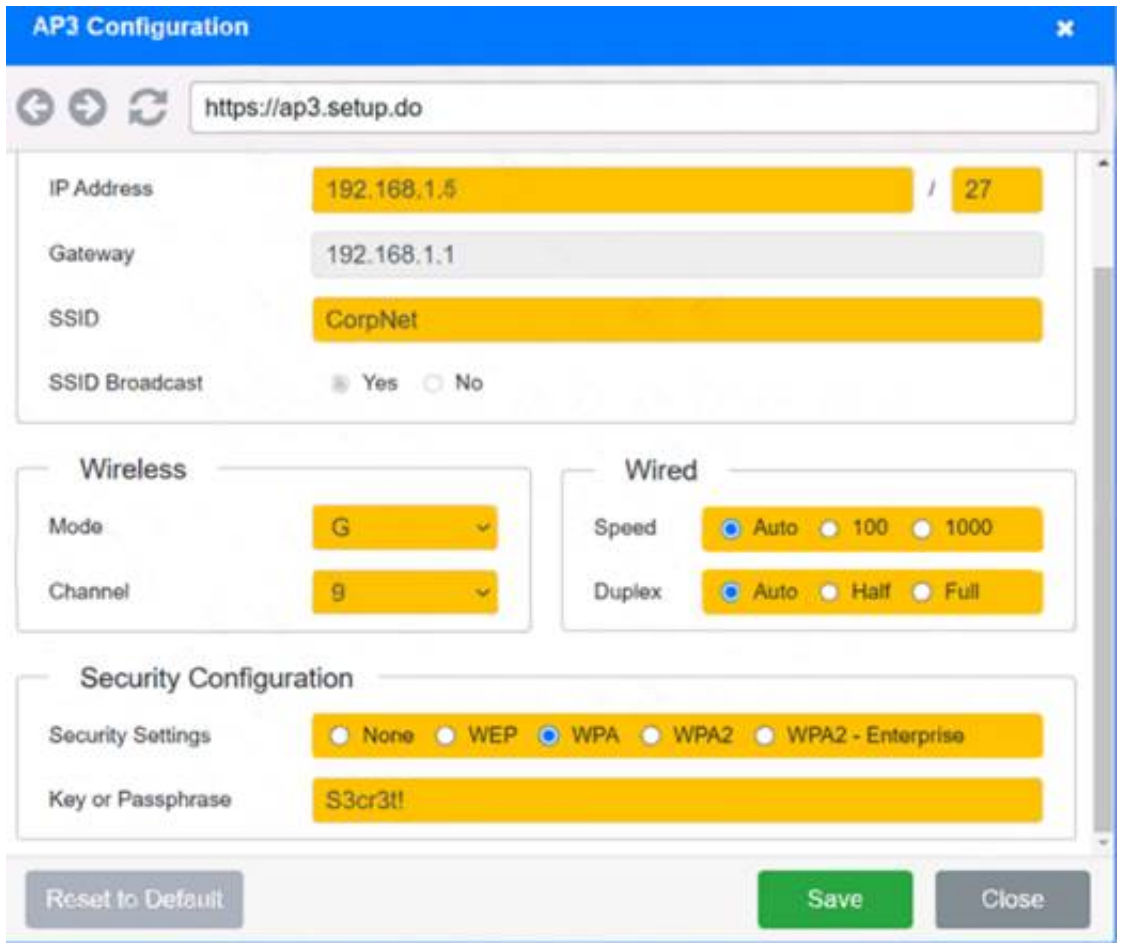


Exhibit 3 as follows Access Point Name AP3
Graphical user interface Description automatically generated



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

Graphical user interface Description automatically generated



NEW QUESTION 71
- (Exam Topic 1)
A network administrator walks into a datacenter and notices an unknown person is following closely. The administrator stops and directs the person to the security desk. Which of the following attacks did the network administrator prevent?

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

Answer: B

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

NEW QUESTION 74
- (Exam Topic 1)
A fiber link connecting two campus networks is broken. Which of the following tools should an engineer use to detect the exact break point of the fiber link?

A. OTDR
B. Tone generator
C. Fusion splicer
D. Cable tester
E. PoE injector

Answer: A

Explanation:
To detect the exact break point of a fiber link, an engineer should use an OTDR (Optical Time Domain Reflectometer). This device sends a series of pulses into the fiber, measuring the time it takes for the pulses to reflect back, and can pinpoint the exact location of the break.
References:
- Network+ N10-007 Certification Exam Objectives, Objective 2.5: Given a scenario, troubleshoot copper cable issues.
- FS: OTDR (Optical Time Domain Reflectometer) Testing Principle and Applications

NEW QUESTION 78
- (Exam Topic 1)
An IT organization needs to optimize speeds for global content distribution and wants to reduce latency in high-density user locations. Which of the following technologies BEST meets the organization’s requirements?

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

Answer: D

Explanation:

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

NEW QUESTION 80
- (Exam Topic 1)
Client devices cannot enter a network, and the network administrator determines the DHCP scope is exhausted. The administrator wants to avoid creating a new DHCP pool. Which of the following can the administrator perform to resolve the issue?

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

Answer: D

Explanation:
To resolve the issue of DHCP scope exhaustion without creating a new DHCP pool, the administrator can reduce the lease time. By decreasing the lease time, the IP addresses assigned by DHCP will be released back to the DHCP scope more quickly, allowing them to be assigned to new devices.
References:
- CompTIA Network+ Certification Study Guide, Exam N10-007, Fourth Edition, Chapter 2: The OSI Model and Networking Protocols, Objective 2.3: Given a scenario, implement and configure the appropriate addressing schema.
- https://www.networkcomputing.com/data-centers/10-tips-optimizing-dhcp-performance

NEW QUESTION 81
- (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 85
- (Exam Topic 1)
A systems administrator needs to improve WiFi performance in a densely populated office tower and use the latest standard. There is a mix of devices that use 2.4 GHz and 5 GHz. Which of the following should the
systems administrator select to meet this requirement?

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

Answer: B

Explanation:
* 802.11 ax is the latest WiFi standard that improves WiFi performance in densely populated environments and supports both 2.4 GHz and 5 GHz bands. 802.11ac is the previous standard that only supports 5 GHz band. 802.11g and 802.11n are older standards that support 2.4 GHz band only or both bands respectively.
References:
https://partners.comptia.org/docs/default-source/resources/comptia-network-n10-008-exam-objectives-(2-0),
https://www.techtarget.com/searchnetworking/tip/Whats-the-difference-between-80211ax-vs-80211ac

NEW QUESTION 89
- (Exam Topic 1)
Which of the following is MOST likely to generate significant East-West traffic in a datacenter?

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

Answer: B

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

NEW QUESTION 93

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

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

Answer: D

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

NEW QUESTION 94
- (Exam Topic 1)
Which of the following connector types would have the MOST flexibility?

A. SFP
B. BNC
C. LC
D. RJ45

Answer: A

Explanation:
SFP (Small Form-factor Pluggable) is a connector type that has the most flexibility. It is a hot-swappable transceiver that can support different speeds, distances, and media types depending on the module inserted. It can be used for both copper and fiber connections and supports various protocols such as Ethernet, Fibre Channel, and SONET. References: https://www.fs.com/what-is-sfp-transceiver-aid-11.html

NEW QUESTION 97
- (Exam Topic 1)
A network administrator redesigned the positioning of the APs to create adjacent areas of wireless coverage. After project validation, some users still report poor connectivity when their devices maintain an association to a distanced AP. Which of the following should the network administrator check FIRST?

A. Validate the roaming settings on the APs and WLAN clients
B. Verify that the AP antenna type is correct for the new layout
C. Check to see if MU-MIMO was properly activated on the APs
D. Deactivate the 2.4GHz band on the APS

Answer: A

Explanation:
The network administrator should check the roaming settings on the APs and WLAN clients first. Roaming is the process of switching from one AP to another without losing connectivity. If the roaming settings are not configured properly, some users may experience poor connectivity when their devices stay connected to a distant AP instead of switching to a closer one. References: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82068-roam-faq.html

NEW QUESTION 100
- (Exam Topic 1)
Which of the following would MOST likely be used to review previous upgrades to a system?

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

Answer: B

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

NEW QUESTION 104
- (Exam Topic 1)
The following configuration is applied to a DHCP server connected to a VPN concentrator:

```
IP address:         10.0.0.1
Subnet mask:        255.255.255.0
Gateway:            10.0.0.254
```

There are 300 non-concurrent sales representatives who log in for one hour a day to upload reports, and 252 of these representatives are able to connect to the VPN without any Issues. The remaining sales representatives cannot connect to the VPN over the course of the day. Which of the following can be done to resolve the issue without utilizing additional resources?

A. Decrease the lease duration

B. Reboot the DHCP server
C. Install a new VPN concentrator
D. Configure a new router

Answer: A

Explanation:
Decreasing the lease duration on the DHCP server will cause clients to renew their IP address leases more frequently, freeing up IP addresses for other clients to use. References: CompTIA Network+ Certification Study Guide, Chapter 3: IP Addressing.

NEW QUESTION 106
- (Exam Topic 1)
A network technician is manually configuring the network settings for a new device and is told the network block is 192.168.0.0/20. Which of the following subnets should the technician use?

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

Answer: C

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

NEW QUESTION 107
- (Exam Topic 2)
A network engineer is designing a new secure wireless network. The engineer has been given the following requirements:
* 1 Must not use plaintext passwords
* 2 Must be certificate based
* 3. Must be vendor neutral
Which of the following methods should the engineer select?

A. TWP-RC4
B. CCMP-AES
C. EAP-TLS
D. WPA2

Answer: C

Explanation:
EAP-TLS is the method that should be selected to meet the requirements for designing a new secure wireless network. EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) is an authentication protocol that uses X.509 digital certificates for both clients and servers. It provides strong security and mutual authentication by using TLS encryption and public key cryptography. It does not use plaintext passwords or shared secrets that can be compromised or guessed. It is also an open standard that is vendor neutral and supported by most wireless devices1. References: https://www.securew2.com/blog/what-is-eap-tls 1

NEW QUESTION 112
- (Exam Topic 2)
A network technician was troubleshooting an issue for a user who was being directed to cloned websites that were stealing credentials. The URLs were correct for the websites but an incorrect IP address was revealed when the technician used ping on the user's PC After checking the is setting, the technician found the DNS server address was incorrect Which of the following describes the issue?

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

Answer: C

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

NEW QUESTION 113
- (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 116
- (Exam Topic 2)
A network technician is reviewing an upcoming project's requirements to implement IaaS. Which of the following should the technician consider?

A. Software installation processes
B. Type of database to be installed
C. Operating system maintenance
D. Server hardware requirements

Answer: D

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. When implementing IaaS, the network technician should consider the server hardware requirements, such as CPU, RAM, disk space, and network bandwidth, that are needed to run the applications and services on the cloud. The other options are not relevant to IaaS, as they are either handled by the cloud provider or by the end-user. References: https://www.comptia.org/blog/what-is-iaas

NEW QUESTION 119
- (Exam Topic 2)
A network administrator is reviewing interface errors on a switch. Which of the following indicates that a switchport is receiving packets in excess of the configured MTU?

A. CRC errors
B. Giants
C. Runts
D. Flooding

Answer: B

Explanation:
Giants are packets that exceed the configured MTU (Maximum Transmission Unit) of a switchport or interface, which causes them to be dropped or fragmented by the switch or router. The MTU is the maximum size of a packet that can be transmitted without fragmentation on a given medium or protocol. Giants can indicate misconfiguration or mismatch of MTU values between devices or interfaces on a network, which can cause performance issues or errors. CRC errors are errors that occur when the cyclic redundancy check (CRC) value of a packet does not match the calculated CRC value at the destination, which indicates corruption or alteration of data during transmission due to noise, interference, faulty cabling, etc., but not necessarily exceeding MTU values. Runts are packets that are smaller than the minimum size allowed by the medium or protocol, which causes them to be dropped or ignored by the switch or router. Flooding is a technique where a switch sends packets to all ports except the source port when it does not have an entry for the destination MAC address in its MAC address table, which can cause congestion or broadcast storms on a network.

NEW QUESTION 122
- (Exam Topic 2)
A network administrator is downloading a large patch that will be uploaded to several enterprise switches simultaneously during the day's upgrade cycle. Which of the following should the administrator do to help ensure the upgrade process will be less likely to cause problems with the switches?

A. Confirm the patch's MD5 hash prior to the upgrade
B. Schedule the switches to reboot after an appropriate amount of time.
C. Download each switch's current configuration before the upgrade
D. Utilize FTP rather than TFTP to upload the patch

Answer: A

Explanation:
The network administrator should confirm the patch’s MD5 hash prior to the upgrade to help ensure the upgrade process will be less likely to cause problems with the switches. MD5 (Message Digest 5) is a cryptographic hash function that produces a 128-bit hash value for any given input. It can be used to verify the integrity and authenticity of a file by comparing its hash value with a known or expected value. If the hash values match, it means that the file has not been corrupted or tampered with during transmission or storage. If the hash values do not match, it means that the file may be damaged or malicious and should not be used for the upgrade. References:
https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/15292-scp.html

NEW QUESTION 126
- (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 129
- (Exam Topic 2)
A user is having difficulty with video conferencing and is looking for assistance. Which of the following would BEST improve performance?

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

Answer: B

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

NEW QUESTION 131
- (Exam Topic 2)
An organization wants to implement a method of centrally managing logins to network services. Which of the following protocols should the organization use to allow for authentication, authorization and auditing?

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

Answer: B

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

NEW QUESTION 133
- (Exam Topic 2)
A network technician has multimode fiber optic cable available in an existing IDF. Which of the following Ethernet standards should the technician use to connect the network switch to the existing fiber?

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

Answer: C

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

NEW QUESTION 135
- (Exam Topic 2)
An ARP request is broadcasted and sends the following request. "Who is 192.168.1.200?
Tell 192.168.1.55"
At which of the following layers of the OSI model does this request operate?

A. Application

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

Answer: B

Explanation:
An ARP request operates at the data link layer of the OSI model. ARP (Address Resolution Protocol) is a protocol that maps IP addresses to MAC addresses on a local area network. It allows devices to communicate with each other without knowing their MAC addresses beforehand. ARP operates at the data link layer (layer 2) of the OSI model, which is responsible for framing and addressing data packets on a physical medium.
References: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

NEW QUESTION 137
- (Exam Topic 2)
A network administrator is talking to different vendors about acquiring technology to support a new project for a large company. Which of the following documents will MOST likely need to be signed before information about the project is shared?

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

Answer: B

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

NEW QUESTION 139
- (Exam Topic 2)
Which of the following policies is MOST commonly used for guest captive portals?

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

Answer: A

Explanation:
AUP stands for Acceptable Use Policy, which is a policy that defines the rules and guidelines for using a network or service. A guest captive portal is a web page that requires users to agree to the AUP before accessing the Internet or other network resources. This is a common way to enforce security and legal compliance for guest users. References:
https://www.arubanetworks.com/techdocs/Instant_87_WebHelp/Content/instant-ug/captive-portal/captive-portal

NEW QUESTION 144
- (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 147
- (Exam Topic 2)
Which of the following is a system that is installed directly on a server's hardware and abstracts the hardware from any guest machines?

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

Answer: B

Explanation:

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

NEW QUESTION 152
- (Exam Topic 2)
A network technician is investigating an issue with handheld devices in a warehouse. Devices have not been connecting to the nearest APs, but they have been connecting to an AP on the far side of the warehouse. Which of the following is the MOST likely cause of this issue?

A. The nearest APs are configured for 802.11g.
B. An incorrect channel assignment is on the nearest APs.
C. The power level is too high for the AP on the far side.
D. Interference exists around the AP on the far side.

Answer: C

Explanation:
The power level is a setting that determines how strong the wireless signal is from an access point (AP). If the power level is too high for an AP on the far side of a warehouse, it can cause interference and overlap with other APs on the same channel or frequency. This can result in handheld devices not connecting to the nearest APs, but connecting to the AP on the far side instead. A technician should adjust the power level of the AP on the far side to reduce interference and improve connectivity. References:
https://www.comptia.org/blog/what-is-power-level

NEW QUESTION 156
- (Exam Topic 2)
Which of the following attacks encrypts user data and requires a proper backup implementation to recover?

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

Answer: C

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

NEW QUESTION 158
- (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 160
- (Exam Topic 2)
A technician is troubleshooting a workstation's network connectivity and wants to confirm which switchport corresponds to the wall jack the PC is using Which of the following concepts would BEST help the technician?

A. Consistent labeling
B. Change management
C. Standard work instructions
D. Inventory management
E. Network baseline

Answer: A

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

NEW QUESTION 165

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

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

Answer: C

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

NEW QUESTION 167
- (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 168
- (Exam Topic 2)
A network administrator decided to use SLAAC in an extensive IPv6 deployment to alleviate IP address management. The devices were properly connected into the LAN but autoconfiguration of the IP address did not occur as expected. Which of the following should the network administrator verify?

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

Answer: A

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

NEW QUESTION 173
- (Exam Topic 2)
A network administrator is required to ensure that auditors have read-only access to the system logs, while systems administrators have read and write access to the system logs, and operators have no access to the system logs. The network administrator has configured security groups for each of these functional categories. Which of the following security capabilities will allow the network administrator to maintain these permissions with the LEAST administrative effort?

A. Mandatory access control
B. User-based permissions
C. Role-based access
D. Least privilege

Answer: C

Explanation:

Role-based access is a security capability that assigns permissions to users based on their roles or functions within an organization. It allows the network administrator to maintain these permissions with the least administrative effort, as they only need to configure the security groups for each role once and then assign users to those groups. Mandatory access control is a security capability that assigns permissions based on security labels or classifications, which requires more administrative effort to maintain. User-based permissions are a security capability that assigns permissions to individual users, which is not scalable or efficient for large organizations. Least privilege is a security principle that states that users should only have the minimum level of access required to perform their tasks, which is not a security capability by itself.

NEW QUESTION 178
- (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 183
- (Exam Topic 2)
A firewall administrator is implementing a rule that directs HTTP traffic to an internal server listening on a non-standard socket Which of the following types of rules is the administrator implementing?

A. NAT
B. PAT
C. STP
D. SNAT
E. ARP

Answer: B

Explanation:
The firewall administrator is implementing a PAT (Port Address Translation) rule that directs HTTP traffic to an internal server listening on a non-standard socket. PAT is a type of NAT (Network Address Translation) that allows multiple devices to share a single public IP address by using different port numbers. PAT can also be used to redirect traffic from one port to another port on the same or different IP address. This can be useful for security or load balancing purposes. For example, a firewall administrator can configure a PAT rule that redirects HTTP traffic (port 80) from the public IP address of the firewall to an internal server that listens on a non-standard port (such as 8080) on its private IP address. References: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html

NEW QUESTION 187
- (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 190
- (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 195
- (Exam Topic 2)
A network administrator needs to implement an HDMI over IP solution. Which of the following will the network administrator MOST likely use to ensure smooth video delivery?

A. Link aggregation control
B. Port tagging
C. Jumbo frames
D. Media access control

Answer: C

Explanation:
Giants are packets that exceed the configured MTU (Maximum Transmission Unit) of a switchport or interface, which causes them to be dropped or fragmented by the switch or router. The MTU is the maximum size of a packet that can be transmitted without fragmentation on a given medium or protocol. Giants can indicate misconfiguration or mismatch of MTU values between devices or interfaces on a network, which can cause performance issues or errors. CRC errors are errors that occur when the cyclic redundancy check (CRC) value of a packet does not match the calculated CRC value at the destination, which indicates corruption or alteration of data during transmission due to noise, interference, faulty cabling, etc., but not necessarily exceeding MTU values. Runts are packets that are smaller than the minimum size allowed by the medium or protocol, which causes them to be dropped or ignored by the switch or router. Flooding is a technique where a switch sends packets to all ports except the source port when it does not have an entry for the destination MAC address in its MAC address table, which can cause congestion or broadcast storms on a network.

NEW QUESTION 199
- (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 202
- (Exam Topic 2)
A systems administrator is running a VoIP network and is experiencing jitter and high latency. Which of the following would BEST help the administrator determine the cause of these issues?

A. Enabling RADIUS on the network
B. Configuring SNMP traps on the network
C. Implementing LDAP on the network
D. Establishing NTP on the network

Answer: B

Explanation:
SNMP (Simple Network Management Protocol) is a protocol that allows network devices to communicate with a network management system (NMS) for monitoring and configuration purposes. SNMP traps are unsolicited messages sent by network devices to the NMS when certain events or conditions occur, such as errors, failures, or thresholds. Configuring SNMP traps on the network would best help the administrator determine the cause of jitter and high latency on a VoIP network, as they would provide real-time alerts and information about the network performance and status. Enabling RADIUS on the network is not relevant to troubleshooting VoIP issues, as RADIUS is a protocol that provides authentication, authorization, and accounting services for network access. Implementing LDAP on the network is also not relevant to troubleshooting VoIP issues, as LDAP is a protocol that provides directory services for storing and querying information about users, groups, devices, etc. Establishing NTP on the network is not directly related to troubleshooting VoIP issues, as NTP is a protocol that synchronizes the clocks of network devices.

NEW QUESTION 207
- (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 209
- (Exam Topic 2)
Which of the following is MOST commonly used to address CVEs on network equipment and/or operating systems?

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

Answer: C

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

NEW QUESTION 213
- (Exam Topic 2)
A user recently made changes to a PC that caused it to be unable to access websites by both FQDN and IP Local resources, such as the file server remain accessible. Which of the following settings did the user MOST likely misconfigure?

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

Answer: B

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

NEW QUESTION 214
- (Exam Topic 2)
A city has hired a new employee who needs to be able to work when traveling at home and at the municipal sourcing of a neighboring city that snares services. The employee is issued a laptop, and a technician needs to train the employee on the appropriate solutions for secure access to the network from all the possible locations On which of the following solutions would the technician MOST likely train the employee?

A. Site-to-site VPNs between the two city locations and client-to-site software on the employee's laptop tor all other remote access
B. Client-to-site VPNs between the travel locations and site-to-site software on the employee's laptop for all other remote access
C. Client-to-site VPNs between the two city locations and site-to-site software on the employee's laptop for all other remote access
D. Site-to-site VPNs between the home and city locations and site-to-site software on the employee's laptop for all other remote access

Answer: A

Explanation:
The technician would most likely train the employee on using site-to-site VPNs between the two city locations and client-to-site software on the employee’s laptop for all other remote access. A VPN (Virtual Private Network) 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. A site-to-site VPN connects two or more networks, such as branch offices or data centers, using a VPN gateway device at each site. A client-to-site VPN connects individual users, such as mobile workers or telecommuters, using a VPN client software on their devices. In this scenario, the employee needs to access the network from different locations, such as home, travel, or another city. Therefore, the technician would train the employee on how to use site-to-site VPNs to connect to the network from another city location that shares services, and how to use client-to-site software to connect to the network from home or travel locations. References: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-work

NEW QUESTION 215
- (Exam Topic 2)
Which of the following would be used to expedite MX record updates to authoritative NSs?

A. UDP forwarding

B. DNS caching
C. Recursive lookup
D. Time to live

Answer: D

Explanation:
Time to live (TTL) is a value that indicates how long a DNS record can be cached by authoritative NSs (name servers) or other DNS servers before it expires and needs to be updated. A lower TTL value would expedite MX record updates to authoritative NSs, as they would refresh the record more frequently. UDP forwarding is not a DNS term, but a technique of sending UDP packets from one host to another. DNS caching is the process of storing DNS records locally for faster resolution, which does not expedite MX record updates. Recursive lookup is a type of DNS query where a DNS server queries other DNS servers on behalf of a client until it finds the answer, which does not expedite MX record updates.

NEW QUESTION 218
- (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 222
- (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 224
- (Exam Topic 3)
A network administrator views a network pcap and sees a packet containing the following:

```
community: public
request-id: 13438
get-response 1.3.6.1.2.1.1.3.0 Value:206801150
```

Which of the following are the BEST ways for the administrator to secure this type of traffic? (Select TWO).

A. Migrate the network to IPv6.
B. Implement 802.1 X authentication
C. Set a private community siring
D. Use SNMPv3.
E. Incorporate SSL encryption
F. Utilize IPSec tunneling.

Answer: CD

Explanation:
The packet shown in the image is an SNMP (Simple Network Management Protocol) packet, which is used to monitor and manage network devices. SNMP uses community strings to authenticate requests and responses between SNMP agents and managers. However, community strings are sent in clear text and can be easily intercepted by attackers. Therefore, one way to secure SNMP traffic is to set a private community string that is not the default or well-known value. Another way to secure SNMP traffic is to use SNMPv3, which is the latest version of the protocol that supports encryption and authentication of SNMP messages. References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 2.5: Given a scenario, use remote access methods.

NEW QUESTION 225
- (Exam Topic 3)

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

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

Answer: A

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

NEW QUESTION 226
- (Exam Topic 3)
A technician is consolidating a topology with multiple SSIDs into one unique SSID deployment. Which of the following features will be possible after this new configuration?

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

Answer: A

NEW QUESTION 227
- (Exam Topic 3)
Which of the following is used to elect an STP root?

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

Answer: B

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

NEW QUESTION 231
- (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 232
- (Exam Topic 3)
A technician performed a manual reconfiguration of a firewall, and network connectivity was reestablished. Some connection events that were previously sent to a syslog server are no longer being generated by the flrewal Which of Vie following should the technician perform to fix the Issue?

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

Answer: A

Explanation:

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

NEW QUESTION 234
- (Exam Topic 3)
A network device needs to discover a server that can provide it with an IPv4 address. Which of the following does the device need to send the request to?

A. Default gateway
B. Broadcast address
C. Unicast address
D. Link local address

Answer: B

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

NEW QUESTION 237
- (Exam Topic 3)
Network connectivity in an extensive forest reserve was achieved using fiber optics. A network fault was detected, and now the repair team needs to check the integrity of the fiber cable. Which of me following actions can reduce repair time?

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

Answer: C

NEW QUESTION 242
- (Exam Topic 3)
A technician is investigating an issue with connectivity at customer's location. The technician confirms that users can access resources locally but not over the internet The technician theorizes that the local router has failed and investigates further. The technician's testing results show that the route is functional: however, users still are unable to reach resources on the internal. Which of the following describes what the technician should do NEXT?

A. Document the lessons learned
B. Escalate the issue
C. identify the symptoms.
D. Question users for additional information

Answer: C

Explanation:
According to the CompTIA Network+ troubleshooting model123, this is the first step in troubleshooting a
network problem. The technician should gather information about the current state of the network, such as error messages, device status, network topology, and user feedback. This can help narrow down the scope of the problem and eliminate possible causes.

NEW QUESTION 246
- (Exam Topic 3)
A company has wireless APS that were deployed with 802.11g. A network engineer has noticed more frequent reports of wireless performance issues during the lunch hour in comparison to the rest of the day. The engineer thinks bandwidth consumption will increase while users are on their breaks, but network utilization logs do not show increased bandwidth numbers. Which Of the following would MOST likely resolve this issue?

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

Answer: C

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

NEW QUESTION 248
- (Exam Topic 3)
A network administrator notices excessive wireless traffic occurring on an access point after normal business hours. The access point is located on an exterior wall. Which of the following should the administrator do to limit wireless access outside the building?

A. Set up a private VLAN.

B. Disable roaming on the WAP.
C. Change to a directional antenna.
D. Stop broadcasting of the SSID.

Answer: C

Explanation:
A directional antenna is a type of antenna that radiates or receives radio waves in a specific direction. This can help limit wireless access outside the building by focusing the signal towards the intended area and reducing the signal strength in other directions. A private VLAN is a feature that isolates network devices within a VLAN. Disabling roaming on the WAP prevents wireless clients from switching to another WAP when the signal is weak. Stopping broadcasting of the SSID hides the network name from wireless clients, but does not prevent them from connecting if they know the SSID.
References: CompTIA Network+ Certification Exam Objectives Version 7.0 (N10-007), Objective 3.1: Given a scenario, install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

NEW QUESTION 250
- (Exam Topic 3)
A network technician needs to ensure that all files on a company's network can be moved in a safe and protected manner without interception from someone who is not the intended recipient. Which of the following would allow the network technician to meet these requirements?

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

Answer: D

NEW QUESTION 254
- (Exam Topic 3)
Which of the following layers of the OSI model has new protocols activated when a user moves from a wireless to a wired connection?

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

Answer: A

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

NEW QUESTION 259
- (Exam Topic 3)
A non-employee was able to enter a server room. Which of the following could have prevented this from happening?

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

Answer: B

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

NEW QUESTION 263
- (Exam Topic 3)
Which of the following devices would be used to extend the range of a wireless network?

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

Answer: A

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

NEW QUESTION 268

- (Exam Topic 3)
Which of the following provides guidance to an employee about restricting non-business access to the company's videoconferencing solution?

A. Acceptable use policy
B. Data loss prevention
C. Remote access policy
D. Standard operating procedure

Answer: A

Explanation:
An acceptable use policy (AUP) is a set of rules that outline the proper and improper use of an organization's resources, such as its videoconferencing solution. An AUP can provide guidance to employees about what is expected of them when using the organization's videoconferencing solution, including restricting non-business access to it.

NEW QUESTION 271
- (Exam Topic 3)
Which of the following OSI model layers would allow a user to access and download files from a remote computer?

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

Answer: D

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

NEW QUESTION 274
- (Exam Topic 3)
A security vendor needs to add a note to the DNS to validate the ownership of a company domain before services begin. Which of the following records did the security company MOST likely ask the company to configure?

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

Answer: A

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

NEW QUESTION 278
- (Exam Topic 3)
A large number of PCs are obtaining an APIPA IP address, and a number of new computers were added to the network. Which of the following is MOST likely causing the PCs to obtain an APIPA address?

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

Answer: D

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

NEW QUESTION 283
- (Exam Topic 3)
A technician thinks one of the router ports is flapping. Which of the following available resources should the technician use in order to determine if the router is flapping?

A. Audit logs

B. NetFlow
C. Syslog
D. Traffic logs

Answer: C

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

NEW QUESTION 285
- (Exam Topic 3)
Which of the following devices Is used to configure and centrally manage access points Installed at different locations?

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

Answer: A

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

NEW QUESTION 287
- (Exam Topic 3)
A network manager is configuring switches in IDFs to ensure unauthorized client computers are not connecting to a secure wired network. Which of the following is the network manager MOST likely performing?

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

Answer: C

NEW QUESTION 288
- (Exam Topic 3)
A network technician is troubleshooting an area where the wireless connection to devices is poor. The technician theorizes that the signal-to-noise ratio in the area is causing the issue. Which of the following should the technician do NEXT?

A. Run diagnostics on the relevant devices.
B. Move the access point to a different location.
C. Escalate the issue to the vendor's support team.
D. Remove any electronics that might be causing interference.

Answer: D

NEW QUESTION 291
- (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 294
- (Exam Topic 3)
Which of the following is the MOST cost-effective alternative that provides proper cabling and supports gigabit Ethernet devices?

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

Answer: A

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

NEW QUESTION 295
- (Exam Topic 3)
A user from a remote office is reporting slow file transfers. Which of the following tools will an engineer MOST likely use to get detailed measurement data?

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

Answer: B

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

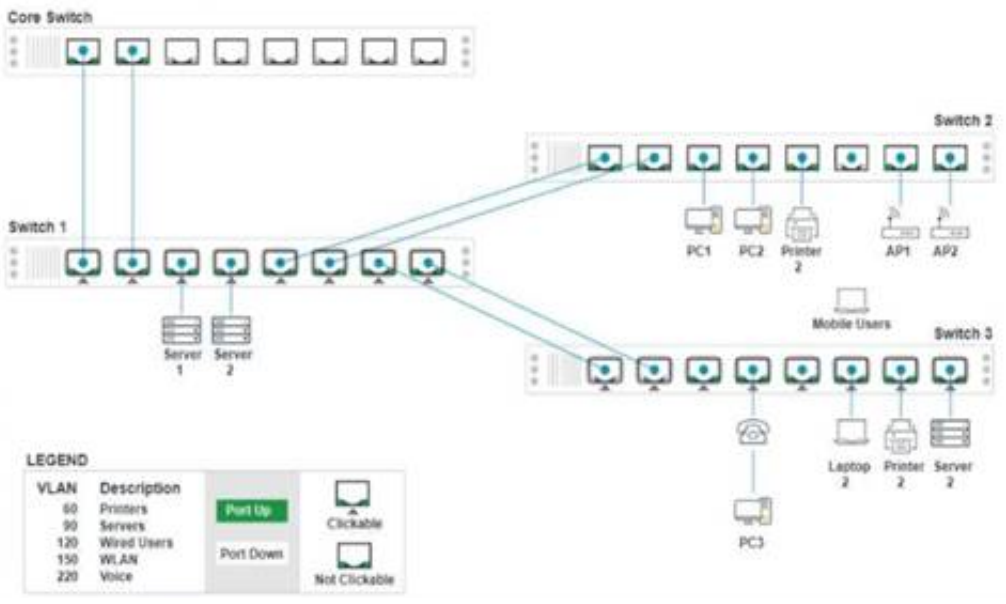
NEW QUESTION 298
- (Exam Topic 3)
Which of the following commands can be used to display the IP address, subnet address, gateway address, and DNS address on a Windows computer?

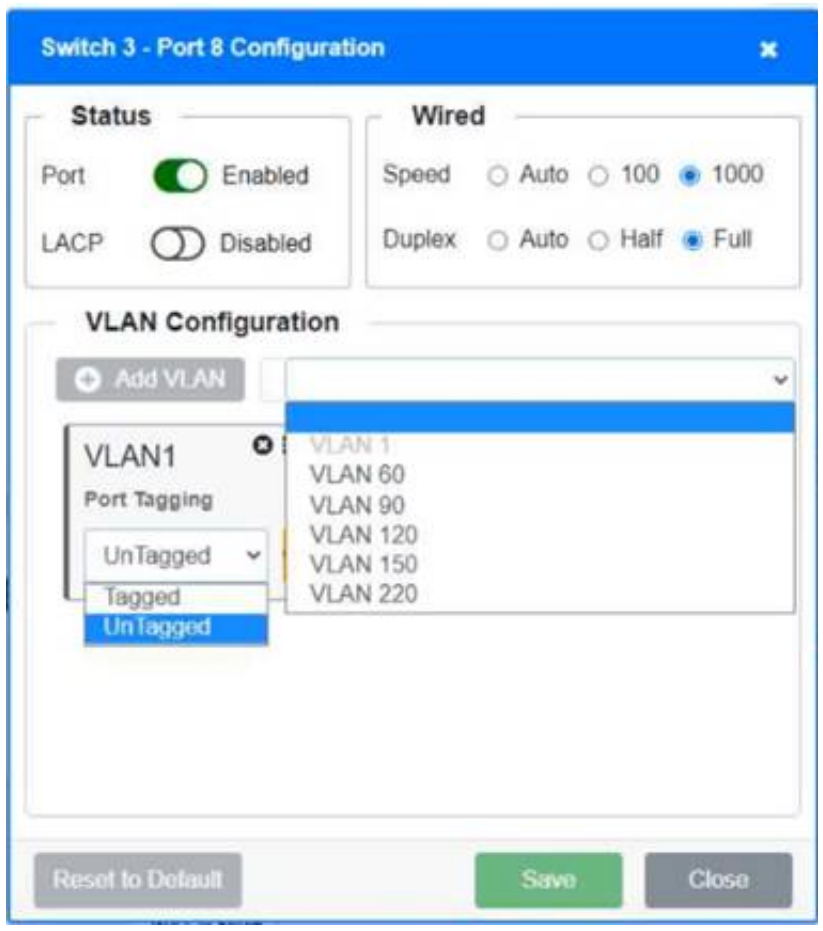
A. netstat -a
B. ifconfig
C. ip addr
D. ipconfig /all

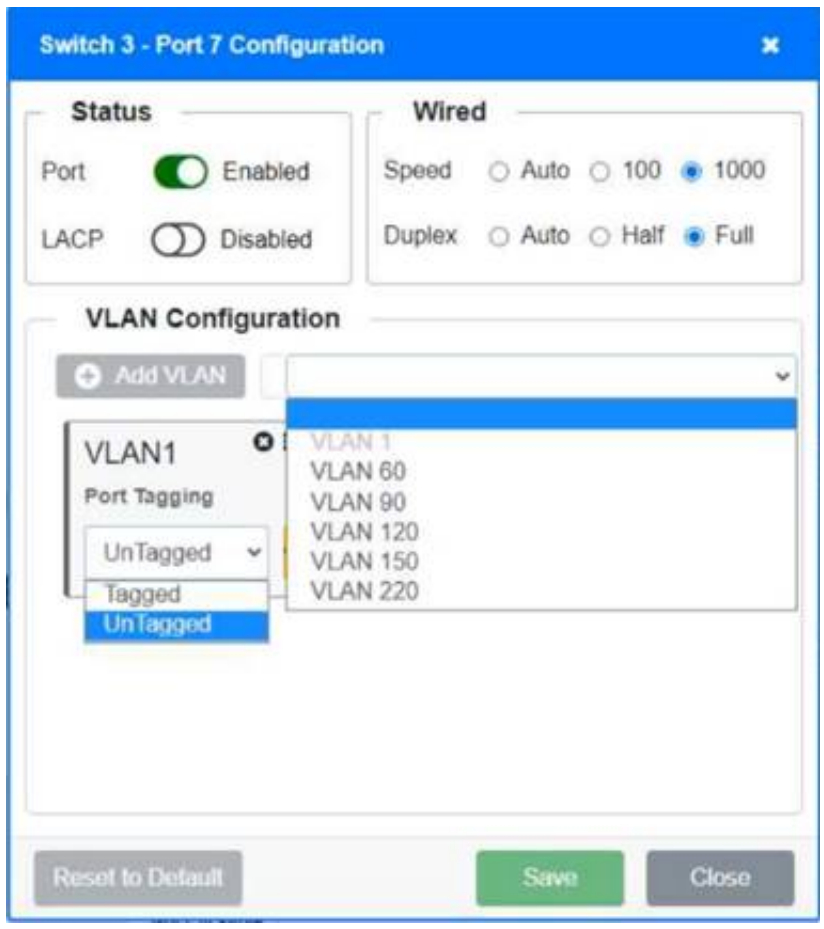
Answer: D

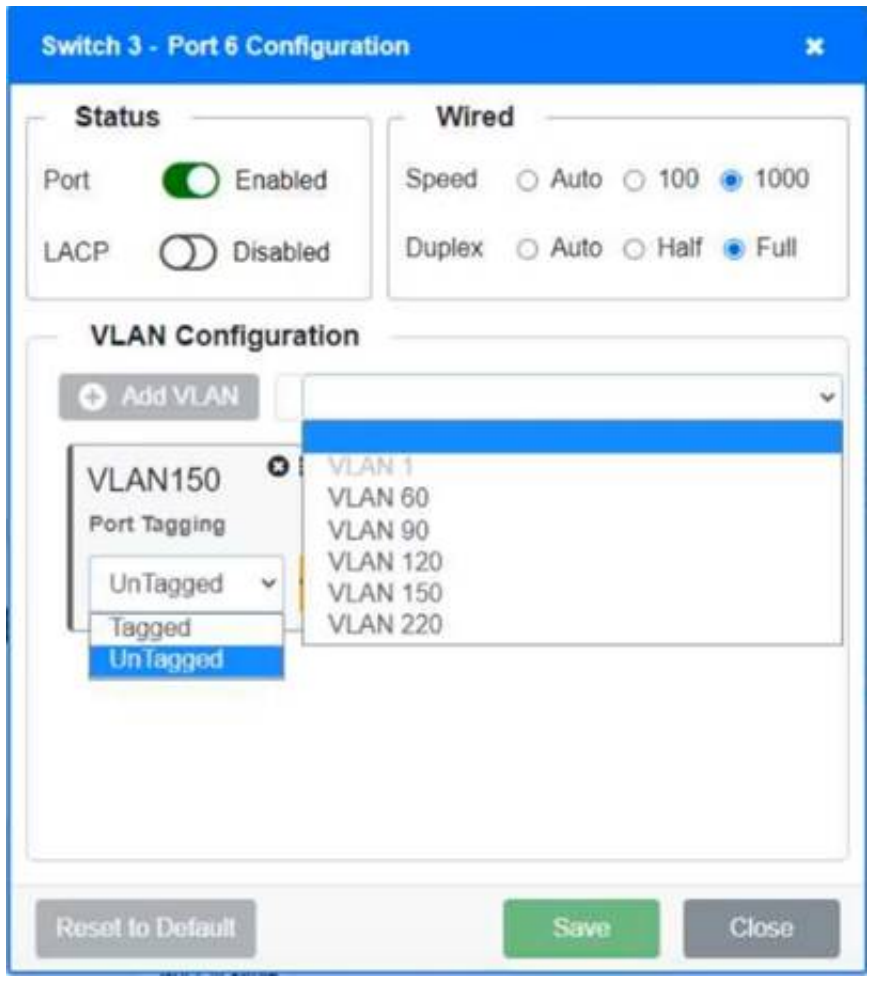
Explanation:
The ipconfig command is a utility that allows you to view and modify the network configuration of a Windows computer. By running the command "ipconfig /all", you can view detailed information about the network configuration of your computer, including the IP address, subnet mask, default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

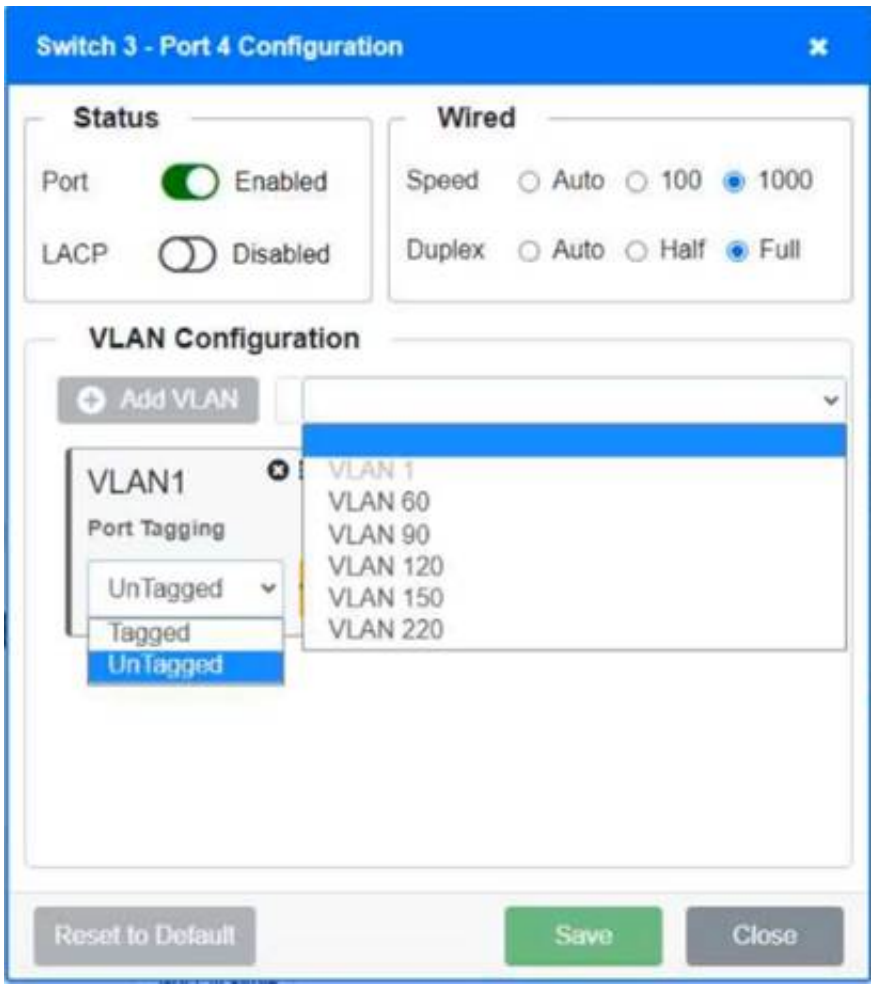
NEW QUESTION 302
- (Exam Topic 3)
SIMULATION
A network technician replaced a switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.
INSTRUCTIONS
Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings:
• Ensure 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.

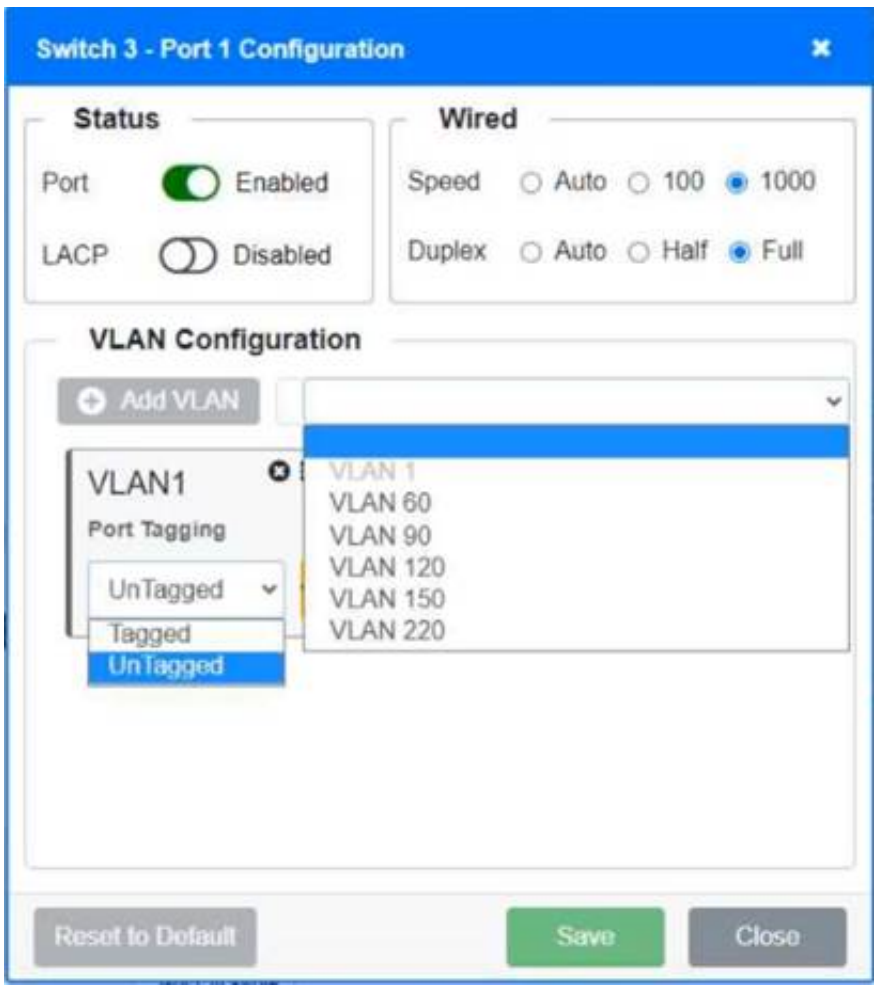


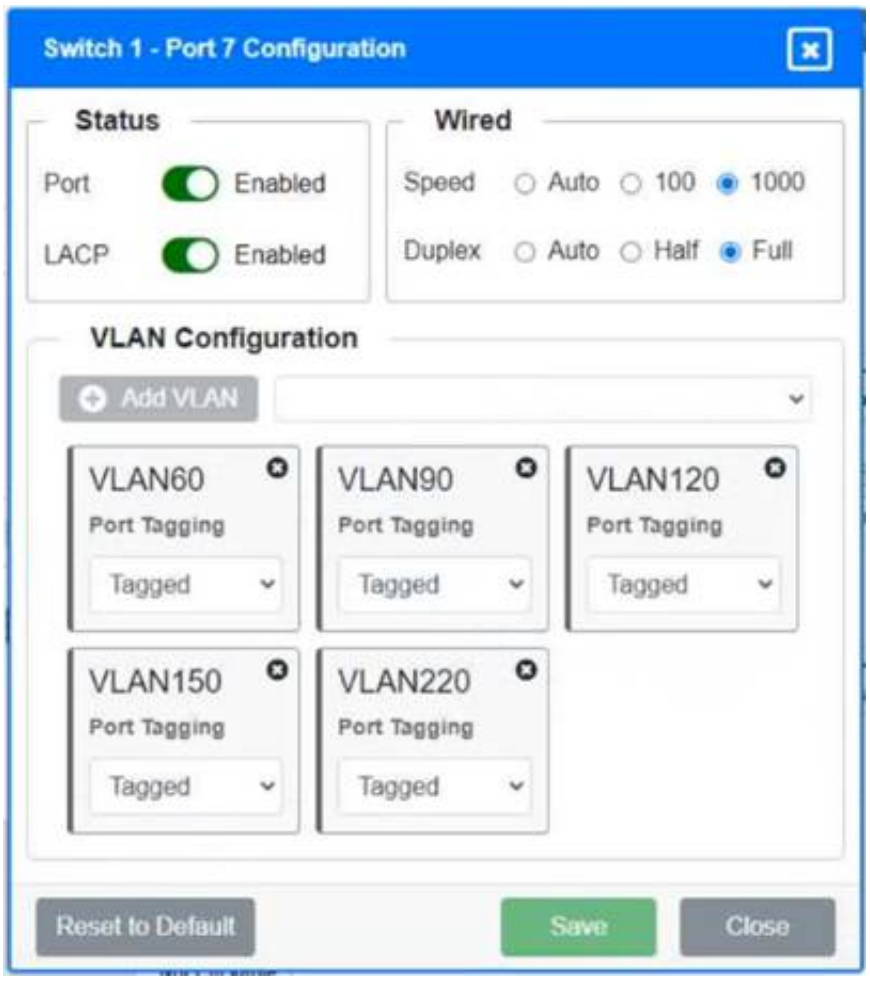

Switch 3 - Port 8 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

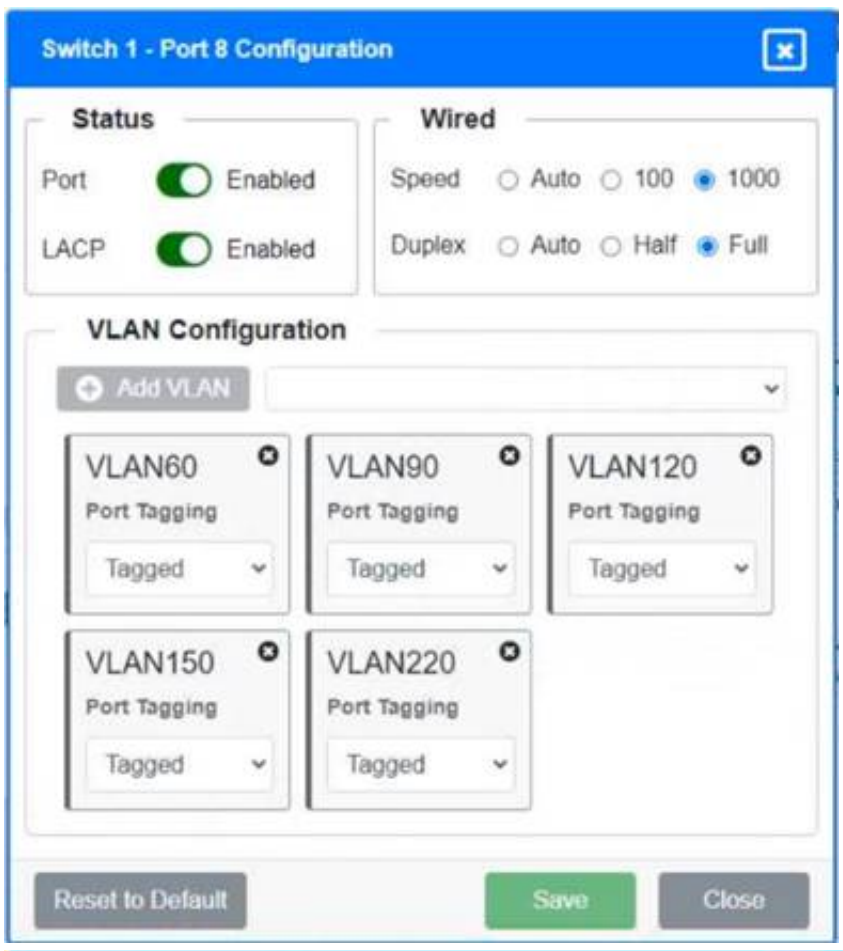

Switch 3 - Port 7 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

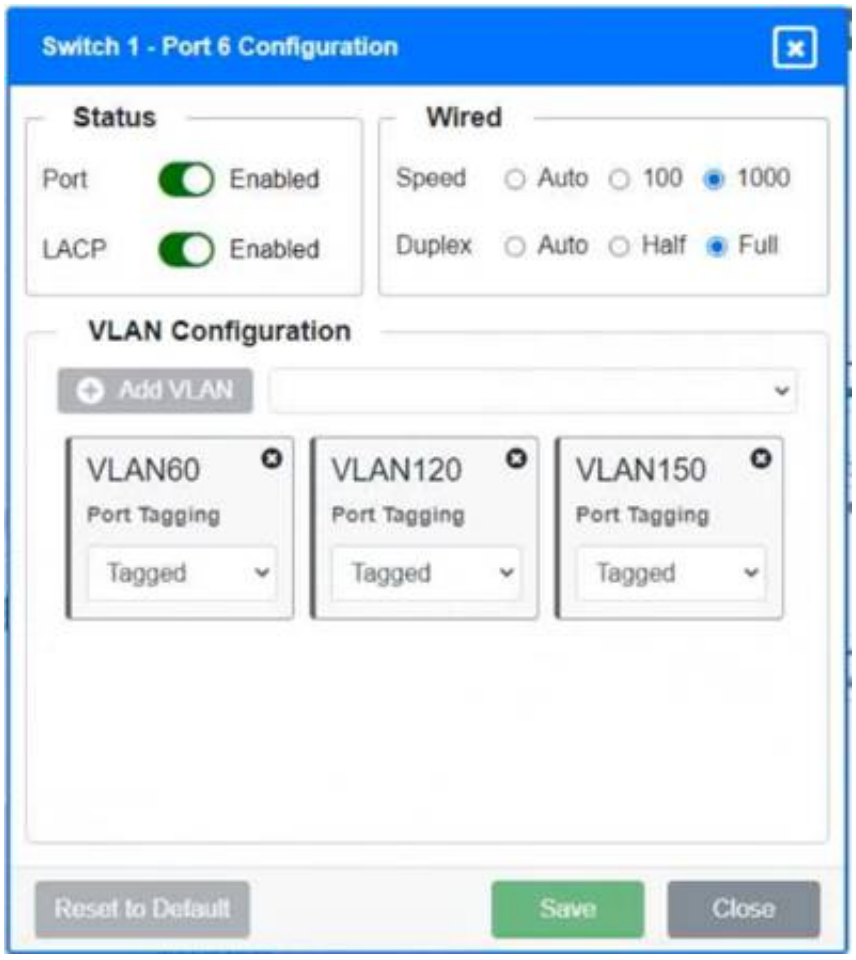

Switch 3 - Port 6 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN150
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

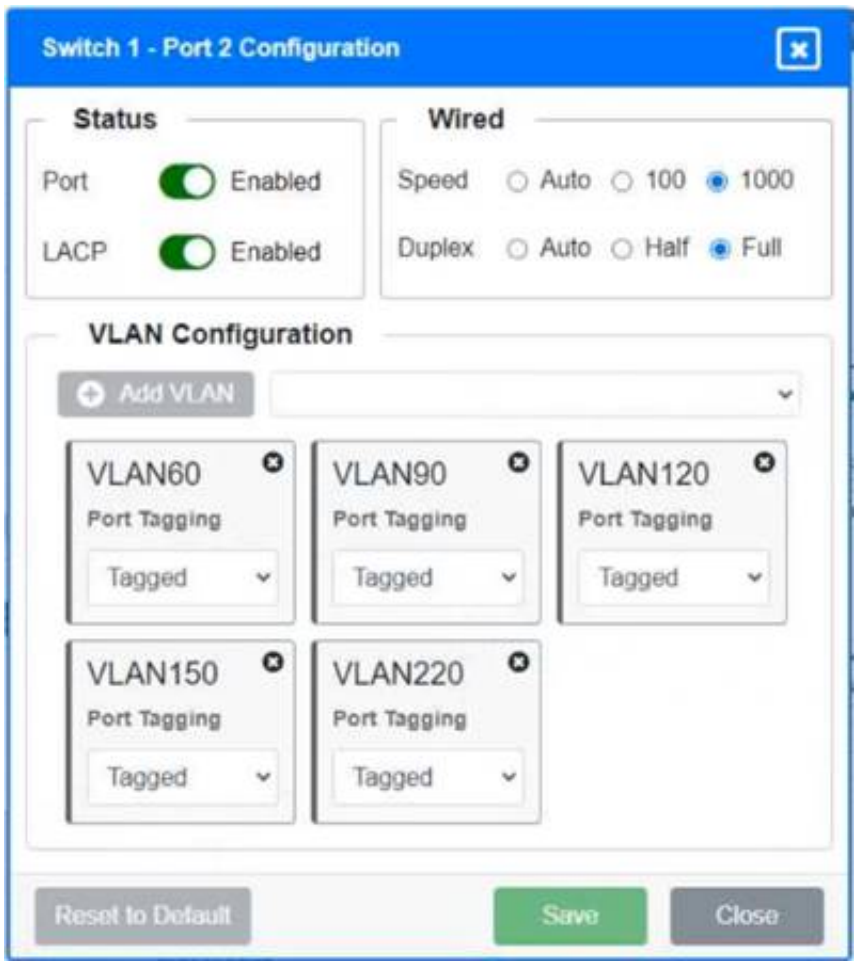

Switch 3 - Port 4 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

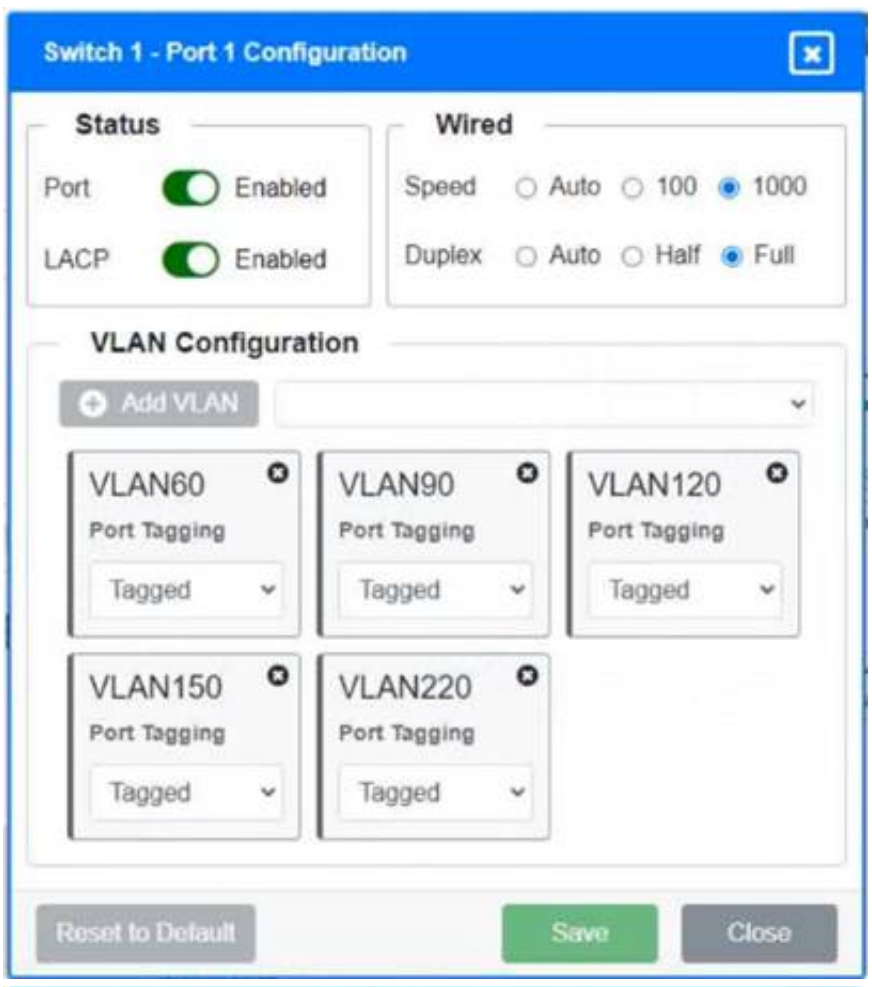

Switch 3 - Port 1 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
Reset to Default
Save
Close

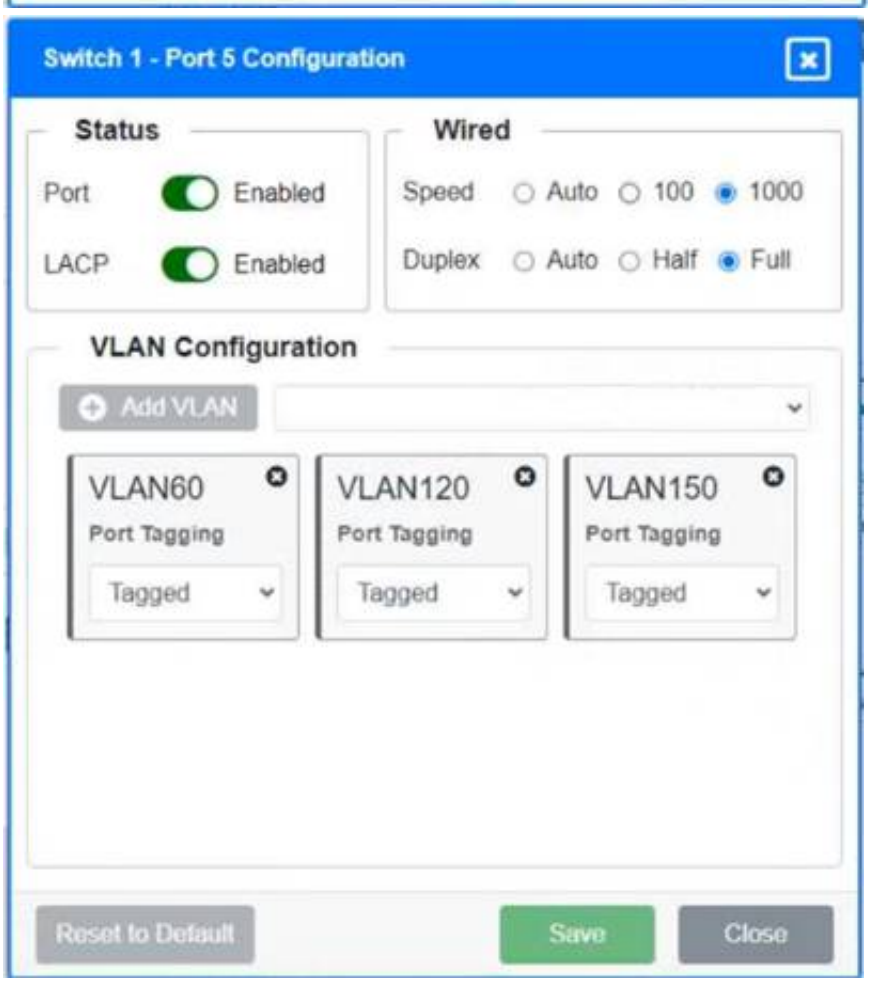

Switch 1 - Port 7 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save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

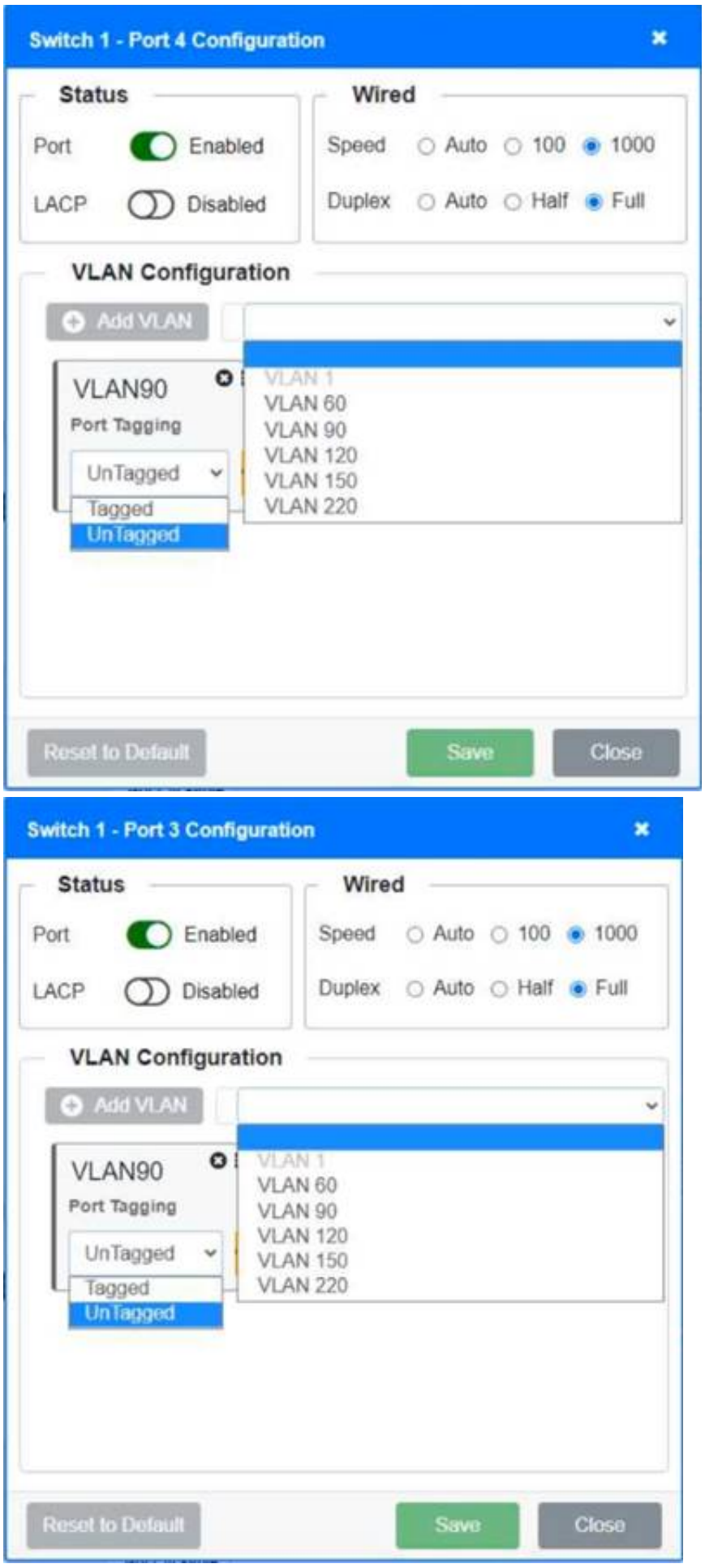

Switch 1 - Port 8 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save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

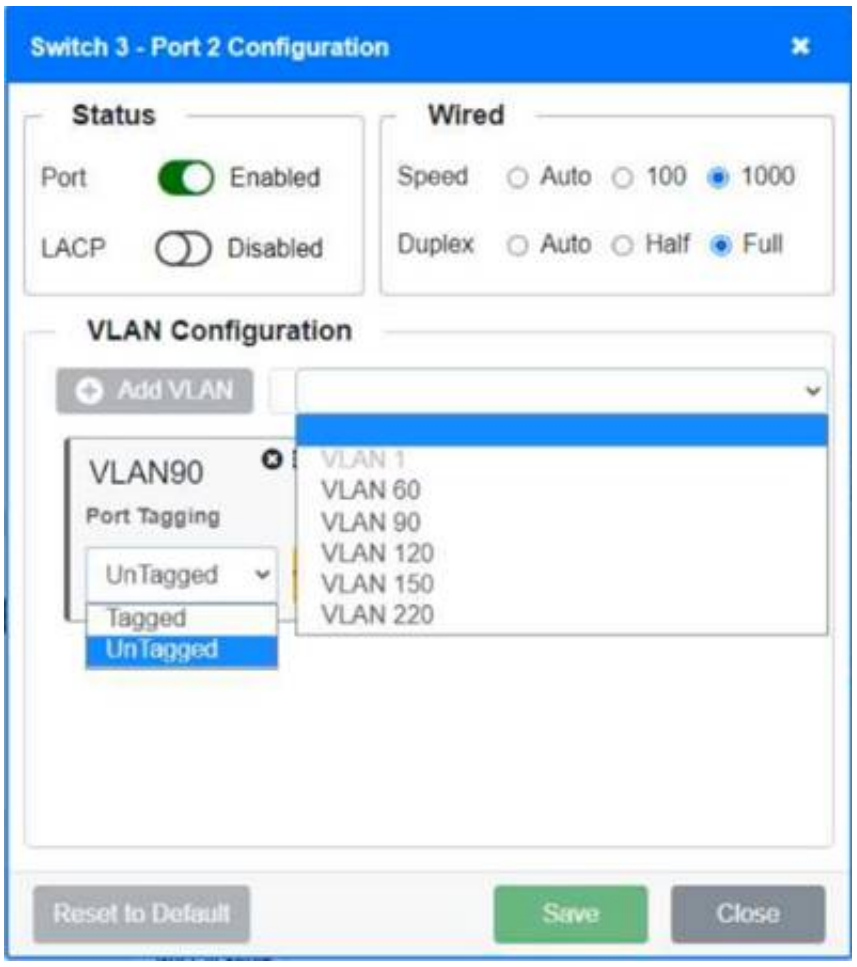

Switch 1 - Port 2 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save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


Switch 3 - Port 2 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 306
- (Exam Topic 3)
An engineer is gathering data to determine the effectiveness of UPSs in use at remote retail locations. Which of the following statistics can the engineer use to determine the availability of the remote network equipment?

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

Answer: A

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

NEW QUESTION 307
- (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 308
- (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 310
- (Exam Topic 3)
A network administrator would like to purchase a device that provides access ports to endpoints and has the ability to route between networks. Which of the following would be BEST for the administrator to purchase?

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

Answer: B

NEW QUESTION 311
- (Exam Topic 3)
An administrator would like to create a fault-tolerant ring between three switches within a Layer 2 network. Which of the following Ethernet features should the administrator employ?

A. Spanning Tree Protocol
B. Open Shortest Path First
C. Port mirroring
D. An interior gateway protocol

Answer: A

Explanation:
Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology in Ethernet networks by actively blocking certain links and enabling others. STP prevents loops by putting some of the links in a blocking state, effectively creating a loop-free topology. This ensures that there is only one active path between two devices, which helps prevent network loops and the associated problems (such as broadcast storms) that can result from them. STP is used to create a fault-tolerant ring between three switches within a Layer 2 network.

NEW QUESTION 313
- (Exam Topic 3)
An administrator is setting up a multicast server on a network, but the firewall seems to be dropping the traffic. After logging in to the device, me administrator sees me following entries:

Rule	Action	Source	Destination	Port
1	Deny	Any	172.30.10.50	Any
2	Deny	Any	232.1.4.9	Any
3	Deny	Any	242.9.15.4	Any
4	Deny	Any	175.50.10.10	Any

Which of the following firewall rules is MOST likely causing the issue?

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

Answer: A

NEW QUESTION 314
- (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 316
- (Exam Topic 3)
Due to concerns around single points of failure, a company decided to add an additional WAN to the network. The company added a second MPLS vendor to the current MPLS WAN and deployed an additional WAN router at each site. Both MPLS providers use OSPF on the WAN network, and EIGRP is run internally. The first site to go live with the new WAN is successful, but when the second site is activated significant network issues occur. Which of the following is the MOST likely cause for the WAN instability?

A. A routing loop
B. Asymmetrical routing
C. A switching loop
D. An incorrect IP address

Answer: B

Explanation:
Asymmetrical routing is the most likely cause for the WAN instability. When two different routing protocols are used, like OSPF and EIGRP, it can cause asymmetrical routing, which results in traffic being routed differently in each direction. This can lead to instability in the WAN. A CDP neighbor change, a switching loop, or an incorrect IP address are not likely causes for WAN instability.

NEW QUESTION 320
- (Exam Topic 3)
On a network with redundant switches, a network administrator replaced one of the switches but was unable to get a connection with another switch. Which of the following should the administrator chock after successfully testing the cable that was wired for TIA/EIA-568A on both ends?

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

Answer: A

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

NEW QUESTION 324
- (Exam Topic 3)
A network administrator needs to provide evidence to confirm that recent network outages were caused by increased traffic generated by a recently released application. Which of the following actions will BEST support the administrator's response?

A. Generate a network baseline report for comparison.
B. Export the firewall traffic logs.
C. Collect the router's NetFlow data.
D. Plot interface statistics for dropped packets.

Answer: C

NEW QUESTION 326
- (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 331
- (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 333
- (Exam Topic 3)
A new company recently moved into an empty office space Within days, users in the next office began noticing increased latency and packet drops with their Wi-Fi-connected devices. Which of the following is the MOST likely reason for this issue?

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

Answer: A

NEW QUESTION 334
- (Exam Topic 3)
Which of the following would be the BEST choice to connect branch sites to a main office securely?

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

Answer: A

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

NEW QUESTION 339
- (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 344
- (Exam Topic 3)
Which of the following bandwidth management techniques uses buffers al the client side to prevent TCP retransmissions from occurring when the ISP starts to drop packets of specific types that exceed the agreed traffic rate?

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

Answer: D

NEW QUESTION 346
- (Exam Topic 3)
A Wi-Fi network was originally configured to be able to handle interference from a microwave oven. The microwave oven was recently removed from the office. Now the network administrator wants to optimize the system to maximize the range of the signal. The main sources of signal degradation are the numerous cubicles and wooden walls between the WAP and the intended destination. Which of the following actions should the administrator take?

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

Answer: D

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

NEW QUESTION 347
- (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 349
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual N10-009 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the N10-009 Product From:

https://www.2passeasy.com/dumps/N10-009/

Money Back Guarantee

N10-009 Practice Exam Features:

* N10-009 Questions and Answers Updated Frequently

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

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

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