CompTIA

N10-009 Exam

CompTIA Network+ Certification

Version : 6.0
[Total Questions : 141]

Question: 1

A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User 3 and sees the Ethernet is properly connected. However, the network interface's indicator lights are not blinking on either the computer or the switch. Which of the following Is the most likely cause?

A. The switch failed.

B. The default gateway is wrong.

C. The port Is shut down.

D. The VLAN assignment is incorrect.

Answer: C

Explanation:

When a network interface's indicator lights are not blinking on either the computer or the switch, it suggests a physical layer issue. Here is the detailed reasoning:

Ethernet Properly Connected: The Ethernet cable is correctly connected, eliminating issues related to a loose or faulty cable.

No Indicator Lights: The absence of blinking indicator lights on both the computer and the switch

typically points to the port being administratively shut down.

Switch Port Shut Down: In networking, a switch port can be administratively shut down, disabling it from passing any traffic. This state is configured by network administrators and can be verified and changed using the command-line interface (CLI) of the switch.

Command to Check and Enable Port:

bash

Copy code

Switch> enable

Switch# configure terminal

Switch(config)# interface [interface id]

Switch(config-if)# no shutdown

The command no shutdown re-enables the interface if it was previously disabled. This will restore the link and the indicator lights should start blinking, showing activity.

Reference: Basic Configuration Commands PDF, sections on interface configuration (e.g., shutdown, no shutdown).

Question: 2

An administrator is setting up an SNMP server for use in the enterprise network and needs to create device IDs within a MIB. Which of the following describes the function of a MIB?

A. DHCP relay device

B. Policy enforcement point

C. Definition file for event translation

D. Network access controller

Answer: C

Explanation:

MIB (Management Information Base): A MIB is a database used for managing the entities in a communication network. The MIB is used by Simple Network Management Protocol (SNMP) to translate events into a readable format, enabling network administrators to manage and monitor network devices effectively.

Function of MIB: MIBs contain definitions and information about all objects that can be managed on a network using SNMP. These objects are defined using a hierarchical namespace containing object identifiers (OIDs).

Reference: CompTIA Network+ materials discussing SNMP and MIB functionality.

Question: 3

Which of the following best explains the role of confidentiality with regard to data at rest?

A. Data can be accessed by anyone on the administrative network.

B. Data can be accessed remotely with proper training.

C. Data can be accessed after privileged access Is granted.

D. Data can be accessed after verifying the hash.

Answer: C

Explanation:

Confidentiality with Data at Rest: Confidentiality is a core principle of data security, ensuring that data stored (at rest) is only accessible to authorized individuals. This protection is achieved through mechanisms such as encryption, access controls, and permissions.

Privileged Access: The statement "Data can be accessed after privileged access is granted" aligns with the confidentiality principle, as it restricts data access to users who have been granted specific permissions or roles. Only those with the appropriate credentials or permissions can access the data.

Incorrect Options:

A . "Data can be accessed by anyone on the administrative network." This violates the principle of confidentiality by allowing unrestricted access.

B . "Data can be accessed remotely with proper training." This focuses on remote access rather than restricting access based on privileges.

D . "Data can be accessed after verifying the hash." This option relates more to data integrity rather than confidentiality.

Reference: CompTIA Network+ materials on data security principles, particularly sections on confidentiality and access control mechanisms.

Question: 4

A network engineer performed a migration to a new mail server. The engineer changed the MX record, verified the change was accurate, and confirmed the new mail server was reachable via the IP address in the A record. However, users are not receiving email. Which of the following should the engineer have done to prevent the issue from occurring?

A. Change the email client configuration to match the MX record.

B. Reduce the TTL record prior to the MX record change.

C. Perform a DNS zone transfer prior to the MX record change.

D. Update the NS record to reflect the IP address change.

Answer: B

Explanation:

Understanding TTL (Time to Live):

TTL is a value in a DNS record that tells how long that record should be cached by DNS servers and clients. A higher TTL value means that the record will be cached longer, reducing the load on the DNS server but delaying the propagation of changes.

Impact of TTL on DNS Changes:

When an MX record change is made, it may take time for the change to propagate across all DNS

servers due to the TTL setting. If the TTL is high, old DNS information might still be cached, leading to email being directed to the old server.

Best Practice Before Making DNS Changes:

To ensure that changes to DNS records propagate quickly, it is recommended to reduce the TTL value to a lower value (such as 300 seconds or 5 minutes) well in advance of making the changes. This ensures that any cached records will expire quickly, and the new records will be used sooner.

Verification of DNS Changes:

After reducing the TTL and making the change to the MX record, it is important to verify the propagation using tools like dig or nslookup.

Comparison with Other Options:

Change the email client configuration to match the MX record: Email clients generally do not need to match the MX record directly; they usually connect to a specific mail server specified in their settings.

Perform a DNS zone transfer prior to the MX record change: DNS zone transfers are used to replicate DNS records between DNS servers, but they are not related to the propagation of individual record changes.

Update the NS record to reflect the IP address change: NS records specify the DNS servers for a domain and are not related to MX record changes.

Reference:

CompTIA Network+ study materials and DNS best practices.

Question: 5

Which of the following IP transmission types encrypts all of the transmitted data?

A. ESP

B. AH

C. GRE

D. UDP

E. TC

P

Answer: A

Explanation:

Definition of ESP (Encapsulating Security Payload):

ESP is a part of the IPsec protocol suite used to provide confidentiality, integrity, and authenticity of data. ESP encrypts the payload and optional ESP trailer, providing data confidentiality.

ESP Functionality:

ESP can encrypt the entire IP packet, ensuring that the data within the packet is secure from interception or eavesdropping. It also provides options for data integrity and authentication.

ESP operates in two modes: transport mode (encrypts only the payload of the IP packet) and tunnel mode (encrypts the entire IP packet).

Comparison with Other Protocols:

AH (Authentication Header): Provides data integrity and authentication but does not encrypt the payload.

GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption.

UDP (User Datagram Protocol) and TCP (Transmission Control Protocol): These are transport layer protocols that do not inherently provide encryption. Encryption must be provided by additional protocols like TLS/SSL.

Use Cases:

ESP is widely used in VPNs (Virtual Private Networks) to ensure secure communication over untrusted networks like the internet.

Reference:

CompTIA Network+ study materials on IPsec and encryption.

Question: 6

A network administrator notices interference with industrial equipment in the 2.4GHz range. Which of the following technologies would most likely mitigate this issue? (Select two).

A. Mesh network

B. 5GHz frequency

C. Omnidirectional antenna

D. Non-overlapping channel

E. Captive portal

F. Ad hoc network

Answer: B

Explanation:

Understanding 2.4GHz Interference:

The 2.4GHz frequency range is commonly used by many devices, including Wi-Fi, Bluetooth, and various industrial equipment. This can lead to interference and degraded performance.

Mitigation Strategies:

5GHz Frequency:

The 5GHz frequency band offers more channels and less interference compared to the 2.4GHz band. Devices operating on 5GHz are less likely to encounter interference from other devices, including industrial equipment.

Non-overlapping Channels:

In the 2.4GHz band, using non-overlapping channels (such as channels 1, 6, and 11) can help reduce interference. Non-overlapping channels do not interfere with each other, providing clearer communication paths for Wi-Fi signals.

Why Other Options are Less Effective:

Mesh Network: While useful for extending network coverage, a mesh network does not inherently address interference issues.

Omnidirectional Antenna: This type of antenna broadcasts signals in all directions but does not mitigate interference.

Captive Portal: A web page that users must view and interact with before accessing a network,

unrelated to frequency interference.

Ad Hoc Network: A decentralized wireless network that does not address interference issues directly.

Implementation:

Switch Wi-Fi devices to the 5GHz band if supported by the network infrastructure and client devices.

Configure Wi-Fi access points to use non-overlapping channels within the 2.4GHz band to minimize interference.

Reference:

CompTIA Network+ study materials on wireless networking and interference mitigation.

Question: 7

Which of the following disaster recovery metrics is used to describe the amount of data that is lost since the last backup?

A. MTTR

B. RTO

C. RPO

D. MTBF

Answer: C

Explanation:

Definition of RPO:

Recovery Point Objective (RPO) is a disaster recovery metric that describes the maximum acceptable amount of data loss measured in time. It indicates the point in time to which data must be recovered to resume normal operations after a disaster.

For example, if the RPO is set to 24 hours, then the business could tolerate losing up to 24 hours'

worth of data in the event of a disruption.

Why RPO is Important:

RPO is critical for determining backup frequency and helps businesses decide how often they need to back up their data. A lower RPO means more frequent backups and less potential data loss.

Comparison with Other Metrics:

MTTR (Mean Time to Repair): Refers to the average time required to repair a system or component and return it to normal operation.

RTO (Recovery Time Objective): The maximum acceptable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.

MTBF (Mean Time Between Failures): The predicted elapsed time between inherent failures of a system during operation.

How RPO is Used in Disaster Recovery:

Organizations establish RPOs to ensure that they can recover data within a timeframe that is acceptable to business operations. This involves creating a backup plan that meets the RPO requirements.

Reference:

CompTIA Network+ study materials and certification guides.

Question: 8

Which of the following can support a jumbo frame?

A. Access point

B. Bridge

C. Hub

D. Switch

Answer: D

Explanation:

Definition of Jumbo Frames:

Jumbo frames are Ethernet frames with more than 1500 bytes of payload, typically up to 9000 bytes. They are used to improve network performance by reducing the overhead caused by smaller frames.

Why Switches Support Jumbo Frames:

Switches are network devices designed to manage data packets and can be configured to support jumbo frames. This capability enhances throughput and efficiency, particularly in high-performance networks and data centers.

Incompatibility of Other Devices:

Access Point: Primarily handles wireless communications and does not typically support jumbo frames.

Bridge: Connects different network segments but usually operates at standard Ethernet frame sizes.

Hub: A simple network device that transmits packets to all ports without distinguishing between devices, incapable of handling jumbo frames.

Practical Application:

Enabling jumbo frames on switches helps in environments where large data transfers are common, such as in storage area networks (SANs) or large-scale virtualized environments.

Reference:

CompTIA Network+ course materials and networking hardware documentation.

Question: 9

Which of the following is created to illustrate the effectiveness of wireless networking coverage in a building?

A. Logical diagram

B. Layer 3 network diagram

C. Service-level agreement

D. Heat map

Answer: D

Explanation:

Definition of Heat Maps:

A heat map is a graphical representation of data where individual values are represented by colors. In the context of wireless networking, a heat map shows the wireless signal strength in different areas of a building.

Purpose of a Heat Map:

Heat maps are used to illustrate the effectiveness of wireless networking coverage, identify dead zones, and optimize the placement of access points (APs) to ensure adequate coverage and performance.

Comparison with Other Options:

Logical Diagram: Represents the logical connections and relationships within the network.

Layer 3 Network Diagram: Focuses on the routing and IP addressing within the network.

Service-Level Agreement (SLA): A contract that specifies the expected service levels between a service provider and a customer.

Creation and Use:

Heat maps are created using specialized software or tools that measure wireless signal strength throughout the building. The data collected is then used to generate a visual map, guiding network administrators in optimizing wireless coverage.

Reference:

CompTIA Network+ certification materials and wireless network planning guides.

Question: 10

A user is unable to navigate to a website because the provided URL is not resolving to the correct IP address. Other users are able to navigate to the intended website without issue. Which of the following is most likely causing this issue?

A. Hosts file

B. Self-signed certificate

C. Nameserver record

D. IP helper

ANS

Answer: A

Explanation:

Role of the Hosts File:

The hosts file is a local file on a computer that maps hostnames to IP addresses. It can be used to override DNS resolution by providing a static mapping of a hostname to an IP address.

Common Issues with the Hosts File:

If an incorrect IP address is mapped to a hostname in the hosts file, it can cause the computer to resolve the hostname to the wrong IP address. This can lead to navigation issues for specific websites while other users, relying on DNS, do not face the same problem.

Why Other Options are Less Likely:

Self-signed certificate: Relates to SSL/TLS and would cause a security warning, not a navigation failure.

Nameserver record: Affects all users, not just one.

IP helper: Used to forward DHCP requests and is unrelated to DNS resolution issues.

Troubleshooting Steps:

Check the hosts file on the affected user's computer (C:\Windows\System32\drivers\etc\hosts on Windows or /etc/hosts on Unix/Linux).

Look for entries that map the problematic hostname to an incorrect IP address and correct or remove them.

Reference:

CompTIA Network+ study materials and system administration documentation.

Question: 11

An IT manager needs to connect ten sites in a mesh network. Each needs to be secured with reduced provisioning time. Which of the following technologies will best meet this requirement?

A. SD-WAN

B. VXLAN

C. VPN

D. NFV

Answer: A

Explanation:

Definition of SD-WAN:

Software-Defined Wide Area Network (SD-WAN) is a technology that simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism. It allows for centralized management and enhanced security.

Benefits of SD-WAN:

Reduced Provisioning Time: SD-WAN enables quick and easy deployment of new sites with centralized control and automation.

Security: Incorporates advanced security features such as encryption, secure tunneling, and integrated firewalls.

Scalability: Easily scales to accommodate additional sites and bandwidth requirements.

Comparison with Other Technologies:

VXLAN (Virtual Extensible LAN): Primarily used for network virtualization within data centers.

VPN (Virtual Private Network): Provides secure connections but does not offer the centralized management and provisioning efficiency of SD-WAN.

NFV (Network Functions Virtualization): Virtualizes network services but does not specifically address WAN management and provisioning.

Implementation:

SD-WAN solutions are implemented by deploying edge devices at each site and connecting them to a central controller. This allows for dynamic routing, traffic management, and security policy enforcement.

Reference:

CompTIA Network+ course materials and networking solution guides.

Question: 12

After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect take to troubleshoot the issue?

A. Check to see if the end connections were wrapped in copper tape before terminating.

B. Use passthrough modular crimping plugs instead of traditional crimping plugs.

C. Connect the RX/TX wires to different pins.

D. Run a speed test on a device that can only achieve 100Mbps speeds.

Answer: A

Explanation:

Importance of Proper Termination:

Cat 8 cabling requires precise termination practices to ensure signal integrity and reduce interference. One common requirement is to wrap the end connections in copper tape to maintain shielding and reduce electromagnetic interference (EMI).

Interference Troubleshooting:

Interference in high-frequency cables like Cat 8 can be caused by improper shielding or grounding. Checking the end connections for proper wrapping in copper tape is a crucial step.

Why Other Options are Less Likely:

Passthrough modular crimping plugs: Not specifically related to interference issues and are typically used for ease of cable assembly.

Connecting RX/TX wires to different pins: Would likely result in no connection or incorrect data transmission rather than interference.

Running a speed test on a device that can only achieve 100Mbps speeds: This would not diagnose interference and would not provide relevant information for Cat 8 cabling rated for higher speeds.

Corrective Actions:

Verify that all end connections are properly wrapped with copper tape before termination.

Ensure that the shielding is continuous and properly grounded throughout the installation.

Retest the cabling for interference after making corrections.

Reference:

CompTIA Network+ study materials and structured cabling installation guides.

Question: 13

Which of the following most likely determines the size of a rack for installation? (Select two).

A. KVM size

B. Switch depth

C. Hard drive size

D. Cooling fan speed

E. Outlet amperage

F. Server height

Answer: B

Explanation:

Understanding Rack Size Determination:

The size of a rack for installation is determined by the dimensions of the equipment to be housed in it, primarily focusing on the depth and height of the devices.

Switch Depth:

Depth of Equipment: The depth of network switches and other rack-mounted devices directly influences the depth of the rack. If the equipment is deeper, a deeper rack is required to accommodate it.

Industry Standards: Most racks come in standard depths, but it is essential to match the depth of the rack to the deepest piece of equipment to ensure proper fit and airflow.

Server Height:

Height of Equipment: The height of servers and other devices is measured in rack units (U), where 1U equals 1.75 inches. The total height of all equipment determines the overall height requirement of the rack.

Rack Units: A rack's height is typically described in terms of the number of rack units it can accommodate, such as 42U, 48U, etc.

Why Other Options are Less Relevant:

KVM Size: While important for management, KVM (Keyboard, Video, Mouse) switches do not typically determine rack size.

Hard Drive Size: Individual hard drives are installed within servers or storage devices, not directly influencing rack dimensions.

Cooling Fan Speed: Fan speed affects cooling but not the physical size of the rack.

Outlet Amperage: Power requirements do not determine rack dimensions but rather the electrical infrastructure supporting the rack.

Reference:

CompTIA Network+ study materials on rack installation and equipment sizing.

Question: 14

A VoIP phone is plugged in to a port but cannot receive calls. Which of the following needs to be done on the port to address the issue?

A. Trunk all VLANs on the port.

B. Configure the native VLAN.

C. Tag the traffic to voice VLAN.

D. Disable VLANs.

Answer: C

Explanation:

Understanding VoIP and VLANs:

VoIP (Voice over IP) phones often use VLANs (Virtual Local Area Networks) to separate voice traffic from data traffic for improved performance and security.

Tagging Traffic to Voice VLAN:

Voice VLAN Configuration: The port on the switch needs to be configured to tag traffic for the specific voice VLAN. This ensures that voice packets are prioritized and handled correctly.

VLAN Tagging: VLAN tagging allows the switch to identify and separate voice traffic from other types of traffic on the network, reducing latency and jitter for VoIP communications.

Comparison with Other Options:

Trunk all VLANs on the port: Trunking all VLANs is typically used for links between switches, not for individual device ports.

Configure the native VLAN: The native VLAN is for untagged traffic and does not address the need for separating and prioritizing voice traffic.

Disable VLANs: Disabling VLANs would mix voice and data traffic, leading to potential performance issues and lack of traffic separation.

Implementation:

Configure the switch port connected to the VoIP phone to tag the traffic for the designated voice VLAN, ensuring proper network segmentation and quality of service.

Reference:

CompTIA Network+ study materials on VLAN configuration and VoIP implementation.

Question: 15

As part of an attack, a threat actor purposefully overflows the content-addressable memory (CAM) table on a switch. Which of the following types of attacks is this scenario an example of?

A. ARP spoofing

B. Evil twin

C. MAC flooding

D. DNS poisoning

Answer: C

Explanation:

Definition of MAC Flooding:

MAC flooding is an attack where a malicious actor sends numerous fake MAC addresses to a switch, overwhelming its CAM table. The CAM table stores MAC addresses and their associated ports for efficient traffic forwarding.

Impact of MAC Flooding:

CAM Table Overflow: When the CAM table is full, the switch cannot learn new MAC addresses and is forced to broadcast traffic to all ports, leading to a degraded network performance and potential data interception.

Switch Behavior: The switch operates in a fail-open mode, treating the network as a hub, which can be exploited for eavesdropping on traffic.

Comparison with Other Attacks:

ARP Spoofing: Involves sending false ARP (Address Resolution Protocol) messages to associate the attacker's MAC address with the IP address of another device.

Evil Twin: Involves creating a rogue wireless access point that mimics a legitimate one to intercept data.

DNS Poisoning: Involves corrupting the DNS cache with false information to redirect traffic to malicious sites.

Preventive Measures:

Port Security: Configure port security on switches to limit the number of MAC addresses per port, preventing CAM table overflow.

Network Segmentation: Use VLANs to segment network traffic and limit the impact of such attacks.

Reference:

CompTIA Network+ study materials on network security threats and mitigation techniques.

Question: 16

A network manager wants to implement a SIEM system to correlate system events. Which of the following protocols should the network manager verify?

A. NTP

B. DNS

C. LDAP

D. DHCP

Answer: A

Explanation:

Role of NTP (Network Time Protocol):

NTP is used to synchronize the clocks of network devices to a reference time source. Accurate time synchronization is critical for correlating events and logs from different systems.

Importance for SIEM Systems:

Event Correlation: SIEM (Security Information and Event Management) systems collect and analyze log data from various sources. Accurate timestamps are essential for correlating events across multiple systems.

Time Consistency: Without synchronized time, it is challenging to piece together the sequence of events during an incident, making forensic analysis difficult.

Comparison with Other Protocols:

DNS (Domain Name System): Translates domain names to IP addresses but is not related to time synchronization.

LDAP (Lightweight Directory Access Protocol): Used for directory services, such as user authentication and authorization.

DHCP (Dynamic Host Configuration Protocol): Assigns IP addresses to devices on a network but does not handle time synchronization.

Implementation:

Ensure that all network devices, servers, and endpoints are synchronized using NTP. This can be achieved by configuring devices to use an NTP server, which could be a local server or an external time source.

Reference:

CompTIA Network+ study materials on network protocols and SIEM systems.

Question: 17

A network engineer is designing a secure communication link between two sites. The entire data stream needs to remain confidential. Which of the following will achieve this goal?

A. GRE

B. IKE

C. ESP

D. AH

Answer: C

Explanation:

Definition of ESP (Encapsulating Security Payload):

ESP is a part of the IPsec protocol suite designed to provide confidentiality, integrity, and authenticity of data by encrypting the payload and optional ESP trailer.

Ensuring Confidentiality:

Encryption: ESP encrypts the payload, ensuring that the data remains confidential during transmission. Only authorized parties with the correct decryption keys can access the data.

Modes of Operation: ESP can operate in transport mode (encrypts only the payload) or tunnel mode (encrypts the entire IP packet), both providing strong encryption to secure data between sites.

Comparison with Other Protocols:

GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption or security features.

IKE (Internet Key Exchange): A protocol used to set up a secure, authenticated communications channel, but it does not encrypt the data itself.

AH (Authentication Header): Provides integrity and authentication for IP packets but does not encrypt the payload.

Implementation:

Use ESP as part of an IPsec VPN configuration to encrypt and secure communication between two sites. This involves setting up IPsec policies and ensuring both endpoints are configured to use ESP for data encryption.

Reference:

CompTIA Network+ study materials on IPsec and secure communication protocols.

Question: 18

Which of the following routing protocols uses an autonomous system number?

A. IS-IS

B. EIGRP

C. OSPF

D. BGP

Answer: D

Explanation:

BGP (Border Gateway Protocol) uses an Autonomous System (AS) number for its operations. An AS is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the Internet. BGP is used to exchange routing information between different ASes on the Internet, making it the only protocol among the listed options that uses an AS number.
Reference: CompTIA Network+ study materials and RFC 4271.

Question: 19

Which of the following is the most secure way to provide site-to-site connectivity?

A. VXLAN

B. IKE

C. GRE

D. IPsec

Answer: D

Explanation:

IPsec (Internet Protocol Security) is the most secure way to provide site-to-site connectivity. It provides robust security services, such as data integrity, authentication, and encryption, ensuring that data sent across the network is protected from interception and tampering. Unlike other options, IPsec operates at the network layer and can secure all traffic that crosses the IP network, making it the most comprehensive and secure choice for site-to-site VPNs.
Reference: CompTIA Network+ study materials and NIST Special Publication 800-77.

Question: 20

A network administrator needs to connect two routers in a point-to-point configuration and conserve

IP space. Which of the following subnets should the administrator use?

A. 724

B. /26

C. /28

D. /30

Answer: D

Explanation:

Using a /30 subnet mask is the most efficient way to conserve IP space for a point-to-point connection between two routers. A /30 subnet provides four IP addresses, two of which can be assigned to the router interfaces, one for the network address, and one for the broadcast address. This makes it ideal for point-to-point links where only two usable IP addresses are needed.
Reference: CompTIA Network+ study materials and subnetting principles.

Question: 21

To reduce costs and increase mobility, a Chief Technology Officer (CTO) wants to adopt cloud services for the organization and its affiliates. To reduce the impact for users, the CTO wants key services to run from the on-site data center and enterprise services to run in the cloud. Which of the following deployment models is the best choice for the organization?

A. Public

B. Hybrid

C. SaaS

D. Private

Answer: B

Explanation:

A hybrid cloud deployment model is the best choice for the CTO's requirements. It allows the organization to run key services from the on-site data center while leveraging the cloud for enterprise services. This approach provides flexibility, scalability, and cost savings, while also minimizing disruptions to users by keeping critical services local. The hybrid model integrates both private and public cloud environments, offering the benefits of both.
Reference: CompTIA Network+ study materials and cloud computing principles.

Question: 22

A technician is troubleshooting a user's laptop that is unable to connect to a corporate server. The technician thinks the issue pertains to routing. Which of the following commands should the technician use to identify the issue?

A. tcpdump

B. dig

C. tracert

D. arp

Answer: C

Explanation:

The tracert (Traceroute) command is used to determine the path packets take from the source to the destination. It helps in identifying routing issues by showing each hop the packets pass through, along with the time taken for each hop. This command can pinpoint where the connection is failing or experiencing delays, making it an essential tool for troubleshooting routing issues.
Reference: CompTIA Network+ study materials and common network troubleshooting commands.

Question: 23

Which of the following fiber connector types is the most likely to be used on a network interface card?

A. LC

B. SC

C. ST

D. MPO

Answer: A

Explanation:

Definition of Fiber Connector Types:

LC (Lucent Connector): A small form-factor fiber optic connector with a push-pull latching mechanism, commonly used for high-density applications.

SC (Subscriber Connector or Standard Connector): A larger form-factor connector with a push-pull latching mechanism, often used in datacom and telecom applications.

ST (Straight Tip): A bayonet-style connector, typically used in multimode fiber optic networks.

MPO (Multi-fiber Push On): A connector designed to support multiple fibers (typically 12 or 24 fibers), used in high-density cabling environments.

Common Usage:

LC Connectors: Due to their small size, LC connectors are widely used in network interface cards (NICs) and high-density environments such as data centers. They allow for more connections in a smaller space compared to SC and ST connectors.

SC and ST Connectors: These are larger and more commonly used in patch panels and older fiber installations but are less suitable for high-density applications.

MPO Connectors: Primarily used for trunk cables in data centers and high-density applications but not typically on individual network interface cards.

Selection Criteria:

The small form-factor and high-density capabilities of LC connectors make them the preferred choice for network interface cards, where space and connection density are critical considerations.

Reference:

CompTIA Network+ study materials on fiber optics and connector types.

Question: 24

A network engineer receives a vendor alert regarding a vulnerability in a router CPU. Which of the following should the engineer do to resolve the issue?

A. Update the firmware.

B. Replace the system board.

C. Patch the OS.

D. Isolate the system.

Answer: A

Explanation:

Understanding the Vulnerability:

Vulnerabilities in the router CPU can be exploited to cause performance degradation, unauthorized access, or other security issues.

Firmware Update:

Firmware Role: The firmware is low-level software that controls the hardware of a device. Updating the firmware can address vulnerabilities by providing patches and enhancements from the manufacturer.

Procedure: Download the latest firmware from the vendor’s website, follow the manufacturer's instructions to apply the update, and verify that the update resolves the vulnerability.

Comparison with Other Options:

Replace the System Board: This is a costly and often unnecessary step if the issue can be resolved with a firmware update.

Patch the OS: Patching the OS is relevant for devices with a full operating system but not directly applicable to addressing a CPU vulnerability on a router.

Isolate the System: Temporarily isolating the system can mitigate immediate risk but does not resolve the underlying vulnerability.

Best Practice:

Regularly check for and apply firmware updates to ensure that network devices are protected against known vulnerabilities.

Reference:

CompTIA Network+ study materials on network security and device management.

Question: 25

A virtual machine has the following configuration:

- IPv4 address: 169.254.10.10
- Subnet mask: 255.255.0.0

The virtual machine can reach colocated systems but cannot reach external addresses on the Internet. Which of the following Is most likely the root cause?

A. The subnet mask is incorrect.

B. The DHCP server is offline.

C. The IP address is an RFC1918 private address.

D. The DNS server is unreachable.

Answer: B

Explanation:

Understanding the 169.254.x.x Address:

An IPv4 address in the range of 169.254.x.x is an Automatic Private IP Addressing (APIPA) address, assigned when a DHCP server is unavailable.

DHCP Server Offline:

APIPA Assignment: When a device cannot obtain an IP address from a DHCP server, it assigns itself an APIPA address to enable local network communication. This allows communication with other devices on the same local subnet but not with external networks.

Resolution: Ensure the DHCP server is operational. Check for connectivity issues between the virtual machine and the DHCP server, and verify the DHCP server settings.

Comparison with Other Options:

The subnet mask is incorrect: The subnet mask 255.255.0.0 is appropriate for the 169.254.x.x range and does not prevent external access by itself.

The IP address is an RFC1918 private address: RFC1918 addresses are private IP ranges (10.x.x.x, 172.16.x.x-172.31.x.x, 192.168.x.x) but 169.254.x.x is not one of them.

The DNS server is unreachable: While this could affect name resolution, it would not prevent the assignment of a non-APIPA address or local network communication.

Troubleshooting Steps:

Verify the DHCP server's status and connectivity.

Restart the DHCP service if necessary.

Renew the IP lease on the virtual machine using commands such as ipconfig /renew (Windows) or dhclient (Linux).

Reference:

CompTIA Network+ study materials on IP addressing and DHCP troubleshooting.

Question: 26

A network technician is troubleshooting a web application's poor performance. The office has two internet links that share the traffic load. Which of the following tools should the technician use to determine which link is being used for the web application?

A. netstat

B. nslookup

C. ping

D. tracert

Answer: D

Explanation:

Understanding Tracert:

Traceroute Tool: tracert (Windows) or traceroute (Linux) is a network diagnostic tool used to trace the path that packets take from a source to a destination. It lists all the intermediate routers the packets traverse.

Determining Traffic Path:

Path Identification: By running tracert to the web application's destination IP address, the technician can identify which route the traffic is taking and thereby determine which internet link is being used.

Load Balancing Insight: If the office uses load balancing for its internet links, tracert can help verify which link is currently handling the traffic for the web application.

Comparison with Other Tools:

netstat: Displays network connections, routing tables, interface statistics, and more, but does not trace the path of packets.

nslookup: Used for querying DNS to obtain domain name or IP address mapping, not for tracing packet routes.

ping: Tests connectivity and measures round-trip time but does not provide path information.

Implementation:

Open a command prompt or terminal.

Execute tracert [destination IP] to trace the route.

Analyze the output to determine the path and the link being used.

Reference:

CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

Question: 27

A network administrator configured a router interface as 10.0.0.95 255.255.255.240. The

administrator discovers that the router is not routing packets to a web server with IP 10.0.0.81/28. Which of the following is the best explanation?

A. The web server Is In a different subnet.

B. The router interface is a broadcast address.

C. The IP address space is a class A network.

D. The subnet is in a private address space.

Answer: B

Explanation:

Understanding Subnetting:

The subnet mask 255.255.255.240 (or /28) indicates that each subnet has 16 IP addresses (14 usable addresses, 1 network address, and 1 broadcast address).

Calculating the Subnet Range:

Subnet Calculation: For the IP address 10.0.0.95 with a /28 subnet mask:

Network address: 10.0.0.80

Usable IP range: 10.0.0.81 to 10.0.0.94

Broadcast address: 10.0.0.95

Router Interface Configuration:

Broadcast Address Issue: The IP address 10.0.0.95 is the broadcast address for the subnet 10.0.0.80/28. Configuring a router interface with the broadcast address will cause routing issues as it is not a valid host address.

Comparison with Other Options:

The web server is in a different subnet: The web server (10.0.0.81) is within the same subnet range (10.0.0.80/28).

The IP address space is a class A network: While 10.0.0.0 is a Class A network, this does not explain the routing issue caused by the broadcast address.

The subnet is in a private address space: The private address space designation (RFC 1918) does not

impact the routing issue related to the broadcast address configuration.

Resolution:

Reconfigure the router interface with a valid host IP address within the usable range, such as 10.0.0.94.

Reference:

CompTIA Network+ study materials on subnetting and IP address configuration.

Question: 28

Which of the following does a full-tunnel VPN provide?

A. Lower bandwidth requirements

B. The ability to reset local computer passwords

C. Corporate Inspection of all network traffic

D. Access to blocked sites

Answer: C

Explanation:

A full-tunnel VPN routes all of a user's network traffic through the corporate network. This means that the organization can inspect all network traffic for security and compliance purposes, as all data is tunneled through the VPN, allowing for comprehensive monitoring and inspection.
Reference: CompTIA Network+ study materials.

Question: 29

A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light does not turn on. Which of the following should a technician try first to troubleshoot this issue?

A. Reverse the fibers.

B. Reterminate the fibers.

C. Verify the fiber size.

D. Examine the cable runs for visual faults.

Answer: A

Explanation:

When working with fiber optic cables, one common issue is that the transmit (TX) and receive (RX) fibers might be reversed. The first step in troubleshooting should be to reverse the fibers at one end to ensure they are correctly aligned (TX to RX and RX to TX). This is a simple and quick step to rule out a common issue before moving on to more complex troubleshooting.
Reference: CompTIA Network+ study materials.

Question: 30

Which of the following protocols has a default administrative distance value of 90?

A. RIP

B. EIGRP

C. OSPF

D. BGP

Answer: B

Explanation:

EIGRP (Enhanced Interior Gateway Routing Protocol) has a default administrative distance (AD) value of 90 for internal routes. The administrative distance is used to rate the trustworthiness of routing

information received from different routing protocols. EIGRP, developed by Cisco, has an AD of 90, which is lower than that of RIP (120) and OSPF (110), making it more preferred if multiple protocols provide a route to the same destination.
Reference: CompTIA Network+ study materials.

Question: 31

Which of the following is a cost-effective advantage of a split-tunnel VPN?

A. Web traffic is filtered through a web filter.

B. More bandwidth is required on the company's internet connection.

C. Monitoring detects insecure machines on the company’s network.

D. Cloud-based traffic flows outside of the company's network.

Answer: D

Explanation:

A split-tunnel VPN allows certain traffic (e.g., cloud-based services) to bypass the VPN and go directly to the Internet. This reduces the amount of traffic that needs to traverse the company's VPN and Internet connection, conserving bandwidth and reducing costs. It also means that not all traffic is subject to the same level of inspection or filtering, which can improve performance for cloud-based services.
Reference: CompTIA Network+ study materials.

Question: 32

Which of the following should be configured so users can authenticate to a wireless network using company credentials?

A. SSO

B. SAML

C. MFA

D. RADIUS

Answer: D

Explanation:

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. RADIUS is often used to manage access to wireless networks, enabling users to authenticate with their company credentials, ensuring secure access to the network.
Reference: CompTIA Network+ study materials.

Question: 33

Which of the following is most likely responsible for the security and handling of personal data in Europe?

A. GDPR

B. SCADA

C. SAML

D. PCI DSS

Answer: A

Explanation:

Definition of GDPR:

General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

Scope and Objectives:

GDPR aims to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

It enforces rules about data protection, requiring companies to protect the personal data and privacy of EU citizens for transactions that occur within EU member states.

Comparison with Other Options:

SCADA (Supervisory Control and Data Acquisition): Refers to control systems used in industrial and infrastructure processes, not related to personal data protection.

SAML (Security Assertion Markup Language): A standard for exchanging authentication and authorization data between parties, not specifically for personal data protection.

PCI DSS (Payment Card Industry Data Security Standard): A set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment, not specific to personal data protection in Europe.

Key Provisions:

GDPR includes provisions for data processing, data subject rights, obligations of data controllers and processors, and penalties for non-compliance.

Reference:

CompTIA Network+ study materials on regulatory and compliance standards.

Question: 34

Users cannot connect to an internal website with an IP address 10.249.3.76. A network administrator runs a command and receives the following output:

1 3ms 2ms 3ms 192.168.25.234

2 2ms 3ms 1ms 192.168.3.100

3 4ms 5ms 2ms 10.249.3.1

4 *

5 ’

6 *

7 •

Which of the following command-line tools is the network administrator using?

A. tracert

B. netstat

C. tcpdump

D. nmap

Answer: A

Explanation:

Understanding Tracert:

tracert (Traceroute in Windows) is a command-line tool used to trace the path that packets take from the source to the destination. It records the route (the specific gateways at each hop) and measures transit delays of packets across an IP network.

Output Analysis:

The output shows a series of IP addresses with corresponding round-trip times (RTTs) in milliseconds.

The asterisks (*) indicate that no response was received from those hops, which is typical for routers or firewalls that block ICMP packets used by tracert.

Comparison with Other Tools:

netstat: Displays network connections, routing tables, interface statistics, and more, but does not trace packet routes.

tcpdump: Captures network packets for analysis, used for detailed network traffic inspection.

nmap: A network scanning tool used to discover hosts and services on a network, not for tracing packet routes.

Usage:

tracert helps identify the path to a destination and locate points of failure or congestion in the network.

Reference:

CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

Question: 35

Which of the following attacks would most likely cause duplicate IP addresses in a network?

A. Rogue DHCP server

B. DNS poisoning

C. Social engineering

D. Denial-of-service

Answer: A

Explanation:

Definition of a Rogue DHCP Server:

A rogue DHCP server is an unauthorized DHCP server on a network, which can assign IP addresses to devices without proper control, leading to IP address conflicts.

Impact of a Rogue DHCP Server:

IP Address Conflicts: Multiple devices may receive the same IP address from different DHCP servers, causing network connectivity issues.

Network Disruption: Devices may be assigned incorrect network configuration settings, disrupting network services and connectivity.

Comparison with Other Attacks:

DNS poisoning: Alters DNS records to redirect traffic to malicious sites, but does not cause IP address conflicts.

Social engineering: Involves manipulating individuals to gain unauthorized access or information, not directly related to IP address conflicts.

Denial-of-service (DoS): Floods a network or service with excessive traffic to disrupt operations, but does not cause duplicate IP addresses.

Prevention and Detection:

Implement network access control measures to prevent unauthorized devices from acting as DHCP servers.

Use DHCP snooping on switches to allow DHCP responses only from authorized DHCP servers.

Reference:

CompTIA Network+ study materials on network security threats and mitigation techniques.

Question: 36

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

A. 4096

B. 8192

C. 32768

D. 36684

Answer: C

Explanation:

Understanding Spanning Tree Protocol (STP):

STP is used to prevent network loops in Ethernet networks by creating a spanning tree that selectively blocks some redundant paths.

Default Priority Value:

Bridge Priority: STP uses bridge priority to determine which switch becomes the root bridge. The default bridge priority value for most switches is 32768.

Priority Range: The bridge priority can be set in increments of 4096, ranging from 0 to 61440.

Configuration and Verification:

When deploying a new switch, the network administrator can verify the bridge priority using commands such as show spanning-tree to ensure it is set to the default value of 32768.

Comparison with Other Values:

4096 and 8192: Lower than the default priority, indicating these would be manually configured for higher preference.

36684: A non-standard value, likely a result of specific configuration changes.

Reference:

CompTIA Network+ study materials on Spanning Tree Protocol and network configuration.

Question: 37

Which of the following steps of the troubleshooting methodology should a technician take to confirm a theory?

A. Duplicate the problem.

B. Identify the symptoms.

C. Gather information.

D. Determine any changes.

Answer: A

Explanation:

Troubleshooting Methodology:

Troubleshooting involves a systematic approach to diagnosing and resolving issues. It typically includes steps such as identifying symptoms, gathering information, formulating and testing theories, and implementing solutions.

Confirming a Theory:

Duplicate the Problem: To confirm a theory, the technician should reproduce the problem in a controlled environment. This helps verify that the identified cause actually leads to the observed issue.

Verification: By duplicating the problem, the technician can observe the issue firsthand, validate the hypothesis, and rule out other potential causes.

Comparison with Other Steps:

Identify the Symptoms: Initial step to understand what the problem is, not specifically for confirming a theory.

Gather Information: Involves collecting data and details about the issue, usually done before formulating a theory.

Determine Any Changes: Involves checking for recent changes that could have caused the issue, a part of the information-gathering phase.

Implementation:

Use similar equipment or software in a test environment to recreate the issue.

Observe the results to see if they match the original problem, thereby confirming the theory.

Reference:

CompTIA Network+ study materials on troubleshooting methodologies and best practices.

Question: 38

Early in the morning, an administrator installs a new DHCP server. In the afternoon, some users report they are experiencing network outages. Which of the following is the most likely issue?

A. The administrator did not provision enough IP addresses.

B. The administrator configured an incorrect default gateway.

C. The administrator did not provision enough routes.

D. The administrator did not provision enough MAC addresses.

Answer: A

Explanation:

When a DHCP server is installed and not enough IP addresses are provisioned, users may start experiencing network outages once the available IP addresses are exhausted. DHCP servers assign IP addresses to devices on the network, and if the pool of addresses is too small, new devices or those renewing their lease may fail to obtain an IP address, resulting in network connectivity issues.
Reference: CompTIA Network+ study materials.

Question: 39

Which of the following network topologies contains a direct connection between every node in the network?

A. Mesh

B. Hub-and-spoke

C. Star

D. Point-to-point

Answer: A

Explanation:

In a mesh topology, every node is directly connected to every other node. This provides high redundancy and reliability, as there are multiple paths for data to travel between nodes. This topology is often used in networks where high availability is crucial.
Reference: CompTIA Network+ study materials.

Question: 40

A company receives a cease-and-desist order from its ISP regarding prohibited torrent activity. Which of the following should be implemented to comply with the cease-and-desist order?

A. MAC security

B. Content filtering

C. Screened subnet

D. Perimeter network

Answer: B

Explanation:

Content filtering can be used to block or restrict access to websites and services that facilitate torrenting and other prohibited activities. By implementing content filtering, the company can comply with the ISP's cease-and-desist order and prevent users from accessing torrent sites and engaging in prohibited activities.
Reference: CompTIA Network+ study materials.

Question: 41

A network administrator is connecting two Layer 2 switches in a network. These switches must transfer data in multiple networks. Which of the following would fulfill this requirement?

A. Jumbo frames

B. 802.1Q tagging

C. Native VLAN

D. Link aggregation

Answer: B

Explanation:

802.1Q tagging, also known as VLAN tagging, is used to identify VLANs on a trunk link between

switches. This allows the switches to transfer data for multiple VLANs (or networks) over a single physical connection. This method ensures that traffic from different VLANs is properly separated and managed across the network.
Reference: CompTIA Network+ study materials.

Question: 42

A systems administrator is investigating why users cannot reach a Linux web server with a browser but can ping the server IP. The server is online, the web server process is running, and the link to the switch is up. Which of the following commands should the administrator run on the server first?

A. traceroute

B. netstat

C. tcpdump

D. arp

Answer: B

Explanation:

The netstat command provides information about network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. Running netstat on the server can help the administrator verify that the web server process is listening on the expected port (e.g., port 80 for HTTP or port 443 for HTTPS) and that there are no issues with network connections. This is a crucial first step in diagnosing why the web server is not accessible via a browser.
Reference: CompTIA Network+ study materials.

Question: 43

Which of the following devices can operate in multiple layers of the OSI model?

A. Hub

B. Switch

C. Transceiver

D. Modem

Answer: B

Explanation:

Understanding Switches:

Layer 2 (Data Link Layer): Traditional switches operate primarily at Layer 2, where they use MAC addresses to forward frames within a local network.

Layer 3 (Network Layer): Layer 3 switches, also known as multilayer switches, can perform routing functions using IP addresses to forward packets between different networks.

Capabilities of Multilayer Switches:

VLANs and Inter-VLAN Routing: Multilayer switches can handle VLAN (Virtual Local Area Network) configurations and perform inter-VLAN routing, enabling communication between different VLANs.

Routing Protocols: They can run routing protocols like OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) to manage traffic between networks.

Comparison with Other Devices:

Hub: Operates only at Layer 1 (Physical Layer) and simply repeats incoming signals to all ports.

Transceiver: Also operates at Layer 1, converting electrical signals to optical signals and vice versa.

Modem: Primarily operates at Layer 1 and Layer 2, modulating and demodulating signals for transmission over different types of media.

Practical Application:

Multilayer switches are commonly used in enterprise networks to optimize performance and manage complex routing and switching requirements within a single device.

Reference:

CompTIA Network+ study materials on network devices and the OSI model.

Question: 44

A critical infrastructure switch is identified as end-of-support. Which of the following is the best next step to ensure security?

A. Apply the latest patches and bug fixes.

B. Decommission and replace the switch.

C. Ensure the current firmware has no issues.

D. Isolate the switch from the network.

Answer: B

Explanation:

Understanding End-of-Support:

End-of-Support Status: When a vendor declares a device as end-of-support, it means the device will no longer receive updates, patches, or technical support. This poses a security risk as new vulnerabilities will not be addressed.

Risks of Keeping an End-of-Support Device:

Security Vulnerabilities: Without updates, the switch becomes susceptible to new security threats.

Compliance Issues: Many regulatory frameworks require that critical infrastructure be maintained with supported and secure hardware.

Best Next Step - Replacement:

Decommission and Replace: The most secure approach is to replace the end-of-support switch with a new, supported model. This ensures the infrastructure remains secure and compliant with current standards.

Planning and Execution: Plan for the replacement by evaluating the network's needs, selecting a suitable replacement switch, and scheduling downtime for the hardware swap.

Comparison with Other Options:

Apply the Latest Patches: While helpful, this does not address future vulnerabilities since no further patches will be provided.

Ensure the Current Firmware Has No Issues: This is only a temporary measure and does not mitigate future risks.

Isolate the Switch from the Network: Isolating the switch may disrupt network operations and is not a viable long-term solution.

Reference:

CompTIA Network+ study materials on network maintenance and security best practices.

Question: 45

Which of the following is the next step to take after successfully testing a root cause theory?

A. Determine resolution steps.

B. Duplicate the problem in a lab.

C. Present the theory for approval.

D. Implement the solution to the problem.

Answer: D

Explanation:

Troubleshooting Methodology:

Confirming the Root Cause: After testing and confirming the theory, the next logical step is to address the issue by implementing a solution.

Implementation of the Solution:

Resolve the Issue: Implement the identified solution to rectify the problem. This step involves making necessary changes to the network configuration, replacing faulty hardware, or applying software patches.

Documentation: Document the solution and the steps taken to resolve the issue to provide a reference for future troubleshooting.

Comparison with Other Steps:

Determine Resolution Steps: This is part of the implementation process where specific actions are outlined, but the actual next step after testing is to implement those steps.

Duplicate the Problem in a Lab: This step is typically done earlier in the troubleshooting process to understand the problem, not after confirming the root cause.

Present the Theory for Approval: In some scenarios, presenting the theory might be necessary for major changes, but generally, once the root cause is confirmed, the solution should be implemented.

Final Verification:

After implementing the solution, it is important to verify that the issue is resolved and that normal operations are restored. This may involve monitoring the network and testing to ensure no further issues arise.

Reference:

CompTIA Network+ study materials on troubleshooting methodologies and best practices.

Question: 46

Which of the following network devices converts wireless signals to electronic signals?

A. Router

B. Firewall

C. Access point

D. Load balancer

Answer: C

Explanation:

Role of an Access Point (AP):

Wireless to Wired Conversion: An access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi. It converts wireless signals (radio waves) into electronic signals that can be understood by wired network devices.

Functionality:

Signal Conversion: The AP receives wireless signals from devices such as laptops, smartphones, and tablets, converts them into electronic signals, and transmits them over the wired network.

Connectivity: APs provide a bridge between wireless and wired segments of the network, enabling seamless communication.

Comparison with Other Devices:

Router: Directs traffic between different networks and may include built-in AP functionality but is not primarily responsible for converting wireless to electronic signals.

Firewall: Protects the network by controlling incoming and outgoing traffic based on security rules, not involved in signal conversion.

Load Balancer: Distributes network or application traffic across multiple servers to ensure reliability and performance, not involved in signal conversion.

Deployment:

APs are commonly used in environments where wireless connectivity is needed, such as offices, homes, and public spaces. They enhance mobility and provide flexible network access.

Reference:

CompTIA Network+ study materials on wireless networking and access points.

Question: 47

Which of the following connectors provides console access to a switch?

A. ST

B. RJ45

C. BNC

D. SFP

Answer: B

Explanation:

Console Access:

Purpose: Console access to a switch allows administrators to configure and manage the device directly. This is typically done using a terminal emulator program on a computer.

RJ45 Connector:

Common Use: The RJ45 connector is widely used for Ethernet cables and also for console connections to network devices like switches and routers.

Console Cables: Console cables often have an RJ45 connector on one end (for the switch) and a DB9 serial connector on the other end (for the computer).

Comparison with Other Connectors:

ST (Straight Tip): A fiber optic connector used for networking, not for console access.

BNC (Bayonet Neill-Concelman): A connector used for coaxial cable, typically in older network setups and not for console access.

SFP (Small Form-factor Pluggable): A modular transceiver used for network interfaces, not for console access.

Practical Application:

Connection Process: Connect the RJ45 end of the console cable to the console port of the switch. Connect the DB9 end (or USB via adapter) to the computer. Use a terminal emulator (e.g., PuTTY, Tera Term) to access the switch's command-line interface (CLI).

Reference:

CompTIA Network+ study materials on network devices and connectors.

Question: 48

A network administrator wants users to be able to authenticate to the corporate network using a port-based authentication framework when accessing both wired and wireless devices. Which of the following is the best security feature to accomplish this task?

A. 802.1X

B. Access control list

C. Port security

D. MAC filtering

Answer: A

Explanation:

802.1X is a port-based network access control (PNAC) protocol that provides an authentication mechanism to devices wishing to connect to a LAN or WLAN. It is widely used for secure network access, ensuring that only authenticated devices can access the network, whether they are connecting via wired or wireless means. 802.1X works in conjunction with an authentication server, such as RADIUS, to validate the credentials of devices trying to connect.
Reference: CompTIA Network+ study materials.

Question: 49

Which of the following attacks can cause users who are attempting to access a company website to be directed to an entirely different website?

A. DNS poisoning

B. Denial-of-service

C. Social engineering

D. ARP spoofing

Answer: A

Explanation:

Network segmentation involves dividing a network into smaller segments or subnets. This is particularly important when integrating OT (Operational Technology) devices to ensure that these devices are isolated from other parts of the network. Segmentation helps protect the OT devices from potential threats and minimizes the impact of any security incidents. It also helps manage traffic and improves overall network performance.

Reference: CompTIA Network+ study materials.

Question: 50

Which of the following should a network administrator configure when adding OT devices to an organization's architecture?

A. Honeynet

B. Data-at-rest encryption

C. Time-based authentication

D. Network segmentation

Answer: D

Explanation:

Network segmentation involves dividing a network into smaller segments or subnets. This is particularly important when integrating OT (Operational Technology) devices to ensure that these devices are isolated from other parts of the network. Segmentation helps protect the OT devices from potential threats and minimizes the impact of any security incidents. It also helps manage traffic and improves overall network performance.
Reference: CompTIA Network+ study materials.

Question: 51

Which of the following are environmental factors that should be considered when installing equipment in a building? (Select two).

A. Fire suppression system

B. UPS location

C. Humidity control

D. Power load

E. Floor construction type

F. Proximity to nearest MDF

Answer: A

Explanation:

When installing equipment in a building, environmental factors are critical to ensure the safety and longevity of the equipment. A fire suppression system is essential to protect the equipment from fire hazards. Humidity control is crucial to prevent moisture-related damage, such as corrosion and short circuits, which can adversely affect electronic components. Both factors are vital for maintaining an optimal environment for networking equipment.
Reference: CompTIA Network+ study materials.

Question: 52

A network administrator is configuring a wireless network with an ESSID. Which of the following is a user benefit of ESSID compared to SSID?

A. Stronger wireless connection

B. Roaming between access points

C. Advanced security

D. Increased throughput

Answer: B

Explanation:

An Extended Service Set Identifier (ESSID) allows multiple access points to share the same SSID, enabling seamless roaming for users. This means that users can move between different access points within the same ESSID without losing connection or having to reauthenticate. This provides a

better user experience, especially in large environments such as office buildings or campuses.
Reference: CompTIA Network+ study materials.

Question: 53

A network administrator needs to divide 192.168.1.0/24 into two equal halves. Which of the following subnet masks should the administrator use?

A. 255.255.0.0

B. 255.255.254.0

C. 255.255.255.0

D. 255.255.255.128

Answer: D

Explanation:

Understanding Subnetting:

Original Network: 192.168.1.0/24 has a subnet mask of 255.255.255.0, which allows for 256 IP addresses (including network and broadcast addresses).

Objective: Divide this network into two equal subnets.

Calculating Subnet Mask:

New Subnet Mask: To divide 192.168.1.0/24 into two equal halves, we need to borrow one bit from the host portion of the address, changing the subnet mask to 255.255.255.128 (/25).

Subnet Breakdown:

First Subnet: 192.168.1.0/25 (192.168.1.0 - 192.168.1.127)

Second Subnet: 192.168.1.128/25 (192.168.1.128 - 192.168.1.255)

Verification:

Each subnet now has 128 IP addresses (126 usable IP addresses, excluding the network and

broadcast addresses).

Comparison with Other Options:

255.255.0.0 (/16): Provides a much larger network, not dividing the original /24 network.

255.255.254.0 (/23): Also creates a larger subnet, encompassing more than the original /24 network.

255.255.255.0 (/24): Maintains the original subnet size, not dividing it.

Reference:

CompTIA Network+ study materials on subnetting and IP addressing.

Question: 54

A network administrator needs to set up a multicast network for audio and video broadcasting. Which of the following networks would be the most appropriate for this application?

A. 172.16.0.0/24

B. 192.168.0.0/24

C. 224.0.0.0/24

D. 240.0.0.0/24

Answer: C

Explanation:

Understanding Multicast:

Multicast IP Address Range: The multicast address range is from 224.0.0.0 to 239.255.255.255, designated for multicast traffic.

Multicast Applications:

Use Case: Multicast is used for one-to-many or many-to-many communication, suitable for applications like audio and video broadcasting where the same data is sent to multiple recipients simultaneously.

Appropriate Network Selection:

224.0.0.0/24 Network: This range is reserved for multicast addresses, making it the appropriate choice for setting up a multicast network.

Comparison with Other Options:

172.16.0.0/24: Part of the private IP address space, used for private networks, not designated for multicast.

192.168.0.0/24: Another private IP address range, also not for multicast.

240.0.0.0/24: Reserved for future use, not suitable for multicast.

Reference:

CompTIA Network+ study materials on IP address ranges and multicast.

Question: 55

A research facility is expecting to see an exponential increase in global network traffic in the near future. The offices are equipped with 2.5Gbps fiber connections from the ISP, but the facility is currently only utilizing 1Gbps connections. Which of the following would need to be configured in order to use the ISP's connection speed?

A. 802.1Q tagging

B. Network address translation

C. Port duplex

D. Link aggregation

Answer: D

Explanation:

Understanding Link Aggregation:

Definition: Link aggregation combines multiple network connections into a single logical link to increase bandwidth and provide redundancy.

Usage in High-Bandwidth Scenarios:

Combining Links: By aggregating multiple 1Gbps connections, the facility can utilize the full 2.5Gbps bandwidth provided by the ISP.

Benefits: Enhanced throughput, load balancing, and redundancy, ensuring better utilization of available bandwidth.

Comparison with Other Options:

802.1Q Tagging: Used for VLAN tagging, which does not affect the physical bandwidth utilization.

Network Address Translation (NAT): Used for IP address translation, not related to link speed or bandwidth aggregation.

Port Duplex: Refers to the mode of communication (full or half duplex) on a port, not the aggregation of bandwidth.

Implementation:

Configure link aggregation (often referred to as LACP - Link Aggregation Control Protocol) on network devices to combine multiple physical links into one logical link.

Reference:

CompTIA Network+ study materials on network configuration and link aggregation.

Question: 56

Which of the following is used to estimate the average life span of a device?

A. RTO

B. RPO

C. MTBF

D. MTTR

Answer: C

Explanation:

Understanding MTBF:

Mean Time Between Failures (MTBF): A reliability metric that estimates the average time between successive failures of a device or system.

Calculation and Importance:

Calculation: MTBF is calculated as the total operational time divided by the number of failures during that period.

Usage: Used by manufacturers and engineers to predict the lifespan and reliability of a device, helping in maintenance planning and lifecycle management.

Comparison with Other Metrics:

RTO (Recovery Time Objective): The maximum acceptable time to restore a system after a failure.

RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time.

MTTR (Mean Time to Repair): The average time required to repair a device or system and return it to operational status.

Application:

MTBF is crucial for planning maintenance schedules, spare parts inventory, and improving the overall reliability of systems.

Reference:

CompTIA Network+ study materials on reliability and maintenance metrics.

Question: 57

A network administrator is implementing security zones for each department. Which of the following should the administrator use to accomplish this task?

A. ACLs

B. Port security

C. Content filtering

D. NAC

Answer: A

Explanation:

Understanding ACLs:

Access Control Lists (ACLs): A set of rules used to control network traffic and restrict access to network resources by filtering packets based on IP addresses, protocols, or ports.

Implementing Security Zones:

Defining Zones: ACLs can be used to create security zones by applying specific rules to different departments, ensuring that only authorized traffic is allowed between these zones.

Control Traffic: ACLs control inbound and outbound traffic at network boundaries, enforcing security policies and preventing unauthorized access.

Comparison with Other Options:

Port Security: Limits the number of devices that can connect to a switch port, preventing MAC address flooding attacks, but not used for defining security zones.

Content Filtering: Blocks or allows access to specific content based on predefined policies, typically used for web filtering rather than network segmentation.

NAC (Network Access Control): Controls access to the network based on the security posture of devices but does not define security zones.

Implementation Steps:

Define ACL rules based on the requirements of each department.

Apply these rules to the appropriate network interfaces or firewall policies to segment the network into security zones.

Reference:

CompTIA Network+ study materials on network security and access control methods.

Question: 58

A network engineer is now in charge of all SNMP management in the organization. The engineer must use a SNMP version that does not utilize plaintext dat

a. Which of the following is the minimum version of SNMP that supports this requirement?

A. v1

B. v2c

C. v2u

D. v3

Answer: D

Explanation:

SNMPv3 is the version of the Simple Network Management Protocol that introduces security enhancements, including message integrity, authentication, and encryption. Unlike previous versions (v1 and v2c), SNMPv3 supports encrypted communication, ensuring that data is not transmitted in plaintext. This provides confidentiality and protects against eavesdropping and unauthorized access. Reference: CompTIA Network+ study materials.

Question: 59

After running a Cat 8 cable using passthrough plugs, an electrician notices that connected cables are experiencing a lot of cross talk. Which of the following troubleshooting steps should the electrician take first?

A. Inspect the connectors for any wires that are touching or exposed.

B. Restore default settings on the connected devices.

C. Terminate the connections again.

D. Check for radio frequency interference in the area.

Answer: A

Explanation:

Cross talk can often be caused by improper termination of cables. The first step in troubleshooting should be to inspect the connectors for any wires that might be touching or exposed. Ensuring that all wires are correctly seated and that no conductors are exposed can help reduce or eliminate cross talk. This step should be taken before attempting to re-terminate the connections or check for other sources of interference.
Reference: CompTIA Network+ study materials.

Question: 60

A network architect needs to create a wireless field network to provide reliable service to public safety vehicles. Which of the following types of networks is the best solution?

A. Mesh

B. Ad hoc

C. Point-to-point

D. Infrastructure

Answer: A

Explanation:

A mesh network is the best solution for providing reliable wireless service to public safety vehicles. In a mesh network, each node (vehicle) can connect to multiple other nodes, providing multiple paths for data to travel. This enhances reliability and redundancy, ensuring continuous connectivity even if one or more nodes fail. Mesh networks are highly resilient and are well-suited for dynamic and mobile environments such as public safety operations.
Reference: CompTIA Network+ study materials.

Question: 61

A network administrator for a small office is adding a passive IDS to its network switch for the purpose of inspecting network traffic. Which of the following should the administrator use?

A. SNMP trap

B. Port mirroring

C. Syslog collection

D. API integration

Answer: B

Explanation:

Port mirroring, also known as SPAN (Switched Port Analyzer), is used to send a copy of network packets seen on one switch port (or an entire VLAN) to another port where the IDS is connected. This allows the IDS to passively inspect network traffic without interfering with the actual traffic flow. Port mirroring is an essential feature for implementing IDS in a network for traffic analysis and security monitoring.
Reference: CompTIA Network+ study materials.

Question: 62

Which of the following requires network devices to be managed using a different set of IP addresses?

A. Console

B. Split tunnel

C. Jump box

D. Out of band

Answer: D

Explanation:

Out-of-band (OOB) management refers to using a dedicated management network that is physically separate from the regular data network. This management network uses a different set of IP addresses to ensure that management traffic is isolated from user data traffic, providing a secure way

to manage network devices even if the main network is down or compromised.
Reference: CompTIA Network+ study materials.

Question: 63

Which of the following is most closely associated with a dedicated link to a cloud environment and may not include encryption?

A. Direct Connect

B. Internet gateway

C. Captive portal

D. VPN

Answer: A

Explanation:

Direct Connect refers to a dedicated network connection between an on-premises network and a cloud service provider (such as AWS Direct Connect). This link bypasses the public internet, providing a more reliable and higher-bandwidth connection. It may not inherently include encryption because it relies on the security measures of the dedicated physical connection itself. In contrast, other options like VPN typically involve encryption as they traverse the public internet.

Reference:

CompTIA Network+ full course material indicates that Direct Connect type services offer dedicated, private connections which might not include encryption due to the dedicated and secure nature of the link itself.

Question: 64

Which of the following protocols provides remote access utilizing port 22?

A. SSH

B. Telnet

C. TLS

D. RDP

Answer: A

Explanation:

SSH (Secure Shell) is a protocol used to securely connect to a remote server/system over a network. It operates on port 22 and provides encrypted communication, unlike Telnet which operates on port 23 and is not secure. TLS is used for securing HTTP connections (HTTPS) and operates on ports like 443, while RDP (Remote Desktop Protocol) is used for remote desktop connections and operates on port 3389.

Reference:

The CompTIA Network+ materials and tutorials cover SSH as the standard protocol for secure remote access, highlighting its operation on port 22.

Question: 65

Which of the following attacks utilizes a network packet that contains multiple network tags?

A. MAC flooding

B. VLAN hopping

C. DNS spoofing

D. ARP poisoning

Answer: B

Explanation:

VLAN hopping is an attack where an attacker crafts packets with multiple VLAN tags, allowing them to traverse VLAN boundaries improperly. This can result in gaining unauthorized access to network segments that are supposed to be isolated. The other options do not involve the use of multiple network tags. MAC flooding aims to overwhelm a switch's MAC address table, DNS spoofing involves forging DNS responses, and ARP poisoning involves sending fake ARP messages.

Reference:

According to the CompTIA Network+ course materials, VLAN hopping exploits the tagging mechanism in network packets to gain unauthorized access.

Question: 66

Which of the following describes the best reason for using BGP?

A. Preventing a loop within a LAN

B. Improving reconvergence times

C. Exchanging router updates with a different ISP

D. Sharing routes with a Layer 3 switch

Answer: C

Explanation:

BGP (Border Gateway Protocol) is used for routing data between different ISPs, making it essential for the functioning of the internet. Its primary use is for exchanging routing information between autonomous systems, especially different ISPs. Preventing loops within a LAN is handled by protocols like Spanning Tree Protocol (STP), while improving reconvergence times and sharing routes with a Layer 3 switch are functions of other protocols or internal mechanisms.

Reference:

The CompTIA Network+ training emphasizes BGP's role in the exchange of routing information across different ISPs and autonomous systems.

Question: 67

A company's marketing team created a new application and would like to create a DNS record for newapplication.comptia.org that always resolves to the same address as www.comptia.org. Which of the following records should the administrator use?

A. SOA

B. MX

C. CNAME

D. NS

Answer: C

Explanation:

A CNAME (Canonical Name) record is used in DNS to alias one domain name to another. This means that newapplication.comptia.org can be made to resolve to the same IP address as www.comptia.org by creating a CNAME record pointing newapplication.comptia.org to www.comptia.org. SOA (Start of Authority) is used for DNS zone information, MX (Mail Exchange) is for mail server records, and NS (Name Server) is for specifying authoritative DNS servers.

Reference:

The DNS section of the CompTIA Network+ materials describes the use of CNAME records for creating domain aliases.

Question: 68

An organization has a security requirement that all network connections can be traced back to a user. A network administrator needs to identify a solution to implement on the wireless network. Which of the following is the best solution?

A. Implementing enterprise authentication

B. Requiring theuse of PSKs

C. Configuring a captive portal for users

D. Enforcing wired equivalent protection

Answer: A

Explanation:

Enterprise authentication (such as WPA2-Enterprise) utilizes unique credentials for each user, typically integrating with an authentication server like RADIUS. This allows for tracking and logging user activity, ensuring that all connections can be traced back to individual users. PSKs (Pre-Shared Keys) are shared among users and do not provide individual accountability. Captive portals can identify users but are less secure than enterprise authentication, and Wired Equivalent Privacy (WEP) is outdated and not recommended for security purposes.

Reference:

CompTIA Network+ materials highlight enterprise authentication methods as the preferred solution for secure and accountable wireless network access.

Question: 69

A network administrator wants to configure a backup route in case the primary route fails. A dynamic routing protocol is not installed on the router. Which of the following routing features should the administrator choose to accomplish this task?

A. Neighbor adjacency

B. Link state flooding

C. Administrative distance

D. Hop count

Answer: C

Explanation:

Introduction to Administrative Distance

Administrative distance (AD) is a value used by routers to rank routes from different routing protocols. AD represents the trustworthiness of the source of the route. Lower AD values are more preferred. If a router has multiple routes to a destination from different sources, it will choose the route with the lowest AD.

Static Routes and Backup Routes

When a dynamic routing protocol is not used, static routes can be employed. Static routes are manually configured routes. To ensure a backup route, multiple static routes to the same destination can be configured with different AD values.

Configuring Static Routes with Administrative Distance

The primary route is configured with a lower AD value, making it the preferred route. The backup route is configured with a higher AD value. In the event of the primary route failure, the router will then use the backup route.

Example Configuration:

plaintext

Copy code

ip route 192.168.1.0 255.255.255.0 10.0.0.1 1

ip route 192.168.1.0 255.255.255.0 10.0.0.2 10

In the above example, 192.168.1.0/24 is the destination network.

10.0.0.1 is the next-hop IP address for the primary route with an AD of 1.

10.0.0.2 is the next-hop IP address for the backup route with an AD of 10.

Verification:

After configuration, use the show ip route command to verify that the primary route is in use and the backup route is listed as a candidate for use if the primary route fails.

Reference:

CompTIA Network+ guide explains the concept of administrative distance and its use in static routing configuration (see page Ref 9†Basic Configuration Commands).

Question: 70

Which of the following is a characteristic of the application layer?

A. It relies upon other layers for packet delivery.

OB. It checks independently for packet loss.

C. It encrypts data in transit.

D. It performs address translation.

Answer: A

Explanation:

Introduction to OSI Model:

The OSI model is a conceptual framework used to understand network interactions in seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

Application Layer:

The application layer (Layer 7) is the topmost layer in the OSI model. It provides network services directly to end-user applications. This layer facilitates communication between software applications and lower layers of the network protocol stack.

Reliance on Other Layers:

The application layer relies on the transport layer (Layer 4) for data transfer across the network. The transport layer ensures reliable data delivery through protocols like TCP and UDP.

The network layer (Layer 3) is responsible for routing packets to their destination.

The data link layer (Layer 2) handles node-to-node data transfer and error detection.

The physical layer (Layer 1) deals with the physical connection between devices.

Explanation of the Options:

A . It relies upon other layers for packet delivery: This is correct. The application layer depends on the lower layers (transport, network, data link, and physical) for the actual delivery of data packets.

B . It checks independently for packet loss: This is incorrect. Packet loss detection is typically handled by the transport layer (e.g., TCP).

C . It encrypts data in transit: This is incorrect. Encryption is typically handled by the presentation layer or at the transport layer (e.g., TLS/SSL).

D . It performs address translation: This is incorrect. Address translation is performed by the network layer (e.g., NAT).

Conclusion:

The application layer's primary role is to interface with the end-user applications and ensure that data is correctly presented to the user. It relies on the underlying layers to manage the actual data transport and delivery processes.

Reference:

CompTIA Network+ guide covering the OSI model and the specific roles and functions of each layer (see page Ref 10†How to Use Cisco Packet Tracer).

Question: 71

Which of the following most likely requires the use of subinterfaces?

A. A router with only one available LAN port

B. A firewall performing deep packet inspection

C. A hub utilizing jumbo frames

D. A switch using Spanning Tree Protocol

Answer: A

Explanation:

Introduction to Subinterfaces:

Subinterfaces are logical interfaces created on a single physical interface. They are used to enable a router to support multiple networks on a single physical interface.

Use Case for Subinterfaces:

Subinterfaces are commonly used in scenarios where VLANs are implemented. A router with a single physical LAN port can be configured with multiple subinterfaces, each associated with a different VLAN.

This setup allows the router to route traffic between different VLANs.

Example Configuration:

Consider a router with a single physical interface GigabitEthernet0/0 and two VLANs, 10 and 20.

```
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
```

The encapsulation dot1Q command specifies the VLAN ID.

Explanation of the Options:

A . A router with only one available LAN port: This is correct. Subinterfaces allow a single physical interface to manage multiple networks, making it essential for routers with limited physical interfaces.

B . A firewall performing deep packet inspection: Firewalls can use subinterfaces, but it is not a requirement for deep packet inspection.

C . A hub utilizing jumbo frames: Hubs do not use subinterfaces as they operate at Layer 1 and do not manage IP addressing.

D . A switch using Spanning Tree Protocol: STP is a protocol for preventing loops in a network and does not require subinterfaces.

Conclusion:

Subinterfaces provide a practical solution for routing between multiple VLANs on a router with limited physical interfaces. They allow network administrators to optimize the use of available hardware resources efficiently.

Reference:

CompTIA Network+ guide detailing VLAN configurations and the use of subinterfaces (see page Ref 9†Basic Configuration Commands).

Question: 72

Which of the following steps of the troubleshooting methodology would most likely include checking through each level of the OSI model after the problem has been identified?

A. Establish a theory.

B. Implement the solution.

C. Create a plan of action.

D. Verify functionality.

Answer: D

Explanation:

Introduction to Troubleshooting Methodology:

Network troubleshooting involves a systematic approach to identifying and resolving network issues. The CompTIA Network+ certification emphasizes a structured troubleshooting methodology.

Troubleshooting Steps:

Identify the problem: Gather information, identify symptoms, and question users.

Establish a theory of probable cause: Consider possible reasons for the issue.

Test the theory to determine cause: Validate the theory with tests.

Establish a plan of action to resolve the problem and implement the solution: Create and execute a resolution plan.

Verify functionality and implement preventive measures: Ensure the solution works and prevent recurrence.

Verifying Functionality:

After implementing a solution, verifying functionality ensures that the problem is fully resolved. This involves testing the network to confirm that it operates correctly.

Checking through each level of the OSI model helps to ensure that all potential issues at different layers (physical, data link, network, transport, session, presentation, and application) are addressed.

Explanation of the Options:

A . Establish a theory: This step involves hypothesizing possible causes, not verifying functionality.

B . Implement the solution: This step involves executing the resolution plan.

C . Create a plan of action: This step involves planning the resolution, not verification.

D . Verify functionality: This step involves comprehensive checks, including OSI model layers, to ensure the issue is fully resolved.

Conclusion:

Verifying functionality is a critical step in the troubleshooting process, ensuring that the network operates correctly after a solution is implemented. It involves thorough testing across all OSI model layers.

Reference:

CompTIA Network+ guide explaining the troubleshooting methodology and the importance of verifying functionality (see page Ref 9†Basic Configuration Commands).

Question: 73

A network administrator wants to implement security zones in the corporate network to control access to only individuals inside of the corporation. Which of the following security zones is the best solution?

A. Extranet

B. Trusted

C. VPN

D. Public

Answer: B

Explanation:

Introduction to Security Zones:

Security zones are logical segments within a network designed to enforce security policies and control access. They help in segregating and securing different parts of the network.

Types of Security Zones:

Trusted Zone: This is the most secure zone, typically used for internal corporate networks where only trusted users have access.

Extranet: This zone allows controlled access to external partners, vendors, or customers.

VPN (Virtual Private Network): While VPNs are used to create secure connections over the internet, they are not a security zone themselves.

Public Zone: This zone is the least secure and is typically used for public-facing services accessible by anyone.

Trusted Zone Implementation:

The trusted zone is configured to include internal corporate users and resources. Access controls, firewalls, and other security measures ensure that only authorized personnel can access this zone.

Internal network segments, such as the finance department, HR, and other critical functions, are usually placed in the trusted zone.

Example Configuration:

Firewall Rules: Set up rules to allow traffic only from internal IP addresses.

Access Control Lists (ACLs): Implement ACLs on routers and switches to restrict access based on IP addresses and other criteria.

Segmentation: Use VLANs and subnetting to segment and isolate the trusted zone from other zones.

Explanation of the Options:

A . Extranet: Suitable for external partners, not for internal-only access.

B . Trusted: The correct answer, as it provides controlled access to internal corporate users.

C . VPN: A method for secure remote access, not a security zone itself.

D . Public: Suitable for public access, not for internal corporate users.

Conclusion:

Implementing a trusted zone is the best solution for controlling access within a corporate network. It ensures that only trusted internal users can access sensitive resources, enhancing network security.

Reference:

CompTIA Network+ guide detailing security zones and their implementation in a corporate network (see page Ref 9†Basic Configuration Commands).

Question: 74

Which of the following disaster recovery concepts is calculated by dividing the total hours of operation by the total number of units?

A. MTTR

B. MTBF

C. RPO

D. RTO

Answer: B

Explanation:

Introduction to Disaster Recovery Concepts:

Disaster recovery involves strategies and measures to ensure business continuity and data recovery in the event of a disaster.

Mean Time Between Failures (MTBF):

MTBF is a reliability metric used to predict the time between failures of a system during operation. It

is calculated by dividing the total operational time by the number of failures.

Formula: MTBF=Total Operational TimeNumber of Failures\text{MTBF} = \frac{\text{Total Operational Time}}{\text{Number of Failures}}MTBF=Number of FailuresTotal Operational Time

This metric helps in understanding the reliability and expected lifespan of systems and components.

Example Calculation:

If a server operates for 1000 hours and experiences 2 failures, the MTBF is:
MTBF=1000 hours2=500 hours\text{MTBF} = \frac{1000 \text{ hours}}{2} = 500 \text{ hours}MTBF=21000 hours=500 hours

Explanation of the Options:

A . MTTR (Mean Time to Repair): The average time required to repair a system after a failure.

B . MTBF (Mean Time Between Failures): The correct answer, representing the average time between failures.

C . RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time.

D . RTO (Recovery Time Objective): The target time set for the recovery of IT and business activities after a disaster.

Conclusion:

MTBF is a crucial metric in disaster recovery and system reliability, helping organizations plan maintenance and predict system performance.

Reference:

CompTIA Network+ guide explaining MTBF, MTTR, RPO, and RTO concepts and their calculations (see page Ref 10†How to Use Cisco Packet Tracer).

Question: 75

SIMULATION

A network administrator has been tasked with configuring a network for a new corporate office. The office consists of two buildings, separated by 50 feet with no physical connectivity. The configuration must meet the following requirements:

. Devices in both buildings should be

able to access the Internet.

. Security insists that all Internet traffic

be inspected before entering the

network.

. Desktops should not see traffic

destined for other devices.

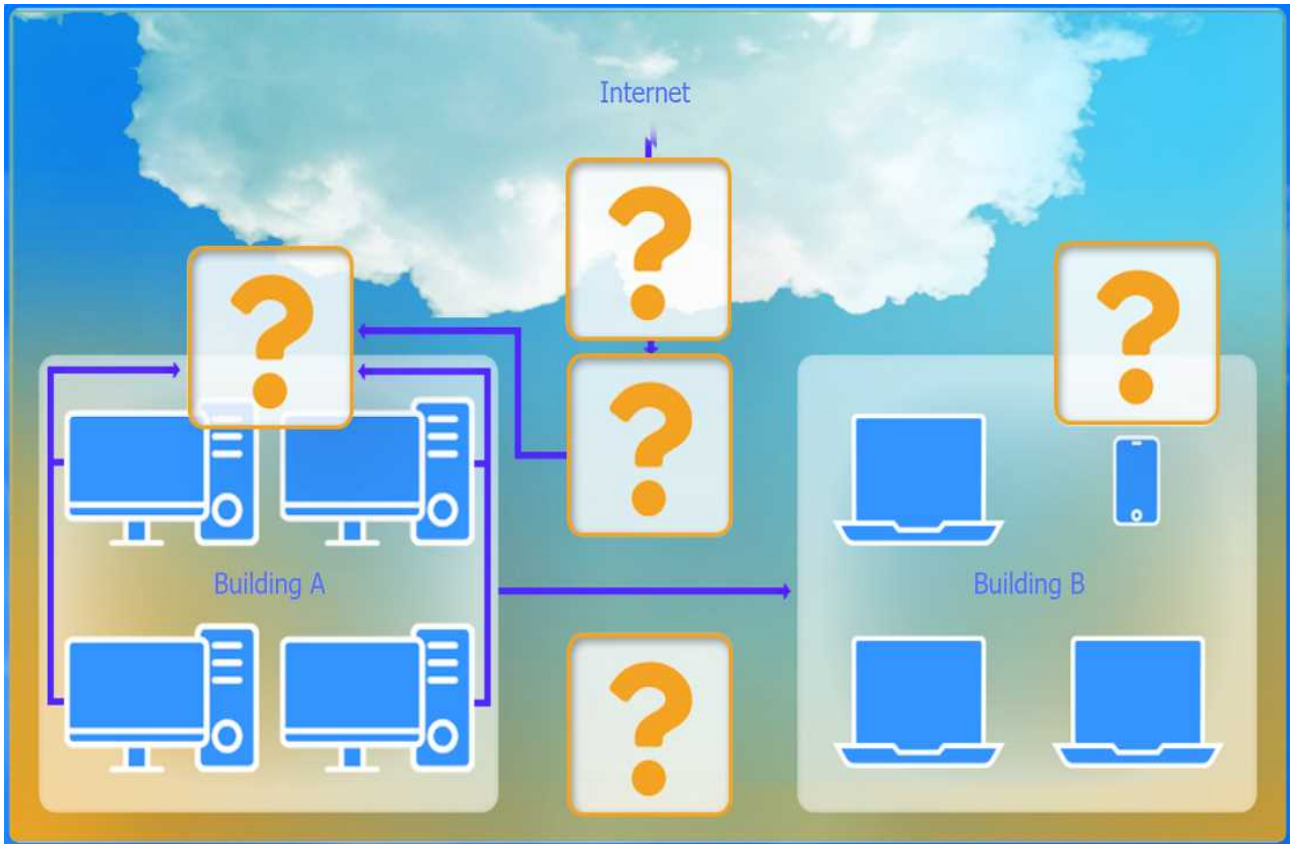
INSTRUCTIONS

Select the appropriate network device for each location. If applicable, click on the magnifying glass next to any device which may require configuration updates and make any necessary changes.

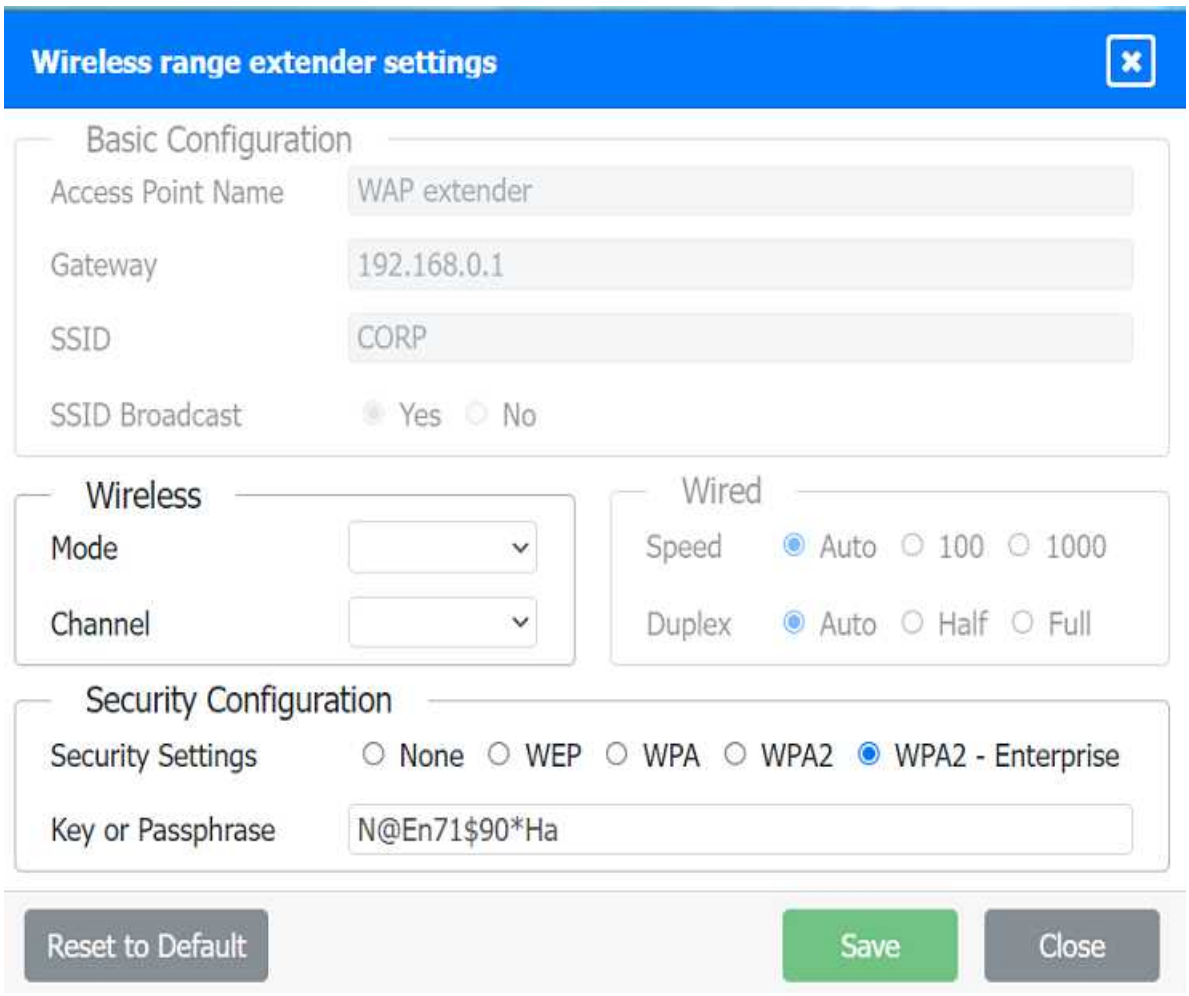
Not all devices will be used, but all locations should be filled.

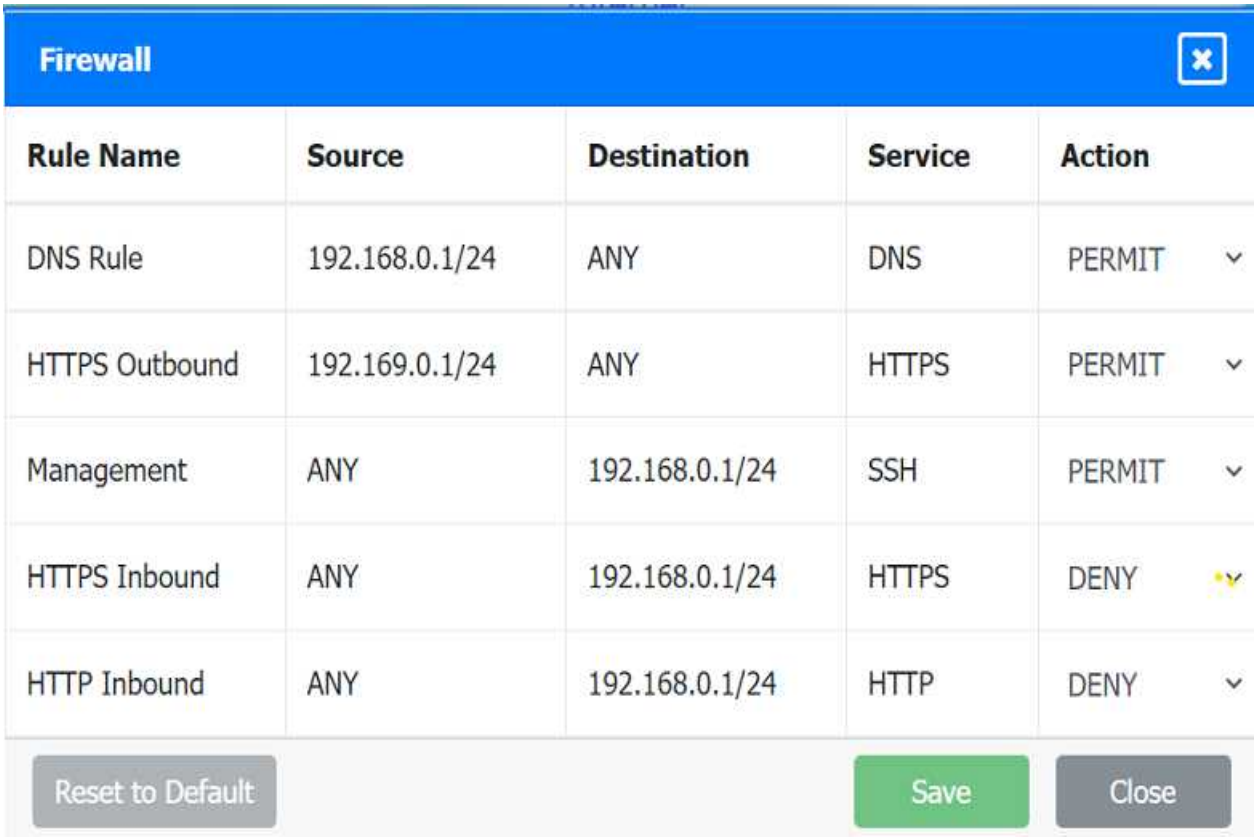
If at any time you would like to bring back the initial state of the simulation, please

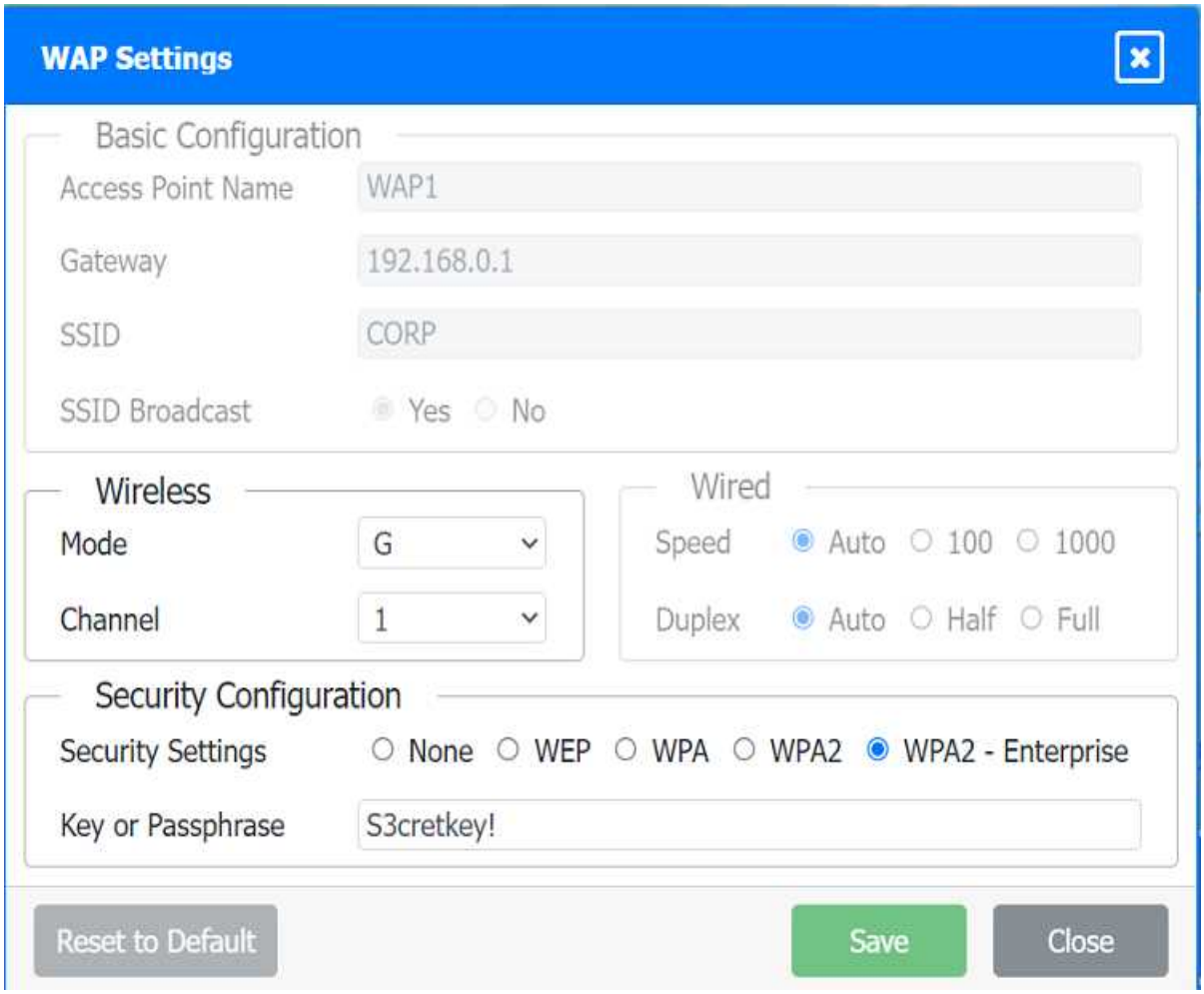
click the Reset All button.



- Hub
- Switch
- WAP
- Firewall
- Router
- Wireless range extender


Wireless range extender settings
Basic Configuration
Access Point Name
WAP extender
Gateway
192.168.0.1
SSID
CORP
SSID Broadcast
Yes
No
Wireless
Mode
Channel
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase
N@En71$90*Ha
Reset to Default
Save
Close


Firewall
Rule Name
Source
Destination
Service
Action
DNS Rule
192.168.0.1/24
ANY
DNS
PERMIT
HTTPS Outbound
192.169.0.1/24
ANY
HTTPS
PERMIT
Management
ANY
192.168.0.1/24
SSH
PERMIT
HTTPS Inbound
ANY
192.168.0.1/24
HTTPS
DENY
HTTP Inbound
ANY
192.168.0.1/24
HTTP
DENY
Reset to Default
Save
Close



Answer: See the step by step complete solution below.

Explanation:

Devices in both buildings should be able to access the Internet.

Security insists that all Internet traffic be inspected before entering the network.

Desktops should not see traffic destined for other devices.

Here is the corrected layout with explanation:

Building A:

Switch: Correctly placed to connect all desktops.

Firewall: Correctly placed to inspect all incoming and outgoing traffic.

Building B:

Switch: Not needed. Instead, place a Wireless Access Point (WAP) to provide wireless connectivity for laptops and mobile devices.

Between Buildings:

Wireless Range Extender: Correctly placed to provide connectivity between the buildings wirelessly.

Connection to the Internet:

Router: Correctly placed to connect to the Internet and route traffic between the buildings and the Internet.

Firewall: The firewall should be placed between the router and the internal network to inspect all traffic before it enters the network.

Corrected Setup:

Top-left (Building A): Switch

Bottom-left (Building A): Firewall (inspect traffic before it enters the network)

Top-middle (Internet connection): Router

Bottom-middle (between buildings): Wireless Range Extender

Top-right (Building B): Wireless Access Point (WAP)

In this corrected setup, the WAP in Building B will connect wirelessly to the Wireless Range Extender, which is connected to the Router. The Router is connected to the Firewall to ensure all traffic is inspected before it enters the network.

Configuration for Wireless Range Extender:

SSID: CORP

Security Settings: WPA2 or WPA2 - Enterprise

Key or Passphrase: [Enter a strong passphrase]

Mode: [Set based on your network plan]

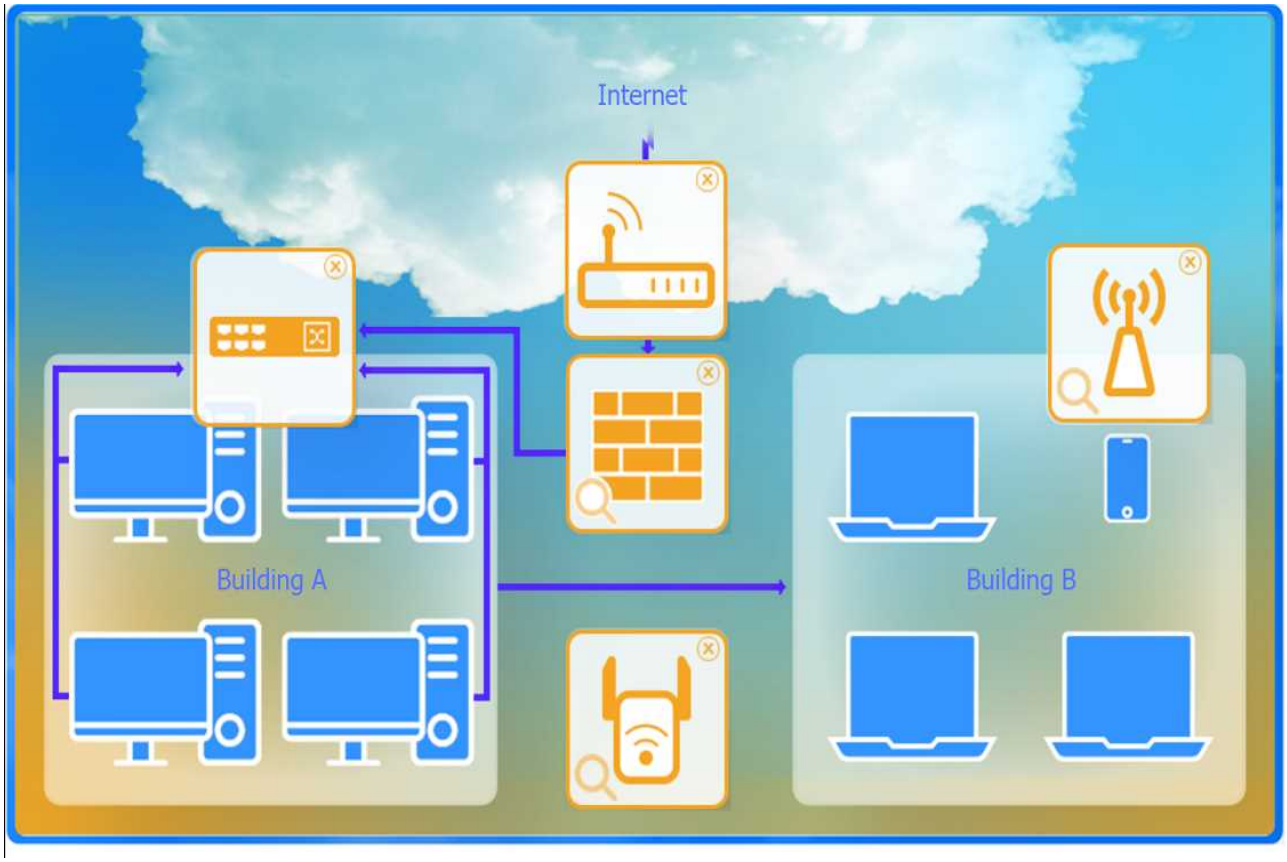
Channel: [Set based on your network plan]

Speed: Auto

Duplex: Auto

With these settings, both buildings will have secure access to the Internet, and all traffic will be

inspected by the firewall before entering the network. Desktops and other devices will not see traffic intended for others, maintaining the required security and privacy.



To configure the wireless range extender for security, follow these steps:

SSID (Service Set Identifier):

Ensure the SSID is set to "CORP" as shown in the exhibit.

Security Settings:

WPA2 or WPA2 - Enterprise: Choose one of these options for stronger security. WPA2-Enterprise provides more robust security with centralized authentication, which is ideal for a corporate environment.

Key or Passphrase:

If you select WPA2, enter a strong passphrase in the "Key or Passphrase" field.

If you select WPA2 - Enterprise, you will need to configure additional settings for authentication servers, such as RADIUS, which is not shown in the exhibit.

Wireless Mode and Channel:

Set the appropriate mode and channel based on your network design and the environment to avoid

interference. These settings are not specified in the exhibit, so set them according to your network plan.

Wired Speed and Duplex:

Set the speed to "Auto" unless you have specific requirements for 100 or 1000 Mbps.

Set the duplex to "Auto" unless you need to specify half or full duplex based on your network equipment.

Save Configuration:

After making the necessary changes, click the "Save" button to apply the settings.

Here is how the configuration should look after adjustments:

SSID: CORP

Security Settings: WPA2 or WPA2 - Enterprise

Key or Passphrase: [Enter a strong passphrase]

Mode: [Set based on your network plan]

Channel: [Set based on your network plan]

Speed: Auto

Duplex: Auto

Once these settings are configured, your wireless range extender will provide secure connectivity for devices in both buildings.

Firewall setting to to ensure complete compliance with the requirements and best security practices, consider the following adjustments and additions:

DNS Rule: This rule allows DNS traffic from the internal network to any destination, which is fine.

HTTPS Outbound: This rule allows HTTPS traffic from the internal network (assuming 192.169.0.1/24 is a typo and should be 192.168.0.1/24) to any destination, which is also good for secure web browsing.

Management: This rule allows SSH access to the firewall for management purposes, which is necessary for administrative tasks.

HTTPS Inbound: This rule denies inbound HTTPS traffic to the internal network, which is good unless you have a web server that needs to be accessible from the internet.

HTTP Inbound: This rule denies inbound HTTP traffic to the internal network, which is correct for

security purposes.

Suggested Additional Settings:

Permit General Outbound Traffic: Allow general outbound traffic for web access, email, etc.

Block All Other Traffic: Ensure that all other traffic is blocked to prevent unauthorized access.

Firewall Configuration Adjustments:

Correct the Network Typo:

Ensure that the subnet 192.169.0.1/24 is corrected to 192.168.0.1/24.

Permit General Outbound Traffic:

Rule Name: General Outbound

Source: 192.168.0.1/24

Destination: ANY

Service: ANY

Action: PERMIT

Deny All Other Traffic:

Rule Name: Block All

Source: ANY

Destination: ANY

Service: ANY

Action: DENY

Here is how your updated firewall settings should look:

Rule Name	Source	Destination	Service	Action
DNS Rule	192.168.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	DENY
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

General Outbound	192.168.0.1/24	ANY	ANY	PERMIT
Block All	ANY	ANY	ANY	DENY

These settings ensure that:

Internal devices can access DNS and HTTPS services externally.

Management access via SSH is permitted.

Inbound HTTP and HTTPS traffic is denied unless otherwise specified.

General outbound traffic is allowed.

All other traffic is blocked by default, ensuring a secure environment.

Make sure to save the settings after making these adjustments.

Question: 76

SIMULATION

A network technician replaced an access layer 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.

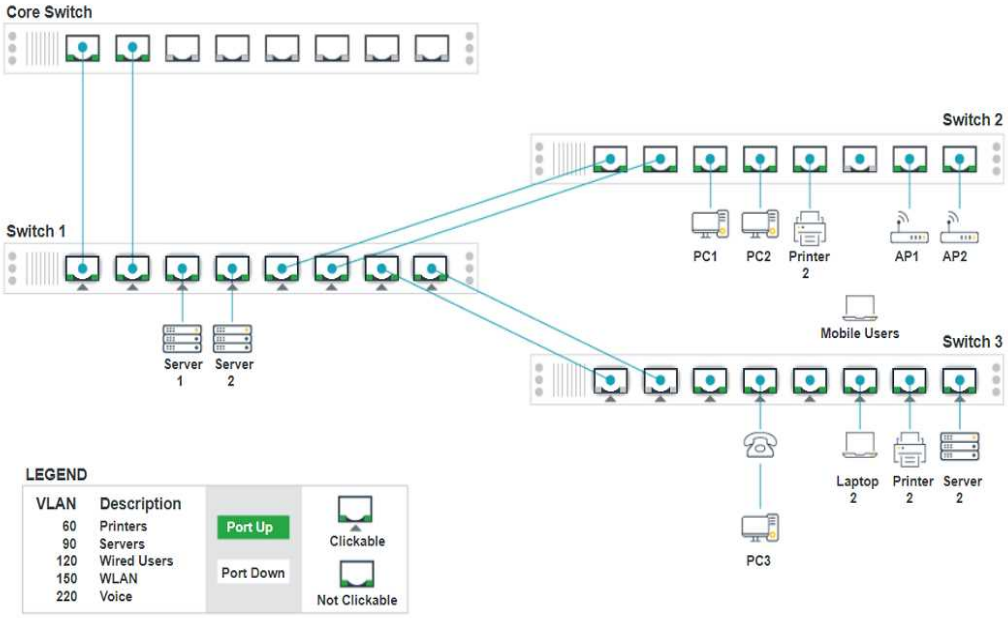
· Disable all unused switchports.

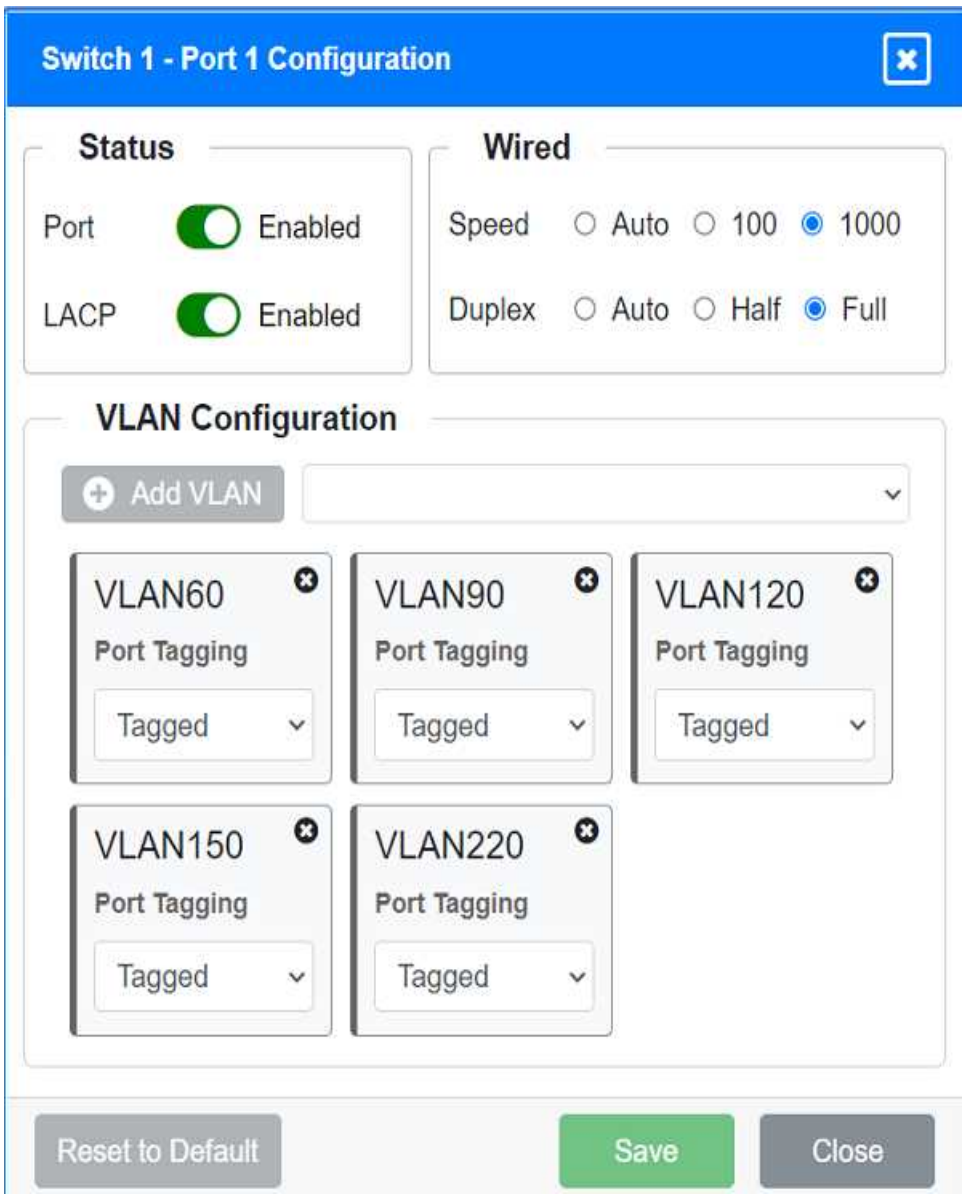
. Require fault-tolerant connections

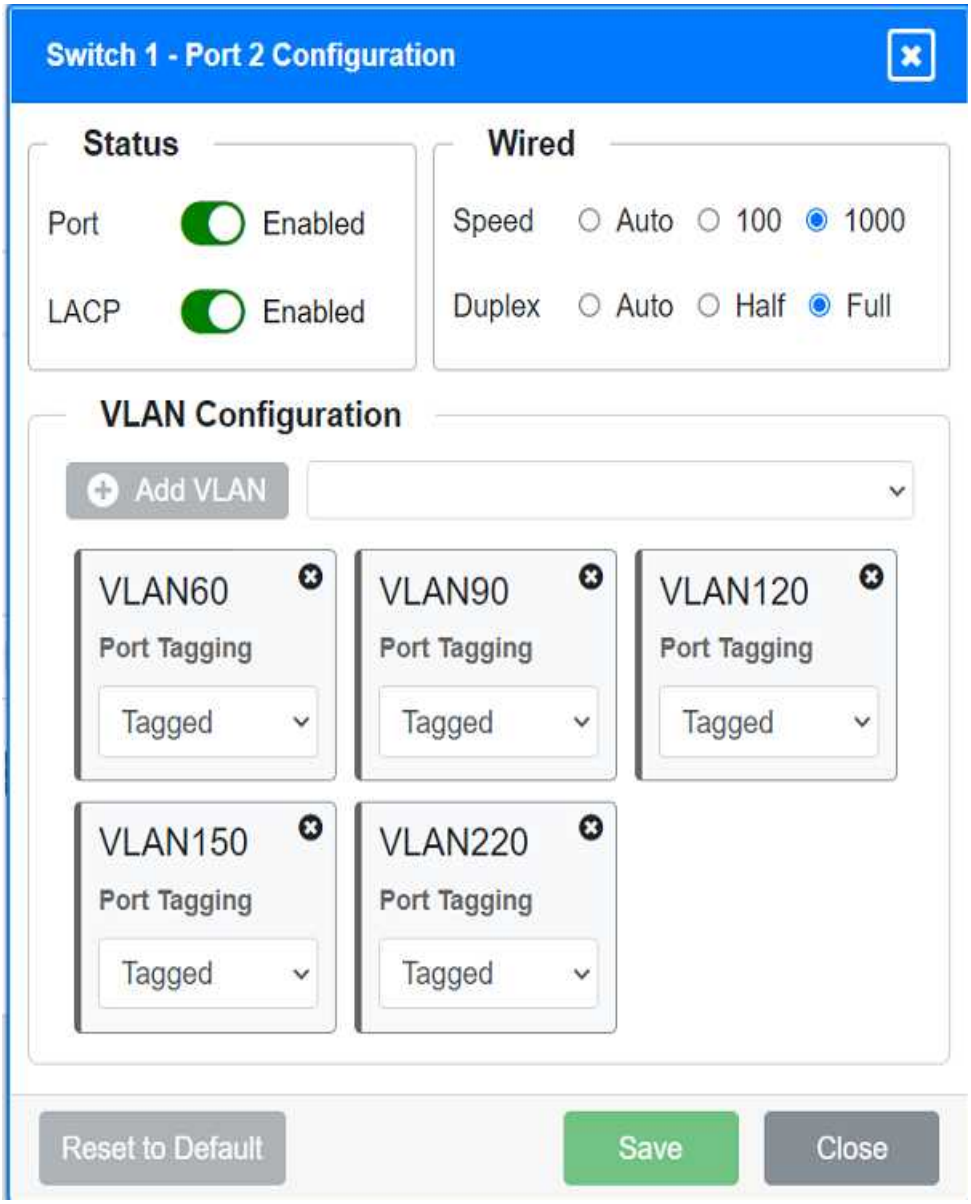
between the switches.

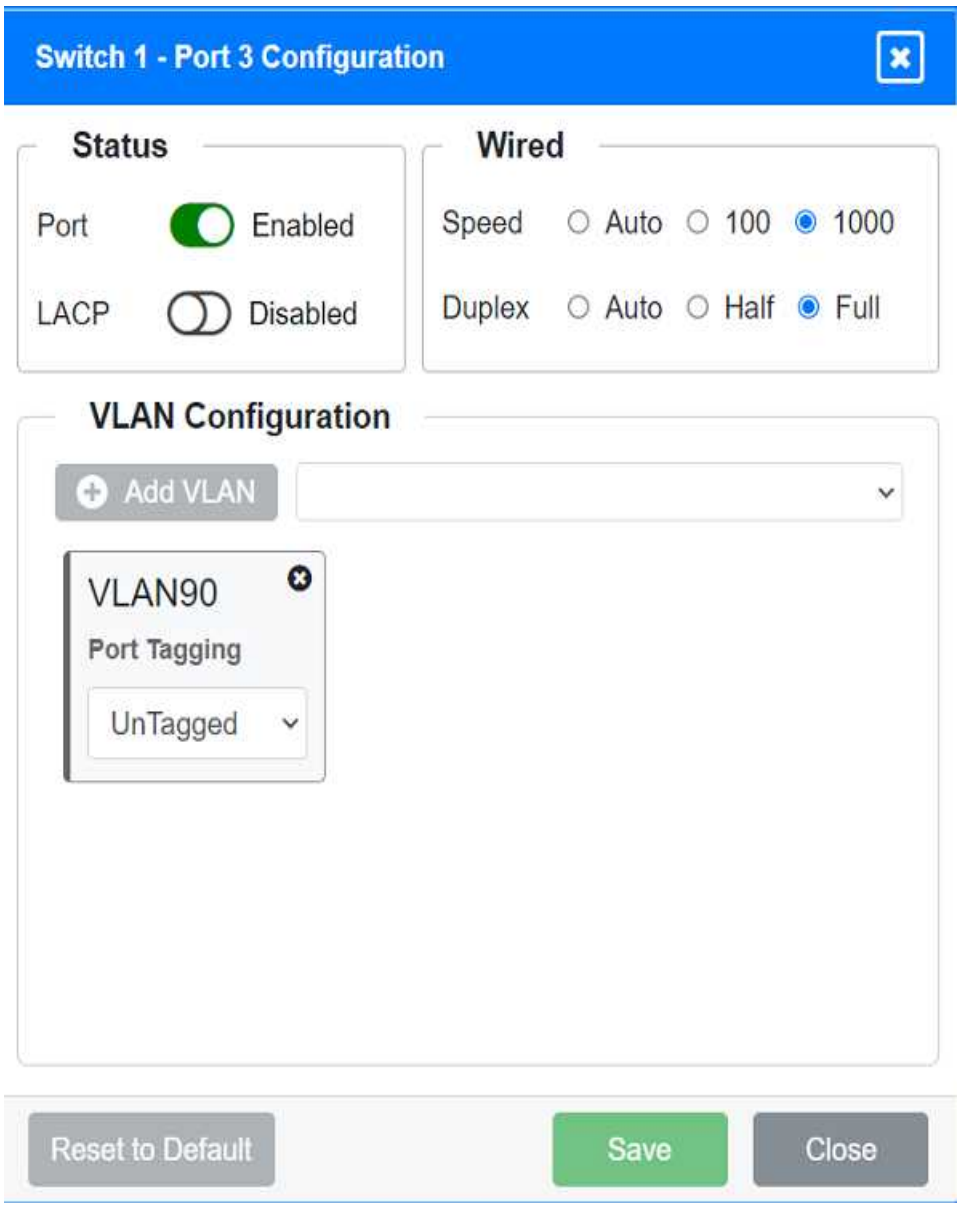
. Only make necessary changes to

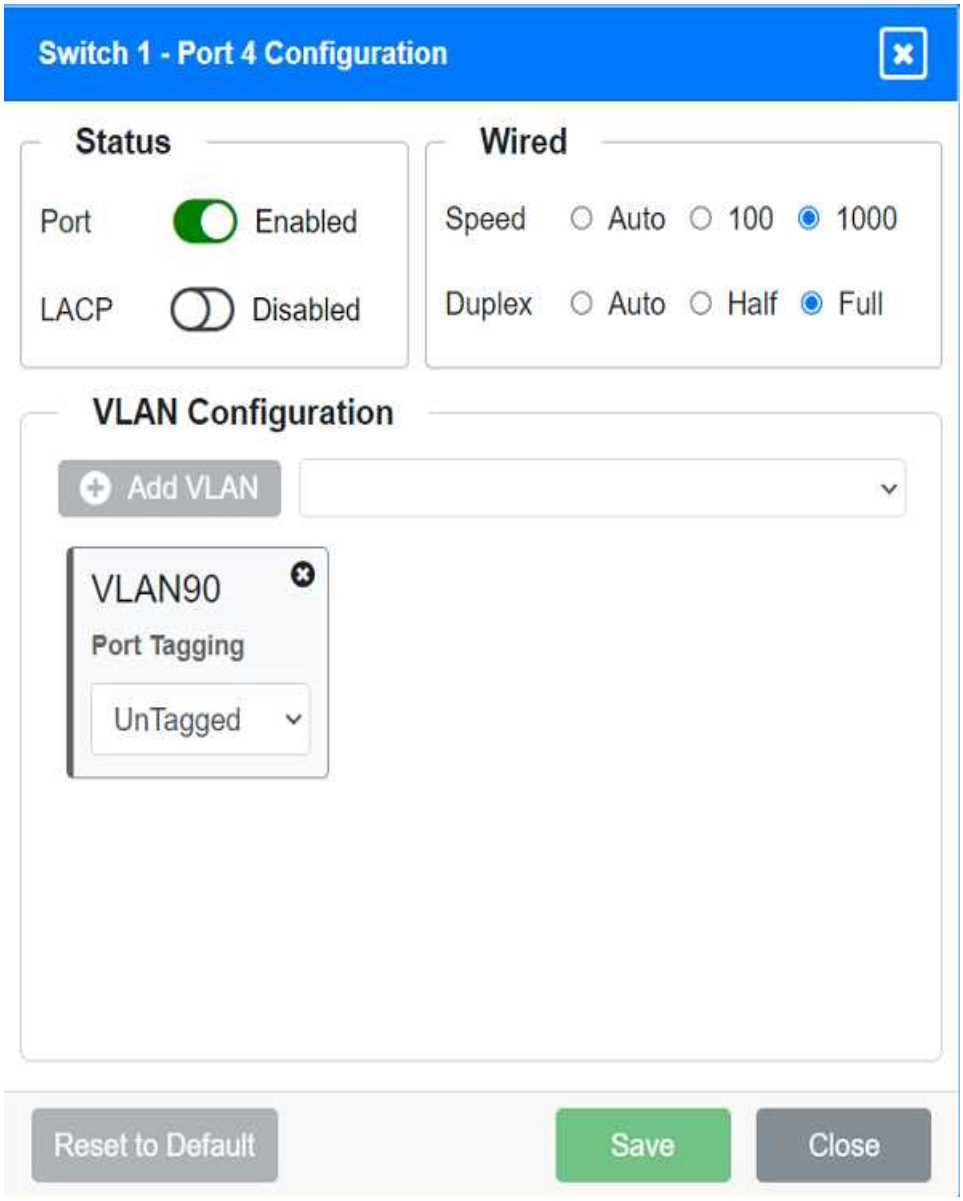
complete the above requirements.

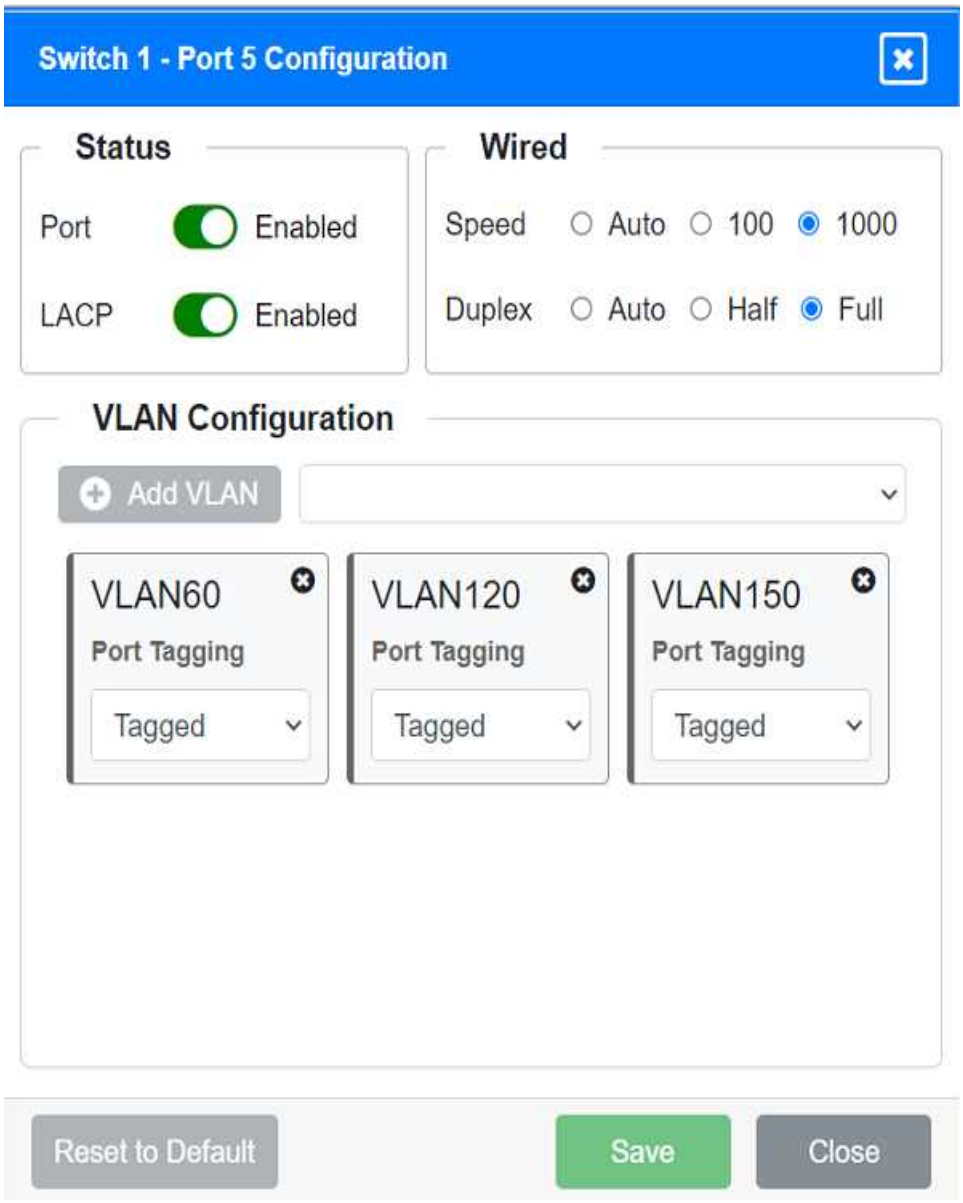

Core Switch
Switch 1
Switch 2
Switch 3
PC1
PC2
Printer 2
AP1
AP2
Mobile Users
Server 1
Server 2
Laptop 2
Printer 2
Server 2
PC3
LEGEND
VLAN
Description
60 Printers
90 Servers
120 Wired Users
150 WLAN
220 Voice
Port Up
Port Down
Clickable
Not Clickable

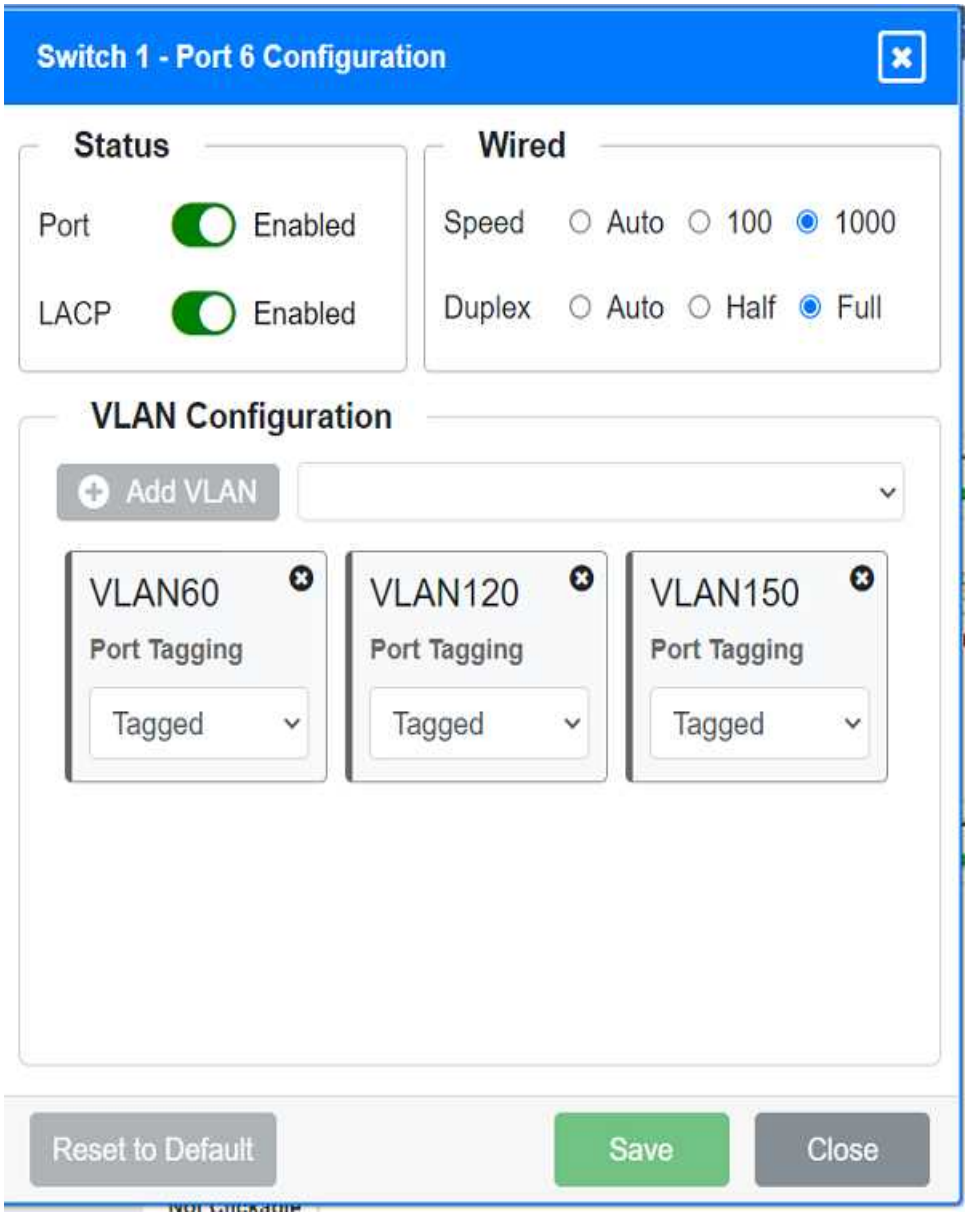

Switch 1 - Port 1 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save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

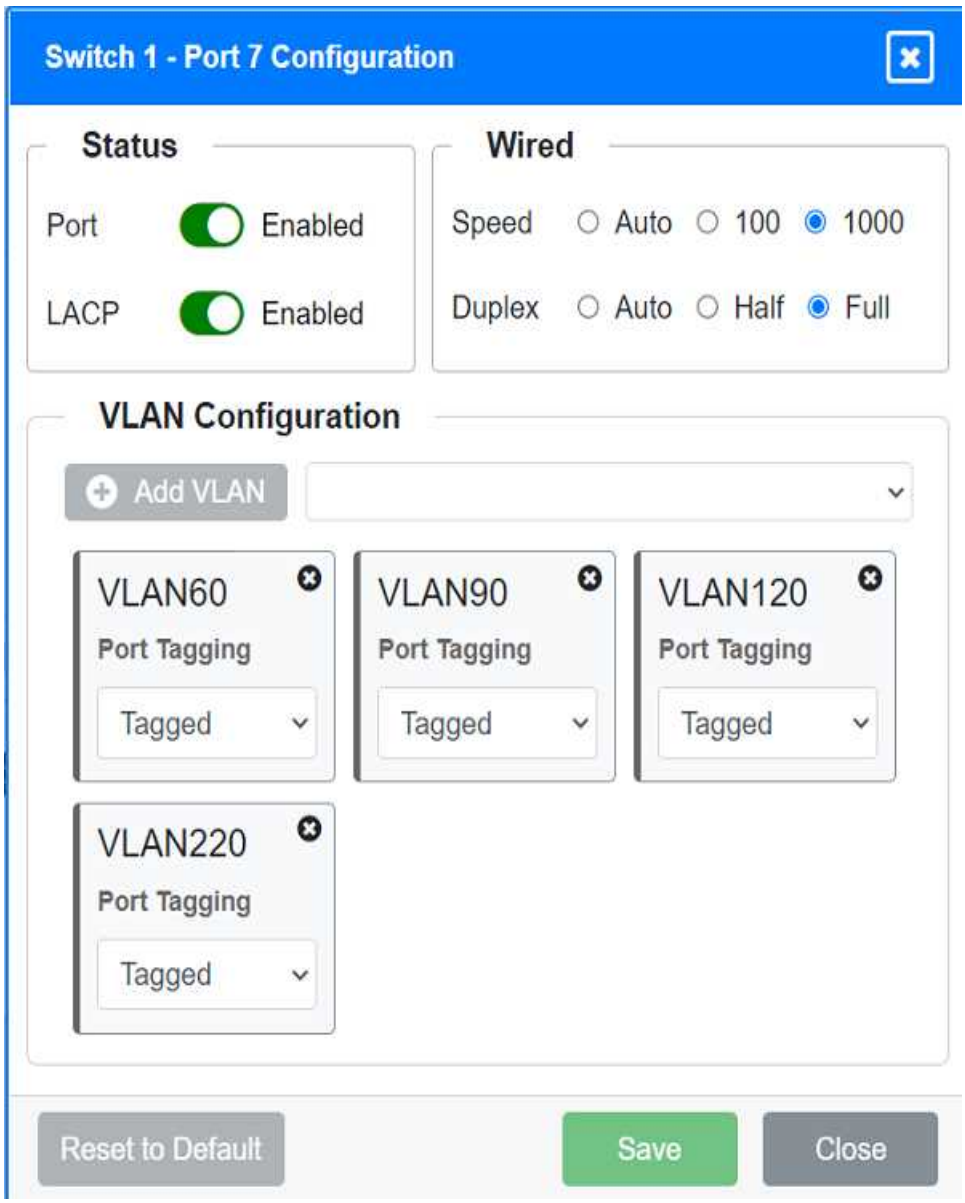

Switch 1 - Port 2 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save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

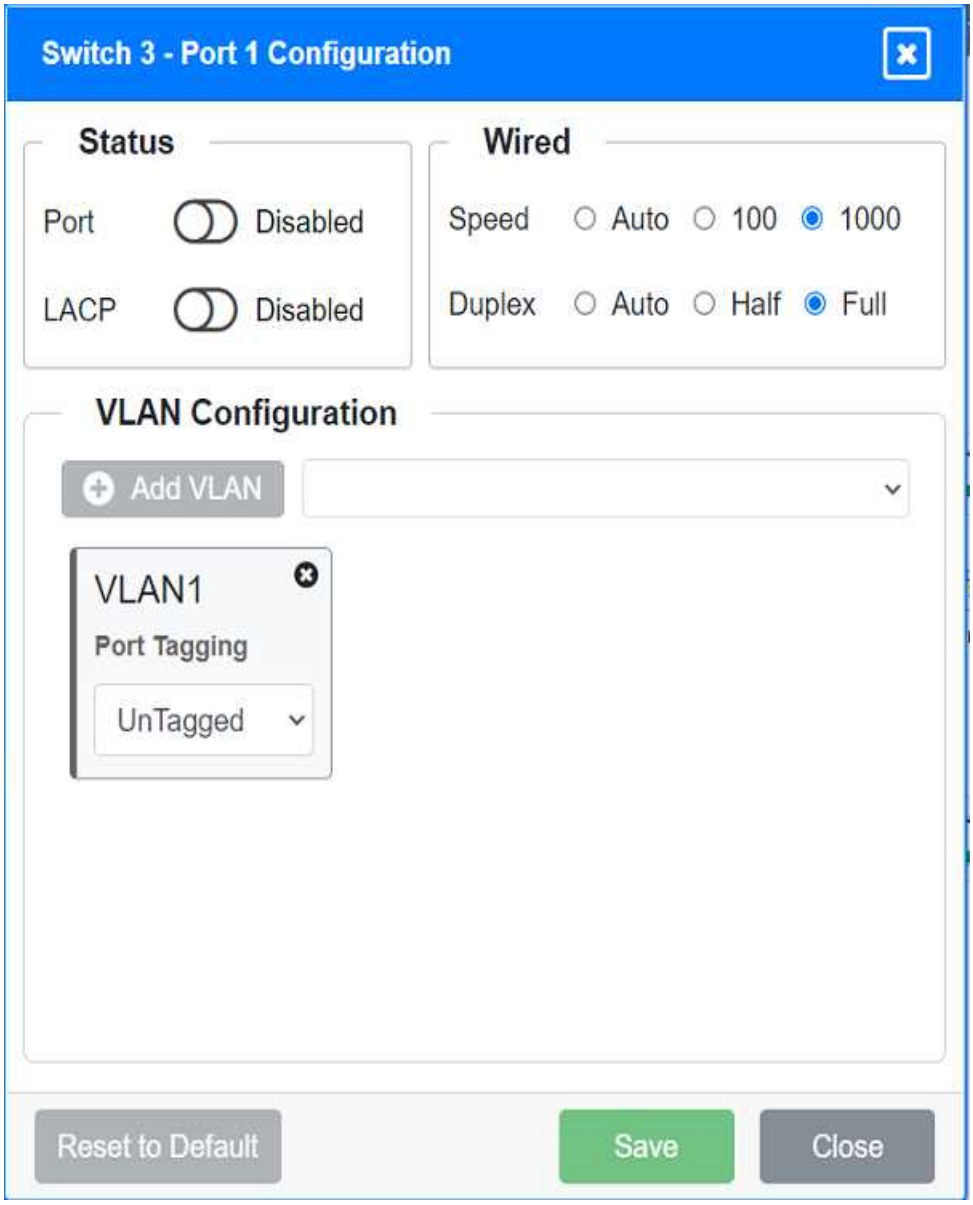

Switch 1 - Port 3 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN90
Port Tagging
UnTagged
Reset to Default
Save
Close

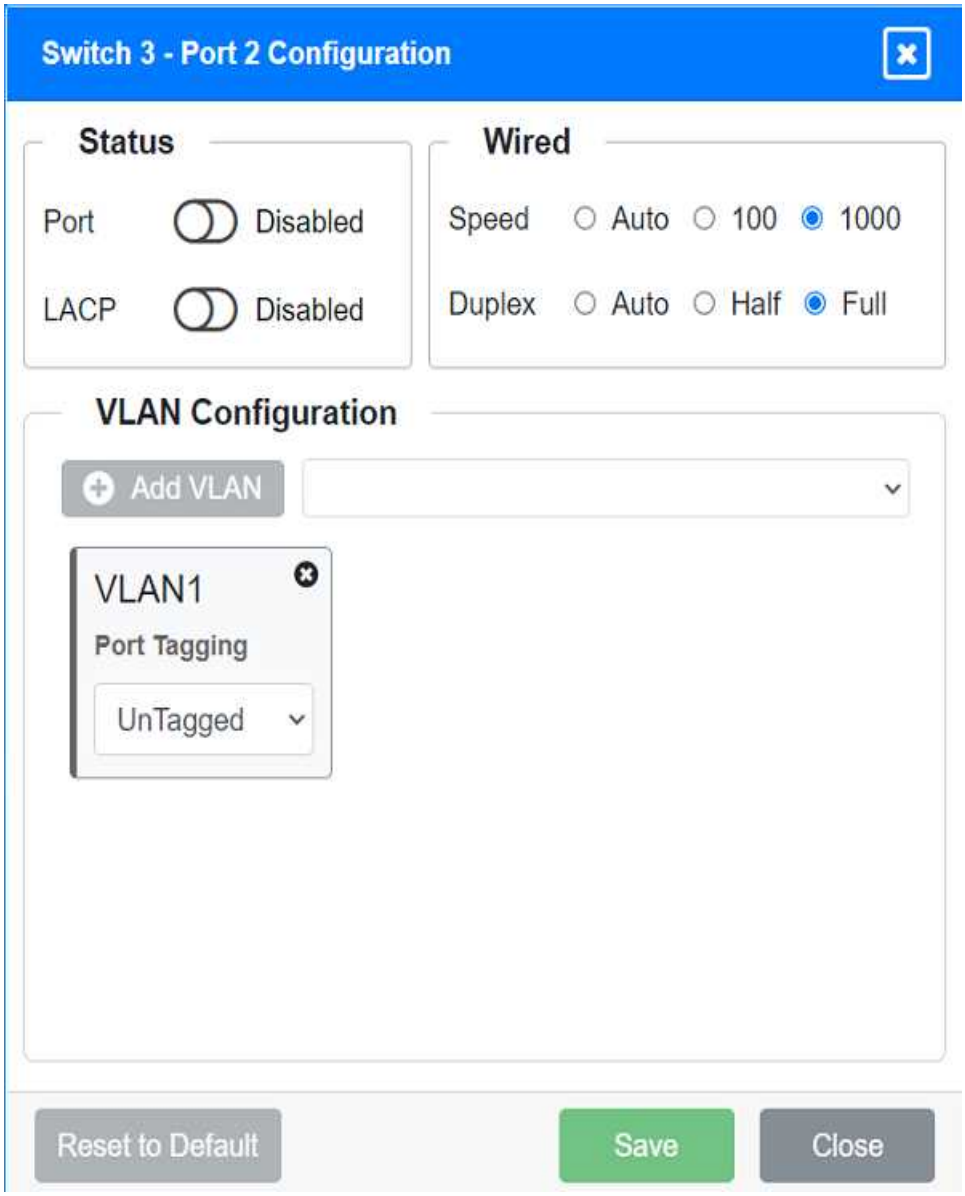

Switch 1 - Port 4 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN90
Port Tagging
UnTagged
Reset to Default
Save
Close

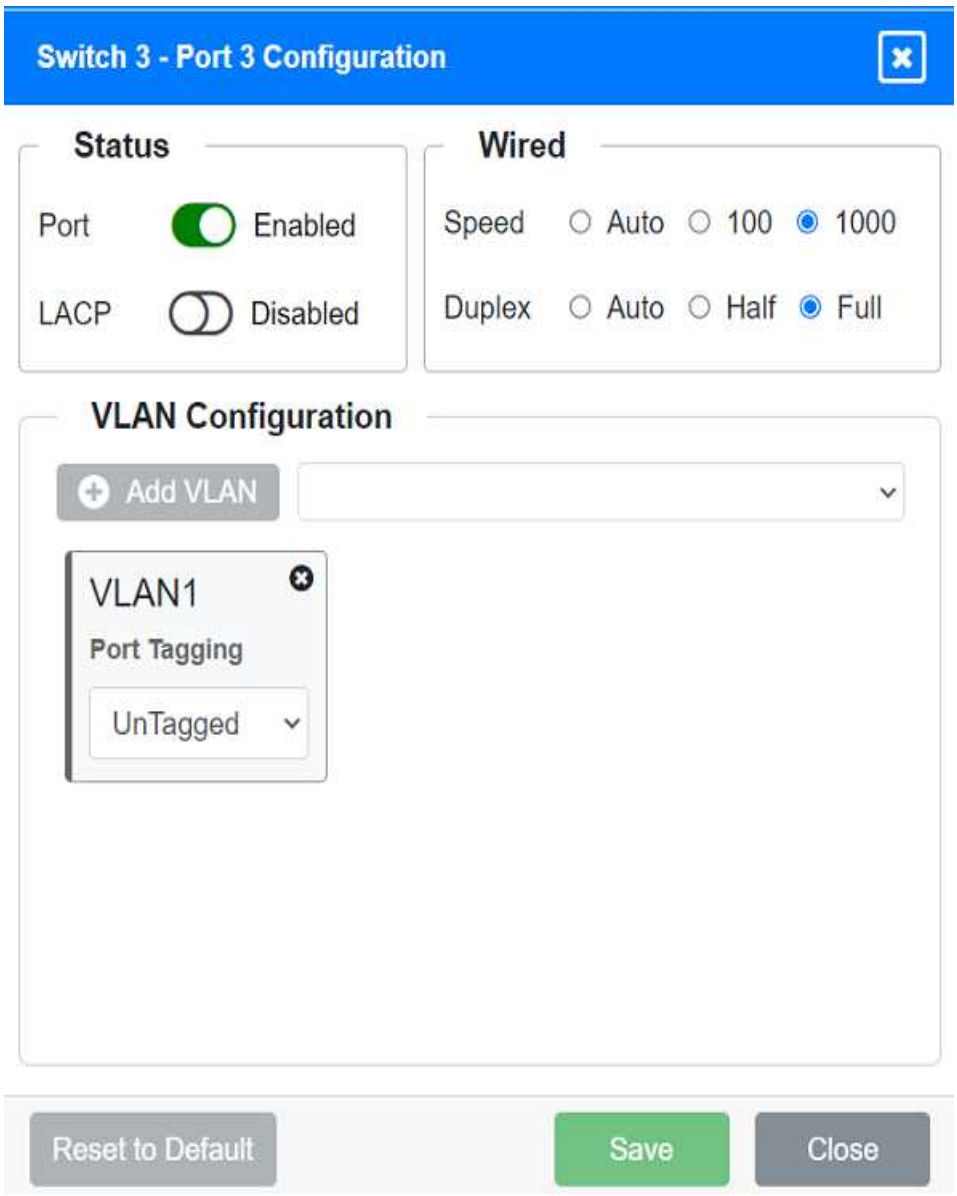

Switch 1 - Port 5 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
Reset to Default
Save
Close

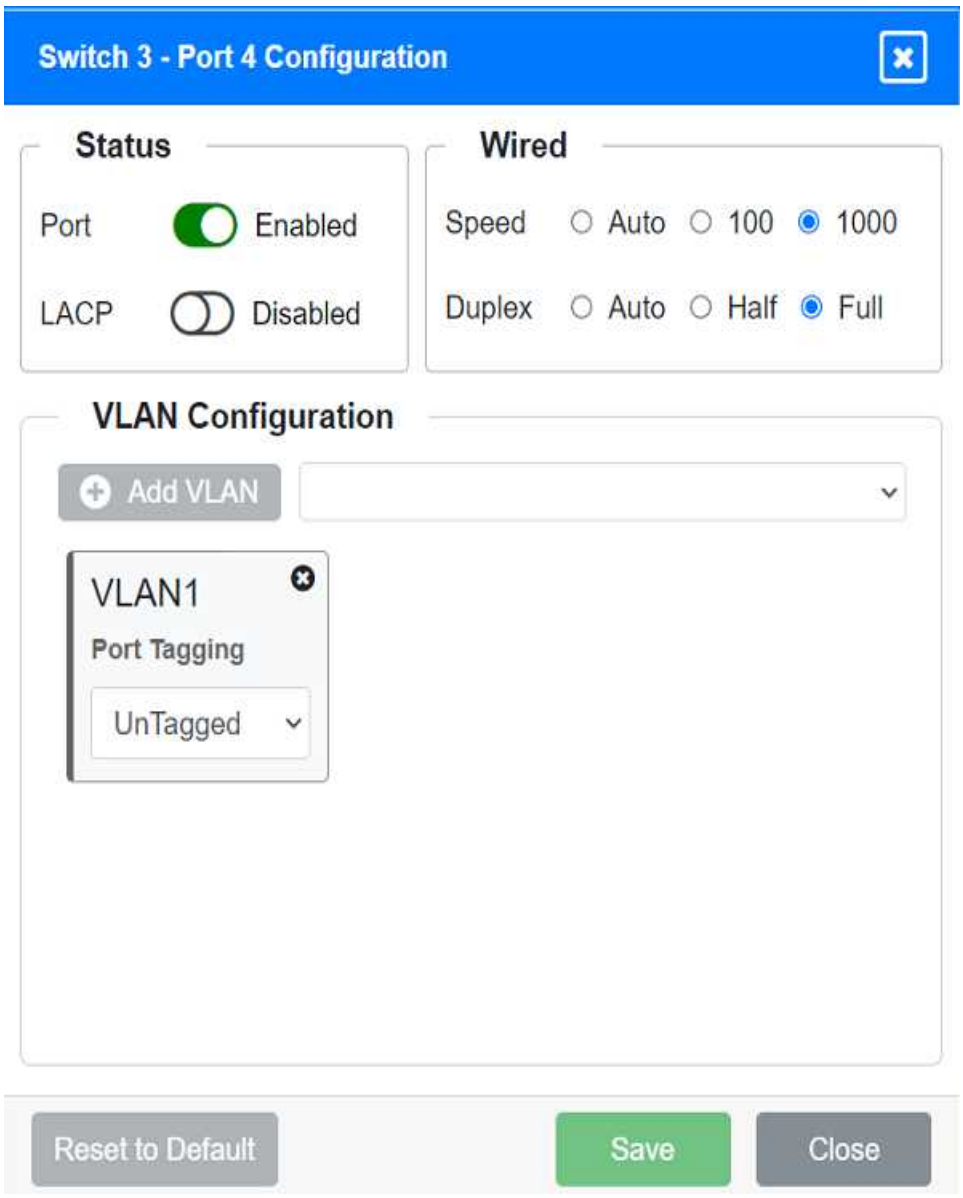

Switch 1 - Port 6 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN150
Port Tagging
Tagged
Reset to Default
Save
Close

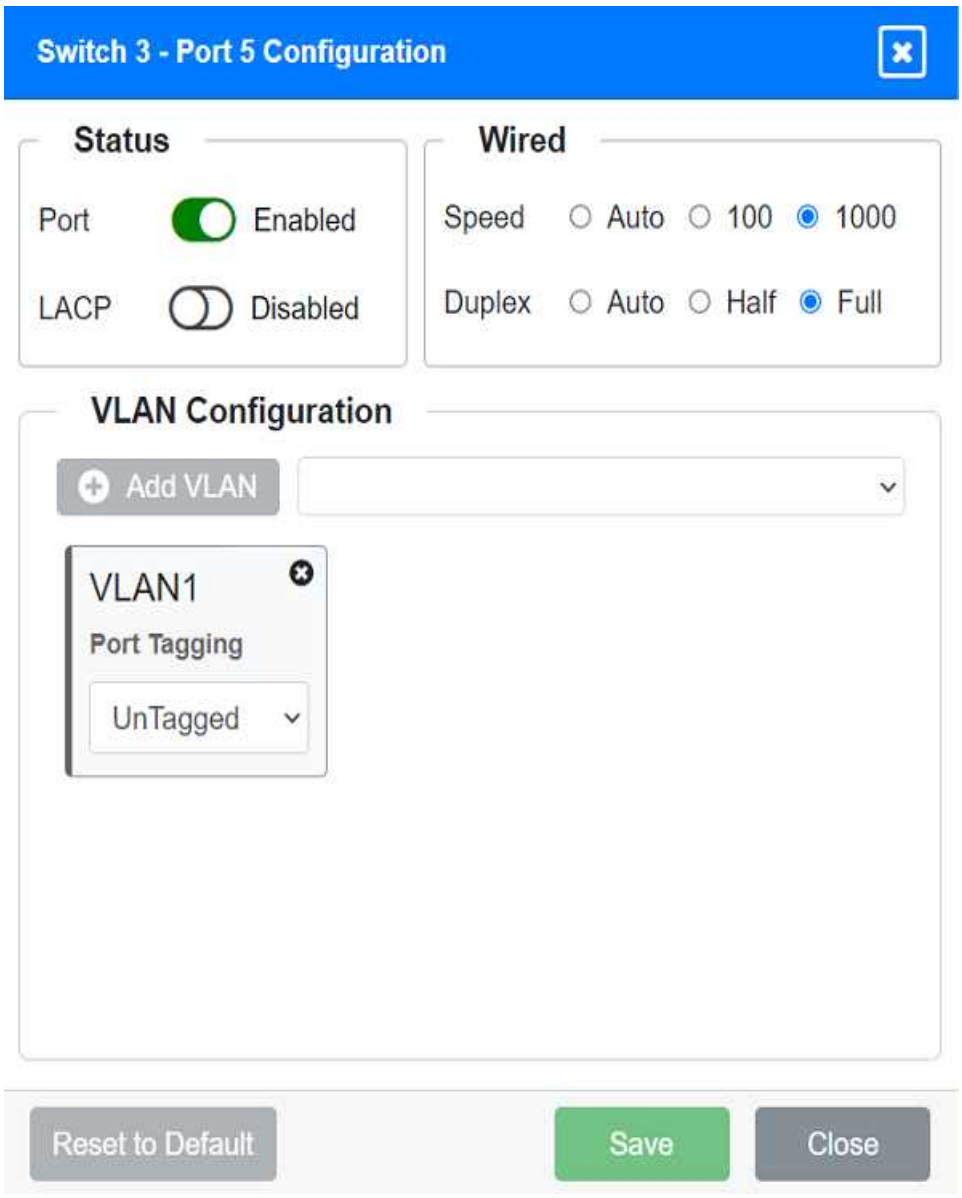

Switch 1 - Port 7 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN60
Port Tagging
Tagged
VLAN90
Port Tagging
Tagged
VLAN120
Port Tagging
Tagged
VLAN220
Port Tagging
Tagged
Reset to Default
Save
Close

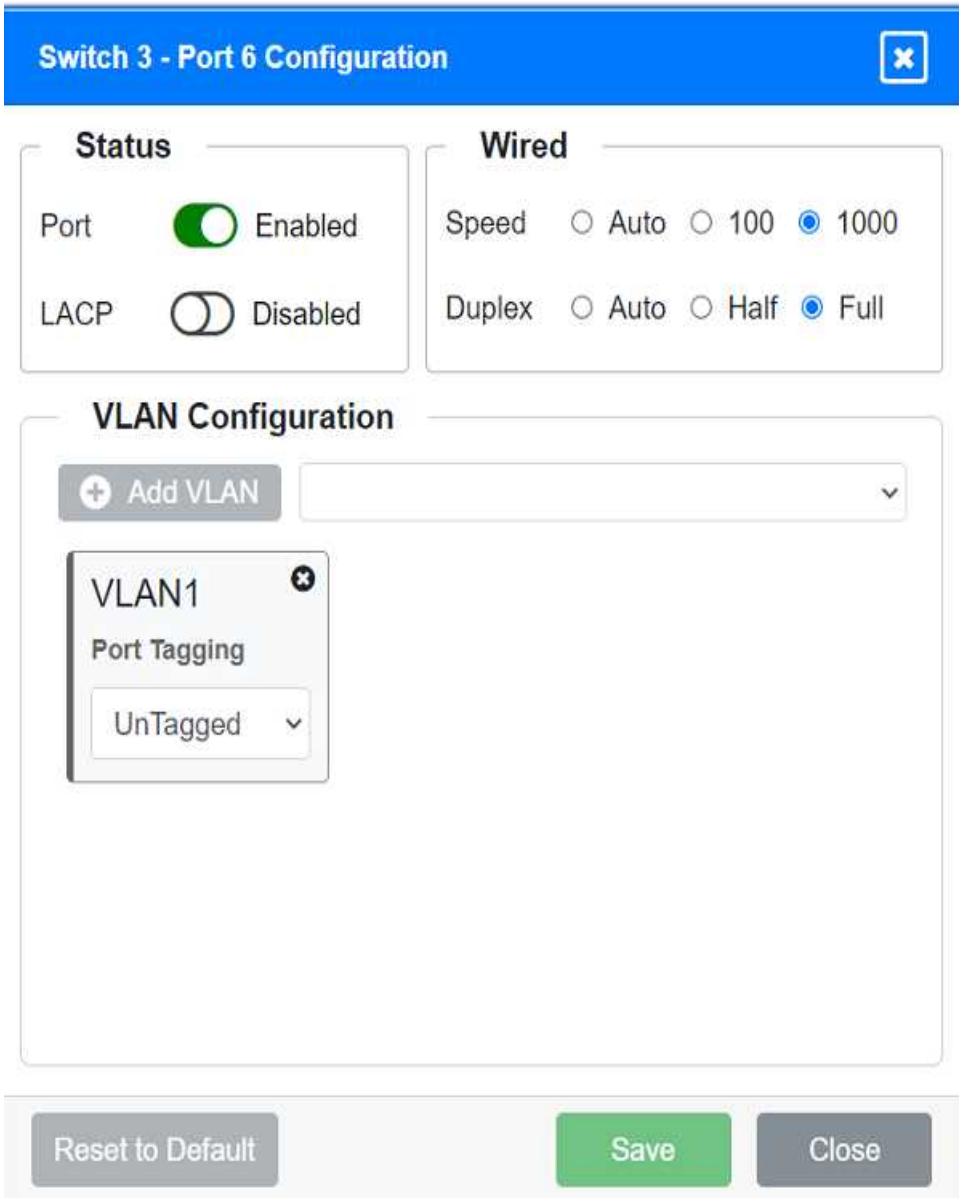

Switch 3 - Port 1 Configuration
Status
Port
Disabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Reset to Default
Save
Close

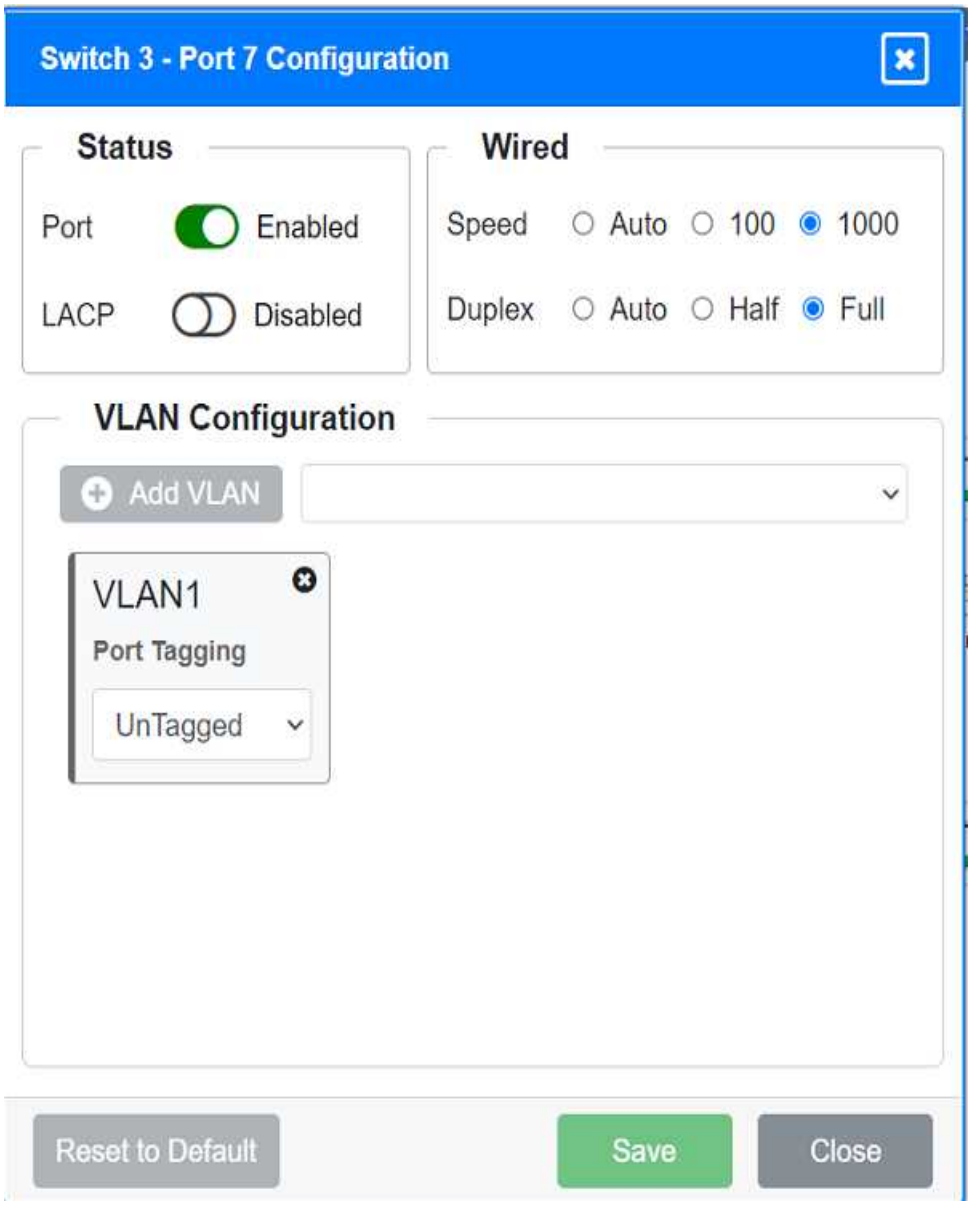

Switch 3 - Port 2 Configuration
Status
Port
Disabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Reset to Default
Save
Close

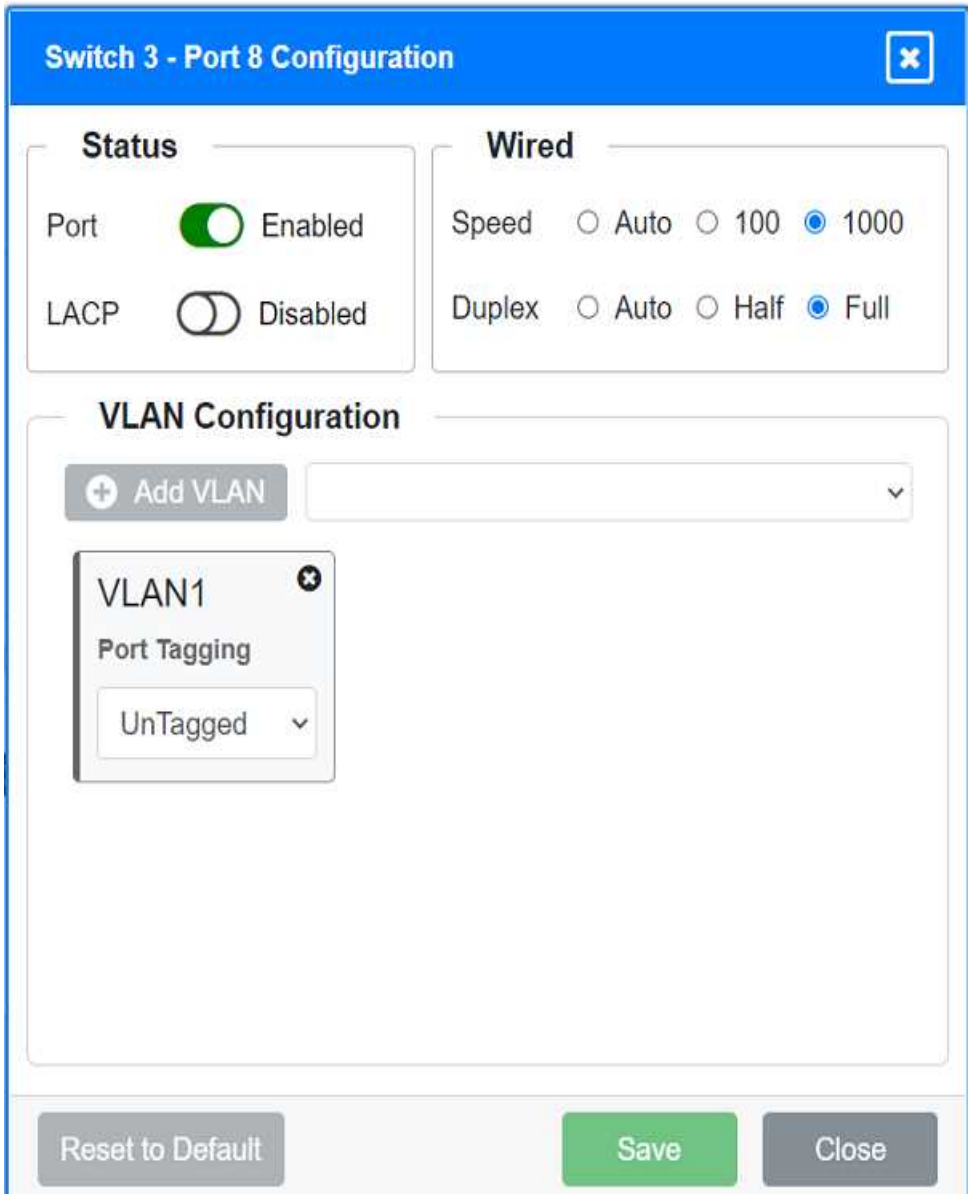

Switch 3 - Port 3 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Reset to Default
Save
Close

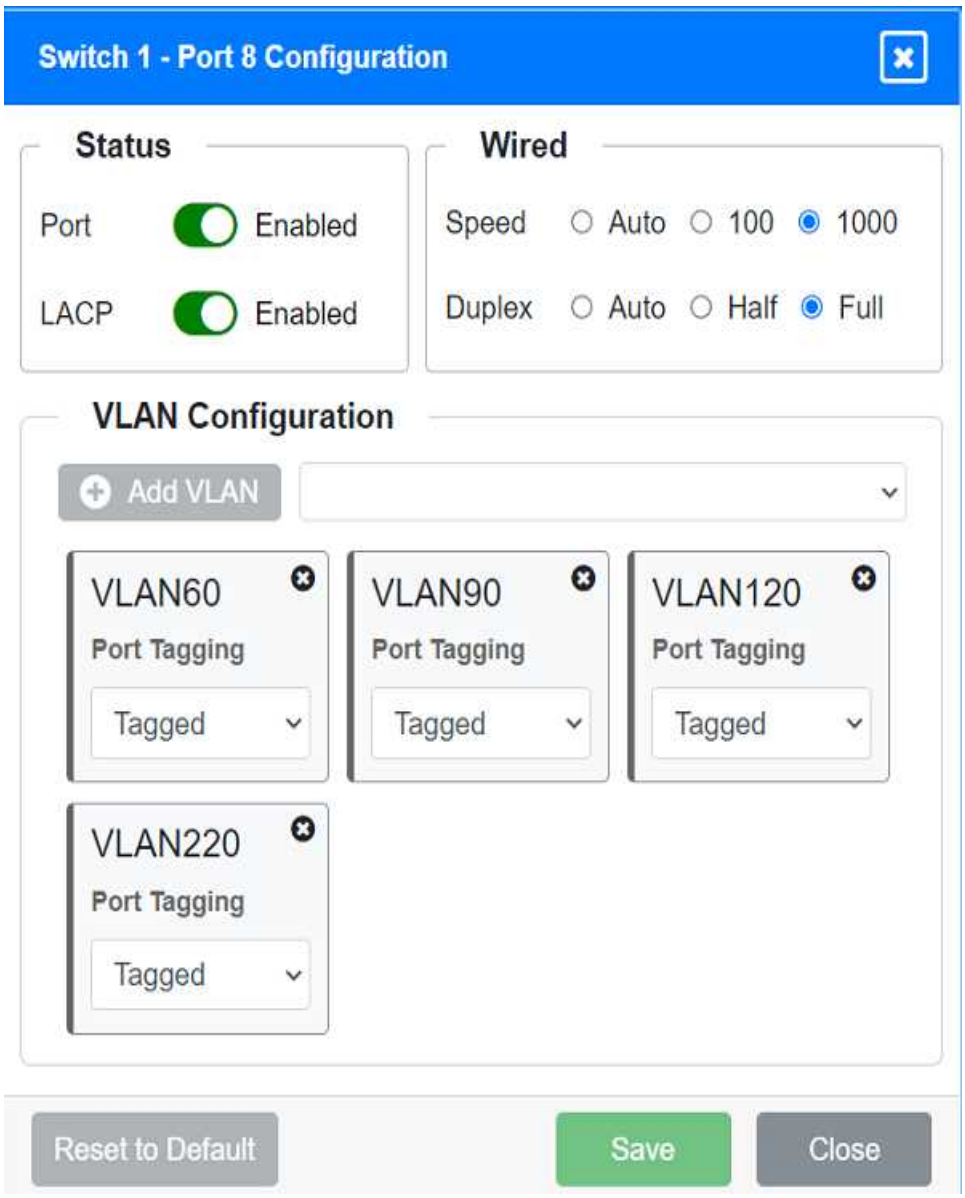

Switch 3 - Port 4 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
Reset to Default
Save
Close


Switch 3 - Port 5 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN1
Port Tagging
UnTagged
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
VLAN1
Port Tagging
UnTagged
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
Reset to Default
Save
Close


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
Reset to Default
Save
Close



Answer: See the solution below in Explanation.

Explanation:

To provide a complete solution for configuring the access layer switches, let's proceed with the following steps:

Identify the correct VLANs for each device and port.

Enable necessary ports and disable unused ports.

Configure fault-tolerant connections between the switches.

Configuration Details

Switch 1

Port 1 Configuration (Uplink to Core Switch)

Status: Enabled

LACP: Enabled

Speed: 1000

Duplex: Full

VLAN Configuration: Tagged for VLAN60, VLAN90, VLAN120, VLAN150, VLAN220

Port 2 Configuration (Uplink to Core Switch)

Status: Enabled

LACP: Enabled

Speed: 1000

Duplex: Full

VLAN Configuration: Tagged for VLAN60, VLAN90, VLAN120, VLAN150, VLAN220

Port 3 Configuration (Server Connection)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN90 (Servers)

Port 4 Configuration (Server Connection)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN90 (Servers)

Port 5 Configuration (Wired Users and WLAN)

Status: Enabled

LACP: Enabled

Speed: 1000

Duplex: Full

VLAN Configuration: Tagged for VLAN60, VLAN120, VLAN150

Port 6 Configuration (Wired Users and WLAN)

Status: Enabled

LACP: Enabled

Speed: 1000

Duplex: Full

VLAN Configuration: Tagged for VLAN60, VLAN120, VLAN150

Port 7 Configuration (Voice and Wired Users)

Status: Enabled

LACP: Enabled

Speed: 1000

Duplex: Full

VLAN Configuration: Tagged for VLAN60, VLAN90, VLAN120, VLAN220

Port 8 Configuration (Voice, Printers, and Wired Users)

Status: Enabled

LACP: Enabled

Speed: 1000

Duplex: Full

VLAN Configuration: Tagged for VLAN60, VLAN90, VLAN120, VLAN220

Switch 3

Port 1 Configuration (Unused)

Status: Disabled

LACP: Disabled

Port 2 Configuration (Unused)

Status: Disabled

LACP: Disabled

Port 3 Configuration (Connection to Device)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN1 (Default)

Port 4 Configuration (Connection to Device)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN1 (Default)

Port 5 Configuration (Connection to Device)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN1 (Default)

Port 6 Configuration (Connection to Device)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN1 (Default)

Port 7 Configuration (Connection to Device)

Status: Enabled

LACP: Disabled

Speed: 1000

Duplex: Full

VLAN Configuration: Untagged for VLAN1 (Default)

Summary of Configurations

Ports 1 and 2 on Switch 1 are configured as trunk ports with VLAN tagging enabled for all necessary VLANs.

Ports 3 and 4 on Switch 1 are configured for server connections with VLAN 90 untagged.

Ports 5, 6, 7, and 8 on Switch 1 are configured for devices needing access to multiple VLANs.

Unused ports on Switch 3 are disabled.

Ports 3, 4, 5, 6, and 7 on Switch 3 are enabled for default VLAN1.

Ensure All Switches and Ports are Configured as per the Requirements:

Core Switch Ports should be configured as needed for uplinks to Switch 1.

Ensure LACP is enabled for redundancy on trunk ports between switches.

By following these configurations, each device will access only its correctly associated network, unused switch ports will be disabled, and fault-tolerant connections will be established between the switches.

Question: 77

SIMULATION

Users are unable to access files on their department share located on file server 2.

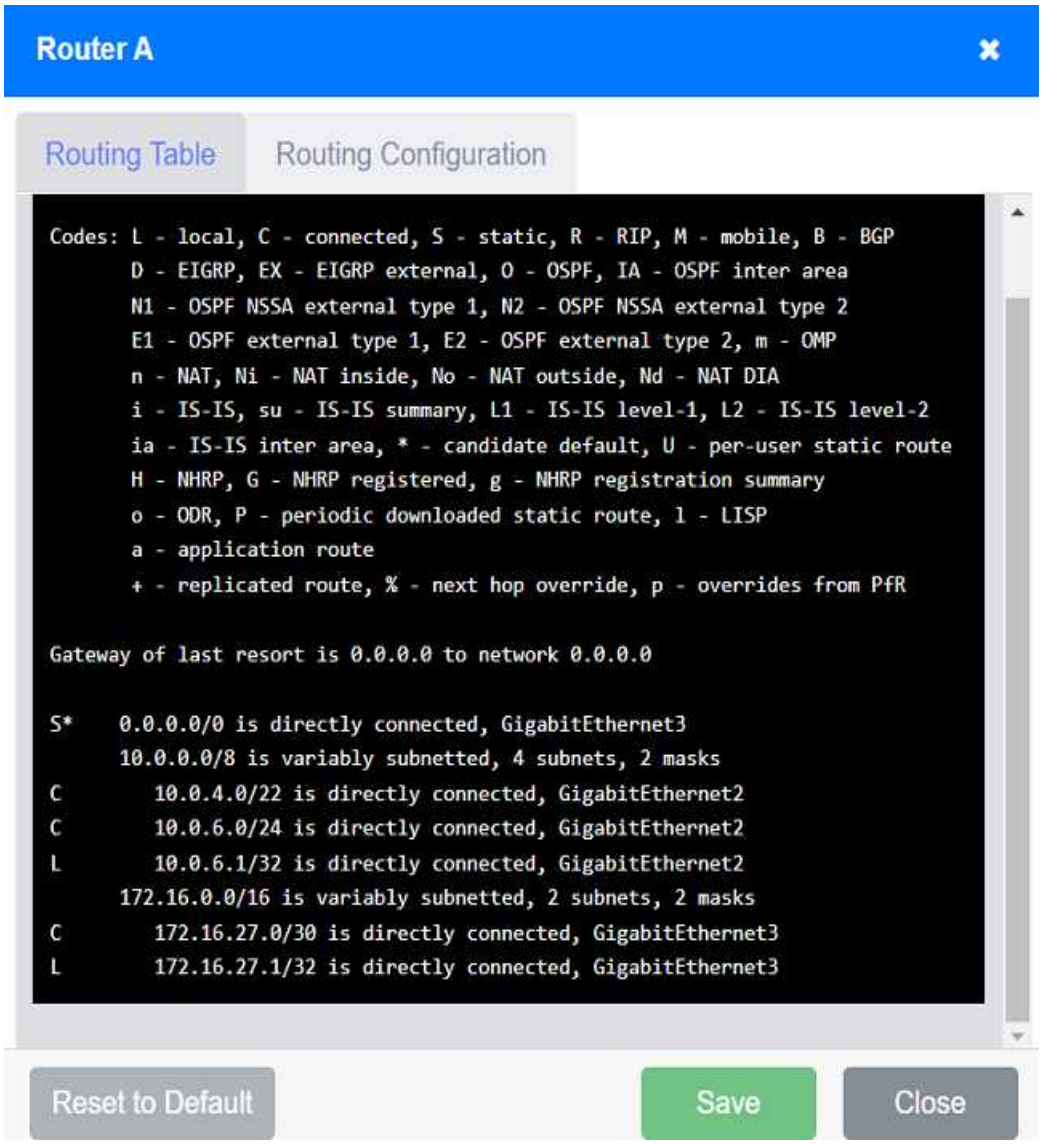
The network administrator has been tasked with validating routing between networks

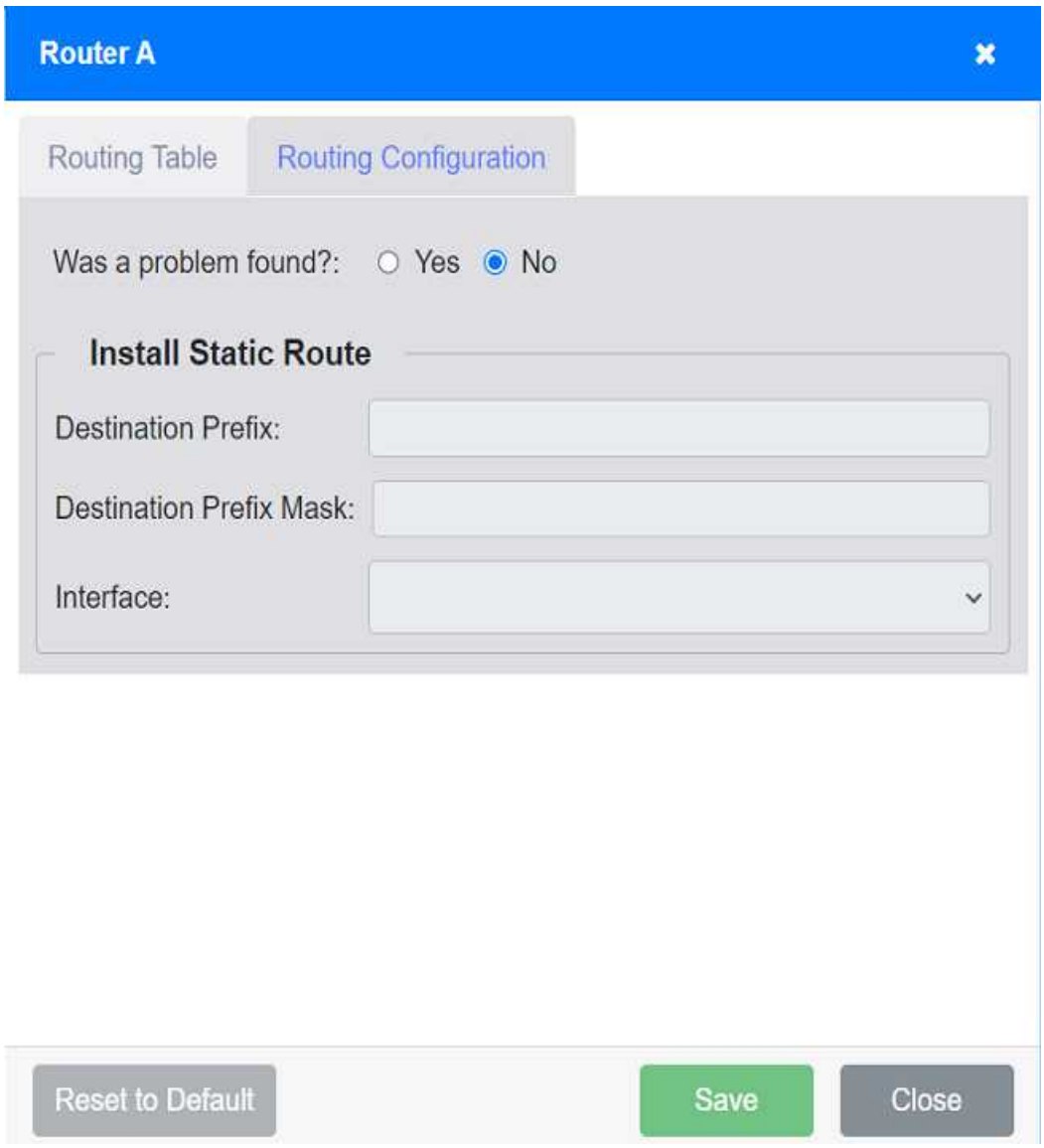
hosting workstation A and file server 2.

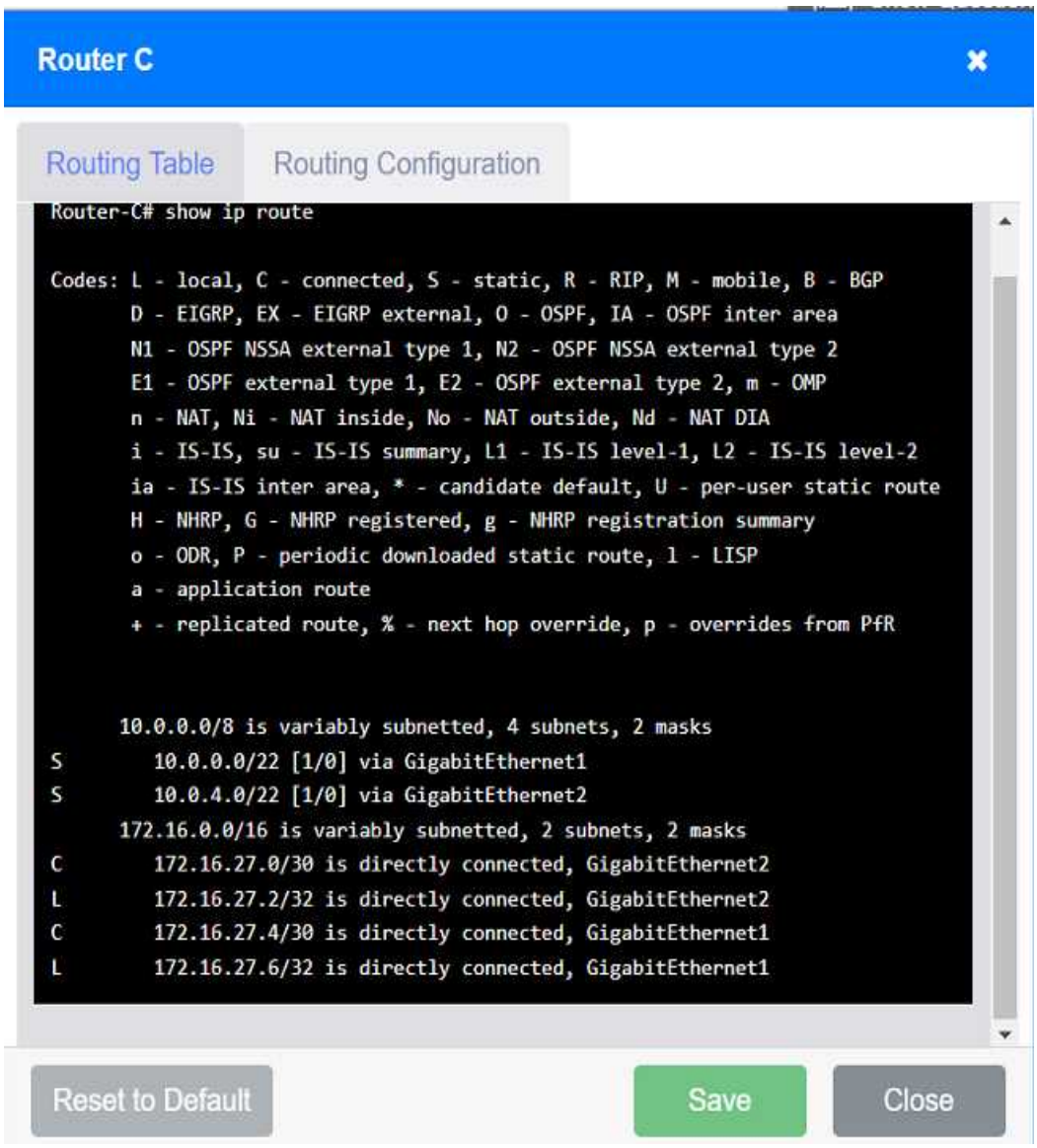
INSTRUCTIONS

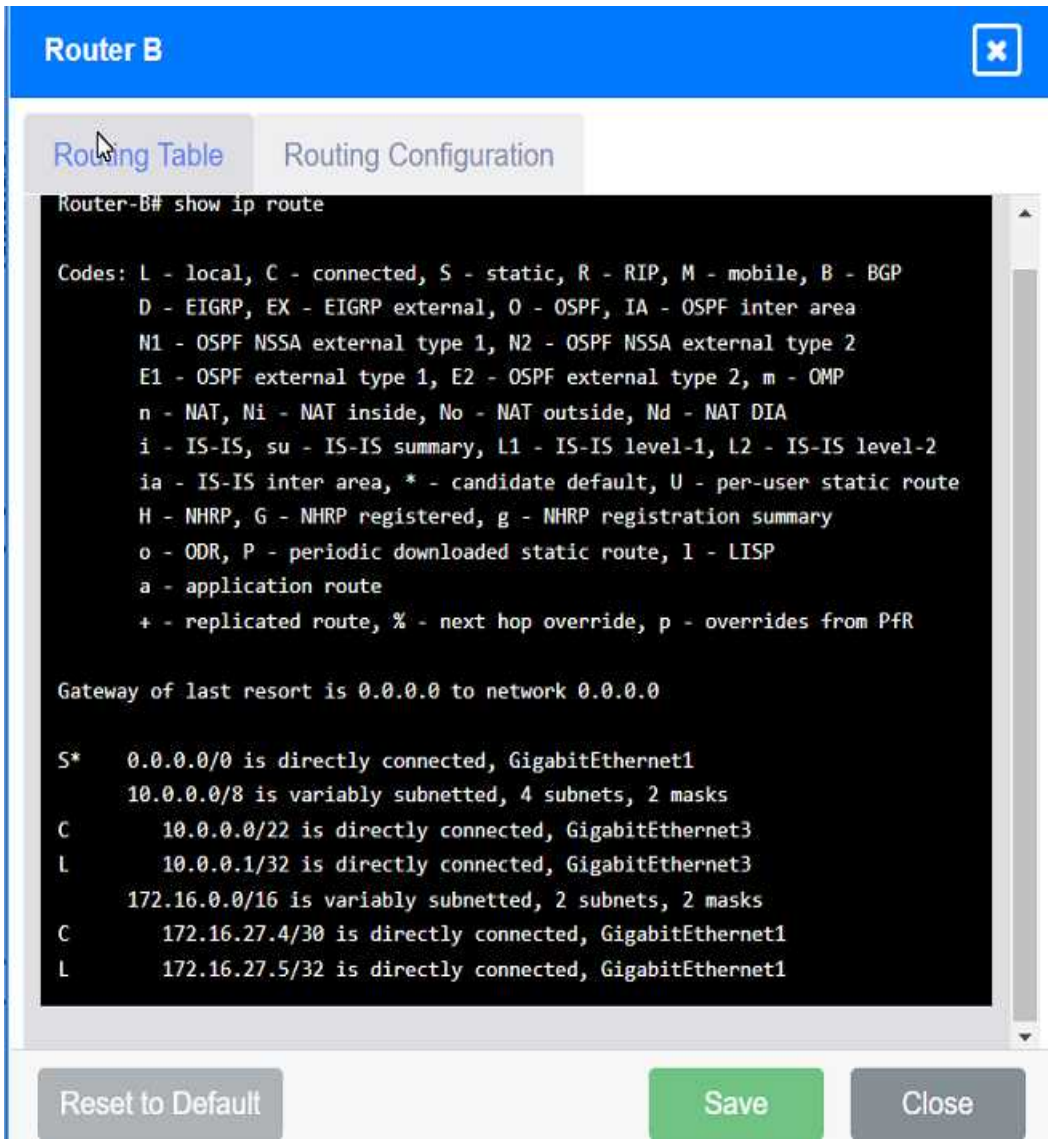
Click on each router to review output, identify any issues, and configure the appropriate solution.

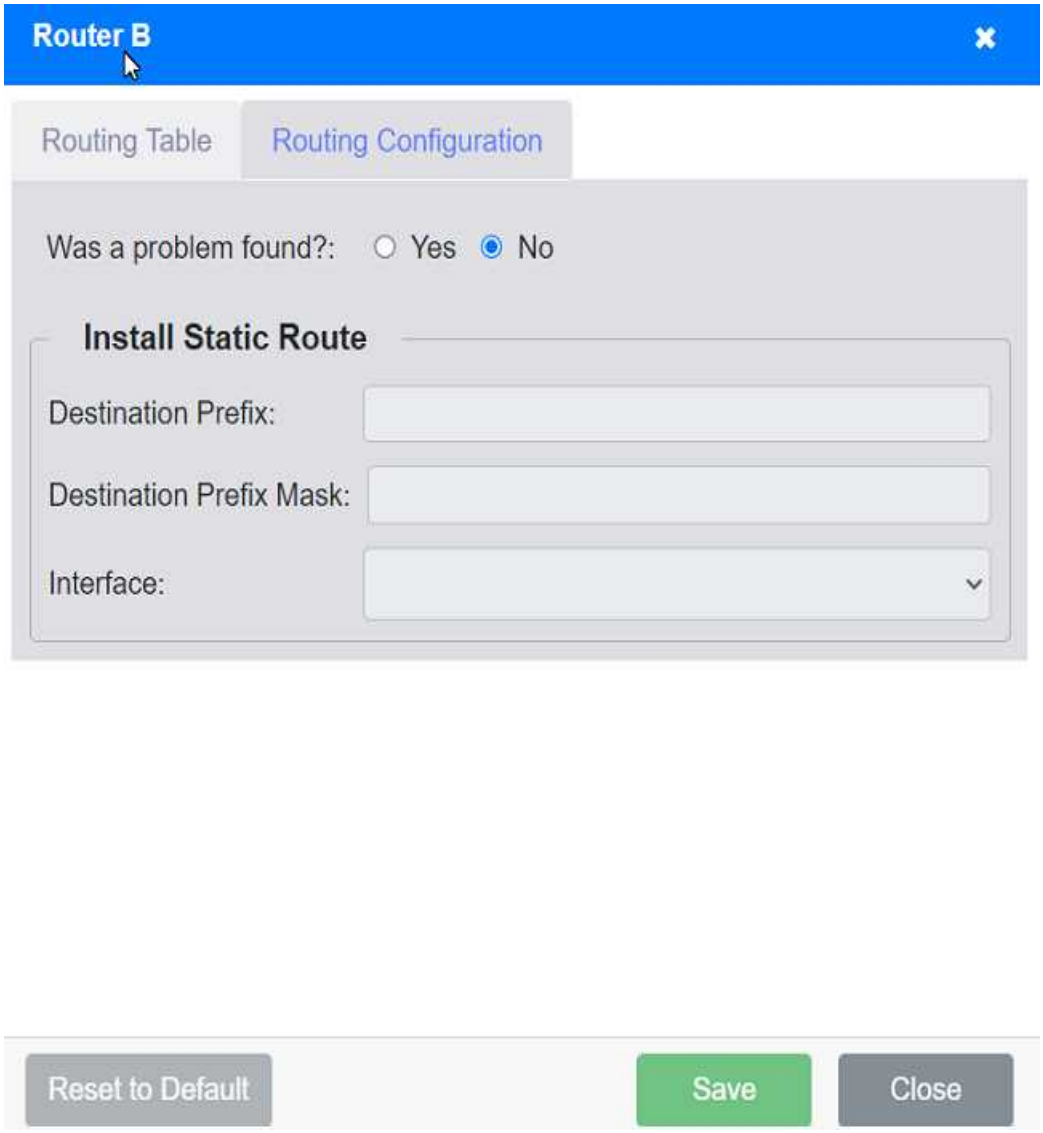
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

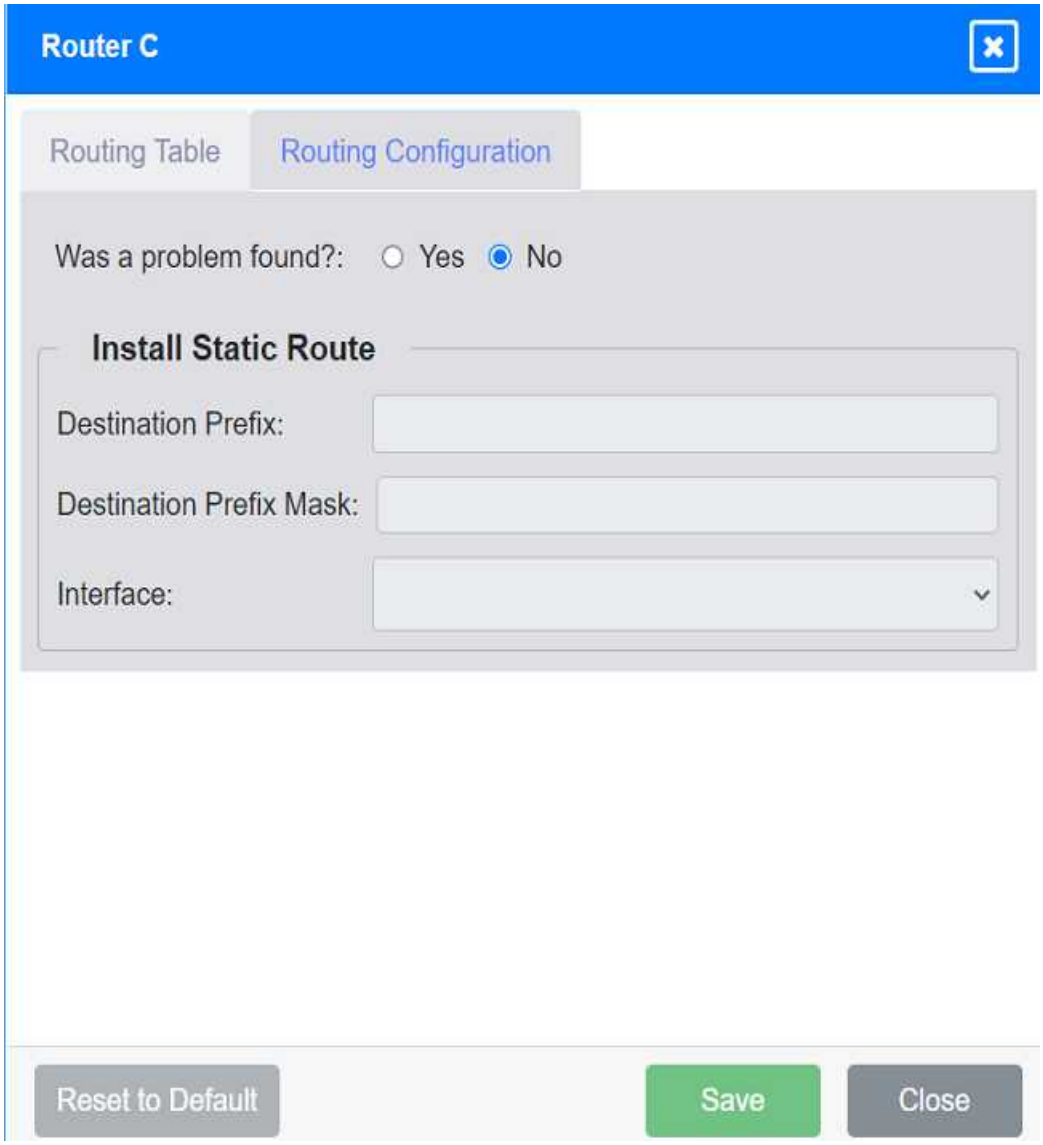



Router A
Routing Table
Routing Configuration
Was a problem found?:
Yes
No
Install Static Route
Destination Prefix:
Destination Prefix Mask:
Interface:
Reset to Default
Save
Close


Router C
Routing Table
Routing Configuration
Router-C# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S 10.0.0.0/22 [1/0] via GigabitEthernet1
S 10.0.4.0/22 [1/0] via GigabitEthernet2
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.27.0/30 is directly connected, GigabitEthernet2
L 172.16.27.2/32 is directly connected, GigabitEthernet2
C 172.16.27.4/30 is directly connected, GigabitEthernet1
L 172.16.27.6/32 is directly connected, GigabitEthernet1
Reset to Default
Save
Close


Router B
Routing Table
Routing Configuration
Router-B# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S* 0.0.0.0/0 is directly connected, GigabitEthernet1
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.0.0.0/22 is directly connected, GigabitEthernet3
L 10.0.0.1/32 is directly connected, GigabitEthernet3
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.27.4/30 is directly connected, GigabitEthernet1
L 172.16.27.5/32 is directly connected, GigabitEthernet1
Reset to Default
Save
Close


Router B
Routing Table
Routing Configuration
Was a problem found?:
Yes
No
Install Static Route
Destination Prefix:
Destination Prefix Mask:
Interface:
Reset to Default
Save
Close



Answer: See the solution in Explanation.

Explanation:

To validate routing between networks hosting Workstation A and File Server 2, follow these steps:

Step-by-Step Solution

Review Routing Tables:

Check the routing tables of Router A, Router B, and Router C to identify any missing routes.

Identify Missing Routes:

Ensure that each router has routes to the networks on which Workstation A and File Server 2 are located.

Add Static Routes:

If a route is missing, add a static route to the relevant destination network via the correct interface.

Detailed Analysis and Configuration

Router A:

Routing Table:

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, GigabitEthernet3

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C 10.0.4.0/22 is directly connected, GigabitEthernet2

C 10.0.6.0/24 is directly connected, GigabitEthernet2

L 10.0.6.1/32 is directly connected, GigabitEthernet2

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.27.0/30 is directly connected, GigabitEthernet3

L 172.16.27.1/32 is directly connected, GigabitEthernet3

Router B:

Routing Table:

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, GigabitEthernet1

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C 10.0.0.0/22 is directly connected, GigabitEthernet1

L 10.0.0.1/32 is directly connected, GigabitEthernet1

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.27.4/30 is directly connected, GigabitEthernet1

L 172.16.27.5/32 is directly connected, GigabitEthernet1

Router C:

Routing Table:

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

S 10.0.0.0/22 [1/0] via GigabitEthernet1

S 10.0.4.0/22 [1/0] via GigabitEthernet2

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.27.0/30 is directly connected, GigabitEthernet2

L 172.16.27.2/32 is directly connected, GigabitEthernet2

C 172.16.27.4/30 is directly connected, GigabitEthernet1

L 172.16.27.6/32 is directly connected, GigabitEthernet1

Configuration Steps:

Router A:

Install Static Route to 10.0.0.0/22 via 172.16.27.1 (assuming Router C's IP is 172.16.27.1):

Destination Prefix: 10.0.0.0

Destination Prefix Mask: 255.255.252.0

Interface: GigabitEthernet3

Router B:

Install Static Route to 10.0.4.0/22 via 172.16.27.5 (assuming Router C's IP is 172.16.27.5):

Destination Prefix: 10.0.4.0

Destination Prefix Mask: 255.255.252.0

Interface: GigabitEthernet1

Router C:

Install Static Route to 10.0.6.0/24 via 172.16.27.2 (assuming Router A's IP is 172.16.27.2):

Destination Prefix: 10.0.6.0

Destination Prefix Mask: 255.255.255.0

Interface: GigabitEthernet2

Install Static Route to 10.0.0.0/22 via 172.16.27.1 (assuming Router B's IP is 172.16.27.1):

Destination Prefix: 10.0.0.0

Destination Prefix Mask: 255.255.252.0

Interface: GigabitEthernet1

Summary of Static Routes:

Router A:

ip route 10.0.0.0 255.255.252.0 GigabitEthernet3

Router B:

ip route 10.0.4.0 255.255.252.0 GigabitEthernet1

Router C:

ip route 10.0.6.0 255.255.255.0 GigabitEthernet2

ip route 10.0.0.0 255.255.252.0 GigabitEthernet1

These configurations ensure that each router knows the correct paths to reach Workstation A and File Server 2, resolving the connectivity issue.

Question: 78

SIMULATION

You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:

The SSIDs need to be configured as CorpNet with a key of S3cr3t!

The wireless signals should not interfere with each other

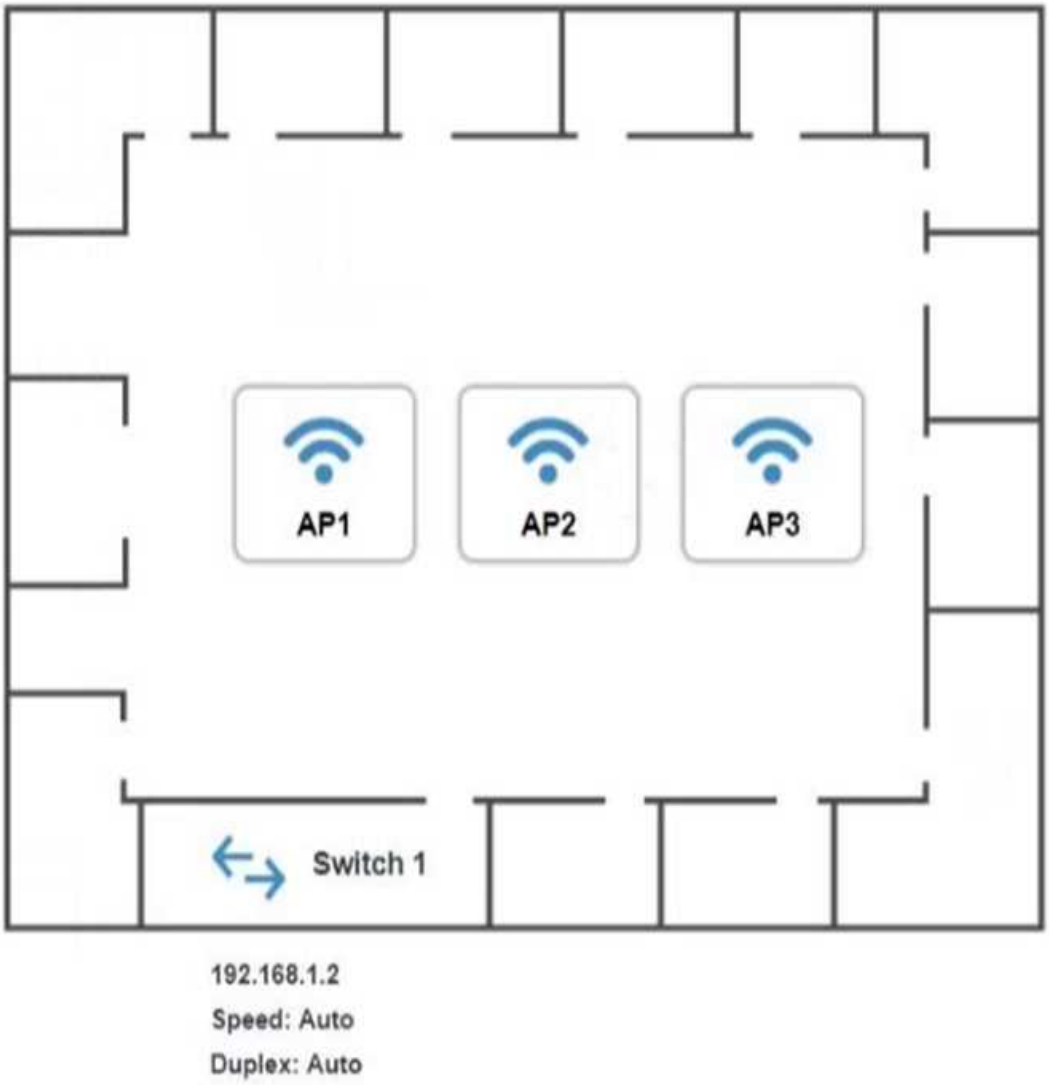
The subnet the Access Points and switch are on should only support 30 devices maximum

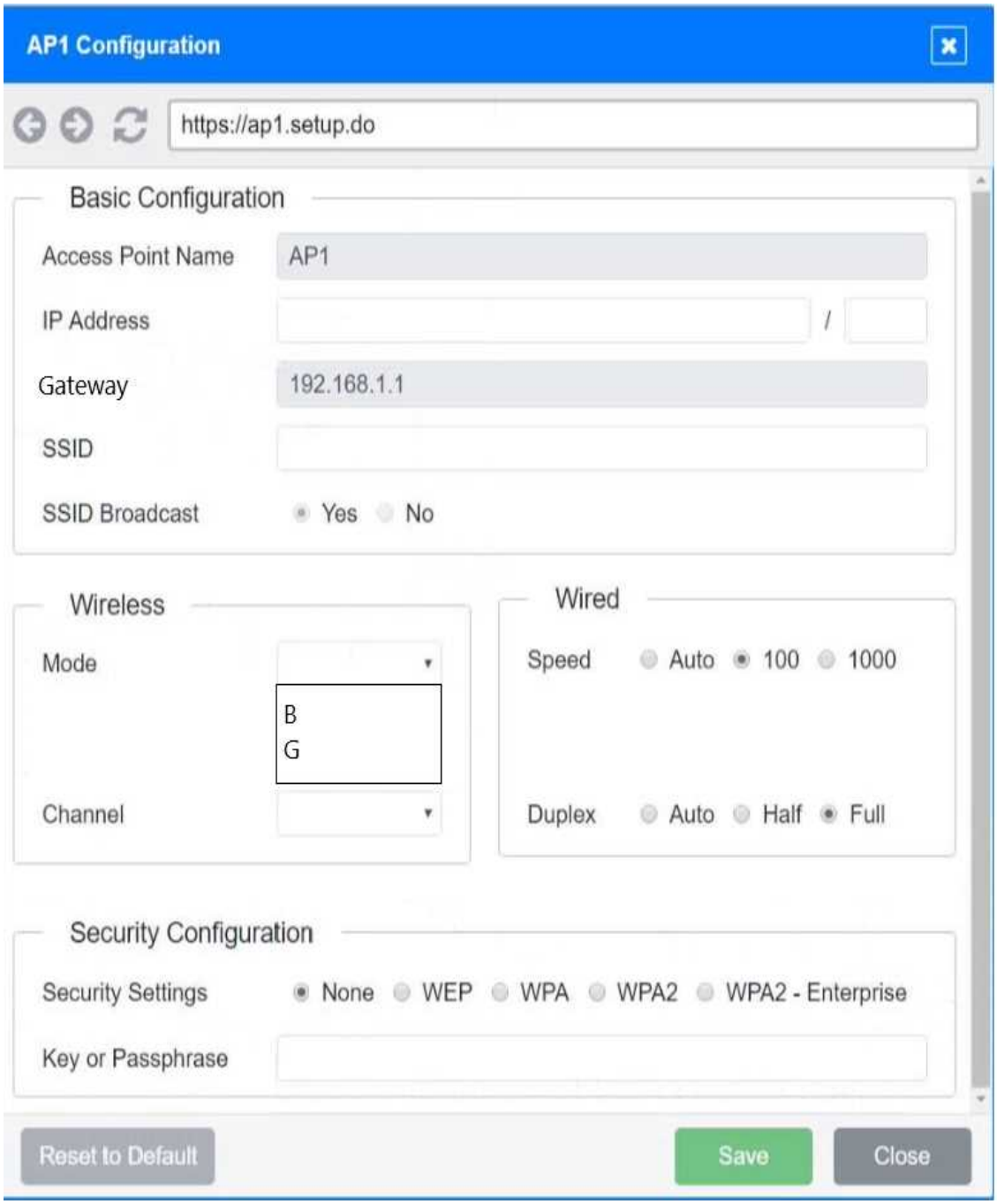
The Access Points should be configured to only support TKIP clients at a maximum speed

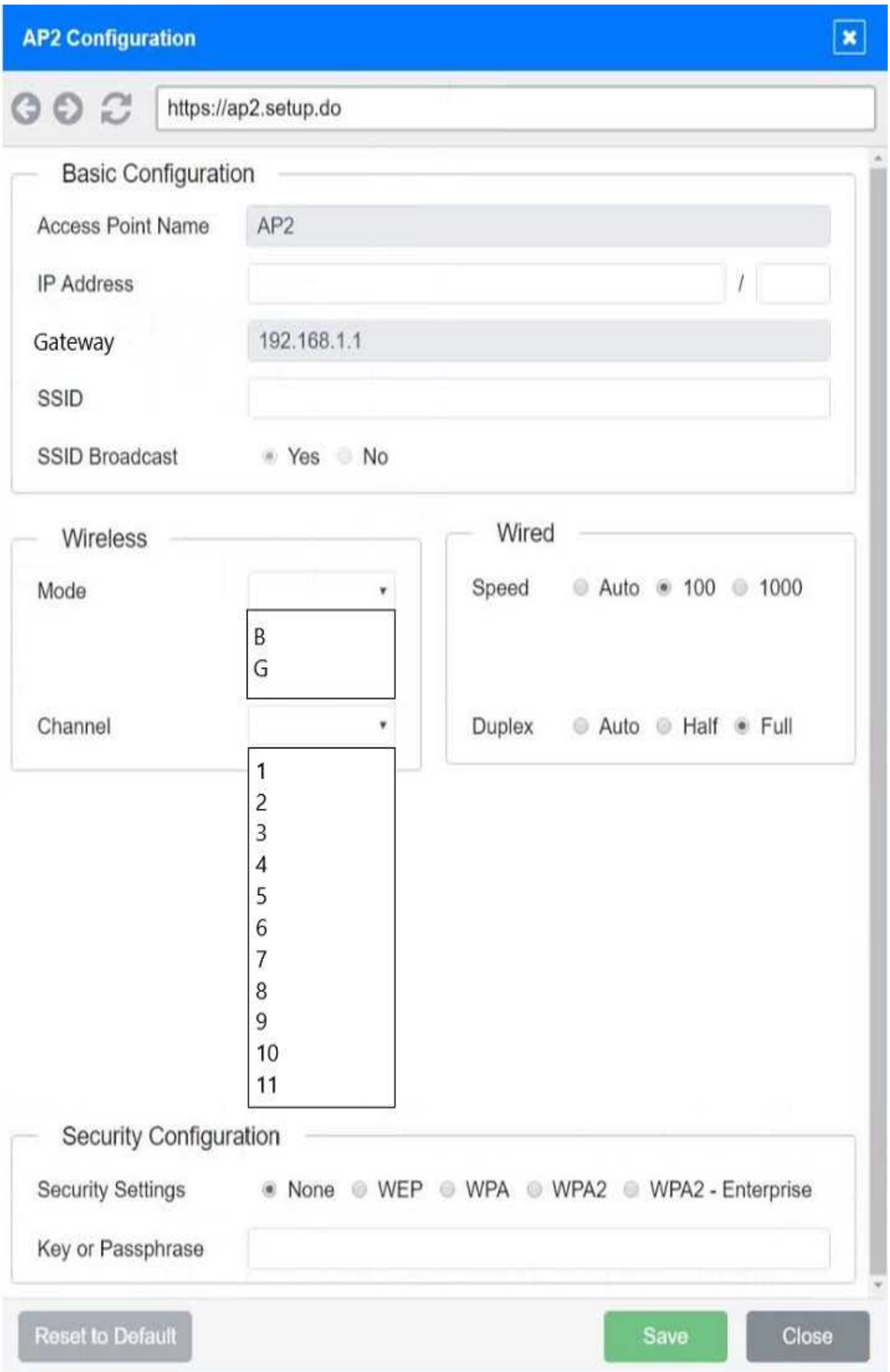
INSTRUCTONS

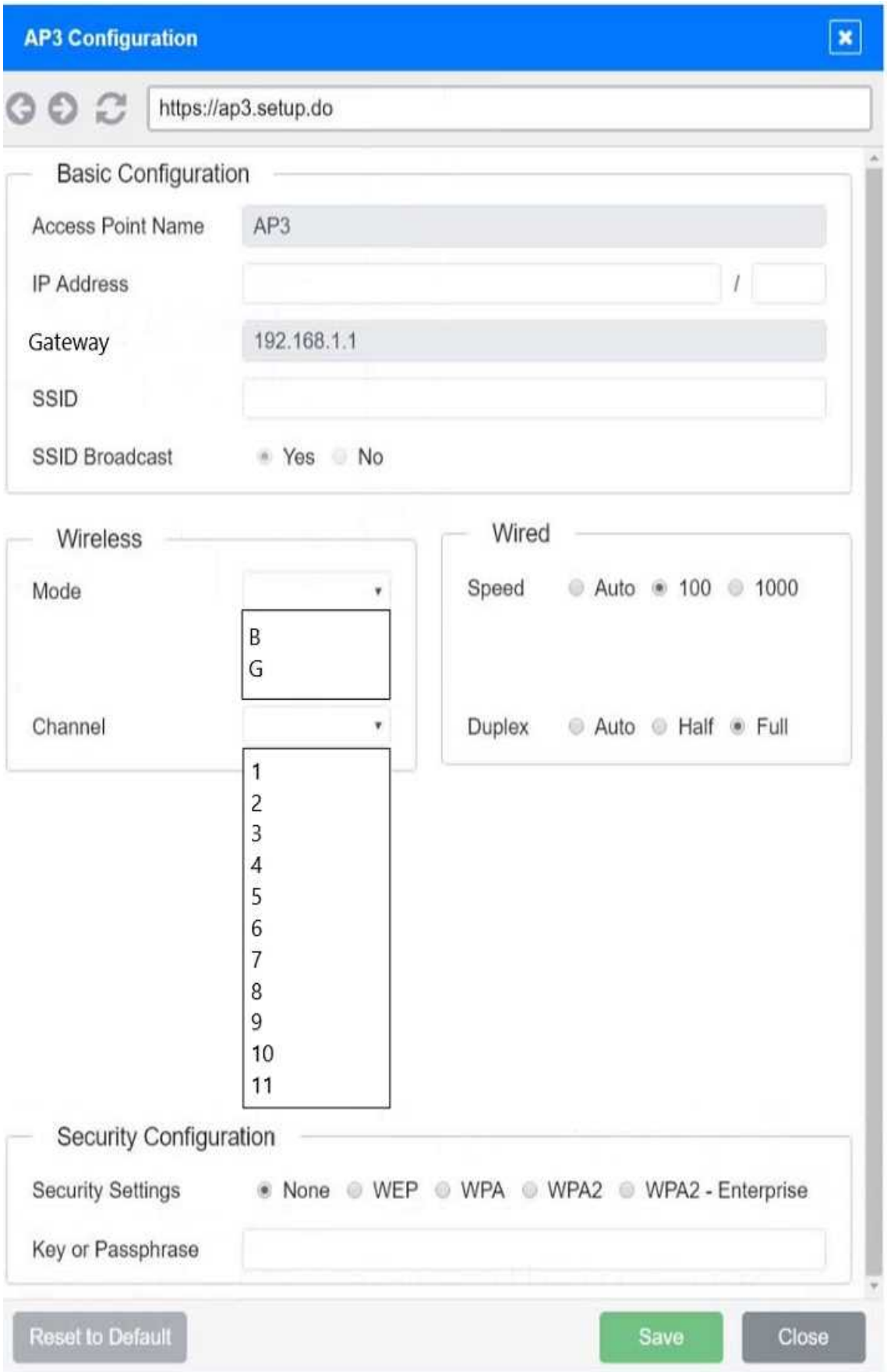
Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


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


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


AP2 Configuration
https://ap2.setup.do
Basic Configuration
Access Point Name
AP2
IP Address
/
Gateway
192.168.1.1
SSID
SSID Broadcast
Yes
No
Wireless
Mode
B
G
Channel
1
2
3
4
5
6
7
8
9
10
11
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase
Reset to Default
Save
Close

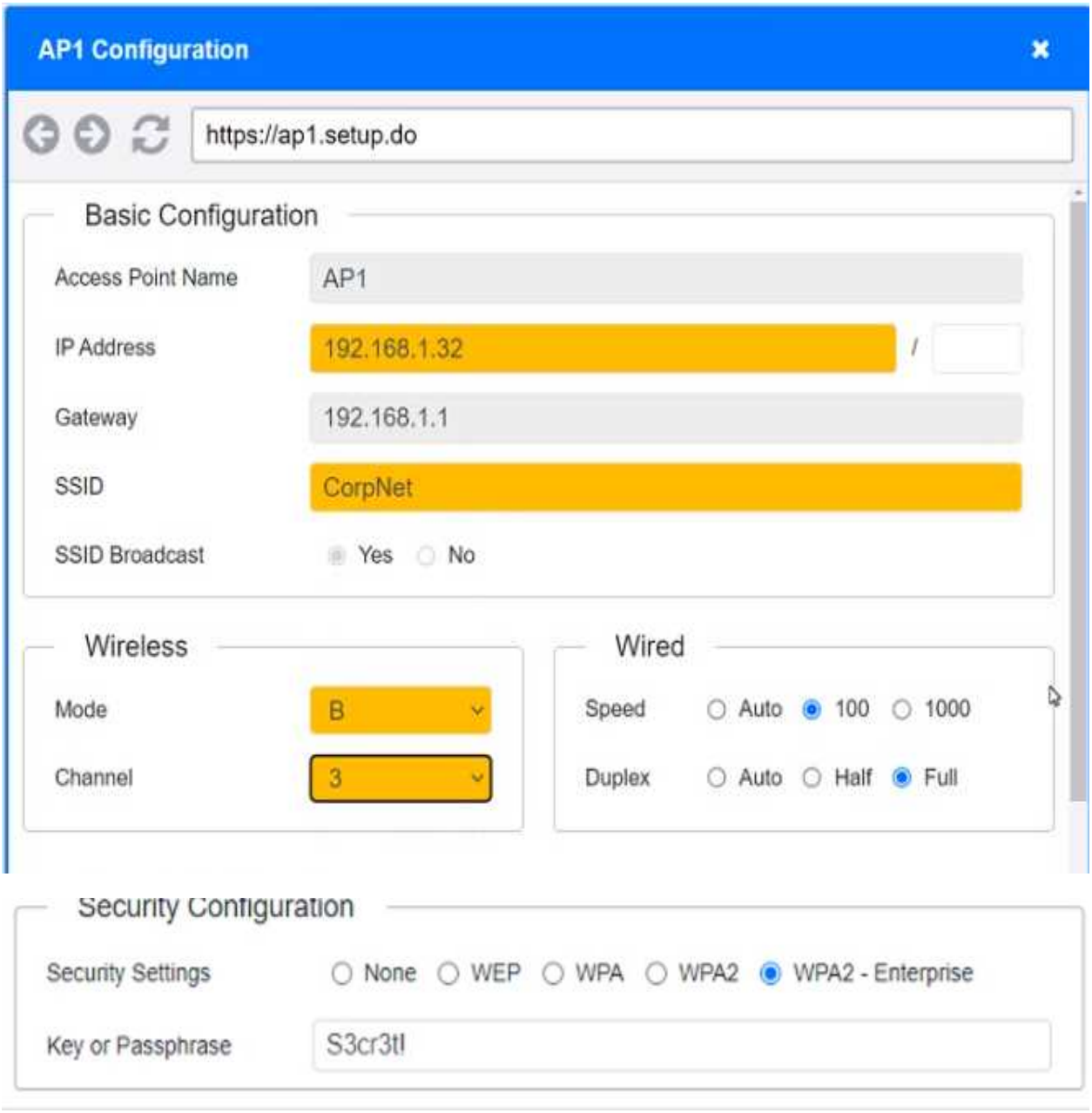

AP3 Configuration
https://ap3.setup.do
Basic Configuration
Access Point Name
AP3
IP Address
Gateway
192.168.1.1
SSID
SSID Broadcast
Yes
No
Wireless
Mode
B
G
Channel
1
2
3
4
5
6
7
8
9
10
11
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase
Reset to Default
Save
Close

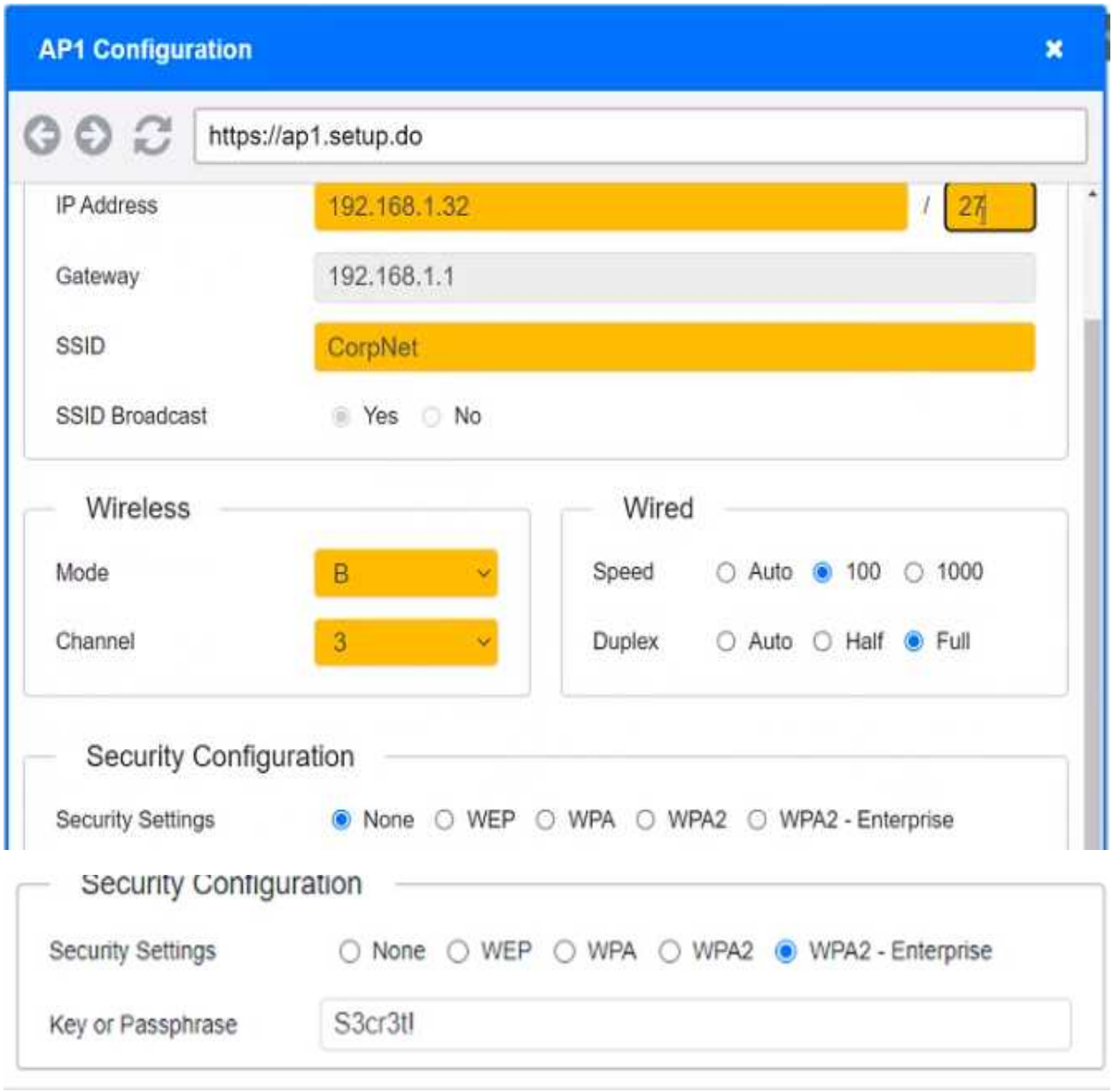
Answer: See

explanation below.

Explanation:

On the first exhibit, the layout should be as follows




AP1 Configuration
https://ap1.setup.do
IP Address
192.168.1.32
/
27
Gateway
192.168.1.1
SSID
CorpNet
SSID Broadcast
Yes
No
Wireless
Mode
B
Channel
3
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise

Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase
S3cr3tl

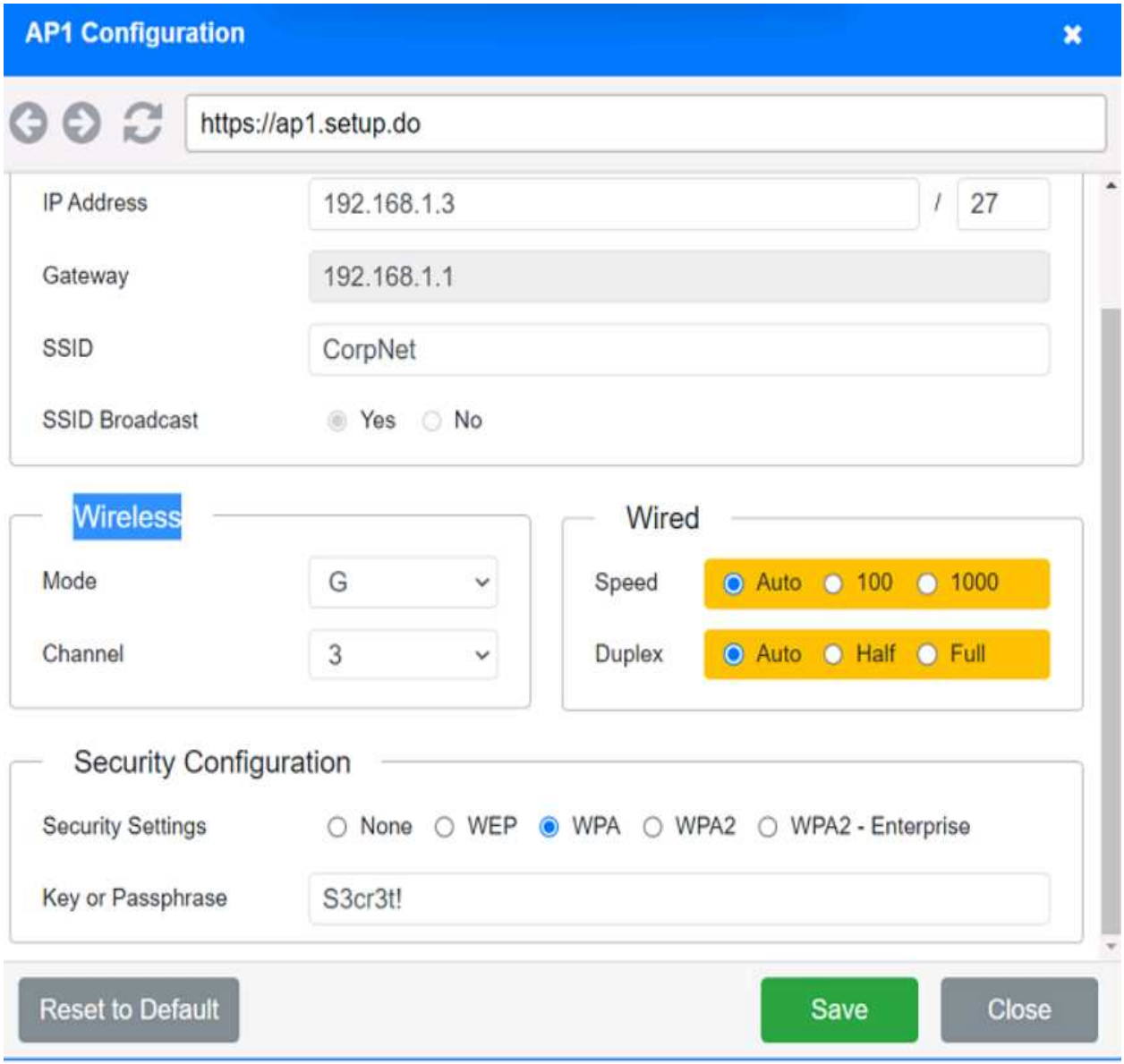
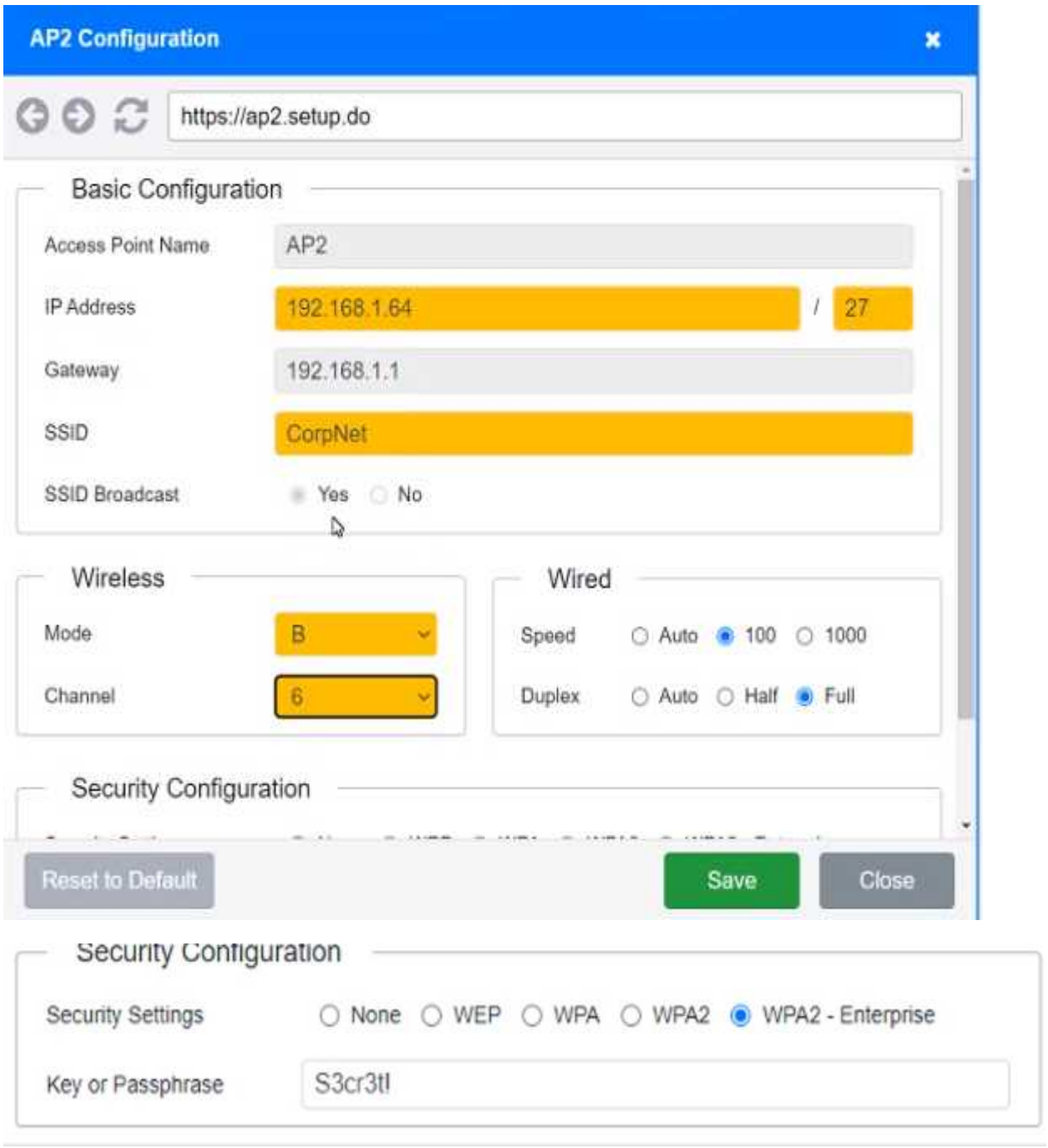


Exhibit 2 as follows

Access Point Name AP2


AP2 Configuration
https://ap2.setup.do
Basic Configuration
Access Point Name
AP2
IP Address
192.168.1.64
/
27
Gateway
192.168.1.1
SSID
CorpNet
SSID Broadcast
Yes
No
Wireless
Mode
B
Channel
6
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Reset to Default
Save
Close

Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase
S3cr3tl

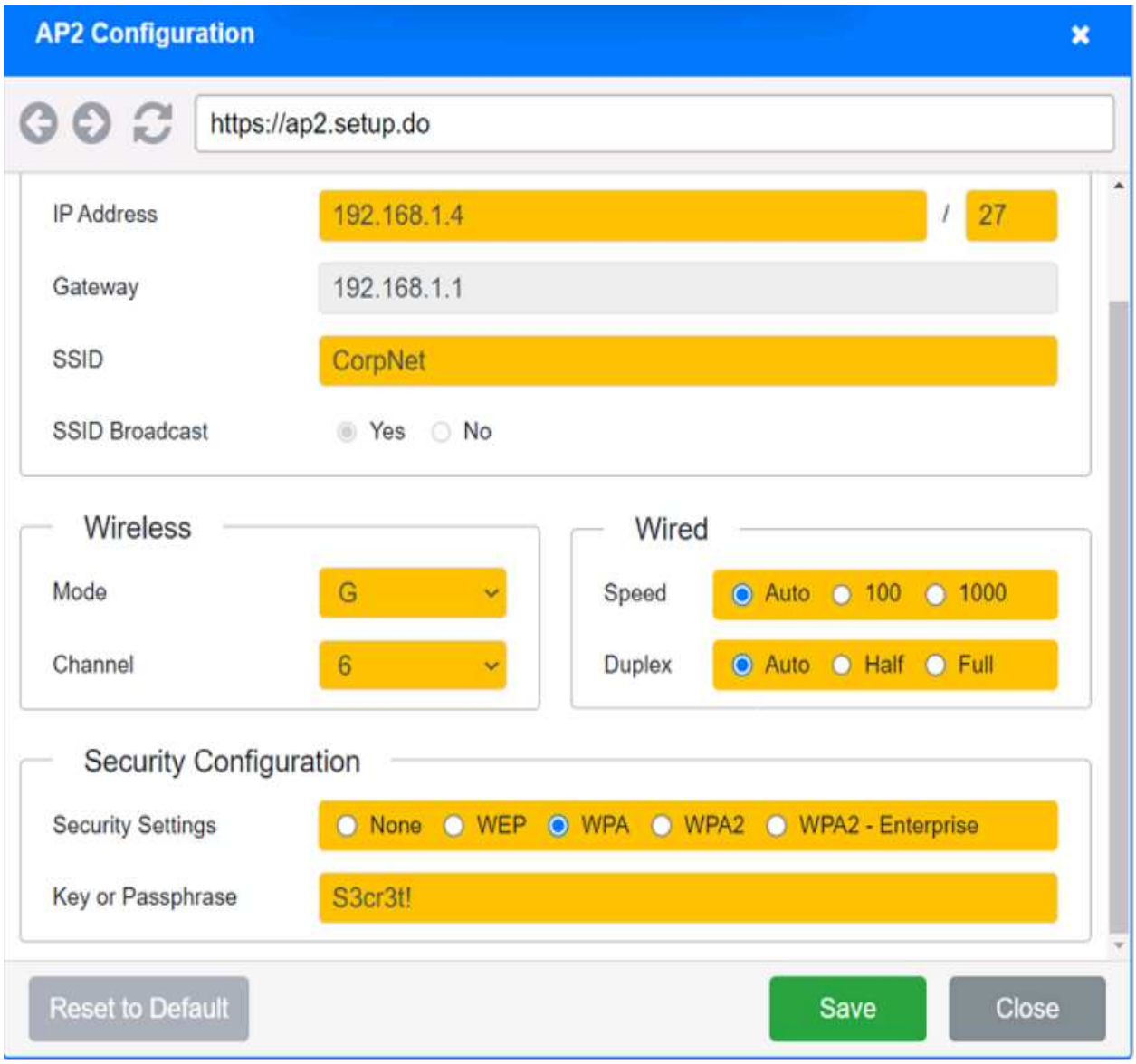
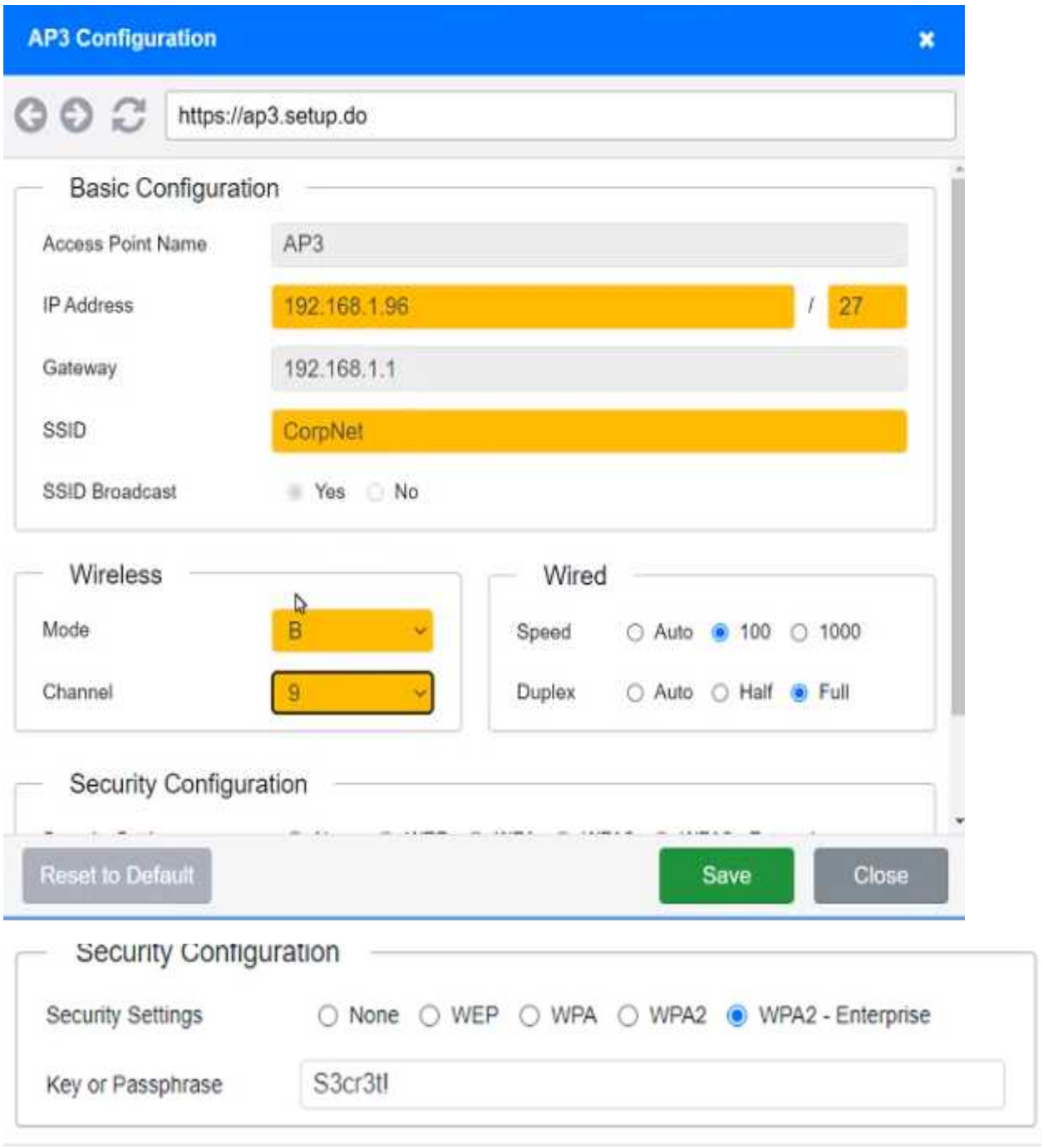
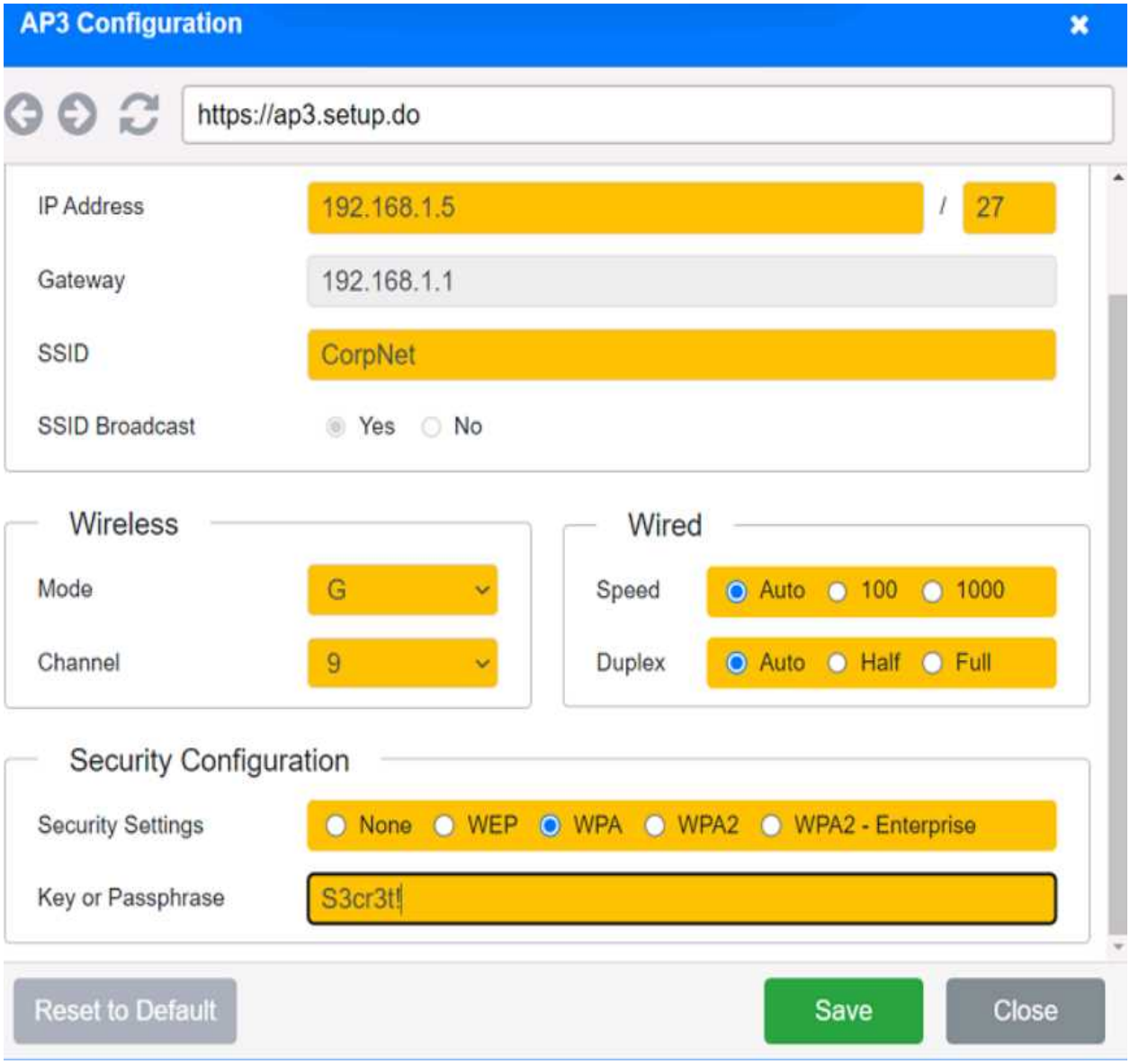


Exhibit 3 as follows

Access Point Name AP3


AP3 Configuration
https://ap3.setup.do
Basic Configuration
Access Point Name
AP3
IP Address
192.168.1.96
/
27
Gateway
192.168.1.1
SSID
CorpNet
SSID Broadcast
Yes
No
Wireless
Mode
B
Channel
9
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Reset to Default
Save
Close

Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase
S3cr3tI



Question: 79

SIMULATION

You are tasked with verifying the following requirements are met in order to ensure network security.

Requirements:

Datacenter

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic

Building A

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide devices to support 5 additional different office users

Add an additional mobile user

Replace the Telnet server with a more secure solution

Screened subnet

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage

Provide a server to handle external 80/443 traffic

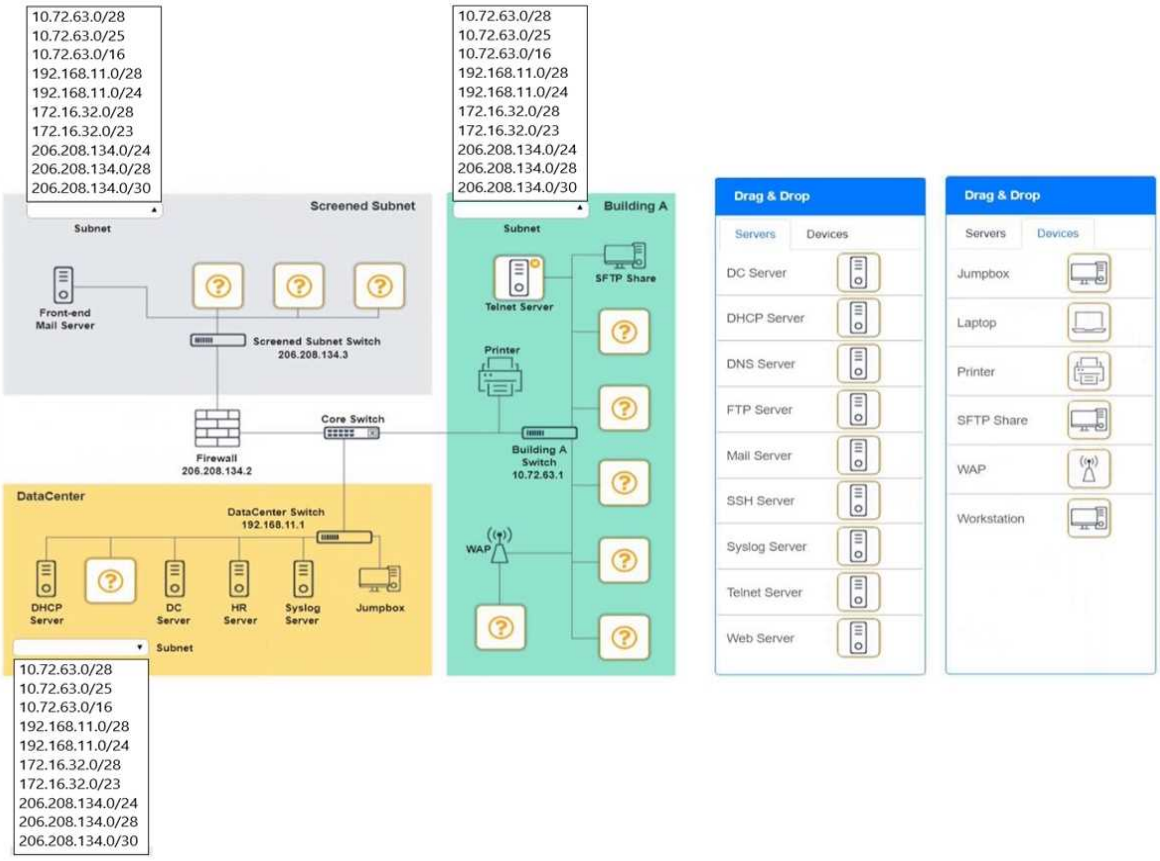
Provide a server to handle port 20/21 traffic

INSTRUCTIONS

Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.

Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



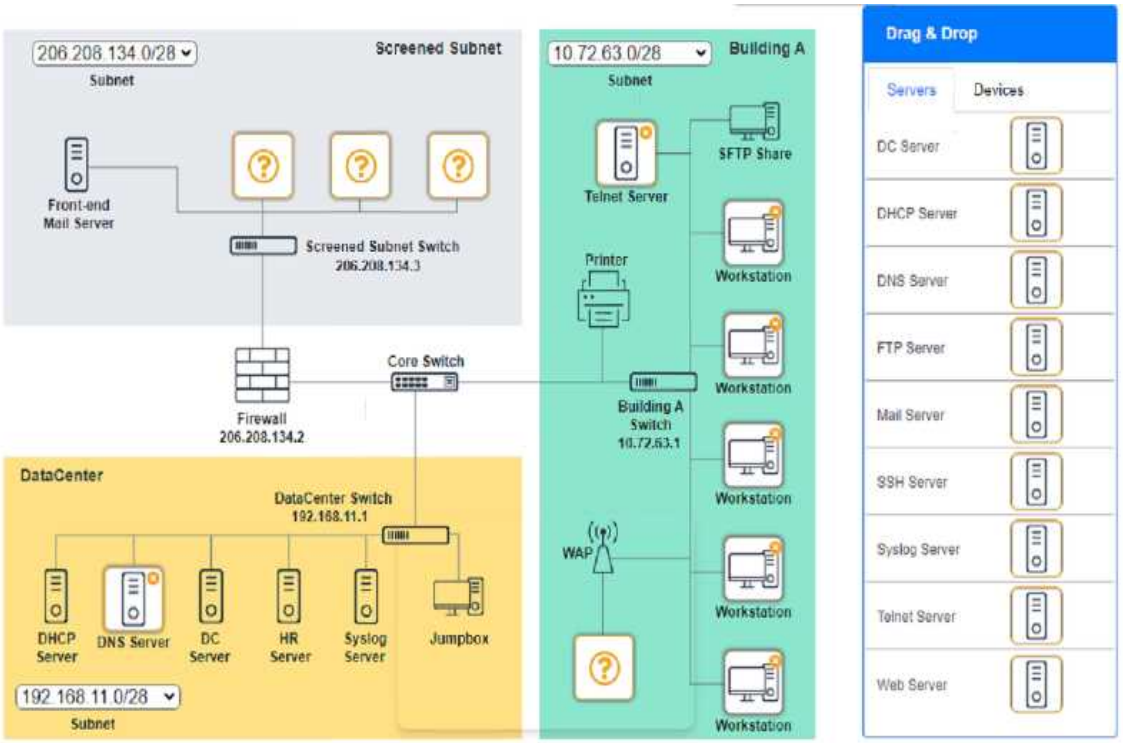
Answer: See explanation below.

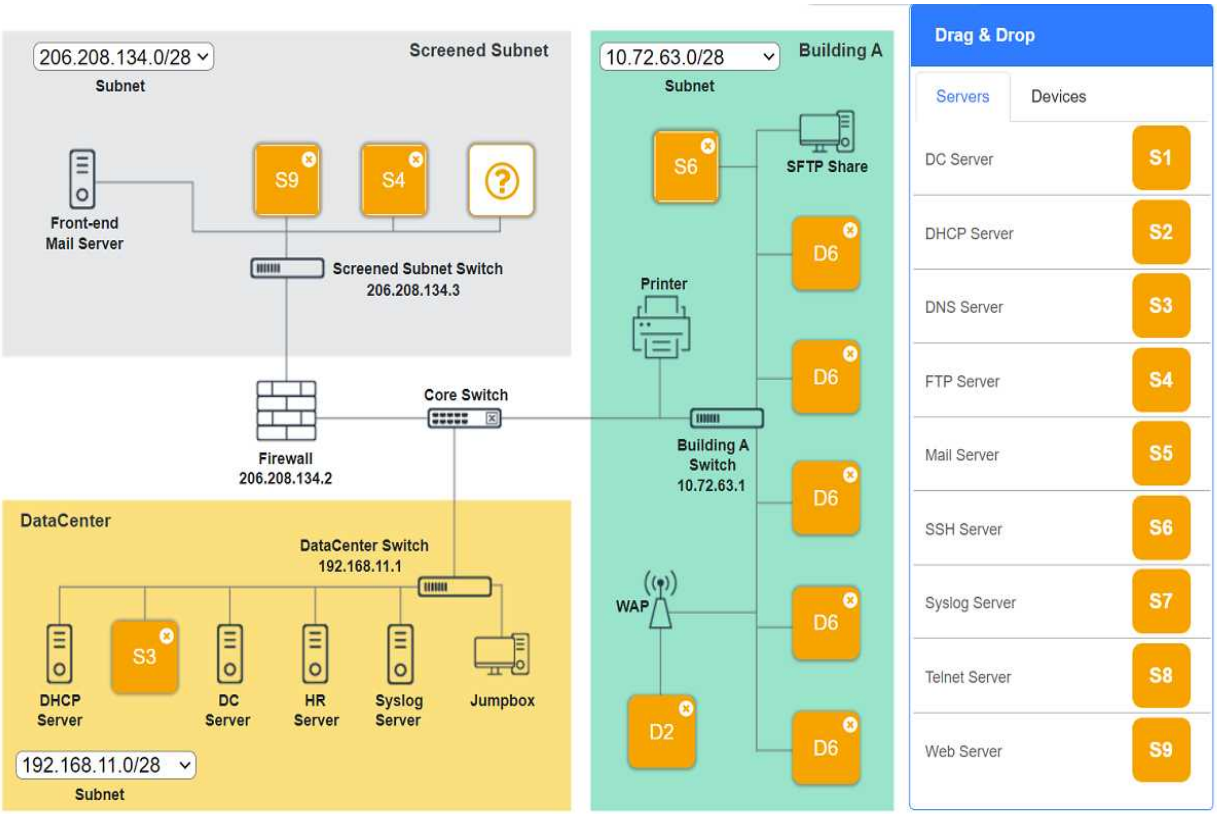
Explanation:

Screened Subnet devices – Web server, FTP server

Building A devices – SSH server top left, workstations on all 5 on the right, laptop on bottom left

DataCenter devices – DNS server.


206.208.134.0/28
Subnet
Screened Subnet
Front-end Mail Server
Screened Subnet Switch 206.208.134.3
Firewall 206.208.134.2
Core Switch
DataCenter
DataCenter Switch 192.168.11.1
DHCP Server
DNS Server
DC Server
HR Server
Syslog Server
Jumpbox
192.168.11.0/28
Subnet
10.72.63.0/28
Subnet
Building A
Telnet Server
SFTP Share
Printer
Workstation
Building A Switch 10.72.63.1
WAP
Drag & Drop
Servers
Devices
DC Server
DHCP Server
DNS Server
FTP Server
Mail Server
SSH Server
Syslog Server
Telnet Server
Web Server


206.208.134.0/28
Subnet
Screened Subnet
Front-end Mail Server
S9
S4
Screened Subnet Switch 206.208.134.3
Firewall 206.208.134.2
Core Switch
DataCenter
DataCenter Switch 192.168.11.1
S3
DHCP Server
DC Server
HR Server
Syslog Server
Jumpbox
192.168.11.0/28
Subnet
10.72.63.0/28
Subnet
Building A
S6
SFTP Share
D6
Printer
Building A Switch 10.72.63.1
WAP
D2
Drag & Drop
Servers
Devices
DC Server
S1
DHCP Server
S2
DNS Server
S3
FTP Server
S4
Mail Server
S5
SSH Server
S6
Syslog Server
S7
Telnet Server
S8
Web Server
S9

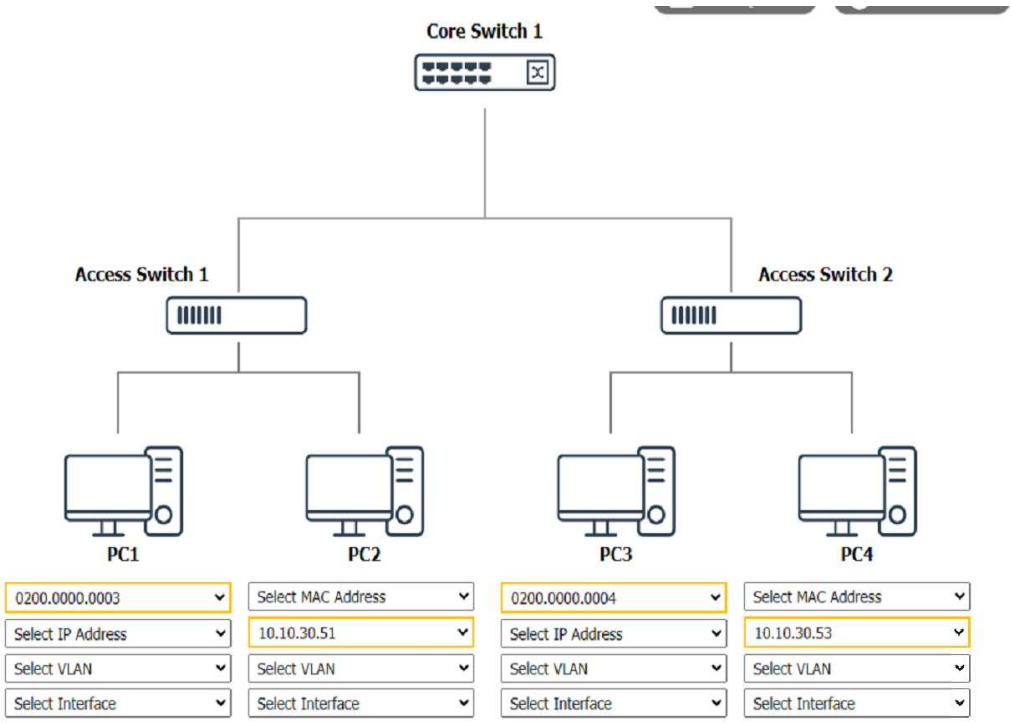
Question: 80

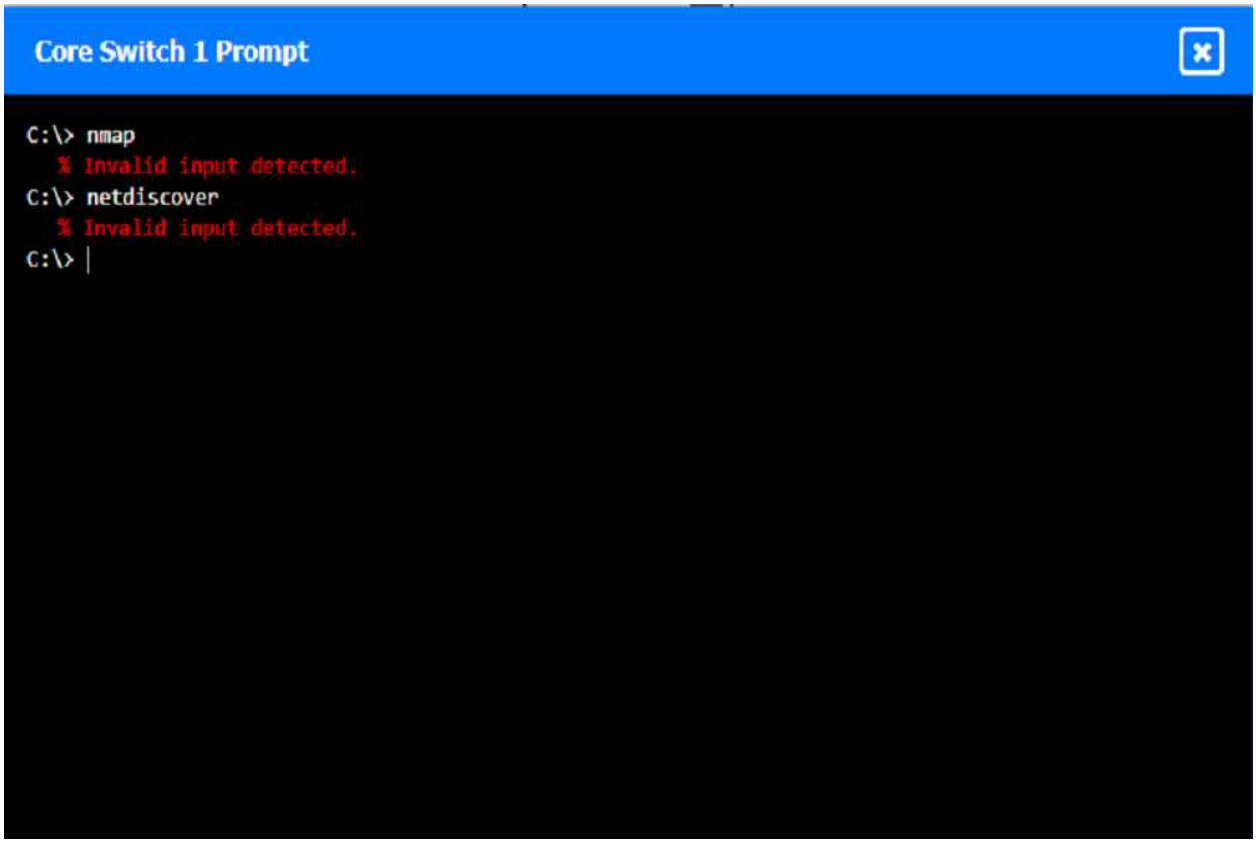
SIMULATION

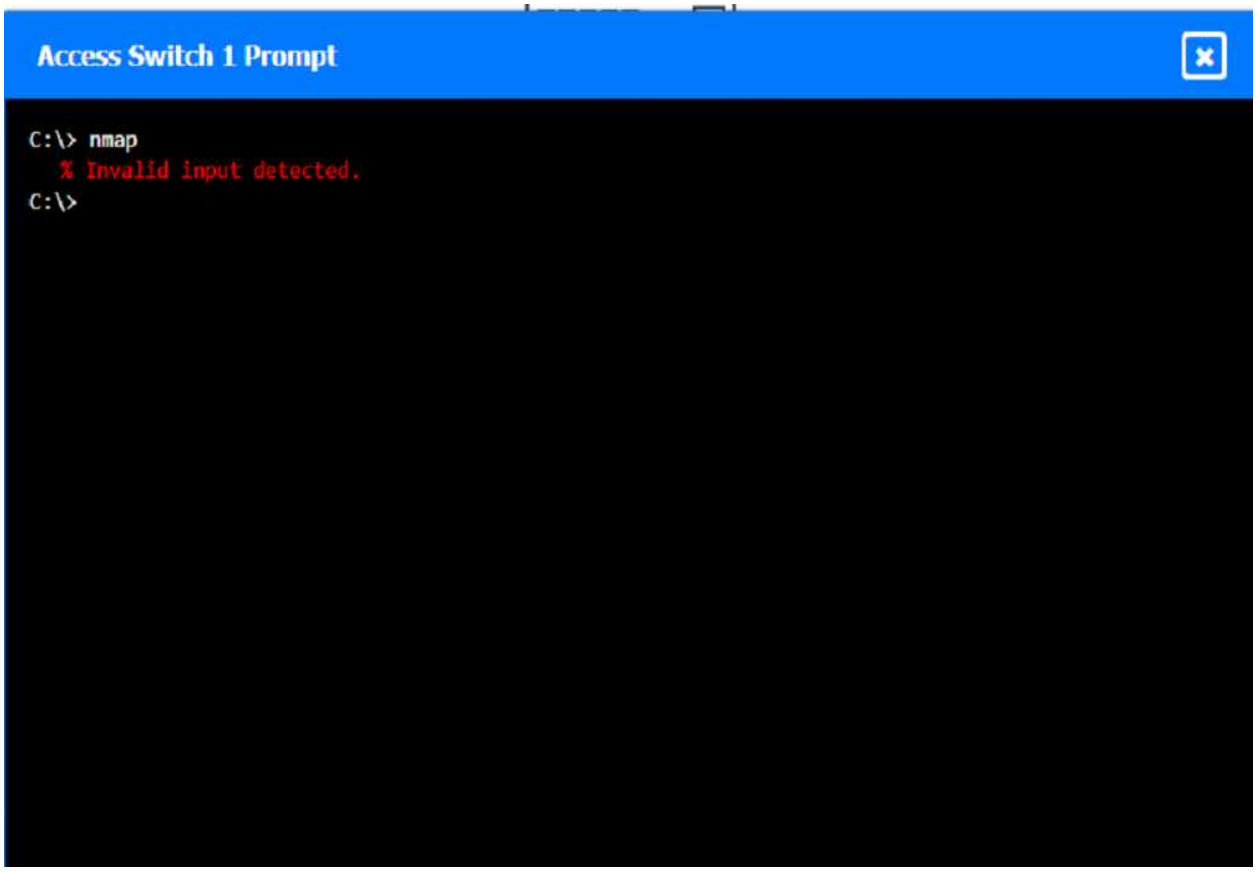
A network technician was recently onboarded to a company. A manager has tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.

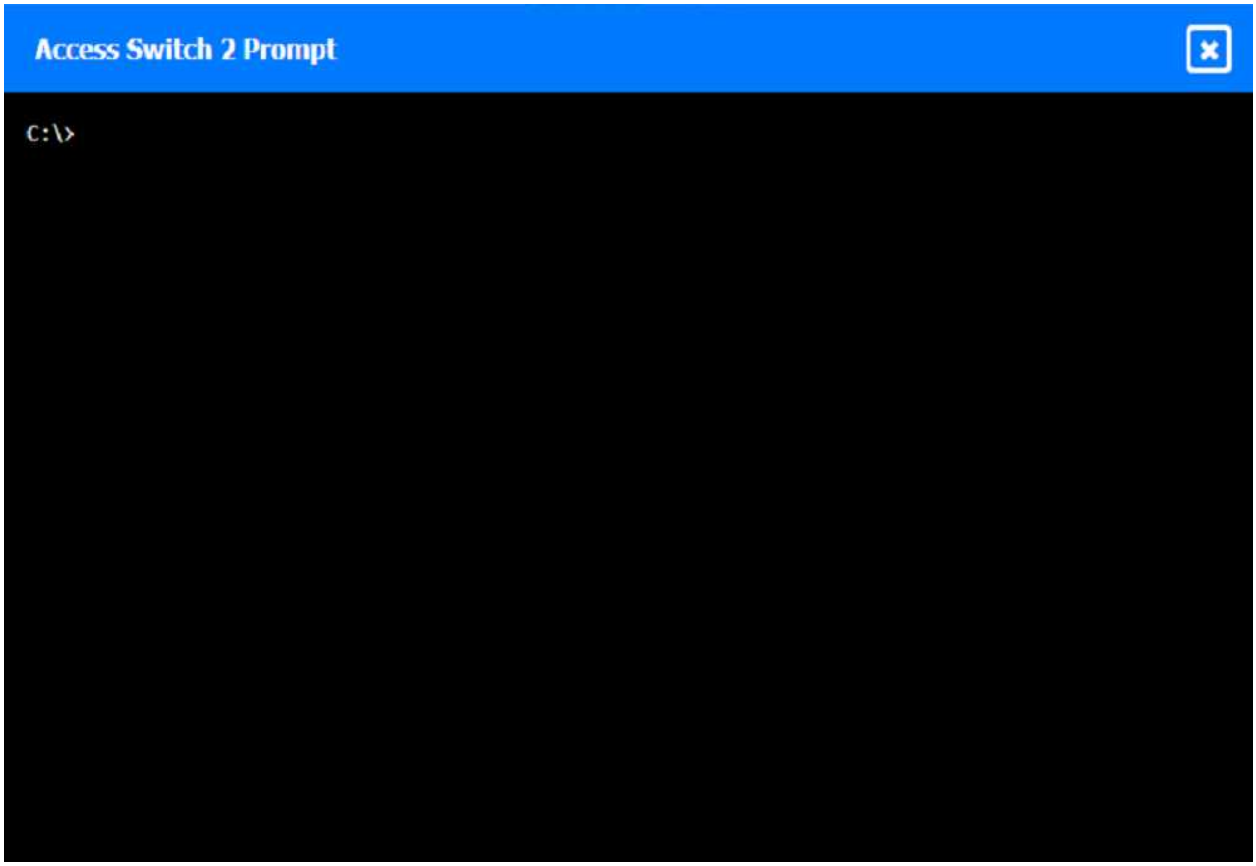
Instructions:

Click on each switch to perform a network discovery by entering commands into the terminal. Fill in the missing information using drop-down menus provided.


Core Switch 1
Access Switch 1
Access Switch 2
PC1
PC2
PC3
PC4
0200.0000.0003
Select MAC Address
0200.0000.0004
Select MAC Address
Select IP Address
10.10.30.51
Select IP Address
10.10.30.53
Select VLAN
Select VLAN
Select VLAN
Select VLAN
Select Interface
Select Interface
Select Interface
Select Interface


Core Switch 1 Prompt
C:\> nmap
% Invalid input detected.
C:\> netdiscover
% Invalid input detected.
C:\>


Access Switch 1 Prompt
C:\> nmap
% Invalid input detected.
C:\>


Access Switch 2 Prompt
C:\>

Answer: See the Explanation for detailed information on this simulation.

Explanation:

(Note: Ips will be change on each simulation task, so we have given example answer for the understanding)

To perform a network discovery by entering commands into the terminal, you can use the following steps:

Click on each switch to open its terminal window.

Enter the command show ip interface brief to display the IP addresses and statuses of the switch interfaces.

Enter the command show vlan brief to display the VLAN configurations and assignments of the switch interfaces.

Enter the command show cdp neighbors to display the information about the neighboring devices that are connected to the switch.

Fill in the missing information in the diagram using the drop-down menus provided.

Here is an example of how to fill in the missing information for Core Switch 1:

The IP address of Core Switch 1 is 192.168.1.1.

The VLAN configuration of Core Switch 1 is VLAN 1: 192.168.1.0/24, VLAN 2: 192.168.2.0/24, VLAN 3: 192.168.3.0/24.

The neighboring devices of Core Switch 1 are Access Switch 1 and Access Switch 2.

The interfaces that connect Core Switch 1 to Access Switch 1 are GigabitEthernet0/1 and GigabitEthernet0/2.

The interfaces that connect Core Switch 1 to Access Switch 2 are GigabitEthernet0/3 and GigabitEthernet0/4.

You can use the same steps to fill in the missing information for Access Switch 1 and Access Switch 2.

Question: 81

SIMULATION

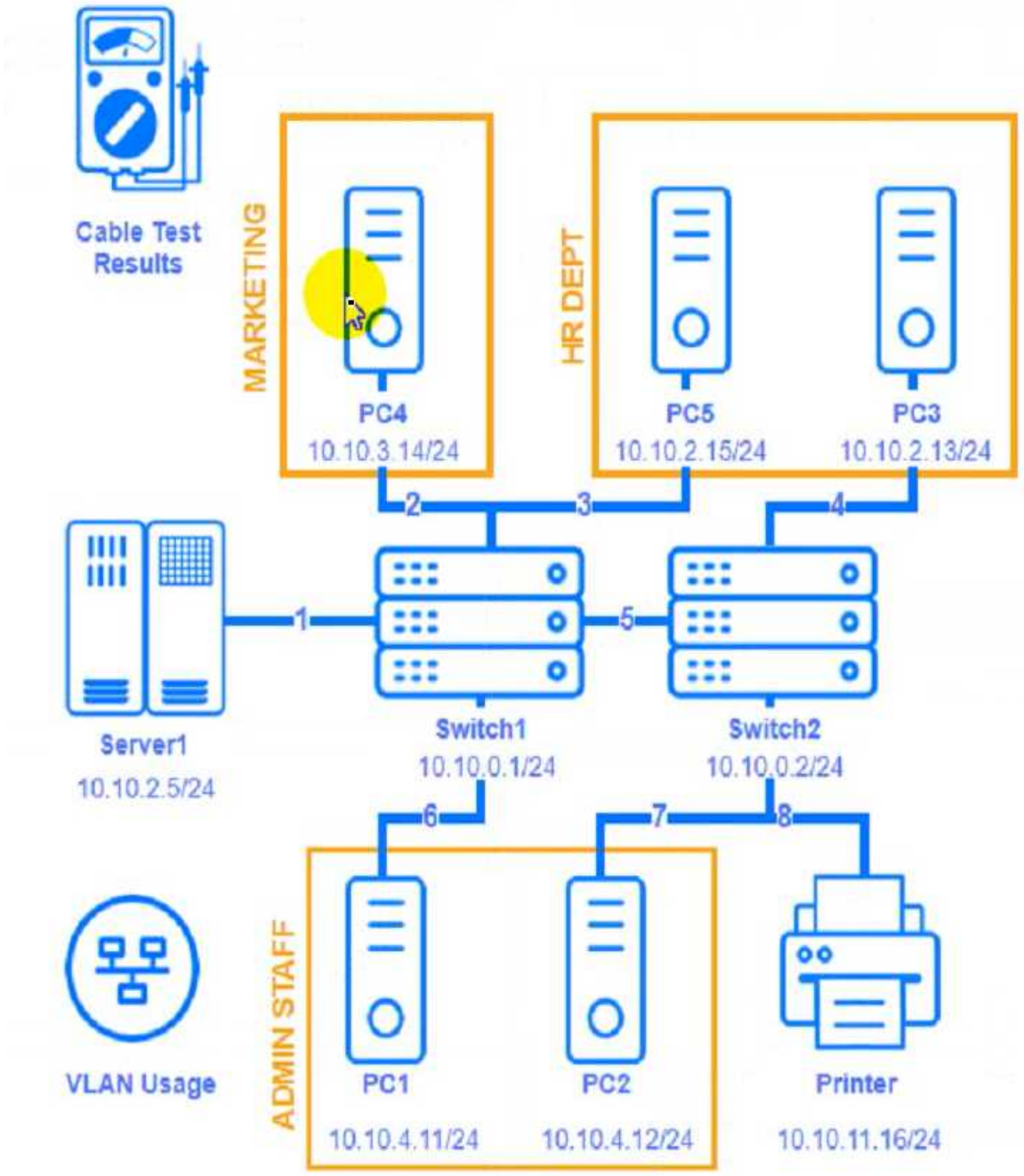
A network technician needs to resolve some issues with a customer's SOHO network.

The customer reports that some of the devices are not connecting to the network, while others appear to work as intended.

INSTRUCTIONS

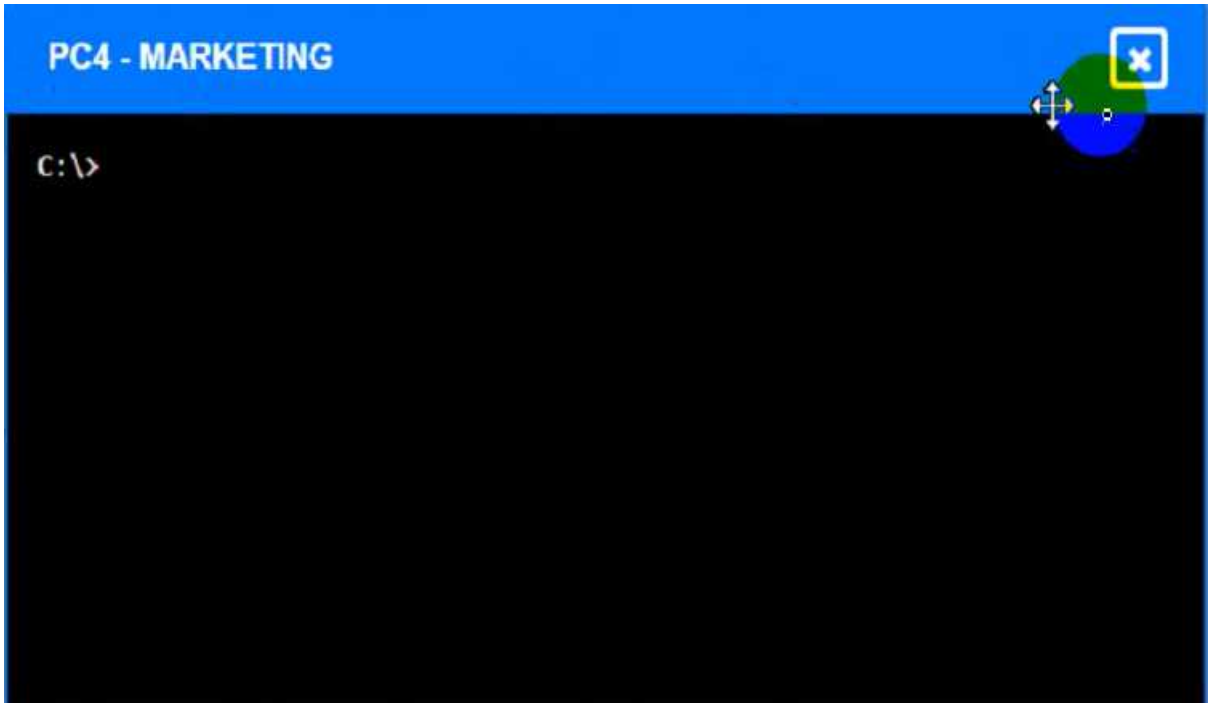
Troubleshoot all the network components and review the cable test results by Clicking on each device and cable.

Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.


Cable Test Results
MARKETING
PC4
10.10.3.14/24
HR DEPT
PC5
10.10.2.15/24
PC3
10.10.2.13/24
2
3
4
1
5
Server1
10.10.2.5/24
Switch1
10.10.0.1/24
Switch2
10.10.0.2/24
6
7
8
VLAN Usage
ADMIN STAFF
PC1
10.10.4.11/24
PC2
10.10.4.12/24
Printer
10.10.11.16/24


PC1 - ADMIN STAFF
C:\>

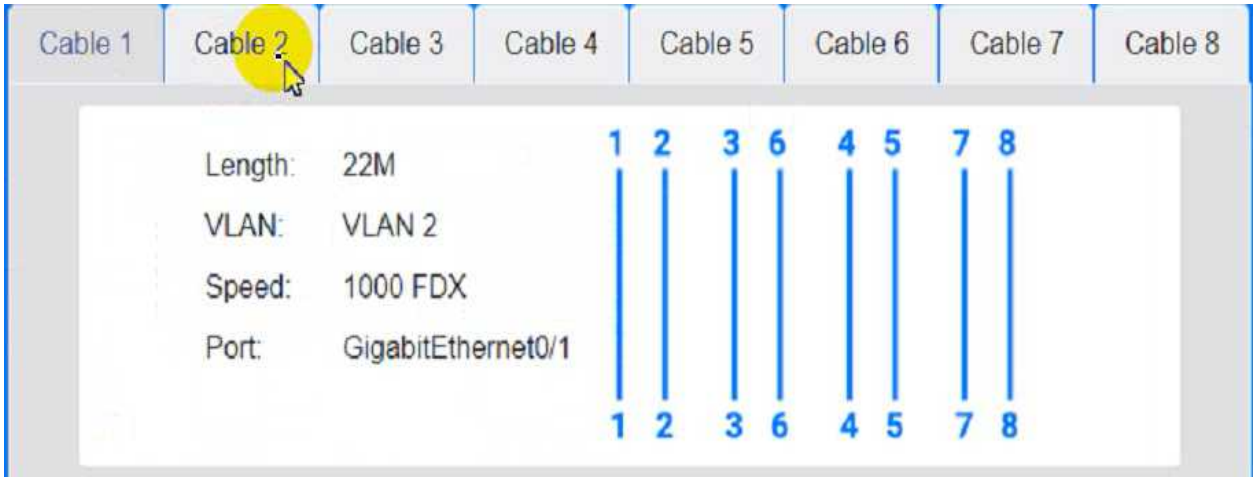

PC3 - HR DEPT
C:\>


PC4 - MARKETING
C:\>

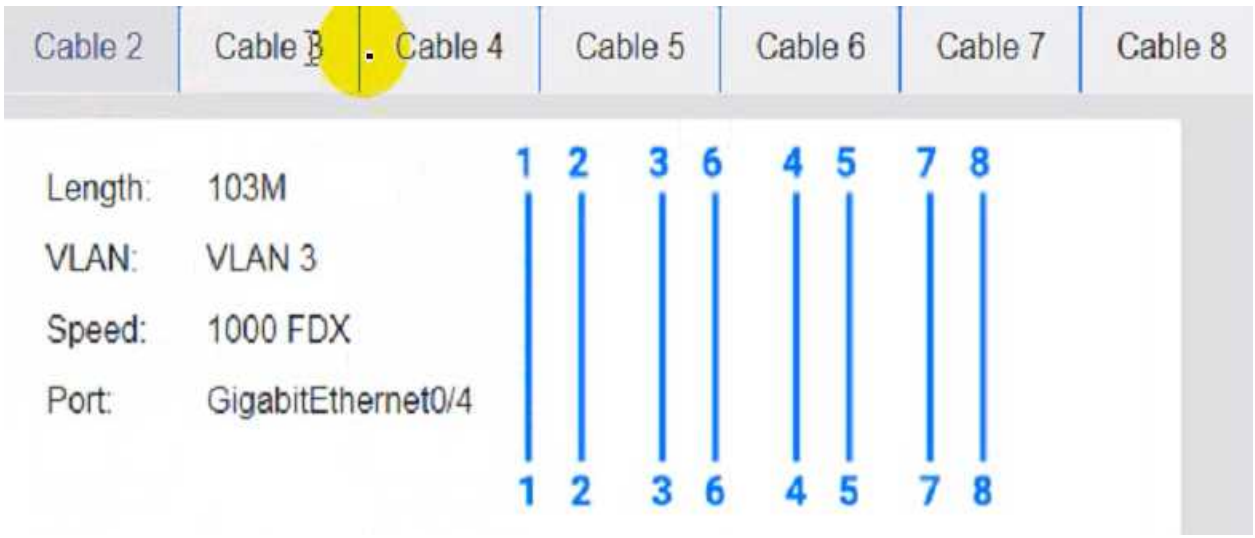

PC5 - HR DEPT
C:\>

Cable Test Results:

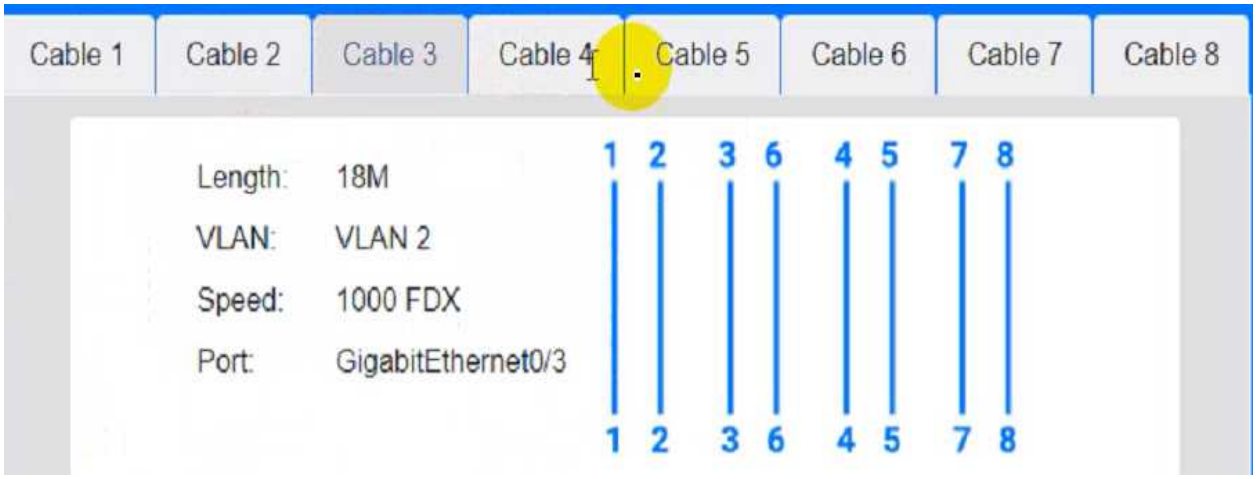
Cable 1:



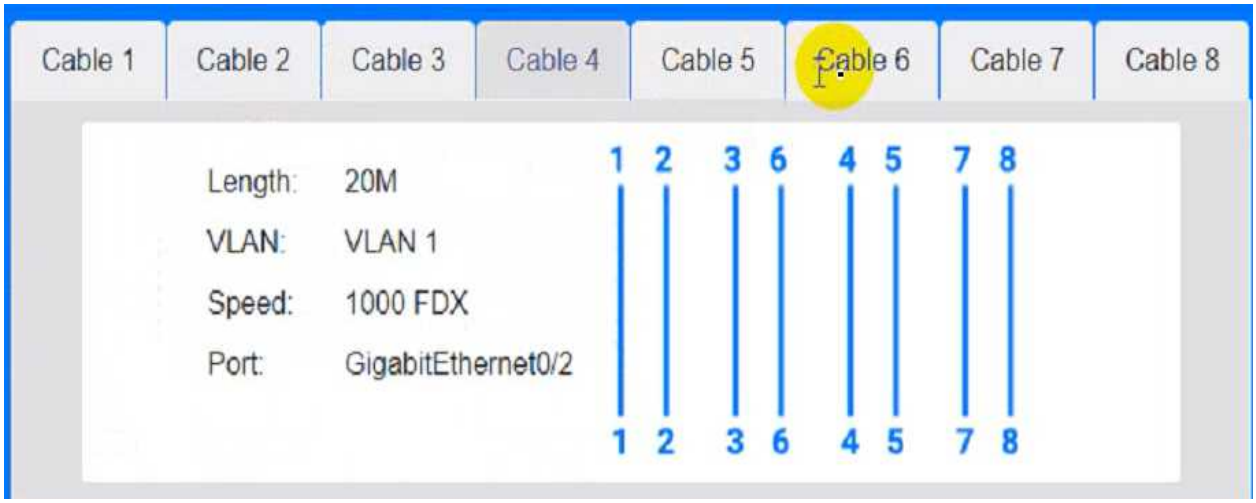
Cable 2:

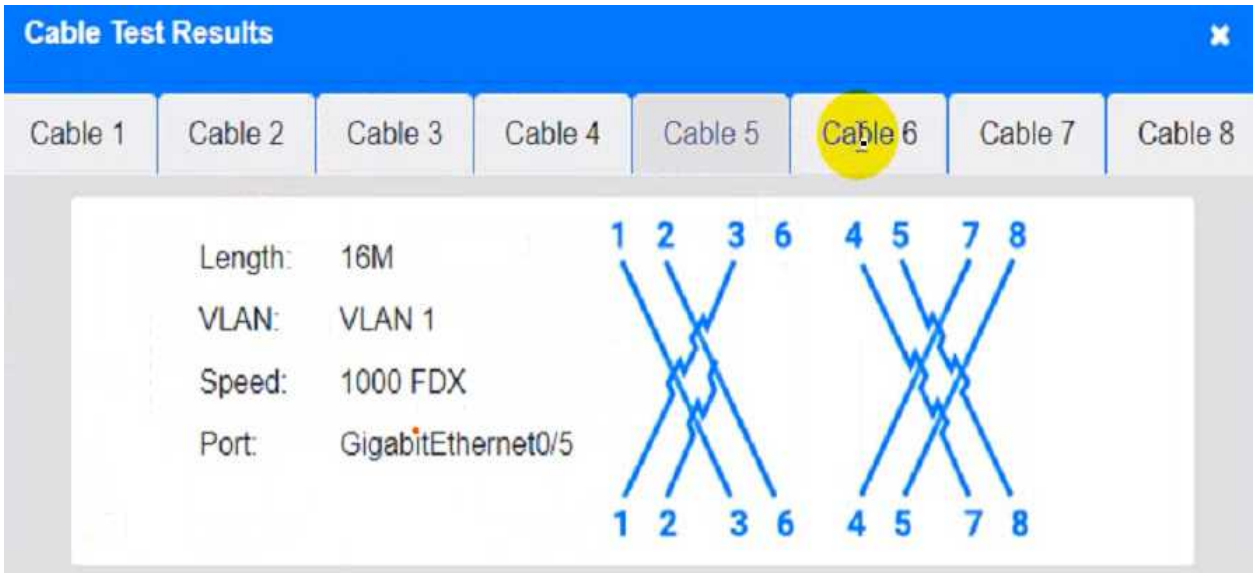


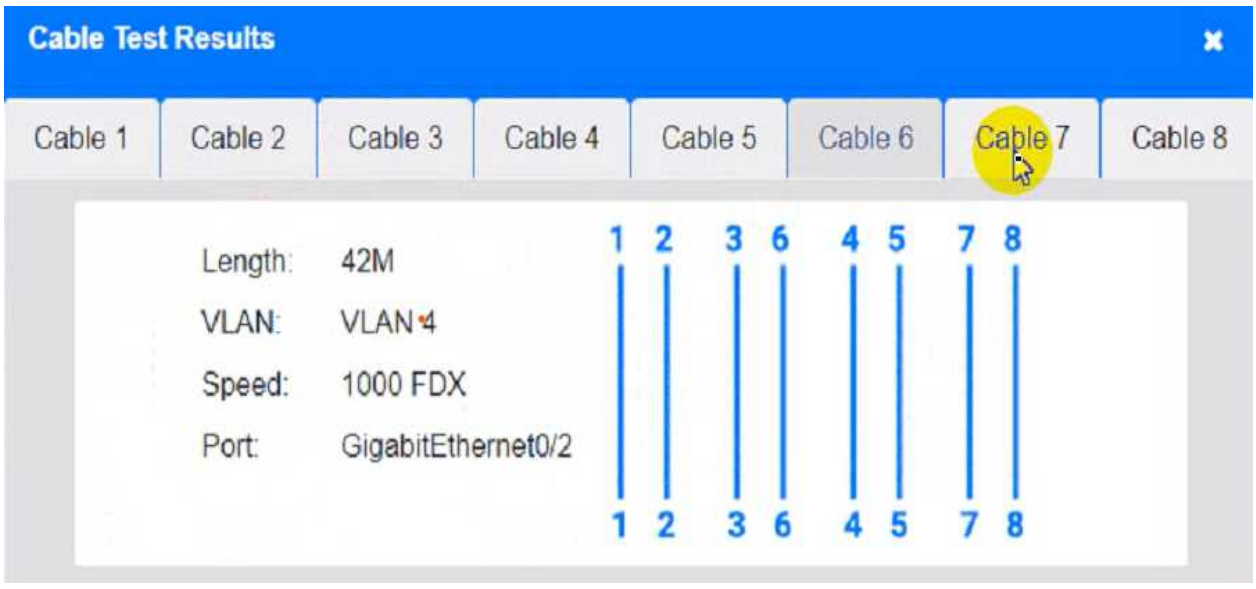
Cable 3:

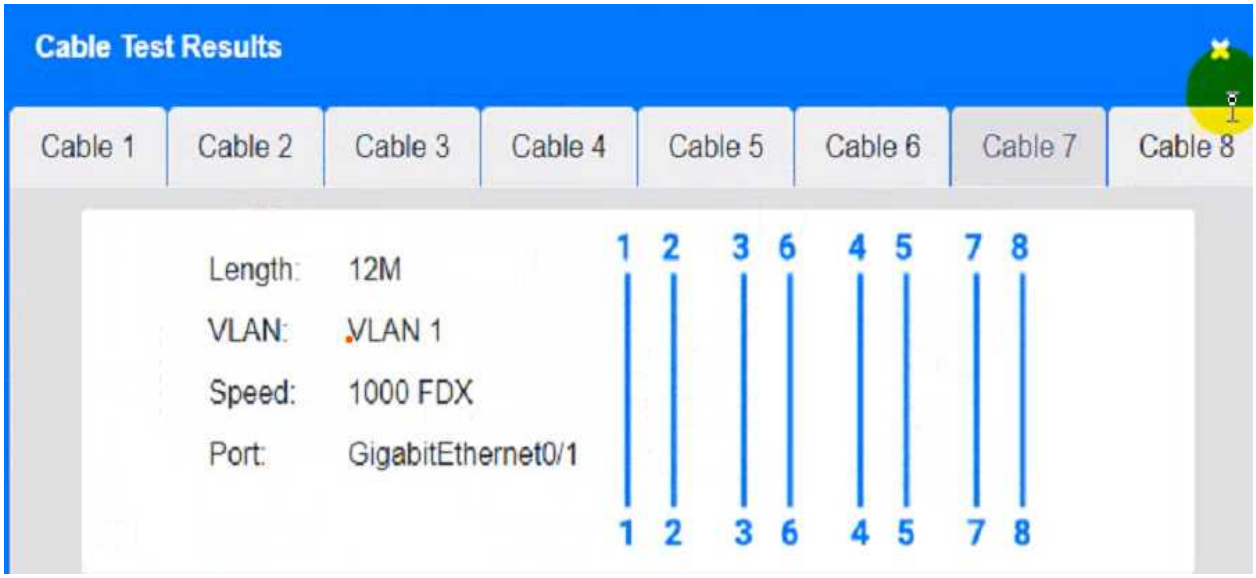


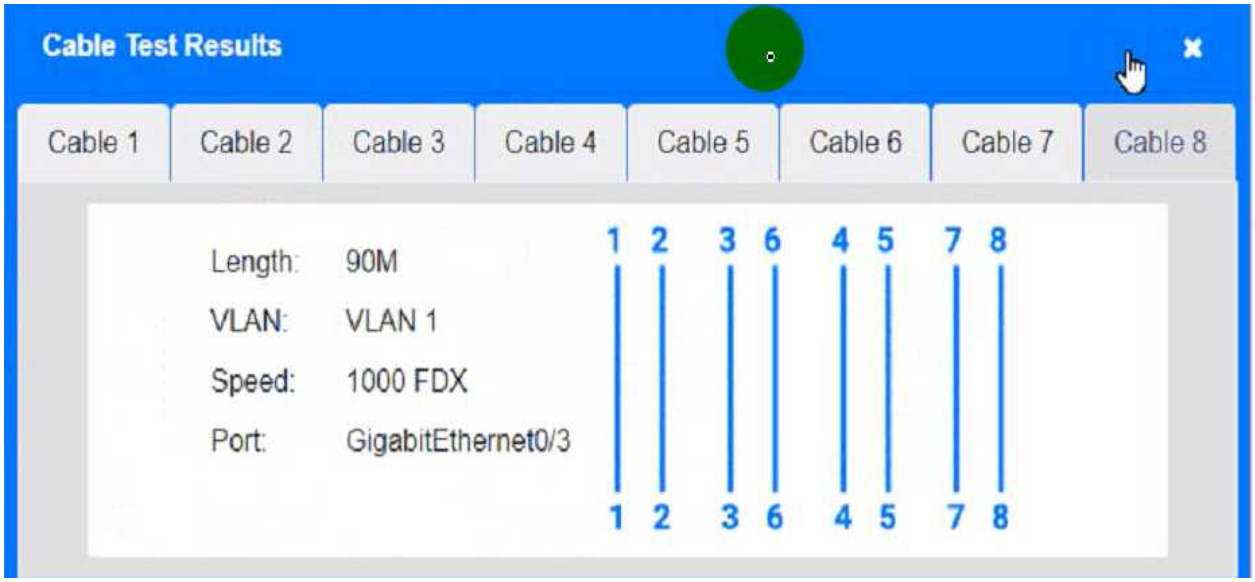
Cable 4:

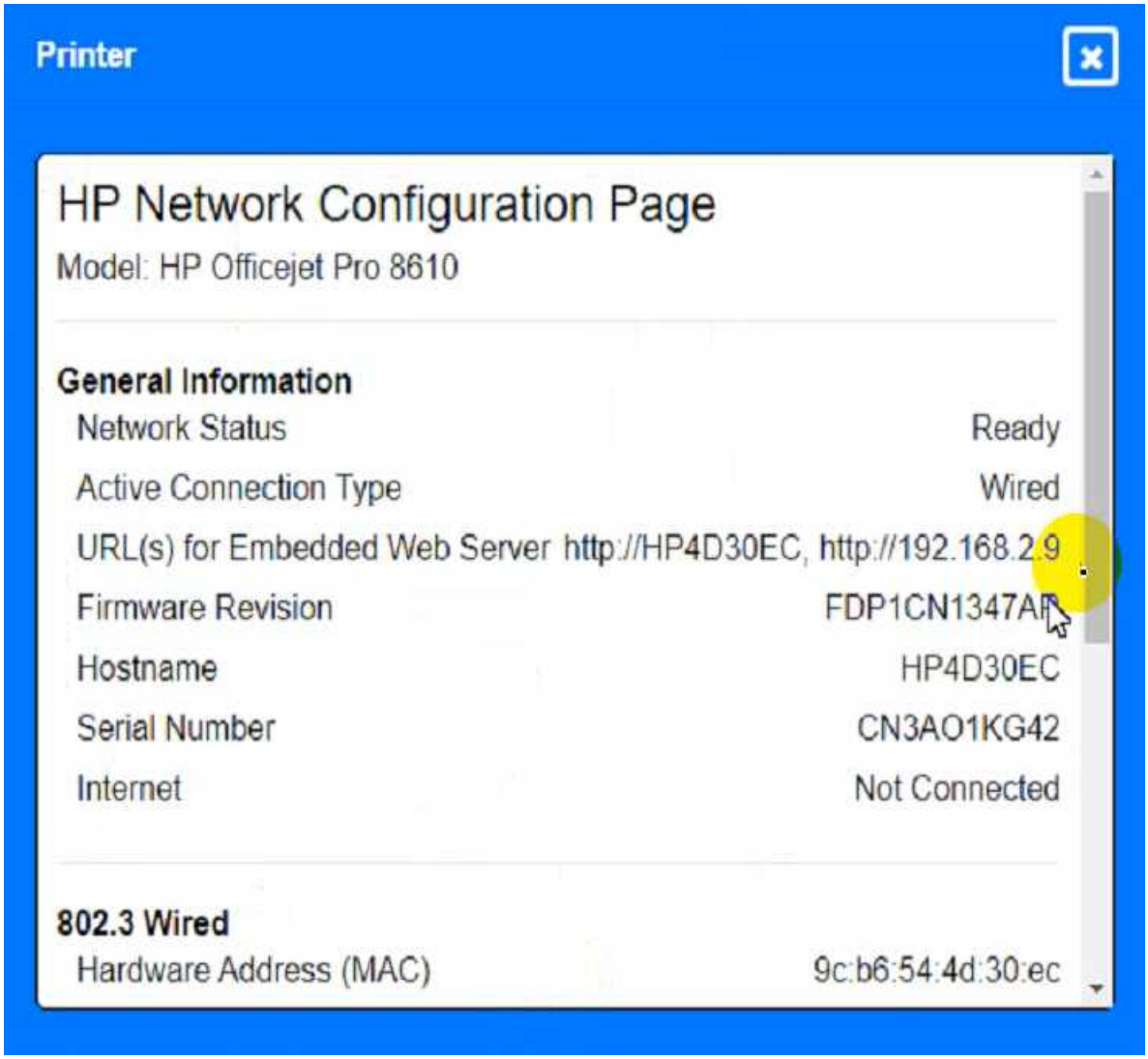

Cable 1
Cable 2
Cable 3
Cable 4
Cable 5
Cable 6
Cable 7
Cable 8
Length: 20M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/2
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

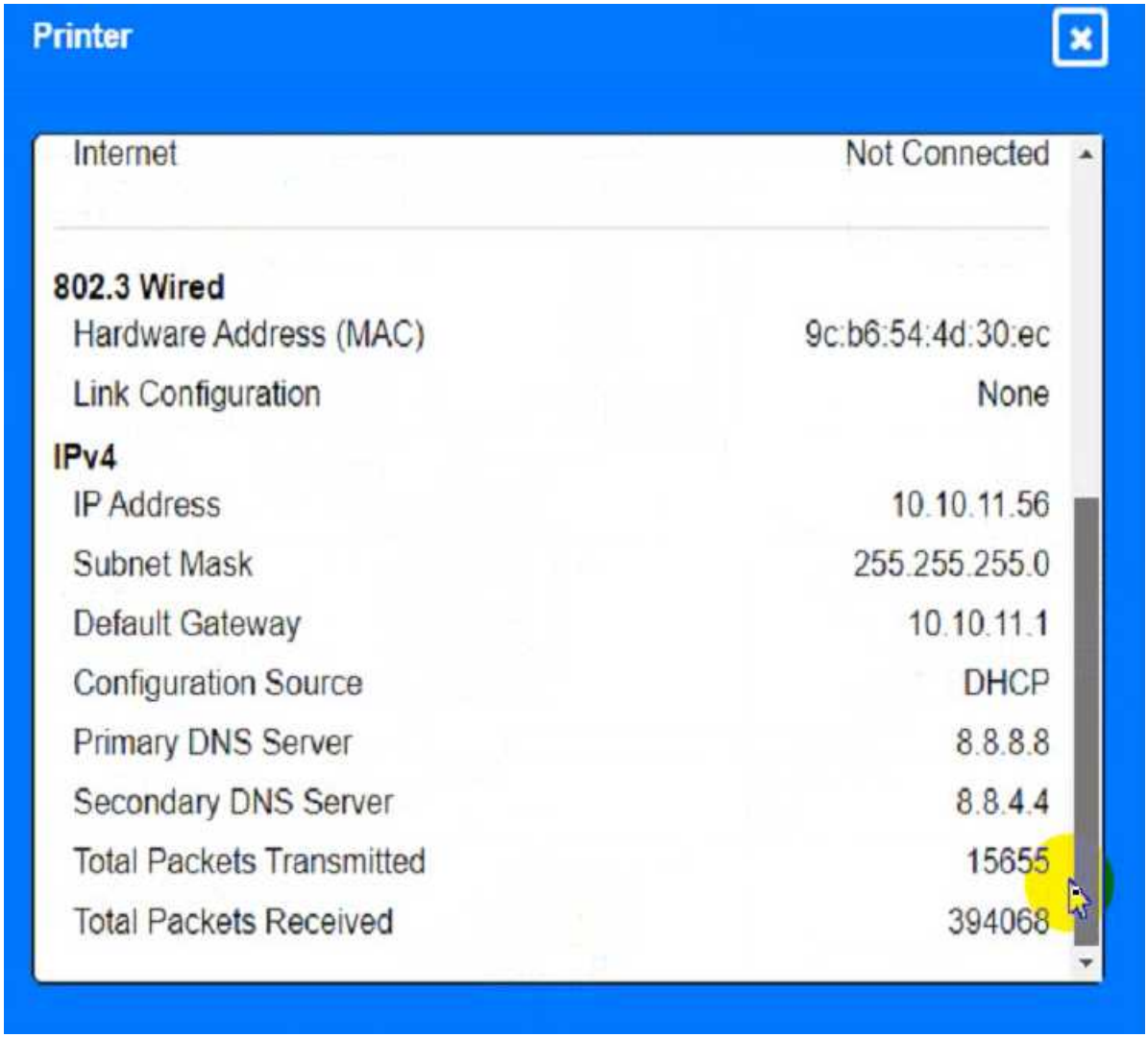

Cable Test Results
Cable 1
Cable 2
Cable 3
Cable 4
Cable 5
Cable 6
Cable 7
Cable 8
Length: 16M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/5
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

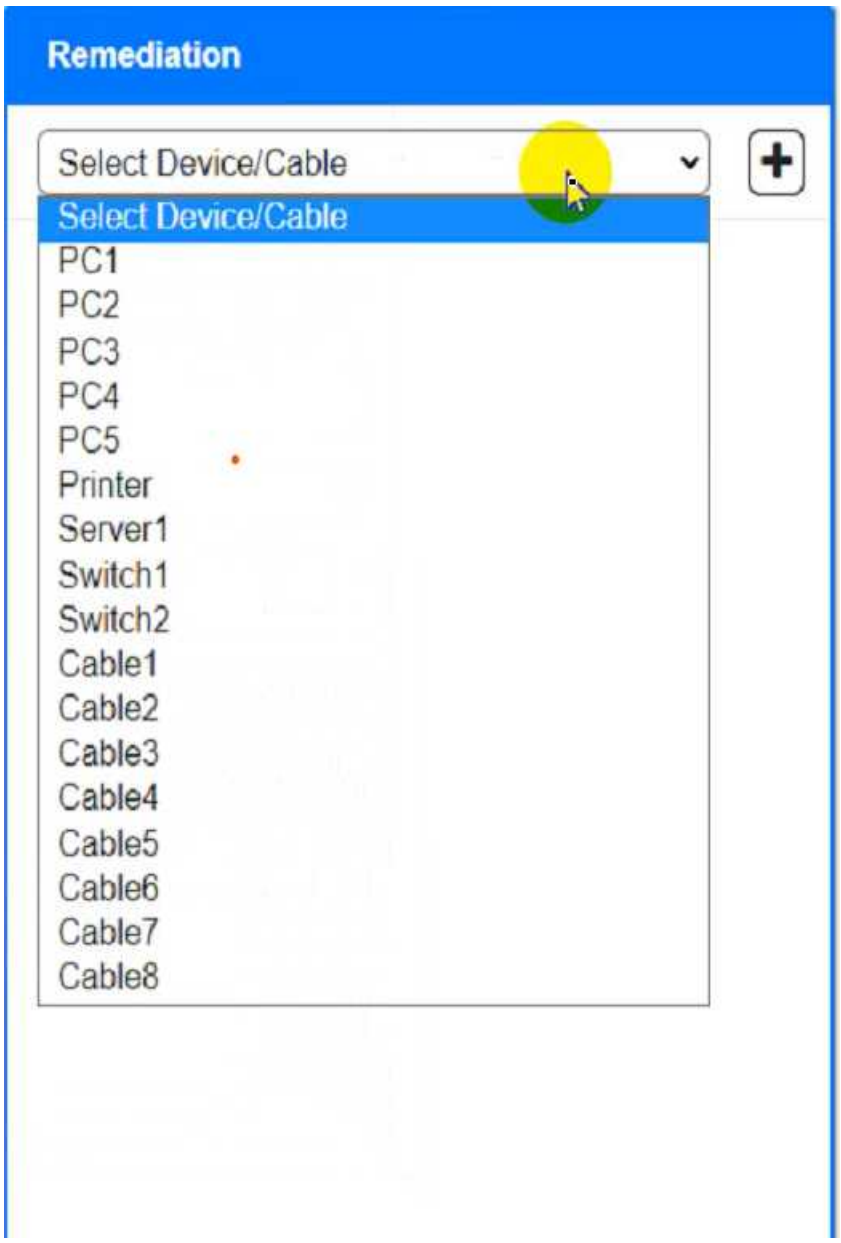

Cable Test Results
Cable 1
Cable 2
Cable 3
Cable 4
Cable 5
Cable 6
Cable 7
Cable 8
Length: 42M
VLAN: VLAN 4
Speed: 1000 FDX
Port: GigabitEthernet0/2
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


Cable Test Results
Cable 1
Cable 2
Cable 3
Cable 4
Cable 5
Cable 6
Cable 7
Cable 8
Length: 12M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/1
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


Cable Test Results
Cable 1
Cable 2
Cable 3
Cable 4
Cable 5
Cable 6
Cable 7
Cable 8
Length: 90M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/3
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


Printer
HP Network Configuration Page
Model: HP Officejet Pro 8610
General Information
Network Status Ready
Active Connection Type Wired
URL(s) for Embedded Web Server http://HP4D30EC, http://192.168.2.9
Firmware Revision FDP1CN1347AR
Hostname HP4D30EC
Serial Number CN3AO1KG42
Internet Not Connected
802.3 Wired
Hardware Address (MAC) 9c:b6:54:4d:30:ec


Printer
Internet
Not Connected
802.3 Wired
Hardware Address (MAC)
9c:b6:54:4d:30:ec
Link Configuration
None
IPv4
IP Address
10.10.11.56
Subnet Mask
255.255.255.0
Default Gateway
10.10.11.1
Configuration Source
DHCP
Primary DNS Server
8.8.8.8
Secondary DNS Server
8.8.4.4
Total Packets Transmitted
15655
Total Packets Received
394068



Answer: See the Explanation for detailed information on this simulation.

Explanation:

(Note: Ips will be change on each simulation task, so we have given example answer for the understanding)

To troubleshoot all the network components and review the cable test results, you can use the

following steps:

Click on each device and cable to open its information window.

Review the information and identify any problems or errors that may affect the network connectivity or performance.

Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.

Fill in the remediation form using the drop-down menus provided.

Here is an example of how to fill in the remediation form for PC1:

The component with a problem is PC1.

The problem is Incorrect IP address.

The solution is Change the IP address to 192.168.1.10.

You can use the same steps to fill in the remediation form for other components.

To enter commands in each device, you can use the following steps:

Click on the device to open its terminal window.

Enter the command ipconfig /all to display the IP configuration of the device, including its IP address, subnet mask, default gateway, and DNS servers.

Enter the command ping <IP address> to test the connectivity and reachability to another device on the network by sending and receiving echo packets. Replace <IP address> with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.

Enter the command tracert <IP address> to trace the route and measure the latency of packets from the device to another device on the network by sending and receiving packets with increasing TTL values. Replace <IP address> with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.

Here is an example of how to enter commands in PC1:

Click on PC1 to open its terminal window.

Enter the command ipconfig /all to display the IP configuration of PC1. You should see that PC1 has an incorrect IP address of 192.168.2.10, which belongs to VLAN 2 instead of VLAN 1.

Enter the command ping 192.168.1.1 to test the connectivity to Core Switch 1. You should see that PC1 is unable to ping Core Switch 1 because they are on different subnets.

Enter the command tracert 192.168.1.1 to trace the route to Core Switch 1. You should see that PC1 is unable to reach Core Switch 1 because there is no route between them.

You can use the same steps to enter commands in other devices, such as PC3, PC4, PC5, and Server 1.

Question: 82

SIMULATION

A network technician needs to resolve some issues with a customer's SOHO network. The customer reports that some of the PCs are not connecting to the network, while others appear to be working as intended.

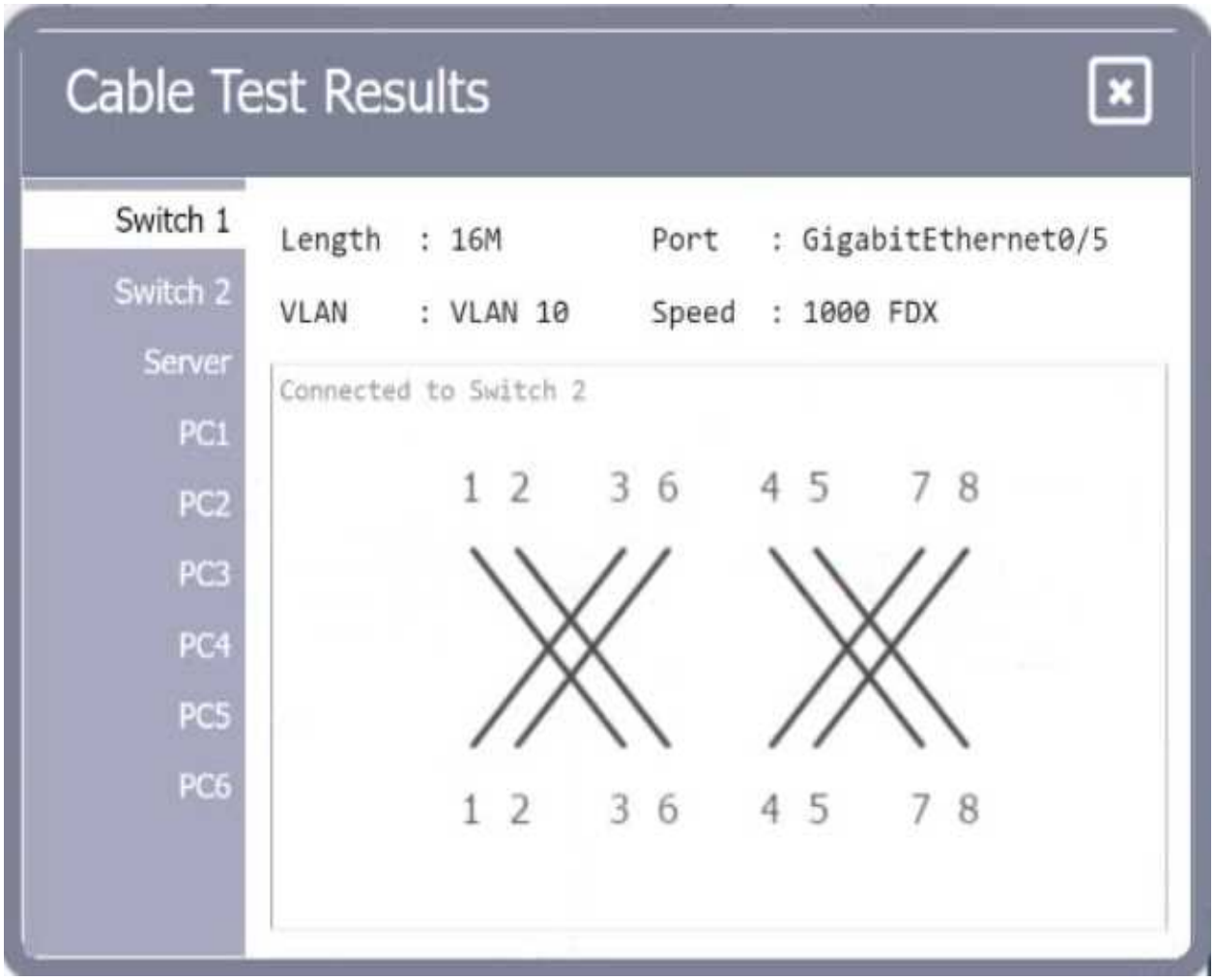
INSTRUCTIONS

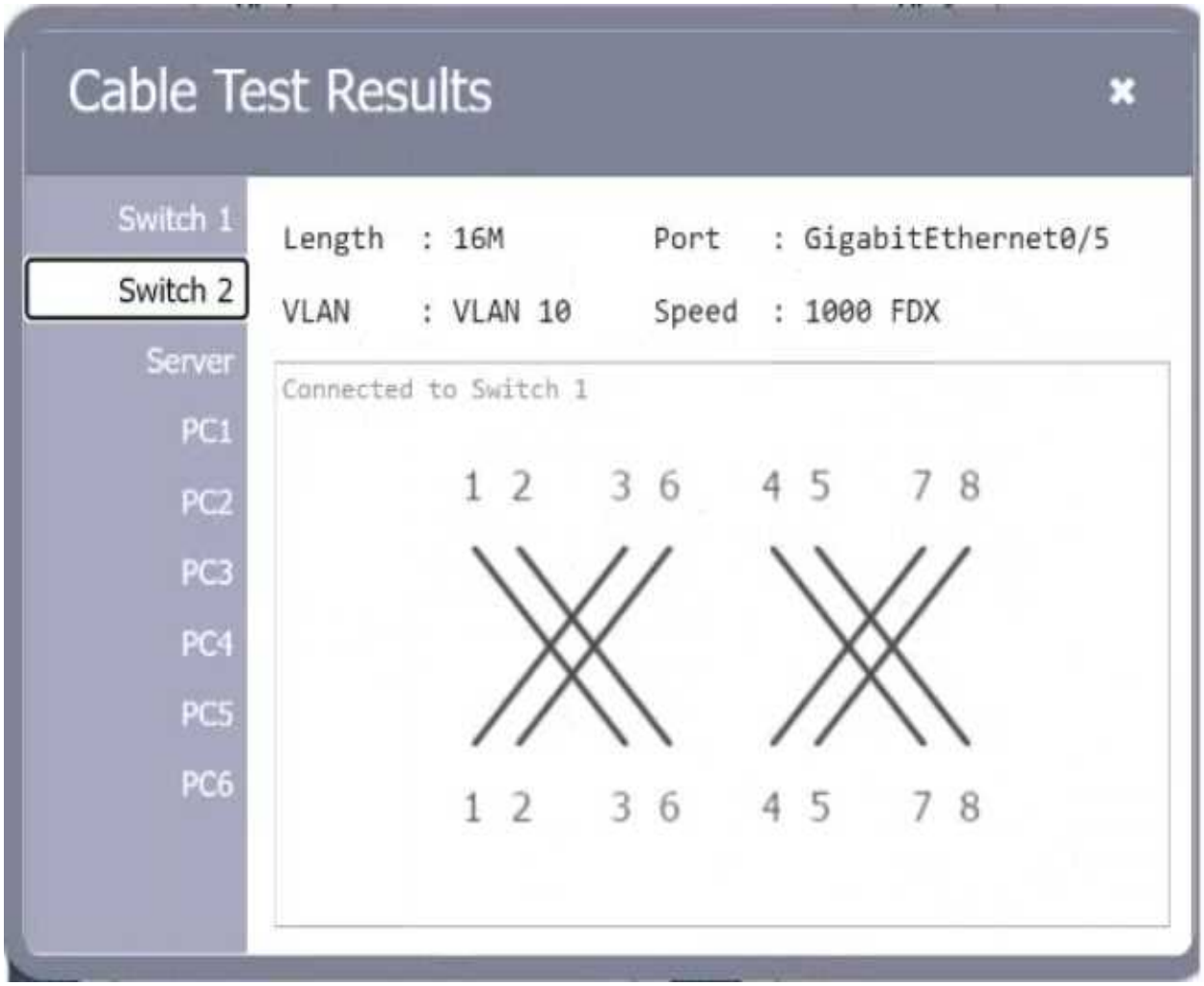
Troubleshoot all the network components.

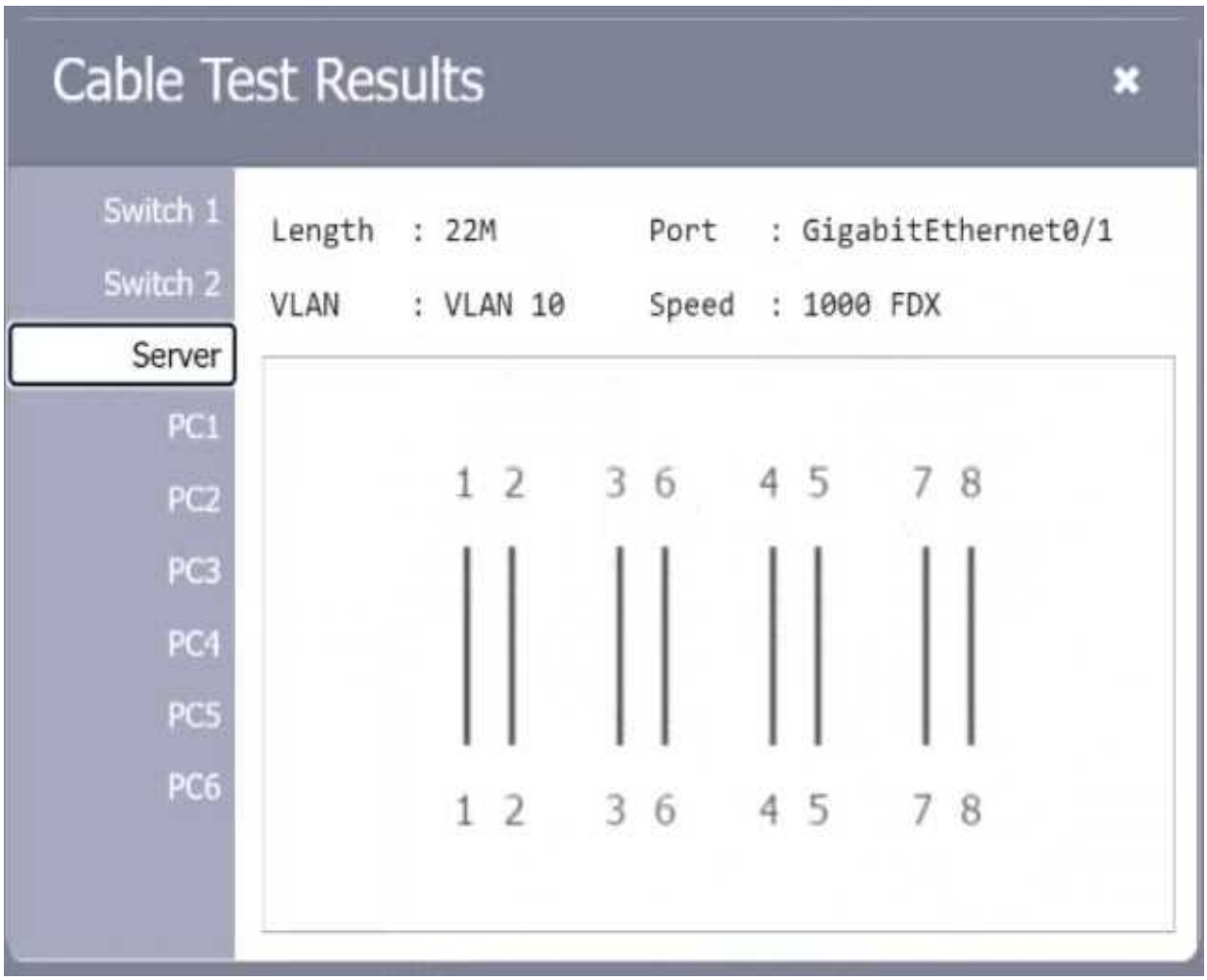
Review the cable test results first, then diagnose by clicking on the appropriate PC, server, and Layer 2 switch.

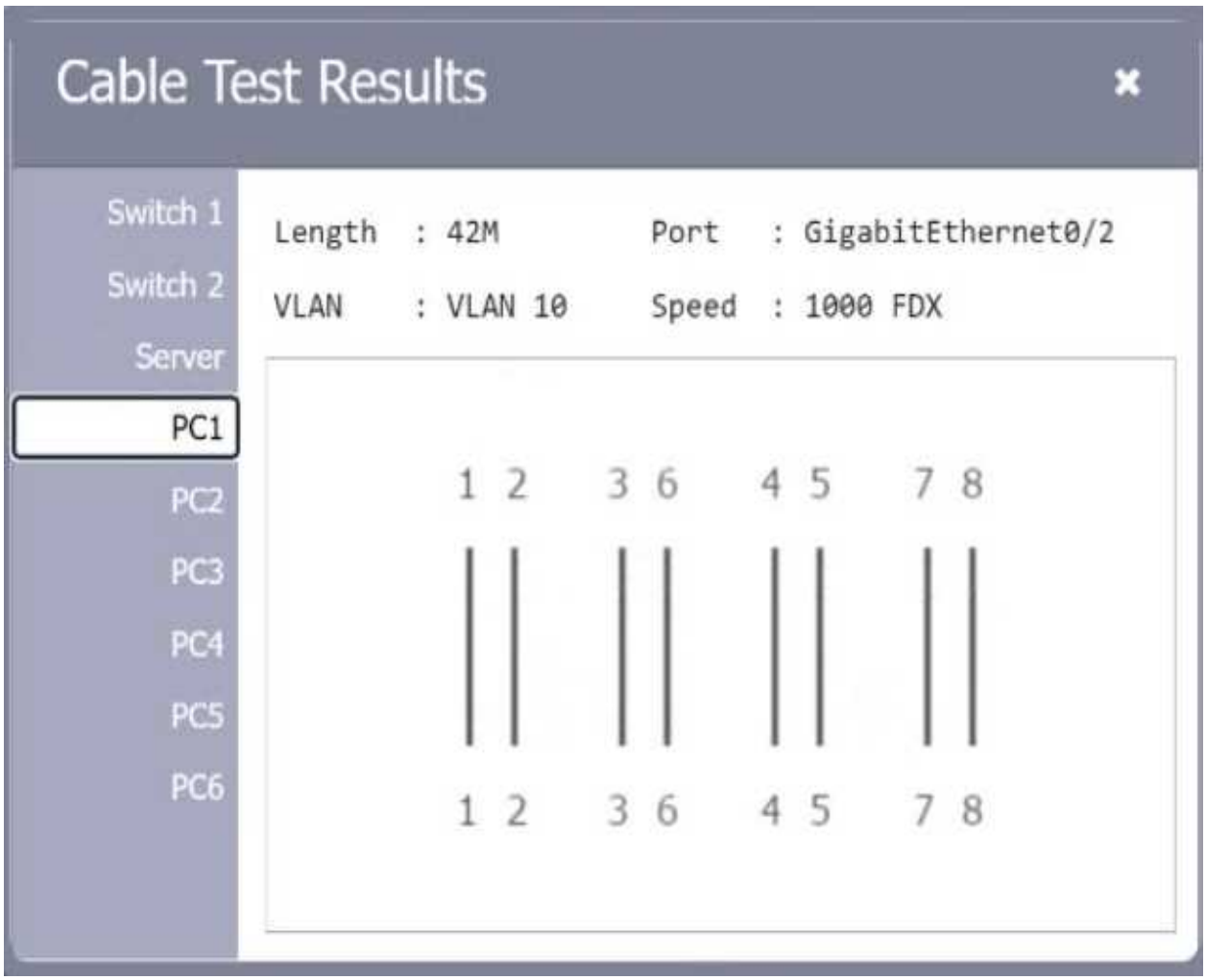
Identify any components with a problem and recommend a solution to correct each problem.

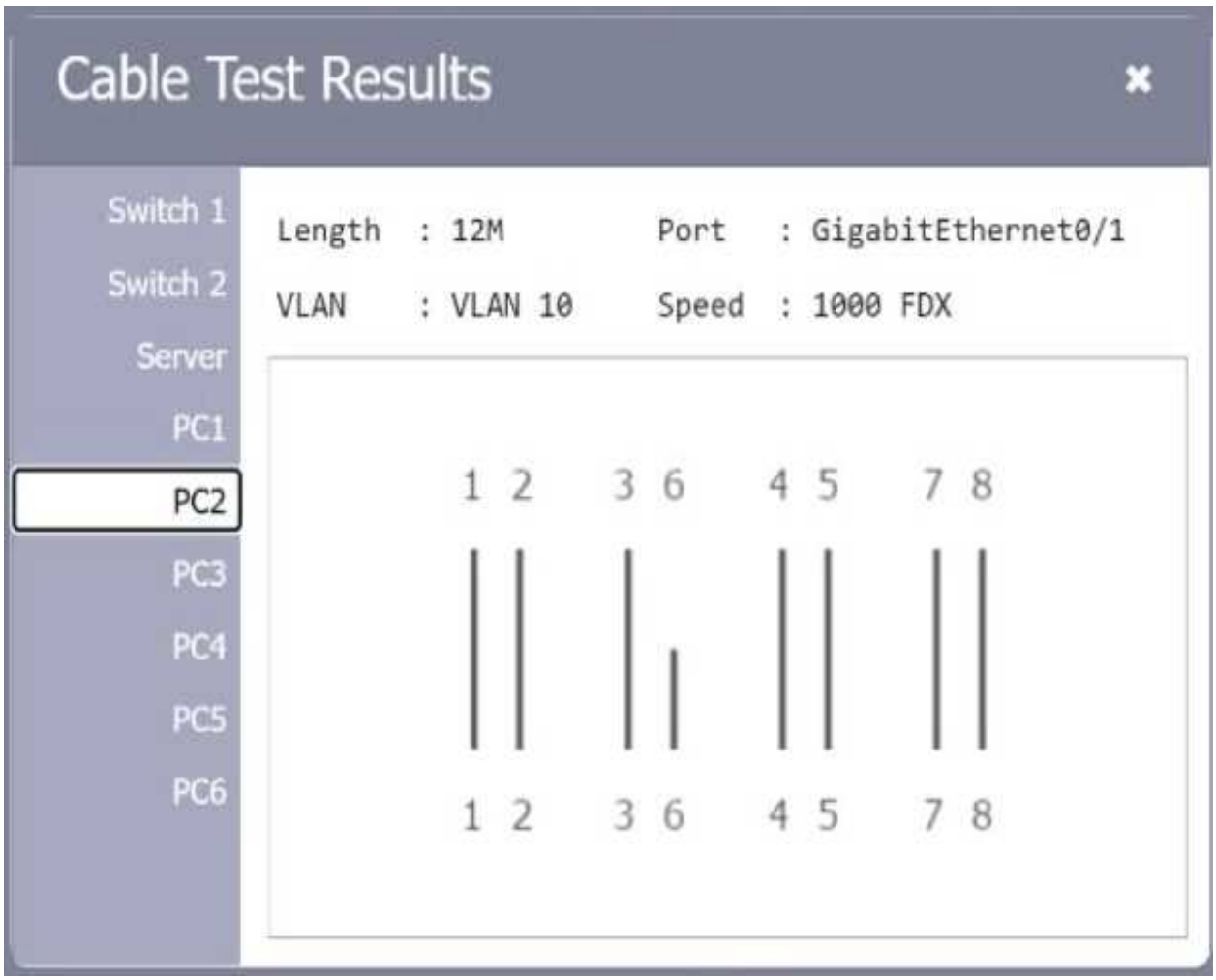
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

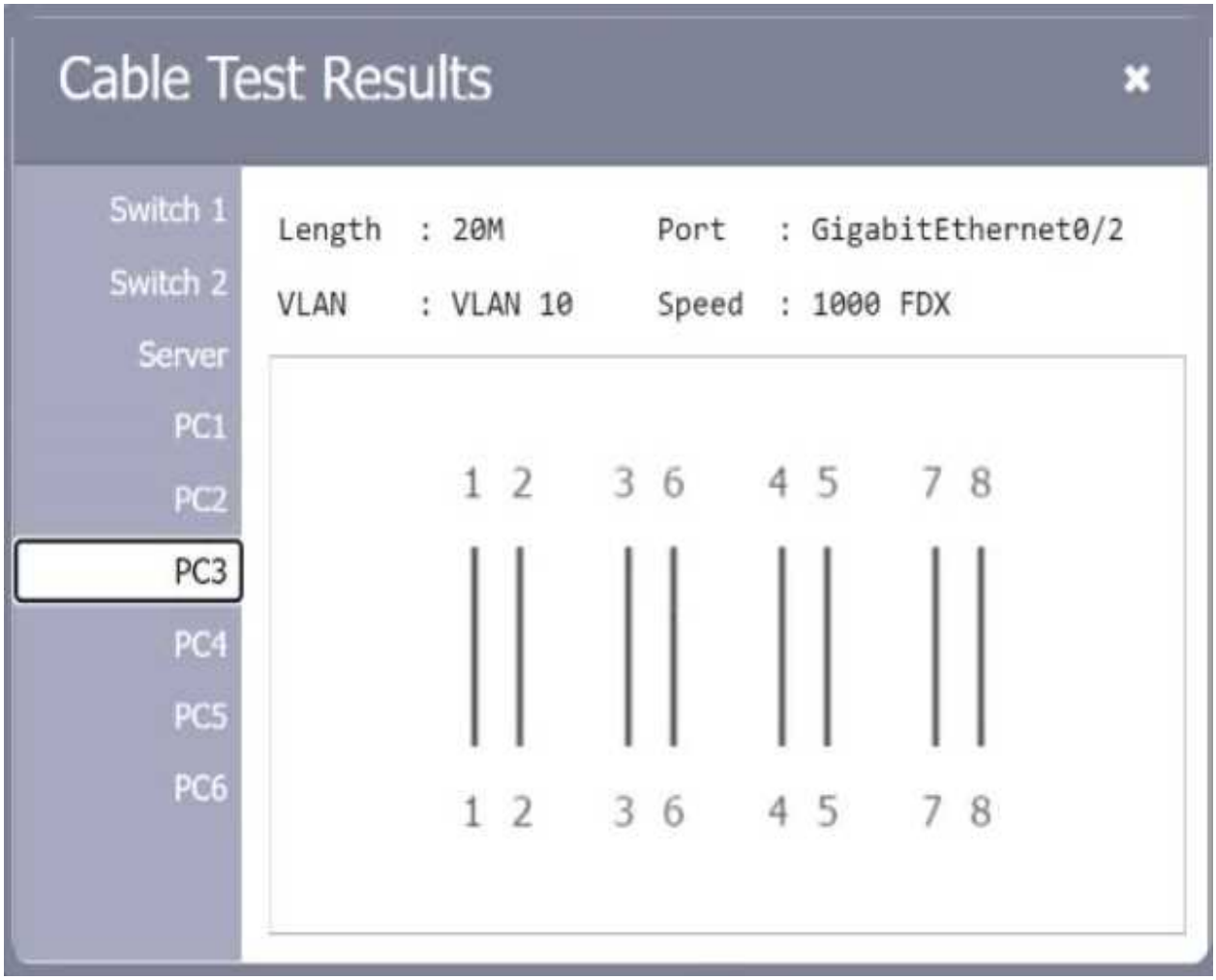

Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 16M
Port : GigabitEthernet0/5
VLAN : VLAN 10
Speed : 1000 FDX
Connected to Switch 2
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

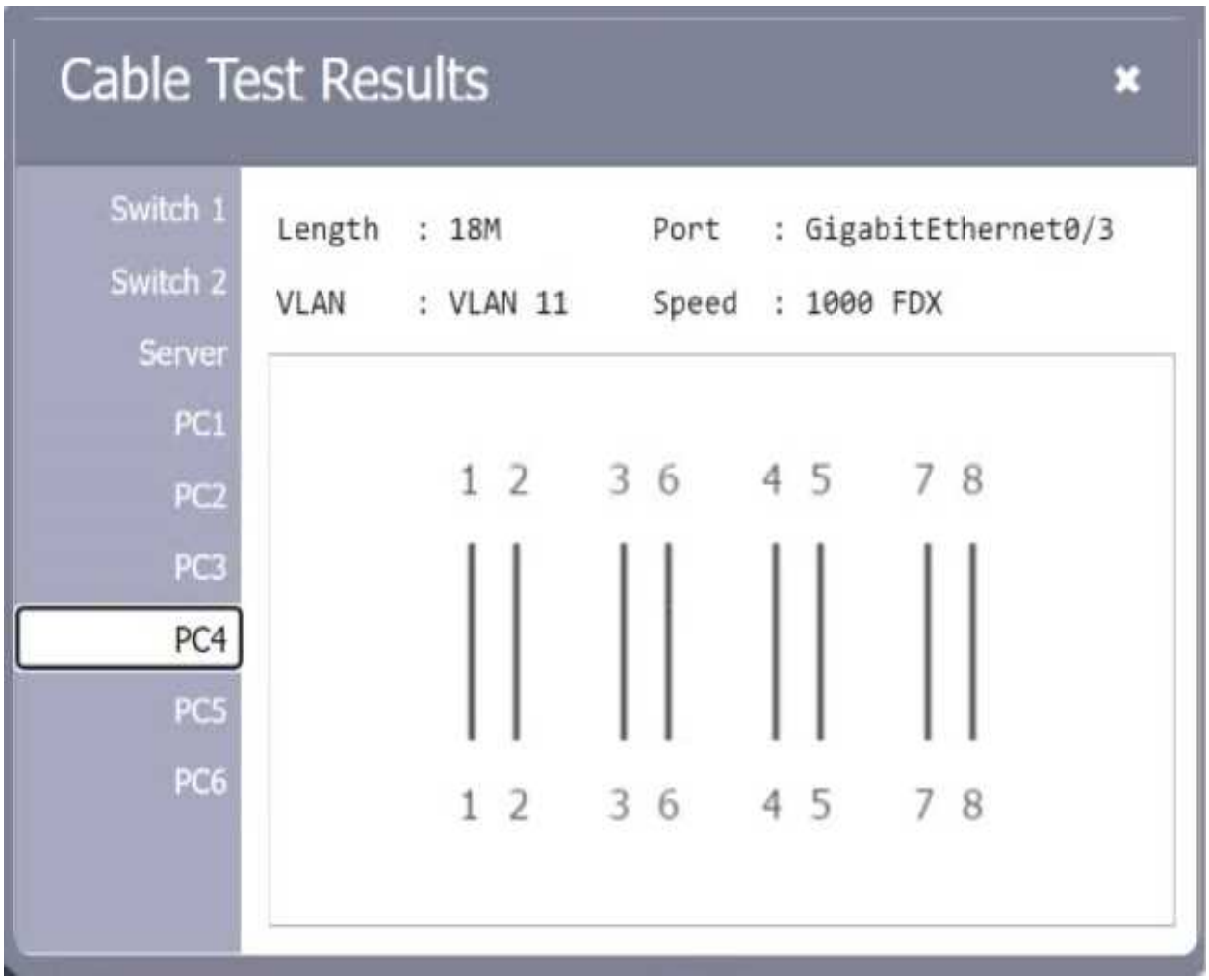

Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 16M
Port : GigabitEthernet0/5
VLAN : VLAN 10
Speed : 1000 FDX
Connected to Switch 1
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

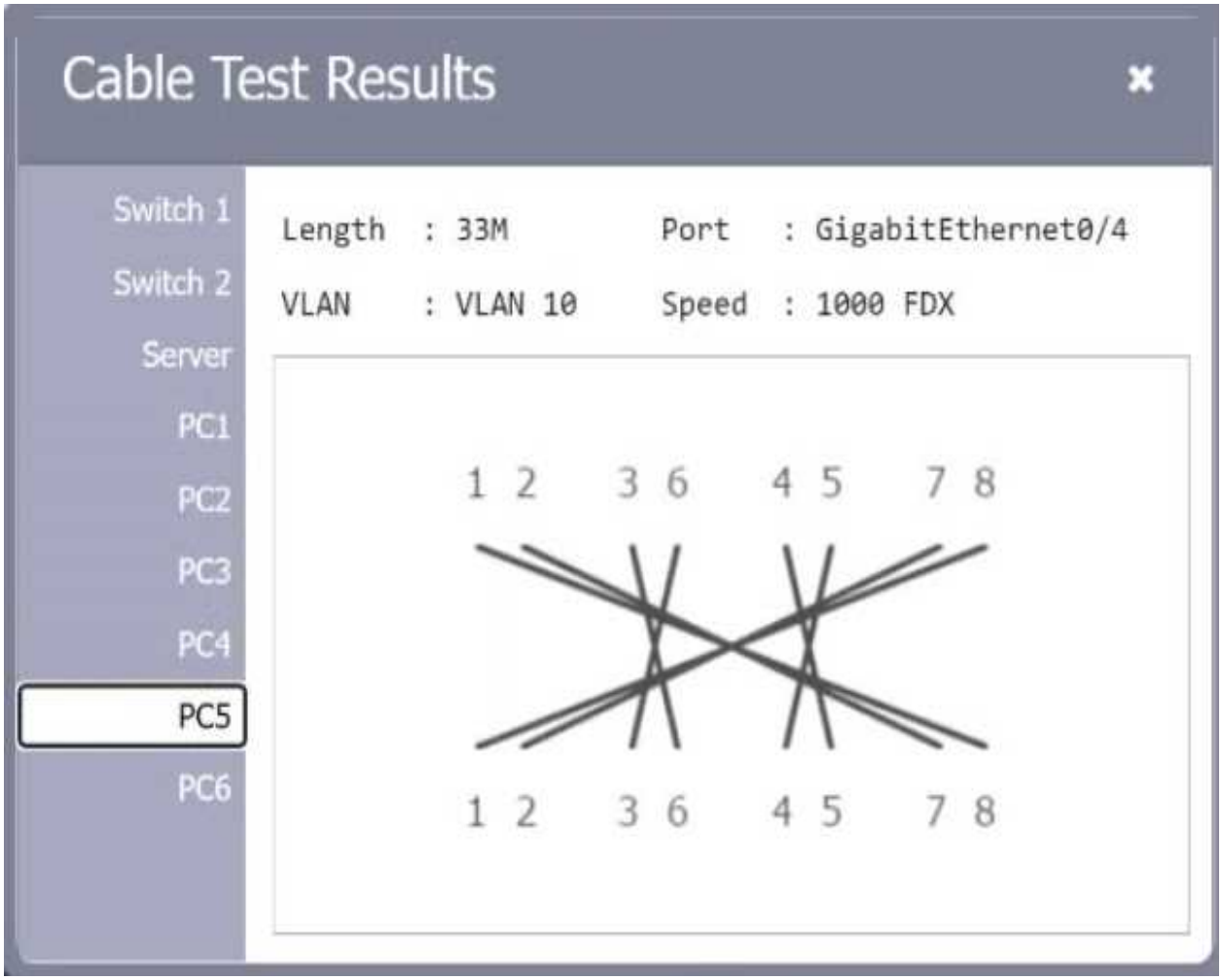

Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 22M
Port : GigabitEthernet0/1
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

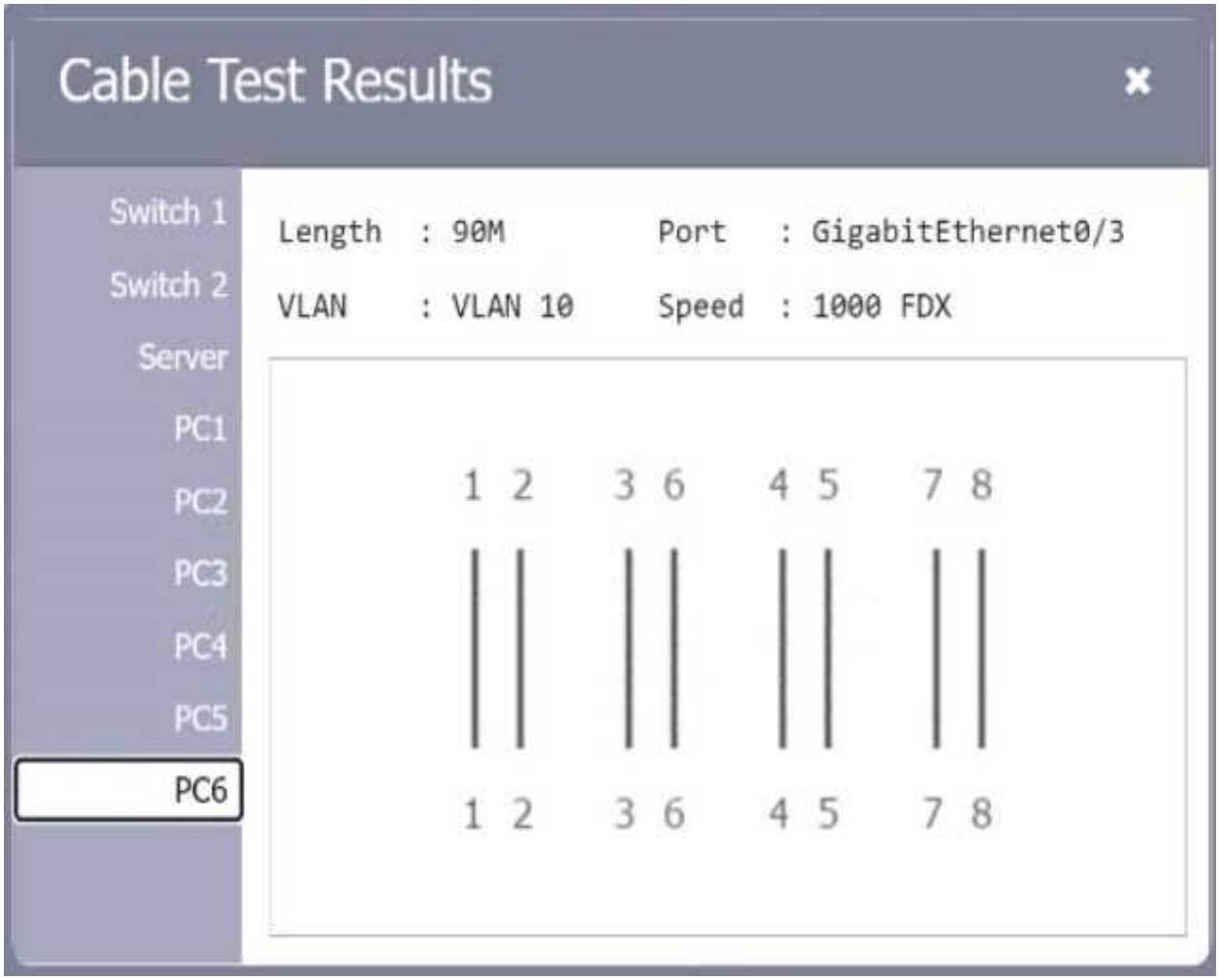

Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 42M
Port : GigabitEthernet0/2
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

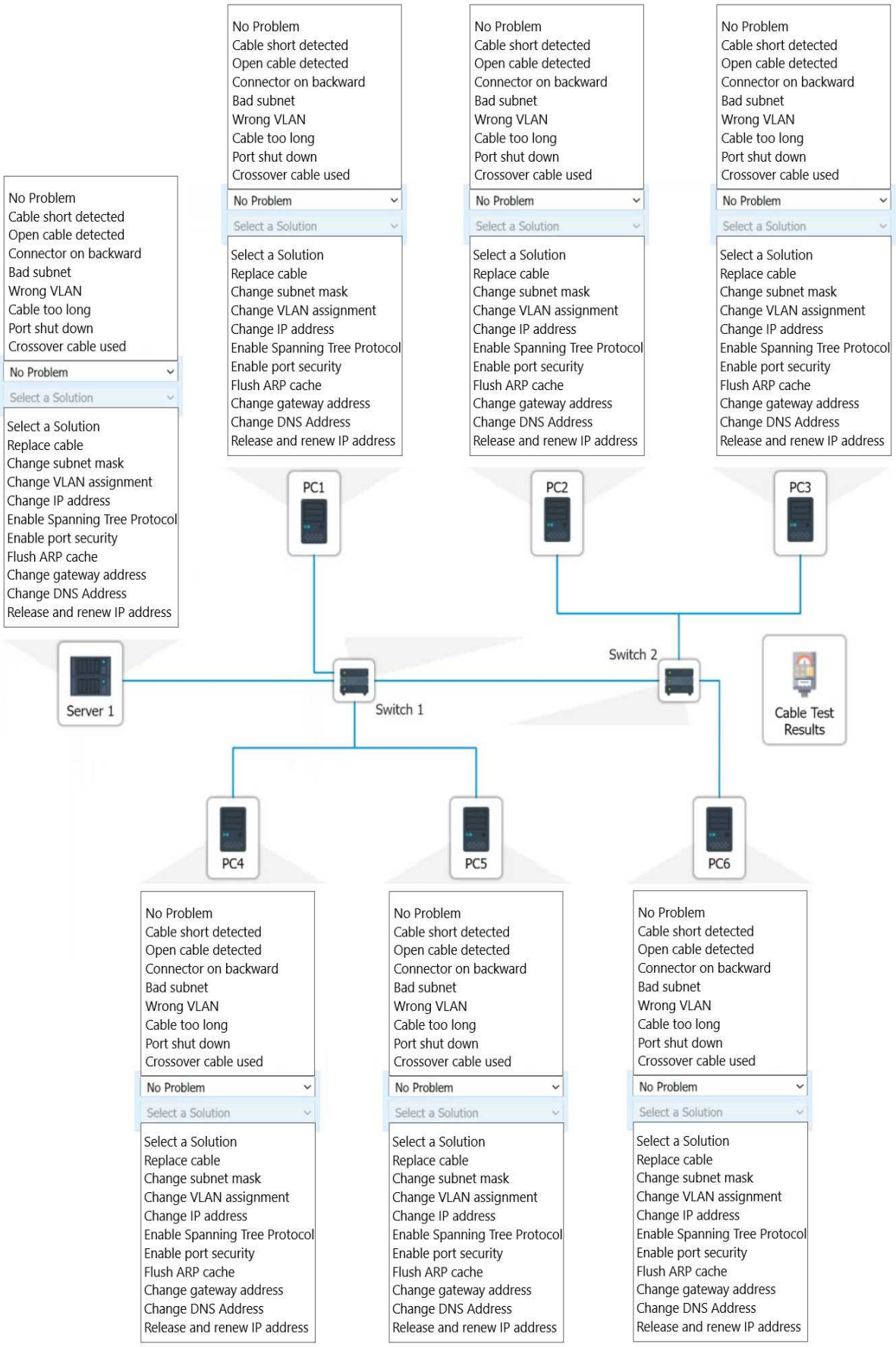

Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 12M
Port : GigabitEthernet0/1
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 20M
Port : GigabitEthernet0/2
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 18M
Port : GigabitEthernet0/3
VLAN : VLAN 11
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

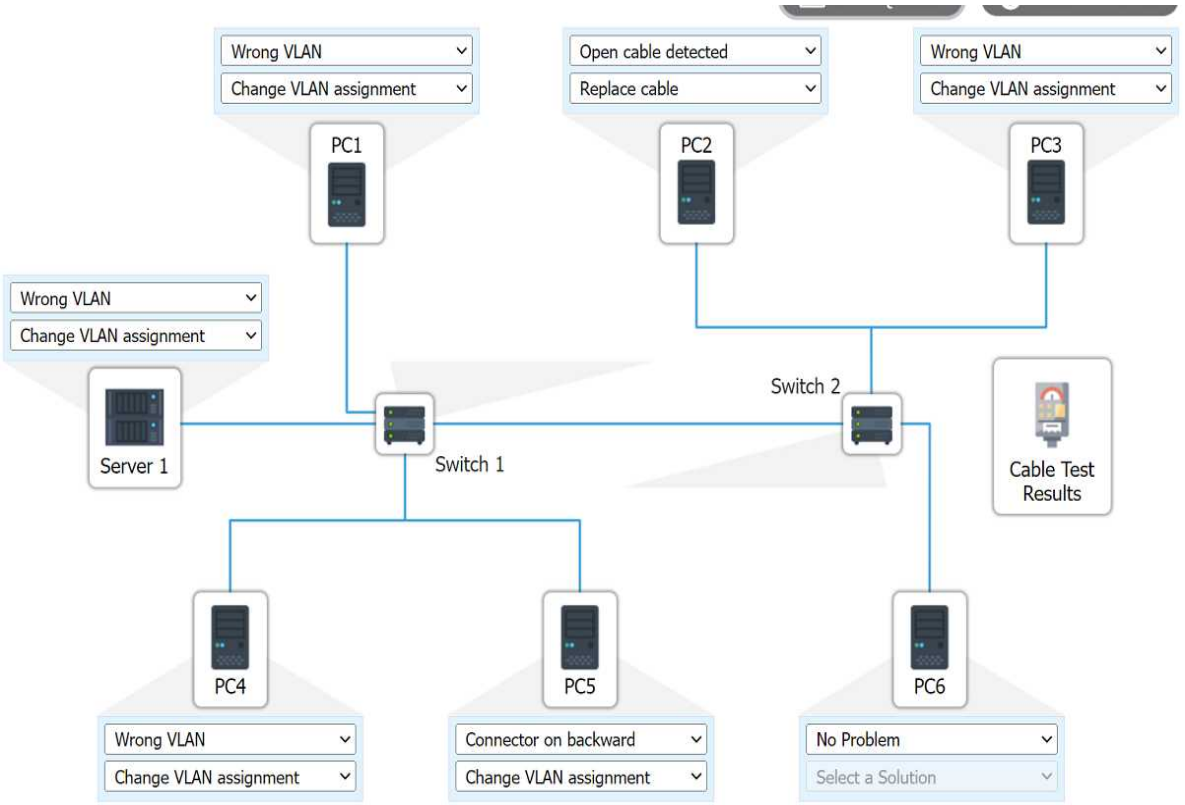

Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 33M
Port : GigabitEthernet0/4
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 90M
Port : GigabitEthernet0/3
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


No Problem
Cable short detected
Open cable detected
Connector on backward
Bad subnet
Wrong VLAN
Cable too long
Port shut down
Crossover cable used
No Problem
Select a Solution
Select a Solution
Replace cable
Change subnet mask
Change VLAN assignment
Change IP address
Enable Spanning Tree Protocol
Enable port security
Flush ARP cache
Change gateway address
Change DNS Address
Release and renew IP address
PC1
PC2
PC3
Server 1
Switch 1
Switch 2
Cable Test Results
PC4
PC5
PC6

Answer: See the answer and solution below:

Explanation:



Question: 83

SIMULATION

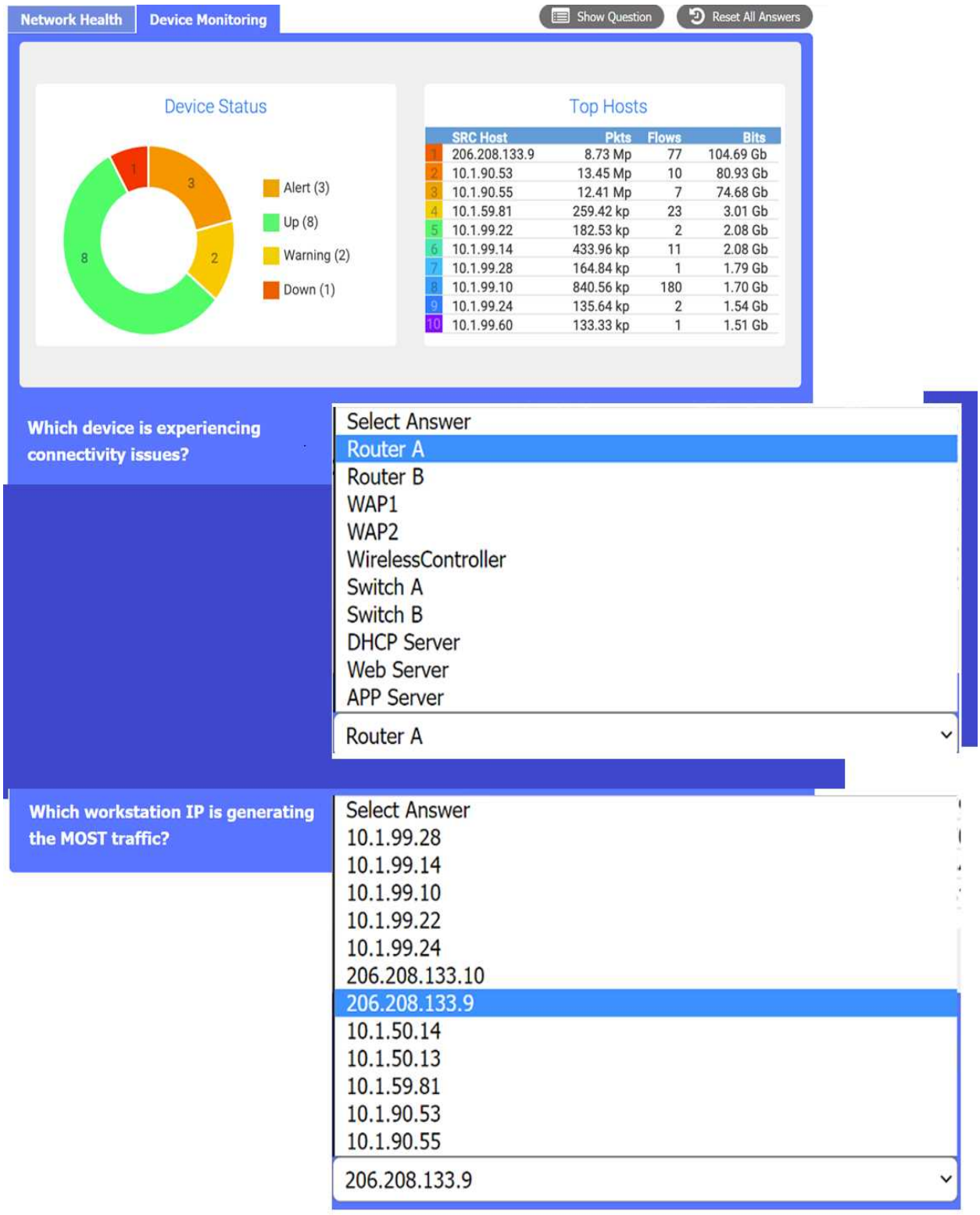
After a recent power outage, users are reporting performance issues accessing the application servers. Wireless users are also reporting intermittent Internet issues.

INSTRUCTIONS

Click on each tab at the top of the screen. Select a widget to view information, then

use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Network Health
Device Monitoring
Show Question
Reset All Answers
Wireless Client Distribution
Wireless Users Connected - 24 Hours
60
50
40
30
20
10
0
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
12:00 AM
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
Ram Usage
90%
80%
70%
60%
50%
10/1/20
10/2/20
10/3/20
10/4/20
10/5/20
10/6/20
10/7/20
Processor Usage
80%
70%
60%
50%
10/1/20
10/2/20
10/3/20
10/4/20
10/5/20
10/6/20
10/7/20
WAN Health
WAN2
WAN1
0
20
40
60
80
100
Uptime
Downtime
Uplink Name
Uplink Speed
Total Usage
Average Throughput
Loss
Average Latency
Jitter
WAN1
10G
26,690GB Up/1,708.4GB Down
353MBs Up/23.42MBs Down
2.51%
24ms
9.5ms
WAN2
1G
930GB Up/138GB Down
12.21MBs Up/1.82MBs Down
0.01%
11ms
3.9ms
Which WAN station should be preferred for VoIP traffice?
WAN 1
Select WAN
WAN 1
WAN 2



Answer: See the answer and solution below.

Explanation:

Network Health:

WAN 2 appears to have a lower average latency and loss percentage, which would make it the preferred WAN station for VoIP traffic. VoIP traffic requires low latency and packet loss to ensure good voice quality and reliability. WAN 1 seems to have higher RAM and processor usage, which could also affect the performance of VoIP traffic.

Here's the summary of the key metrics for WAN 1 and WAN 2 from the image provided:

WAN 1:

Uplink Speed: 10G

Total Usage: 26.969GB Up / 1.748GB Down

Average Throughput: 353MBps Up / 23.42MBps Down

Loss: 2.51%

Average Latency: 24ms

Jitter: 9.5ms

WAN 2:

Uplink Speed: 1G

Total Usage: 930GB Up / 138GB Down

Average Throughput: 12.21MBps Up / 1.82MBps Down

Loss: 0.01%

Average Latency: 11ms

Jitter: 3.9ms

For VoIP traffic, low latency and jitter are particularly important to ensure voice quality. While WAN 1 has higher bandwidth and throughput, it also has higher latency and jitter compared to WAN 2. However, WAN 2 has much lower loss, lower latency, and lower jitter, which are more favorable for VoIP traffic that is sensitive to delays and variation in packet arrival times.

Given this information, WAN 2 would generally be preferred for VoIP traffic due to its lower latency, lower jitter, and significantly lower loss percentage, despite its lower bandwidth compared to WAN 1. The high bandwidth of WAN 1 may be more suitable for other types of traffic that are less sensitive

to latency and jitter, such as bulk data transfers.

Device Monitoring:

the device that is experiencing connectivity issues is the APP Server or Router 1, which has a status of Down. This means that the server is not responding to network requests or sending any dat

a. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.

Question: 84

SIMULATION

You have been tasked with implementing an ACL on the router that will:

1. Permit the most commonly used secure remote access technologies from the management network to all other local network segments

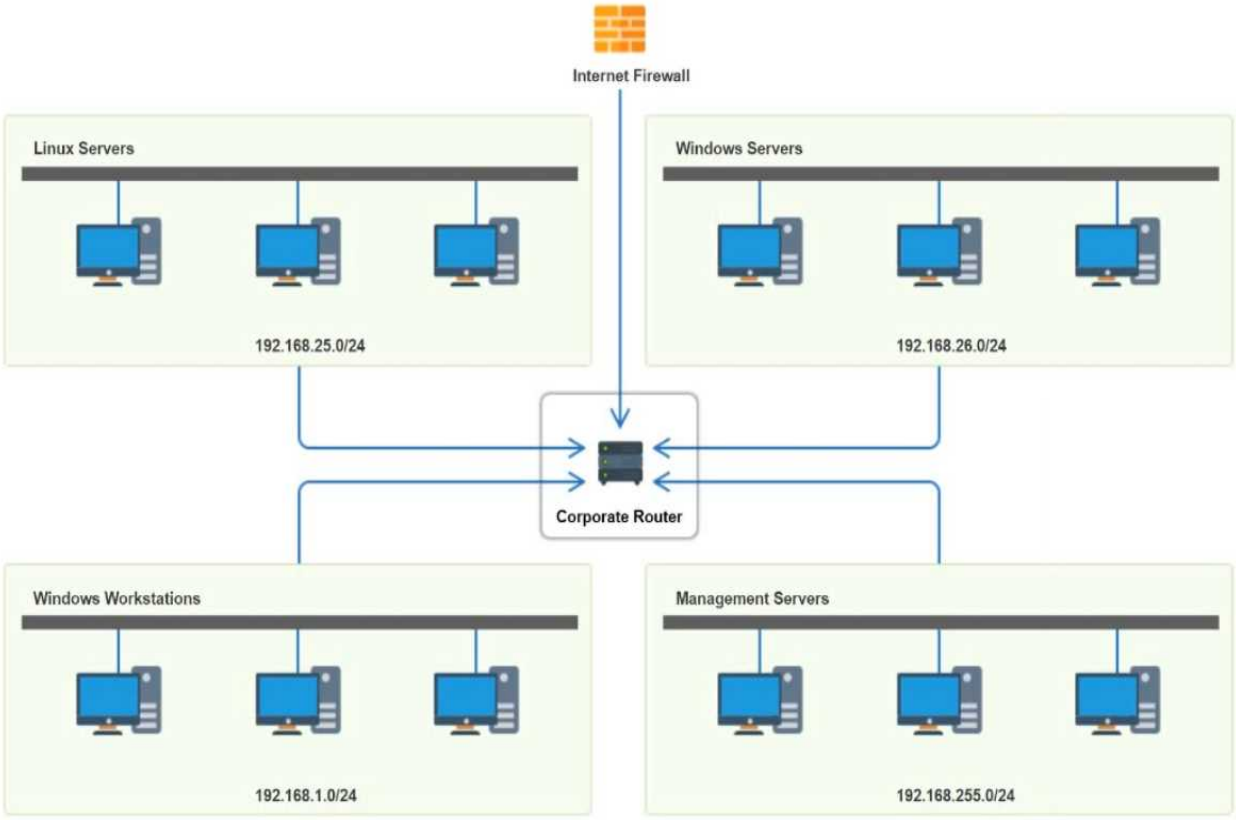
2. Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.

3. Prohibit any traffic that has not been specifically allowed.

INSTRUCTIONS

Use the drop-downs to complete the ACL

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Internet Firewall
Linux Servers
192.168.25.0/24
Windows Servers
192.168.26.0/24
Corporate Router
Windows Workstations
192.168.1.0/24
Management Servers
192.168.255.0/24

Router Access Control List

Rule	Source	Destination	Protocol	Service	Action
1	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
2	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
3	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
7	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	TCP	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny
8	192.168.1.0	Any	Any	Any	Allow
9	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	192.168.1.0 192.168.25.0 192.168.255.0 192.168.26.0 Any	Any	SSH Telnet HTTP RDP VNC SMB Any	Allow Deny

Answer: See the answer and solution below.

Explanation:

Router Access Control List

Rule	Source	Destination	Protocol	Service	Action
1	192.168.255.0	192.168.26.0	TCP	SSH	Allow
2	192.168.255.0	192.168.25.0	TCP	SSH	Allow
3	192.168.255.0	192.168.1.0	TCP	SSH	Allow
4	192.168.255.0	192.168.26.0	TCP	SMB	Allow
5	192.168.255.0	Any	Any	Any	Deny
6	192.168.1.0	Any	TCP	RDP	Deny
7	192.168.1.0	Any	TCP	VNC	Deny
8	192.168.1.0	Any	Any	Any	Allow
9	Any	Any	Any	Any	Deny

Question: 85

A network administrator is configuring access points for installation in a dense environment where coverage is often overlapping. Which of the following channel widths should the administrator choose to help minimize interference in the 2.4GHz spectrum?

A. 11MHz

B. 20MHz

C. 40MHz

D. 80MHz

E. 160MHz

Answer: B

Explanation:

In the 2.4GHz spectrum, channels are spaced 5MHz apart but have a bandwidth of 20MHz, resulting in overlapping channels. To minimize interference, especially in a dense environment where access point coverage overlaps, a narrower channel width of 20MHz should be used. Using wider channel widths like 40MHz, 80MHz, or 160MHz in the 2.4GHz band will increase the overlap and interference. The 20MHz channel width provides a good balance between performance and minimal interference.
Reference: CompTIA Network+ Certification Exam Objectives - Wireless Networks section.

Question: 86

Which of the following cloud service models most likely requires the greatest up-front expense by the customer when migrating a data center to the cloud?

A. Infrastructure as a service

B. Software as a service

C. Platform as a service

D. Network as a service

Answer: A

Explanation:

Infrastructure as a Service (IaaS) typically requires the greatest up-front expense by the customer when migrating a data center to the cloud. IaaS provides virtualized computing resources over the internet, where customers rent virtual machines, storage, and networks. The customer is responsible for managing the operating systems, applications, and data. This model often necessitates significant

initial investment in planning, migration, and configuring the infrastructure. In contrast, Software as a Service (SaaS) and Platform as a Service (PaaS) models usually involve lower up-front costs because they offer more managed services.
Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

Question: 87

Which of the following steps in the troubleshooting methodology includes checking logs for recent changes?

A. Identify the problem.

B. Document the findings and outcomes.

C. Test the theory to determine cause.

D. Establish a plan of action.

Answer: A

Explanation:

Checking logs for recent changes is part of the "Identify the problem" step in the CompTIA troubleshooting methodology. This step involves gathering information, including reviewing logs and documentation, to understand what might have changed or caused the issue. This preliminary analysis is critical for forming an accurate theory about the problem.
Reference: CompTIA Network+ Certification Exam Objectives - Troubleshooting section.

Question: 88

Which of the following is the most closely associated with segmenting compute resources within a single cloud account?

A. Network security group

B. laaS

C. VPC

D. Hybrid cloud

Answer: C

Explanation:

A Virtual Private Cloud (VPC) is most closely associated with segmenting compute resources within a single cloud account. A VPC allows you to define a virtual network that closely resembles a traditional network, complete with subnets, route tables, and gateways. This segmentation enables the isolation of different parts of a network within a cloud environment, ensuring security and efficient resource management. VPCs are a key component in many cloud infrastructures, providing the flexibility to manage and control network settings and resources.
Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

Question: 89

A user connects to a corporate VPN via a web browser and is able to use TLS to access the internal financial system to input a time card. Which of the following best describes how the VPN is being used?

A. Clientless

B. Client-to-site

C. Full tunnel

D. Site-to-site

Answer: A

Explanation:

The scenario describes a user connecting to a corporate VPN via a web browser using TLS to access

an internal system. This setup is best described as a "clientless" VPN. Clientless VPNs do not require a VPN client to be installed on the user's device; instead, they rely on a standard web browser to establish the connection. This method is particularly useful for providing secure, remote access to applications through a web interface without the need for additional software installations.
Reference: CompTIA Network+ Certification Exam Objectives - Remote Access Methods section.

Question: 90

A network engineer wants to implement a new IDS between the switch and a router connected to the LAN. The engineer does not want to introduce any latency by placing the IDS in line with the gateway. The engineer does want to ensure that the IDS sees all packets without any loss. Which of the following is the best way for the engineer to implement the IDS?

A. Use a network tap.

B. Use Nmap software.

C. Use a protocol analyzer.

D. Use a port mirror.

Answer: D

Explanation:

To ensure that an IDS sees all packets without any loss and without introducing latency, the best approach is to use a port mirror, also known as a SPAN (Switched Port Analyzer) port. Port mirroring copies network packets seen on one switch port (or an entire VLAN) to another port where the IDS is connected. This method allows the IDS to monitor traffic passively without being in the direct path of network traffic, thus avoiding any additional latency.
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

Question: 91

Which of the following panels would be best to facilitate a central termination point for all network cables on the floor of a company building?

A. Patch

B. UPS

C. MDF

D. Rack

Answer: A

Explanation:

A patch panel is the best choice to facilitate a central termination point for all network cables on the floor of a company building. Patch panels are used to manage and organize multiple network cables, providing a central point where all cables converge. This setup allows for easy management, troubleshooting, and reconfiguration of network connections. The other options, such as UPS (Uninterruptible Power Supply), MDF (Main Distribution Frame), and rack, serve different purposes and are not specifically designed for the central termination of network cables.
Reference: CompTIA Network+ Certification Exam Objectives - Network Installation section.

Question: 92

A customer needs six usable IP addresses. Which of the following best meets this requirement?

A. 255.255.255.128

B. 255.255.255.192

C. 255.255.255.224

D. 255.255.255.240

Answer: D

Explanation:

To meet the requirement of six usable IP addresses, the subnet mask 255.255.255.240 (also represented as /28) is the best fit. A /28 subnet provides 16 total IP addresses, out of which 14 are usable (the first address is the network address, and the last address is the broadcast address). This meets and exceeds the requirement for six usable IP addresses, ensuring there are enough addresses for future expansion if needed. The other options provide either too few or too many addresses for this specific requirement.
Reference: CompTIA Network+ Certification Exam Objectives - IP Addressing section.

Question: 93

A network administrator is configuring a new switch and wants to ensure that only assigned devices can connect to the switch. Which of the following should the administrator do?

A. Configure ACLs.

B. Implement a captive portal.

C. Enable port security.

D. Disable unnecessary services.

Answer: C

Explanation:

To ensure that only assigned devices can connect to a switch, the network administrator should enable port security. Port security restricts port access based on MAC addresses, allowing only pre-configured devices to connect to the network. This helps prevent unauthorized devices from gaining access to the network. Other options like configuring ACLs, implementing a captive portal, or disabling unnecessary services serve different security purposes and do not directly restrict physical port access based on device identity.
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

Question: 94

A network administrator needs to set up a multicast network for audio and video broadcasting.

Which of the following networks would be the most appropriate for this application?

A. 172.16.0.0/24

B. 192.168.0.0/24

C. 224.0.0.0/24

D. 240.0.0.0/24

Answer: C

Explanation:

The address range 224.0.0.0/24 falls within the Class D IP address range (224.0.0.0 to 239.255.255.255), which is reserved for multicast traffic. Multicast addresses are used for the delivery of information to multiple destinations simultaneously, making them ideal for applications like audio and video broadcasting. The other options (172.16.0.0/24, 192.168.0.0/24, and 240.0.0.0/24) are not suitable for multicast as they are within different IP ranges used for other purposes (private addressing and future use, respectively).
Reference: CompTIA Network+ Certification Exam Objectives - IP Addressing section.

Question: 95

A company wants to implement data loss prevention by restricting user access to social media platforms and personal cloud storage on workstations. Which of the following types of filtering should the company deploy to achieve these goals?

A. Port

B. DNS

C. MAC

D. Content

Answer: D

Explanation:

To implement data loss prevention (DLP) and restrict user access to social media platforms and personal cloud storage, the company should deploy content filtering. Content filtering examines the data being transmitted over the network and can block specific types of content or websites based on predefined policies. This type of filtering is effective in preventing access to specific web services and ensuring that sensitive information does not leave the network through unauthorized channels. Port, DNS, and MAC filtering serve different purposes and are not as effective for DLP in this context.
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

Question: 96

A network administrator's device is experiencing severe Wi-Fi interference within the corporate headquarters causing the device to constantly drop off the network. Which of the following is most likely the cause of the issue?

A. Too much wireless reflection

B. Too much wireless absorption

C. Too many wireless repeaters

D. Too many client connections

Answer: A

Explanation:

Severe Wi-Fi interference within a corporate headquarters causing devices to constantly drop off the network is most likely due to too much wireless reflection. Wireless reflection occurs when Wi-Fi signals bounce off surfaces like walls, metal, or glass, causing multipath interference. This can lead to poor signal quality and frequent disconnections. Other causes like wireless absorption, too many repeaters, or too many client connections can also affect Wi-Fi performance, but excessive reflection is a common culprit in environments with many reflective surfaces.
Reference: CompTIA Network+ Certification Exam Objectives - Wireless Networks section.

Question: 97

While troubleshooting a VoIP handset connection, a technician's laptop is able to successfully connect to network resources using the same port. The technician needs to identify the port on the switch. Which of the following should the technician use to determine the switch and port?

A. LLDP

B. IKE

C. VLAN

D. netstat

Answer: A

Explanation:

Link Layer Discovery Protocol (LLDP) is a network protocol used for discovering devices and their capabilities on a local area network, primarily at the data link layer (Layer 2). It helps in identifying the connected switch and the specific port to which a device is connected. When troubleshooting a VoIP handset connection, the technician can use LLDP to determine the exact switch and port where the handset is connected. This protocol is widely used in network management to facilitate the discovery of network topology and simplify troubleshooting.

Other options such as IKE (Internet Key Exchange), VLAN (Virtual LAN), and netstat (network statistics) are not suitable for identifying the switch and port information. IKE is used in setting up secure IPsec connections, VLAN is used for segmenting networks, and netstat provides information about active connections and listening ports on a host but not for discovering switch port details.

Reference: CompTIA Network+ Certification Exam Objectives - Network Troubleshooting and Tools section.

Question: 98

Before using a guest network, an administrator requires users to accept the terms of use Which of

the following is the best way to accomplish this goal?

A. Pre-shared key
B. Autonomous access point
C. Captive portal
D. WPA2 encryption

Answer: C

Explanation:

A captive portal is a web page that users must view and interact with before being granted access to a network. It is commonly used in guest networks to enforce terms of use agreements. When a user connects to the network, they are redirected to this portal where they must accept the terms of use before proceeding. This method ensures that users are aware of and agree to the network's policies, making it the best choice for this scenario. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 99

Which of the following is the correct order of components in a bottom-up approach for the three-tier hierarchical model?

A. Access, distribution, and core
B. Core, root, and distribution
C. Core, spine, and leaf
D. Access, core, and roof

Answer: A

Explanation:

The three-tier hierarchical model in network design consists of three layers: access, distribution, and core. The access layer is where devices like PCs and printers connect to the network. The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer, which is responsible for high-speed data transfer and routing. This approach improves scalability and performance in larger networks. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 100

Which of the following is a company most likely enacting if an accountant for the company can only see the financial department's shared folders?

A. General Data Protection Regulation
B. Least privilege network access
C. Acceptable use policy
D. End user license agreement

Answer: B

Explanation:

Least privilege network access is a principle that restricts users' access rights to only what is necessary for them to perform their job functions. In this case, the accountant's access is limited to only the financial department's shared folders, ensuring that they cannot access other parts of the network unnecessarily. This reduces the risk of unauthorized access and potential data breaches. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 101

Which of the following best describes a group of devices that is used to lure unsuspecting attackers and to study the attackers' activities?

A. Geofencing
B. Honeynet
C. Jumpbox
D. Screened subnet

Answer: B

Explanation:

A honeynet is a network of honeypots designed to attract and study attackers. Honeypots are decoy systems set up to lure cyber attackers and analyze their activities. A honeynet, being a collection of these systems, provides a broader view of attack methods and patterns, helping organizations improve their security measures. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 102

A customer recently moved into a new office and notices that some wall plates are not working and are not properly labeled Which of the following tools would be best to identify the proper wiring in the IDF?

A. Toner and probe
B. Cable tester
C. Visual fault locator
D. Network tap

Answer: A

Explanation:

A toner and probe tool, also known as a tone generator and probe, is used to trace and identify individual cables within a bundle or to locate the termination points of cables in wiring closets and patch panels. It generates a tone that can be picked up by the probe, helping technicians quickly and accurately identify and label wall plates and wiring. This is the best tool for identifying proper wiring in the Intermediate Distribution Frame (IDF). Reference: CompTIA Network+ Exam Objectives and

official study guides.

Question: 103

A network administrator is planning to host a company application in the cloud, making the application available for all internal and third-party users. Which of the following concepts describes this arrangement?

A. Multitenancy
B. VPC
C. NFV
D. SaaS

Answer: A

Explanation:

Multitenancy is a cloud computing architecture where a single instance of software serves multiple customers or tenants. Each tenant's data is isolated and remains invisible to other tenants. Hosting a company application in the cloud to be available for both internal and third-party users fits this concept, as it allows shared resources and infrastructure while maintaining data separation and security. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 104

Which of the following best describes the transmission format that occurs at the transport layer over connectionless communication?

A. Datagram
B. Segment
C. Frames
D. Packets

Answer: A

Explanation:

At the transport layer, connectionless communication is typically handled using the User Datagram Protocol (UDP), which transmits data in units called datagrams. Unlike TCP, UDP does not establish a connection before sending data and does not guarantee delivery, making datagrams the correct term for the transmission format in this context. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 105

A user's VoIP phone and workstation are connected through an inline cable. The user reports that the VoIP phone intermittently reboots, but the workstation is not having any network-related issues Which of the following is the most likely cause?

A. The PoE power budget is exceeded.
B. Port security is violated.
C. The signal is degraded
D. The Ethernet cable is not working

Answer: A

Explanation:

Power over Ethernet (PoE) delivers power to devices such as VoIP phones over the same cables used for data. If the total power requirement of connected devices exceeds the PoE power budget of the switch or injector, some devices may not receive adequate power and could intermittently reboot. This issue would not affect the workstation, which is likely receiving power separately. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 106

Which of the following are the best device-hardening techniques for network security? (Select two).

A. Disabling unused ports
B. Performing regular scanning of unauthorized devices
C. Monitoring system logs for irregularities
D. Enabling logical security such as SSO
E. Changing default passwords
F. Ensuring least privilege concepts are in place

Answer: AE

Explanation:

Disabling unused ports prevents unauthorized access and reduces the attack surface by ensuring that no inactive or unmonitored entry points are available for exploitation. Changing default passwords is critical for security because default credentials are widely known and can easily be exploited by attackers. These techniques are fundamental steps in hardening devices against unauthorized access and ensuring network security. Reference: CompTIA Network+ Exam Objectives and official study guides.

Question: 107

Which of the following network cables involves bounding light off of protective cladding?

A. Twinaxial
B. Coaxial
C. Single-mode
D. Multimode

Answer: D

Explanation:

Multimode fiber optic cables involve the transmission of light signals that bounce off the core's cladding as they travel down the fiber. This characteristic differentiates it from single-mode fiber, where the light travels directly down the fiber without reflecting off the cladding.
Here are some detailed points about multimode fiber cables:
Construction: Multimode fibers have a larger core diameter, typically 50 or 62.5 microns, compared to single-mode fibers, which have a core diameter of about 9 microns.
Light Propagation: The larger core of multimode fiber allows multiple light modes to propagate. These modes travel at different angles, leading to reflections off the core-cladding boundary.
Distance and Bandwidth: Due to modal dispersion, where different light modes arrive at the receiver at different times, multimode fibers are suited for shorter distance applications compared to single-mode fibers. Typical distances are up to 550 meters for 10 Gbps Ethernet using OM4 multimode fiber.
Applications: Multimode fibers are commonly used in LANs (Local Area Networks), data centers, and for shorter distance data transmission due to their cost-effectiveness and ease of installation.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide, which covers fiber optic technologies, including the differences between multimode and single-mode fibers.
Cisco Networking Academy: Provides training materials and reference guides on the properties of different fiber optic cables.
Fiber Optic Association (FOA): A professional society dedicated to fiber optics, offering extensive information and certification on fiber optic technologies.
Multimode fibers are specifically designed for short-range communication with higher data rates and are typically used in environments like data centers, where high bandwidth over shorter distances is crucial. The reflections off the cladding, inherent to multimode fiber, facilitate this high-capacity communication.

Question: 108

A network administrator performed upgrades on a server and installed a new NIC to improve performance. Following the upgrades, usera are unable to reach the server. Which of the following is the most likely reason.

A. The PoE power budget was exceeded.
B. TX/RX was transposed.
C. A port security violation occured.
D. An incorrect cable type was installed.

Answer: D

Explanation:

When a network administrator installs a new Network Interface Card (NIC) and users are unable to reach the server, one of the common issues is the use of an incorrect cable type. Network cables must match the specifications required by the NIC and the network infrastructure (e.g., Cat5e, Cat6 for Ethernet).
NIC Compatibility: The new NIC might require a specific type of cable to function properly. Using a cable not rated for the NIC's required speeds or capabilities can result in connectivity issues.
Cable Standards: Different NICs and network devices might need different cabling standards

(straight-through vs. crossover cables, or specific fiber optic types).
Connection Types: Ensuring that the cable connectors are appropriate for the NIC ports (e.g., RJ45 for Ethernet, LC connectors for fiber optics).
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses network cabling standards and NIC specifications.
Cisco Networking Academy: Provides insights into cabling and NIC configurations for optimal network performance.
Network+ Certification All-in-One Exam Guide: Offers comprehensive details on troubleshooting network connectivity issues, including cabling problems.

Question: 109

Which of the following is a cost-effective advantage of a split-tunnel VPN?

A. Web traffic is filtered through a web filter.
B. More bandwidth is required on the company's internet connection.
C. Monitoring detects insecure machines on the company's network.
D. Cloud-based traffic flows outside of the company's network.

Answer: D

Explanation:

A split-tunnel VPN allows some traffic to be routed through the VPN while other traffic goes directly to the internet. This setup offers several advantages, with a primary one being cost-effectiveness due to cloud-based traffic not consuming company bandwidth.
Bandwidth Utilization: Split-tunnel VPNs reduce the amount of traffic passing through the company's network, freeing up bandwidth for other uses.
Performance: By allowing internet-bound traffic to bypass the VPN, it can reduce latency and improve the performance for users accessing cloud services directly.
Cost Savings: Reduced load on the company's VPN infrastructure can lead to lower costs in terms of both hardware and bandwidth.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Covers VPN types, including split-tunnel configurations and their advantages.
Cisco Networking Academy: Discusses VPN technologies and the benefits of split-tunneling.
Network+ Certification All-in-One Exam Guide: Provides detailed information on VPN setups, including the cost-effectiveness of split-tunnel VPNs.
By allowing cloud-based traffic to flow outside the company's network, a split-tunnel VPN optimizes resource usage and enhances the overall network performance without incurring extra costs for bandwidth.

Question: 110

A network technician needs to install patch cords from the UTP patch panel to the access switch for a newly occupied set of offices. The patch panel is not labeled for easy jack identification. Which of the following tools provides the easiest way to identify the appropriate patch panel port?

A. Toner
B. Laptop
C. Cable tester
D. Visual fault locator

Answer: A

Explanation:

A toner probe, often referred to as a toner and probe kit, is the easiest and most effective tool for identifying individual cables in a bundle, especially in situations where the patch panel is not labeled. The toner sends an audible tone through the cable, and the probe detects the tone at the other end, allowing the technician to quickly identify the correct cable.
Functionality: The toner generates a tone that travels along the cable. When the probe is placed near the correct cable, it detects the tone and emits a sound.
Ease of Use: Toner probes are straightforward to use, even in environments with many cables, making them ideal for identifying cables in unlabeled patch panels.
Efficiency: This method is much faster and more reliable than manual tracing, especially in complex setups.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Details tools used for cable identification and troubleshooting.
Cisco Networking Academy: Provides training on using toner probes and other cable testing tools.
Network+ Certification All-in-One Exam Guide: Explains the use of different tools for network cable identification and management.

Question: 111

A network administrator is in the process of installing 35 PoE security cameras. After the administrator installed and tested the new cables, the administrator installed the cameras. However, a small number of the cameras do not work. Which of the following is the most reason?

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

Answer: B

Explanation:

When installing multiple Power over Ethernet (PoE) devices like security cameras, it is crucial to ensure that the total power requirement does not exceed the power budget of the PoE switch. Each PoE switch has a maximum power capacity, and exceeding this capacity can cause some devices to fail to receive power.
PoE Standards: PoE switches conform to standards such as IEEE 802.3af (PoE) and 802.3at (PoE+), each with specific power limits per port and total power capacity.
Power Calculation: Adding up the power requirements of all connected PoE devices can help

determine if the total power budget of the switch is exceeded.
Symptoms: When the power budget is exceeded, some devices, typically those farthest from the switch or connected last, may not power up or function correctly.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Covers PoE standards and troubleshooting power issues.
Cisco Networking Academy: Discusses PoE technologies, power budgeting, and managing PoE devices.
Network+ Certification All-in-One Exam Guide: Provides information on PoE setup, including power budget considerations.

Question: 112

Which of the following network traffic type is sent to all nodes on the network?

A. Unicast
B. Broadcast
C. Multicast
D. Anycast

Answer: B

Explanation:

Broadcast traffic is sent to all nodes on the network. In a broadcast, a single packet is transmitted to all devices in the network segment. This is commonly used for tasks like ARP (Address Resolution Protocol) requests.
Broadcast Domain: All devices within the same broadcast domain will receive broadcast traffic.
Network Types: Ethernet networks commonly use broadcast traffic for certain functions, including network discovery and addressing.
IPv4 Broadcast: An IPv4 broadcast address (e.g., 255.255.255.255) ensures the packet is sent to all devices on the network.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Explains network traffic types, including broadcast, unicast, and multicast.
Cisco Networking Academy: Provides training on network communication methods and traffic types.
Network+ Certification All-in-One Exam Guide: Discusses different types of network traffic and their uses in various network scenarios.
Broadcast traffic is essential for network operations that require communication with all nodes, such as ARP requests or DHCP discovery messages.

Question: 113

A client wants to increase overall security after a recent breach. Which of the following would be best to implement? (Select two.)

A. Least privilege network access
B. Dynamic inventeries

C. Central policy management
D. Zero-touch provisioning
E. Configuration drift prevention
F. Subnet range limits

Answer: A, C

Explanation:

To increase overall security after a recent breach, implementing least privilege network access and central policy management are effective strategies.
Least Privilege Network Access: This principle ensures that users and devices are granted only the access necessary to perform their functions, minimizing the potential for unauthorized access or breaches. By limiting permissions, the risk of an attacker gaining access to critical parts of the network is reduced.
Central Policy Management: Centralized management of security policies allows for consistent and streamlined implementation of security measures across the entire network. This helps in quickly responding to security incidents, ensuring compliance with security protocols, and reducing the chances of misconfigurations.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses network security principles, including least privilege and policy management.
Cisco Networking Academy: Provides training on implementing security policies and access controls.
Network+ Certification All-in-One Exam Guide: Covers strategies for enhancing network security and managing policies effectively.

Question: 114

A support agent receives a report that a remote user's wired devices are constantly disconnecting and have slow speeds. Upon inspection, the support agent sees that the user's coaxial modern has a signal power of -97dB.

A. Removing any spliters connecte to the line
B. Switching the devices to wireless
C. Moving the devices closer to the modern
D. Lowering the network speed

Answer: A

Explanation:

A signal power of -97dB indicates a very weak signal, which can cause connectivity issues and slow speeds. Splitters on a coaxial line can degrade the signal quality further, so removing them can help improve the signal strength and overall connection quality.
Signal Quality: Splitters can reduce the signal strength by dividing the signal among multiple lines, which can be detrimental when the signal is already weak.
Direct Connection: Ensuring a direct connection from the modem to the incoming line can maximize signal quality and reduce potential points of failure.
Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses troubleshooting connectivity issues and the impact of signal strength on network performance.
Cisco Networking Academy: Provides insights on maintaining optimal signal quality in network setups.
Network+ Certification All-in-One Exam Guide: Covers common network issues, including those related to signal degradation and ways to mitigate them.

Question: 115

A company wants to implement a disaster recovery site or non-critical applicance, which can tolerance a short period of downltime. Which of the followig type of sites should the company impelement to achive this goal?

A. Hot
B. Cold
C. Warm
D. Passive

Answer: C

Explanation:

A warm site is a compromise between a hot site and a cold site, providing a balance between cost and recovery time. It is partially equipped with the necessary hardware, software, and infrastructure, allowing for a quicker recovery compared to a cold site but at a lower cost than a hot site.
Recovery Time: Warm sites can be operational within hours to a day, making them suitable for non-critical applications that can tolerate short downtimes.
Cost-Effectiveness: Warm sites are more economical than hot sites as they do not require all systems to be fully operational at all times.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses disaster recovery strategies and the different types of recovery sites.
Cisco Networking Academy: Provides training on disaster recovery planning and site selection.
Network+ Certification All-in-One Exam Guide: Explains the characteristics of hot, warm, and cold sites and their use cases in disaster recovery planning.
Warm sites offer a practical solution for maintaining business continuity for non-critical applications, balancing the need for availability with cost considerations.

Question: 116

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

A. Dig
B. Nmap
C. Tracert

D. nslookup

Answer: B

Explanation:

Nmap (Network Mapper) is a powerful network scanning tool used to discover hosts and services on a computer network. It can be used to identify which ports are open on a remote server, which can help diagnose access issues to services like a remote file server.
Port Scanning: Nmap can perform comprehensive port scans to determine which ports are open and what services are running on those ports.
Network Discovery: It provides detailed information about the host's operating system, service versions, and network configuration.
Security Audits: Besides troubleshooting, Nmap is also used for security auditing and identifying potential vulnerabilities.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Covers network scanning tools and their uses.
Nmap Documentation: Official documentation provides extensive details on how to use Nmap for port scanning and network diagnostics.
Network+ Certification All-in-One Exam Guide: Discusses various network utilities, including Nmap, and their applications in network troubleshooting.

Question: 117

A technician is planning an equipement installation into a rack in a data center that practices hot aisle/cold aise ventilation. Which of the following directions should the equipement exhaust face when installed in the rack?

A. Sides
B. Top
C. Front
D. Rear

Answer: D

Explanation:

In a data center that practices hot aisle/cold aisle ventilation, equipment should be installed so that the exhaust faces the rear of the rack. This setup ensures that hot air is expelled into the hot aisle, maintaining proper airflow and cooling efficiency.
Hot Aisle/Cold Aisle Configuration: Equipment intake should face the cold aisle where cool air is supplied, and exhaust should face the hot aisle where hot air is expelled.
Cooling Efficiency: Proper orientation of equipment helps maintain an efficient cooling environment by segregating hot and cold air, preventing overheating and improving energy efficiency.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses data center design principles, including hot aisle/cold aisle configurations.
Cisco Data Center Design Guide: Provides best practices for data center layout and equipment

installation.
Network+ Certification All-in-One Exam Guide: Covers data center environmental controls and ventilation strategies.

Question: 118

Which of the following technologies are X.509 certificates most commonly associated with?

A. PKI
B. VLAN tagging
C. LDAP
D. MFA

Answer: A

Explanation:

X.509 certificates are most commonly associated with Public Key Infrastructure (PKI). These certificates are used for a variety of security functions, including digital signatures, encryption, and authentication.
PKI: X.509 certificates are a fundamental component of PKI, used to manage encryption keys and authenticate users and devices.
Digital Certificates: They are used to establish secure communications over networks, such as SSL/TLS for websites and secure email communication.
Authentication and Encryption: X.509 certificates provide the means to securely exchange keys and verify identities in various applications, ensuring data integrity and confidentiality.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Covers PKI and the role of X.509 certificates in network security.
Cisco Networking Academy: Provides training on PKI, certificates, and secure communications.
Network+ Certification All-in-One Exam Guide: Explains PKI, X.509 certificates, and their applications in securing network communications.

Question: 119

A company is hosting a secure that requires all connections to the server to be encrypted. A junior administrator needs to harded the web server. The following ports on the web server. The following ports on the web server are open:

Which of the following ports should be disabled?

A. 22
B. 80
C. 443
D. 587

Answer: B

Explanation:

For a web server that requires all connections to be encrypted, port 80 (HTTP) should be disabled. Port 80 is used for unencrypted web traffic, whereas port 443 is used for HTTPS, which provides encrypted communication.
Port 80 (HTTP): This port is used for unsecured web traffic. Disabling this port ensures that all web traffic must use HTTPS, which encrypts the data in transit.
Port 443 (HTTPS): This port is used for secure web traffic via SSL/TLS encryption. Keeping this port open ensures that secure connections can be made to the web server.
Other Ports:
Port 22: Used for SSH, providing secure remote access and file transfers.
Port 587: Used for secure email submission (SMTP) with encryption.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses the roles and security implications of various ports and protocols.
Cisco Networking Academy: Provides training on secure web server configuration and port management.
Network+ Certification All-in-One Exam Guide: Covers port security and best practices for securing web servers.

Question: 120

A network administrator is planning to implement device monitoring to enhance network visibility. The security that the solution provies authentication and encryption. Which of the following meets these requirements?

A. SIEM
B. Syslog
C. NetFlow
D. SNMPv3

Answer: D

Explanation:

SNMPv3 (Simple Network Management Protocol version 3) provides device monitoring with authentication and encryption. This enhances network visibility and security by ensuring that monitoring data is securely transmitted and access to network devices is authenticated.
Authentication: SNMPv3 includes robust mechanisms for authenticating users accessing network devices.
Encryption: It provides encryption to protect the integrity and confidentiality of the data being transmitted.
Network Management: SNMPv3 allows for detailed monitoring and management of network devices, ensuring better control and security.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Covers SNMP versions, their features, and security enhancements in SNMPv3.

Cisco Networking Academy: Provides training on implementing and securing SNMP for network management.
Network+ Certification All-in-One Exam Guide: Explains the benefits and security features of SNMPv3 for network monitoring.

Question: 121

A network administrator needs to change where the outside DNS records are hosted. Which of the following records should the administrator change the registrar to accomplish this task?

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

Answer: A

Explanation:

To change where the outside DNS records are hosted, the network administrator needs to update the NS (Name Server) records at the domain registrar. NS records specify the authoritative name servers for a domain, directing where DNS queries should be sent.
NS (Name Server) Records: These records indicate the servers that are authoritative for a domain. Changing the NS records at the registrar points DNS resolution to the new hosting provider.
SOA (Start of Authority): Contains administrative information about the domain, including the primary name server.
PTR (Pointer) Records: Used for reverse DNS lookups, mapping IP addresses to domain names.
CNAME (Canonical Name) Records: Used to alias one domain name to another, not relevant for changing DNS hosting.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses DNS records, their purposes, and how to manage them.
Cisco Networking Academy: Provides training on DNS management and the role of different DNS record types.
Network+ Certification All-in-One Exam Guide: Explains DNS records and their configuration for domain management.

Question: 122

Which of the following ports is used for secure email?

A. 25
B. 110
C. 143
D. 587

Answer: D

Explanation:

Port 587 is used for secure email submission. This port is designated for message submission by mail clients to mail servers using the SMTP protocol, typically with STARTTLS for encryption.
Port 25: Traditionally used for SMTP relay, but not secure and often blocked by ISPs for outgoing mail due to spam concerns.
Port 110: Used for POP3 (Post Office Protocol version 3), not typically secured.
Port 143: Used for IMAP (Internet Message Access Protocol), which can be secured with STARTTLS or SSL/TLS.
Port 587: Specifically used for authenticated email submission (SMTP) with encryption, ensuring secure transmission of email from clients to servers.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses email protocols and ports, including secure email transmission.
Cisco Networking Academy: Provides training on securing email communications and the use of appropriate ports.
Network+ Certification All-in-One Exam Guide: Explains email protocols, ports, and security considerations for email transmission.

Question: 123

A company is implementing a wireless solution in a high-density environment. Which of the following 802.11 standards is used when a company is concerned about device saturation and converage?

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

Answer: B

Explanation:

802.11ax, also known as Wi-Fi 6, is designed for high-density environments and improves device saturation and coverage compared to previous standards.
802.11ac: While it offers high throughput, it is not optimized for high-density environments as effectively as 802.11ax.
802.11ax (Wi-Fi 6): Introduces features like OFDMA, MU-MIMO, and BSS Coloring, which enhance performance in crowded environments, reduce latency, and increase the number of devices that can be connected simultaneously.
802.11g and 802.11n: Older standards that do not offer the same level of efficiency or support for high device density as 802.11ax.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Covers the 802.11 standards and their capabilities.
Cisco Networking Academy: Provides training on Wi-Fi technologies and best practices for high-density deployments.
Network+ Certification All-in-One Exam Guide: Discusses the various 802.11 standards and their applications in different environments.

Question: 124

Which of the following appliances provides users with an extended footprint that allows connections from multiple devices within a designated WLAN?

A. Router
B. Switch
C. Access point
D. Firewall

Answer: C

Explanation:

An access point (AP) provides users with an extended footprint that allows connections from multiple devices within a designated Wireless Local Area Network (WLAN).
Router: Typically used to connect different networks, not specifically for extending wireless coverage.
Switch: Used to connect devices within a wired network, not for providing wireless access.
Access Point (AP): Extends wireless network coverage, allowing multiple wireless devices to connect to the network.
Firewall: Primarily used for network security, controlling incoming and outgoing traffic based on security rules, not for providing wireless connectivity.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Explains the roles and functions of network appliances, including access points.
Cisco Networking Academy: Provides training on deploying and managing wireless networks with access points.
Network+ Certification All-in-One Exam Guide: Covers network devices and their roles in creating and managing networks.

Question: 125

Which of the following is an XML-based security concept that works by passing sensitve information about users, such as log-in information and attributes, to providers.

A. IAM
B. MFA
C. RADIUS
D. SAML

Answer: D

Explanation:

Security Assertion Markup Language (SAML) is an XML-based standard used for exchanging authentication and authorization data between parties, particularly between an identity provider (IdP) and a service provider (SP). SAML is commonly used in Single Sign-On (SSO) solutions to pass sensitive user information, such as login credentials and attributes, securely between the identity

provider and the service provider.
SAML (Security Assertion Markup Language): Facilitates web-based authentication and authorization, allowing users to access multiple services with a single set of credentials.
XML-based: Uses XML to encode the authentication and authorization data, ensuring secure transmission of user information.
Identity Federation: Enables secure sharing of identity information across different security domains, making it ideal for enterprise SSO solutions.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Covers authentication protocols, including SAML.
Cisco Networking Academy: Provides training on identity management and federation technologies.
Network+ Certification All-in-One Exam Guide: Explains SAML and its role in secure identity management and SSO.

Question: 126

A newtwork administrator needs to create an SVI on a Layer 3-capable device to separate voice and data traffic. Which of the following best explains this use case?

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

Answer: C

Explanation:

An SVI (Switched Virtual Interface) is a logical interface on a Layer 3-capable switch used to route traffic between VLANs. This is particularly useful in environments where voice and data traffic need to be separated, as each type of traffic can be assigned to different VLANs and routed accordingly.
SVI (Switched Virtual Interface): A virtual interface created on a switch for inter-VLAN routing.
VLAN Routing: Enables the routing of traffic between VLANs on a Layer 3 switch, allowing for logical separation of different types of traffic, such as voice and data.
Use Case: Commonly used in scenarios where efficient and segmented traffic management is required, such as in VoIP implementations.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses VLANs, SVIs, and their applications in network segmentation and routing.
Cisco Networking Academy: Provides training on VLAN configuration and inter-VLAN routing using SVIs.
Network+ Certification All-in-One Exam Guide: Covers network segmentation techniques, including the use of SVIs for VLAN routing.

Question: 127

A storage network requires reduced overhead and increased efficiency for the amout of data being sent. Which of the following should an engineer likely configure to meet these requirements>?

A. Link speed
B. Jumbo frames
C. QoS
D. 802.1q tagging

Answer: B

Explanation:

Jumbo frames are Ethernet frames with a payload greater than the standard maximum transmission unit (MTU) of 1500 bytes. Configuring jumbo frames can reduce overhead and increase efficiency in storage networks by allowing more data to be sent in each frame, thus reducing the number of frames needed to transmit the same amount of data.
Reduced Overhead: By sending larger frames, the relative overhead for headers and acknowledgments is reduced.
Increased Efficiency: Larger frames mean fewer packets to process, leading to better utilization of network bandwidth and improved performance in high-throughput environments like storage networks.
Configuration: Requires support from all devices in the network path, including switches and network interface cards (NICs).
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Explains jumbo frames and their benefits in reducing network overhead.
Cisco Networking Academy: Provides training on network optimization techniques, including the use of jumbo frames.
Network+ Certification All-in-One Exam Guide: Covers advanced Ethernet features, including jumbo frames and their configuration for improved network performance.

Question: 128

An administrator is configuring a switch that will be placed in an area of the office that is accessible to customers. Which of the following is the best way for the administrator to mitigate unknown devices from connecting to the network?

A. SSE
B. ACL
C. Perimeter network
D. 802.1x

Answer: D

Explanation:

802.1x is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. This ensures that only authorized devices can access the network, making it ideal for mitigating the risk of unknown devices connecting to the network, especially in accessible areas.
802.1x Authentication: Requires devices to authenticate using credentials (e.g., username and

password, certificates) before gaining network access.
Access Control: Prevents unauthorized devices from connecting to the network, enhancing security in public or semi-public areas.
Implementation: Typically used in conjunction with a RADIUS server to manage authentication requests.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Covers 802.1x and its role in network security.
Cisco Networking Academy: Provides training on implementing 802.1x for secure network access control.
Network+ Certification All-in-One Exam Guide: Explains the benefits and configuration of 802.1x authentication in securing network access.

Question: 129

Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?

A. To encrypt sensitive data in transit
B. To secure the endpoint
C. To maintain contractual agreements
D. To comply with data retentin requirements

Answer: A

Explanation:

The most likely reason an insurance brokerage would enforce VPN usage is to encrypt sensitive data in transit. VPNs (Virtual Private Networks) create a secure tunnel between the user's device and the corporate network, ensuring that data is encrypted and protected from interception.
Encryption: VPNs encrypt data, preventing unauthorized access and ensuring data privacy during transmission over public or unsecured networks.
Data Protection: Essential for industries handling sensitive information, such as insurance brokerages, to protect customer data and comply with regulatory requirements.
Security: Enhances overall network security by providing secure remote access for employees.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses the role of VPNs in securing data in transit.
Cisco Networking Academy: Provides training on VPN technologies and their importance in data security.
Network+ Certification All-in-One Exam Guide: Explains VPN usage and its benefits in protecting sensitive information.

Question: 130

A network engineer configures a new switch and connects it to an existing switch for expansion and redundancy. Users immediately lose connectivity to the network. The network engineer notes the

following spanning tree information from both switches:

Switch 1
Port State Cost
1 Forward 2
2 Forward 2

Switch 2
Port State Cost
1 Forward 2
2 Forward 2

Which of the following best describes the issue?

A. The port cost should not be equal.
B. The ports should use link aggregation.
C. A root bridge needs to be identified.
D. The switch should be configured for RSTP.

Answer: C

Explanation:

The issue is that no root bridge has been identified. In STP, a root bridge is necessary to manage redundant paths and avoid loops in the network. Without a root bridge, all switches will assume they can forward traffic, causing a network loop and connectivity problems.

Question: 131

Which of the following facilities is the best example of a warm site in the event of information system disruption?

A. A combination of public and private cloud services to restore data
B. A partial infrastructure, software, and data on site
C. A full electrical infrastructure in place, but no customer devices on site
D. A full infrastructure in place, but no current data on site

Answer: D

Explanation:

A warm site typically has a full infrastructure ready, but it lacks the most up-to-date data or is not immediately operational. It requires some configuration or data restoration to become fully functional.

Question: 132

Which of the following would be violated if an employee accidentally deleted a customer's data?

A. Integrity
B. Confidentiality
C. Vulnerability
D. Availability

Answer: D

Explanation:

Availability refers to ensuring that data is accessible when needed. If a customer's data is accidentally deleted, it impacts availability, as the data can no longer be accessed.

Question: 133

Which of the following is used to describe the average duration of an outage for a specific service?

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

Answer: B

Explanation:

MTTR (Mean Time to Repair) is the average time it takes to repair a system or service after a failure. It helps in measuring the downtime and planning recovery processes.

Question: 134

Three access points have Ethernet that runs through the ceiling. One of the access points cannot reach the internet. Which of the following tools can help identify the issue?

A. Network tap
B. Cable tester
C. Visual fault locator
D. Toner and probe

Answer: B

Explanation:

A cable tester is a tool that can help identify issues with the physical cabling, such as breaks or improper terminations, which may prevent the access point from reaching the internet.

Question: 135

Following a fire in a data center, the cabling was replaced. Soon after, an administrator notices network issues. Which of the following are the most likely causes of the network issues? (Select two).

A. The switches are not the correct voltage.
B. The HVAC system was not verified as fully functional after the fire.
C. The VLAN database was not deleted before the equipment was brought back online.
D. The RJ45 cables were replaced with unshielded cables.
E. The wrong transceiver type was used for the new termination.

F. The new RJ45 cables are a higher category than the old ones.

Answer: D, E

Explanation:

Unshielded cables (D) are more prone to interference and may not be suitable for certain environments, especially after a fire where interference could be heightened.

Using the wrong transceiver (E) for new terminations can lead to compatibility issues, causing network failures.

Question: 136

Which of the following steps in the troubleshooting methodology would be next after putting preventive measures in place?

A. Implement the solution.
B. Verify system functionality.
C. Establish a plan of action.
D. Test the theory to determine cause.

Answer: B

Explanation:

After implementing a solution and putting preventive measures in place, the next step is to verify that the system is functioning correctly. This ensures that the issue has been fully resolved.

Question: 137

An organization wants to ensure that incoming emails were sent from a trusted source. Which of the following DNS records is used to verify the source?

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

Answer: A

Explanation:

A TXT record can be used to store SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) information, which help verify that an email has been sent from a trusted source.

Question: 138

A network technician is examining the configuration on an access port and notices more than one VLAN has been set. Which of the following best describes how the port is configured?

A. With a voice VLAN
B. With too many VLANs
C. With a default VLAN
D. With a native VLAN

Answer: A

Explanation:

It is common for an access port to have both a voice VLAN and a data VLAN. A voice VLAN separates voice traffic from regular data traffic, ensuring better quality and security for voice communications.

Question: 139

Which of the following can also provide a security feature when implemented?

A. NAT
B. BGP
C. FHRP
D. EIGRP

Answer: A

Explanation:

NAT (Network Address Translation) helps hide internal IP addresses from external networks, adding a layer of security by preventing direct access to internal systems from the outside.

Question: 140

A systems administrator is configuring a new device to be added to the network. The administrator is planning to perform device hardening prior to connecting the device. Which of the following should the administrator do first?

A. Update the network ACLs.

B. Place the device in a screened subnet.

C. Enable content filtering.

D. Change the default admin passwords.

Answer: D

Explanation:

Changing default admin passwords is a fundamental first step in device hardening to prevent unauthorized access.

Question: 141

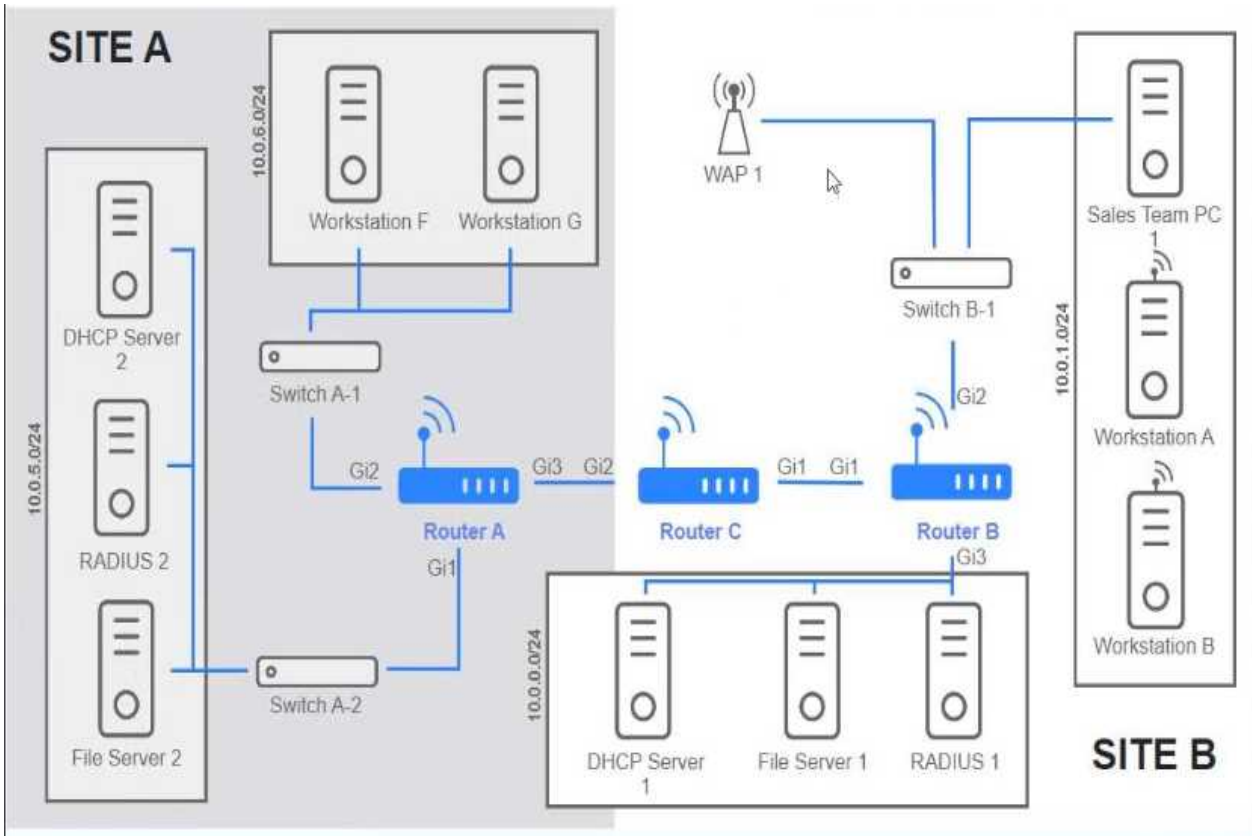
SIMULATION

Users are unable to access files on their department share located on flle_server 2. The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.

INSTRUCTIONS

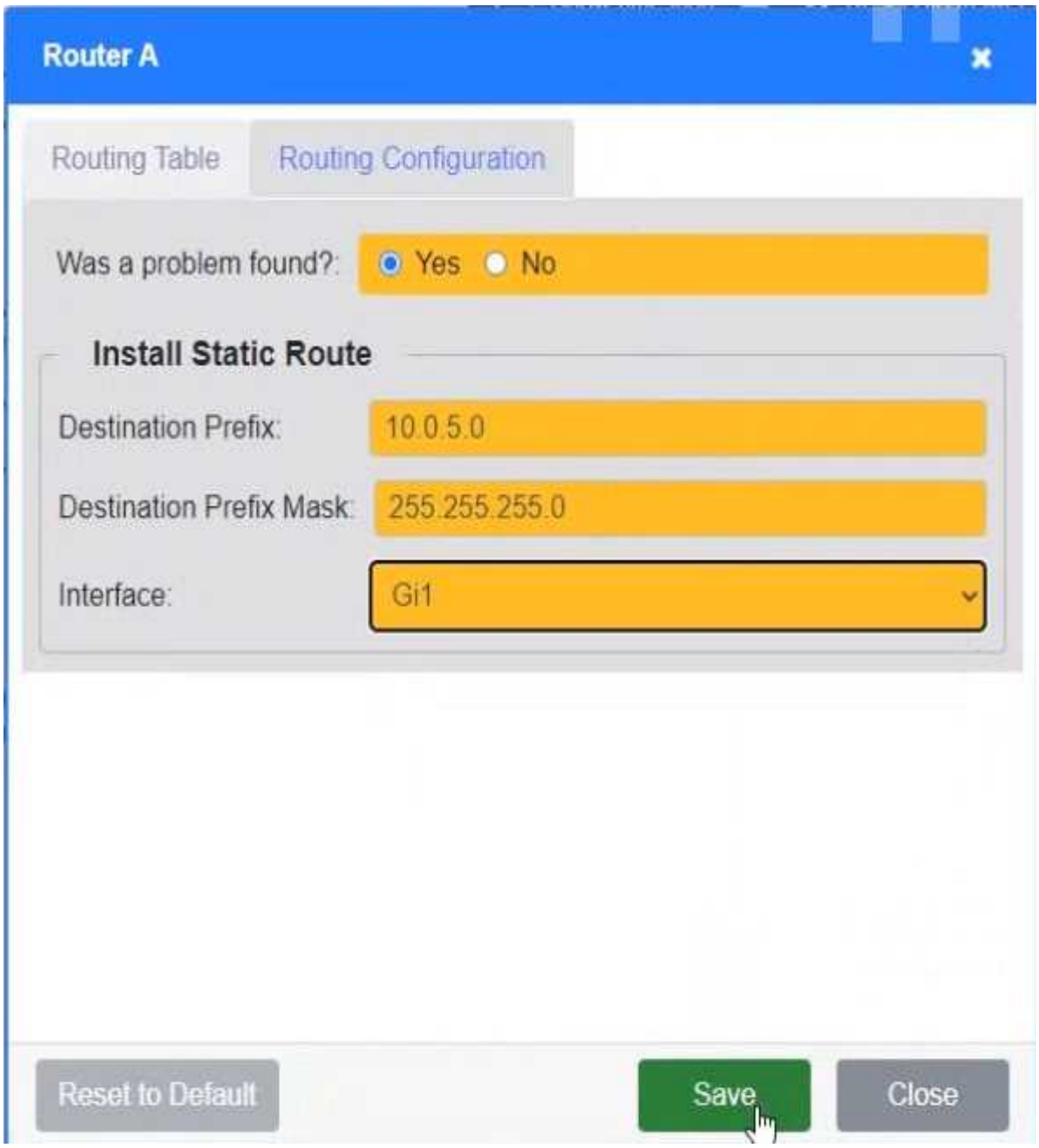
Click on each router to review output, identity any Issues, and configure the appropriate solution

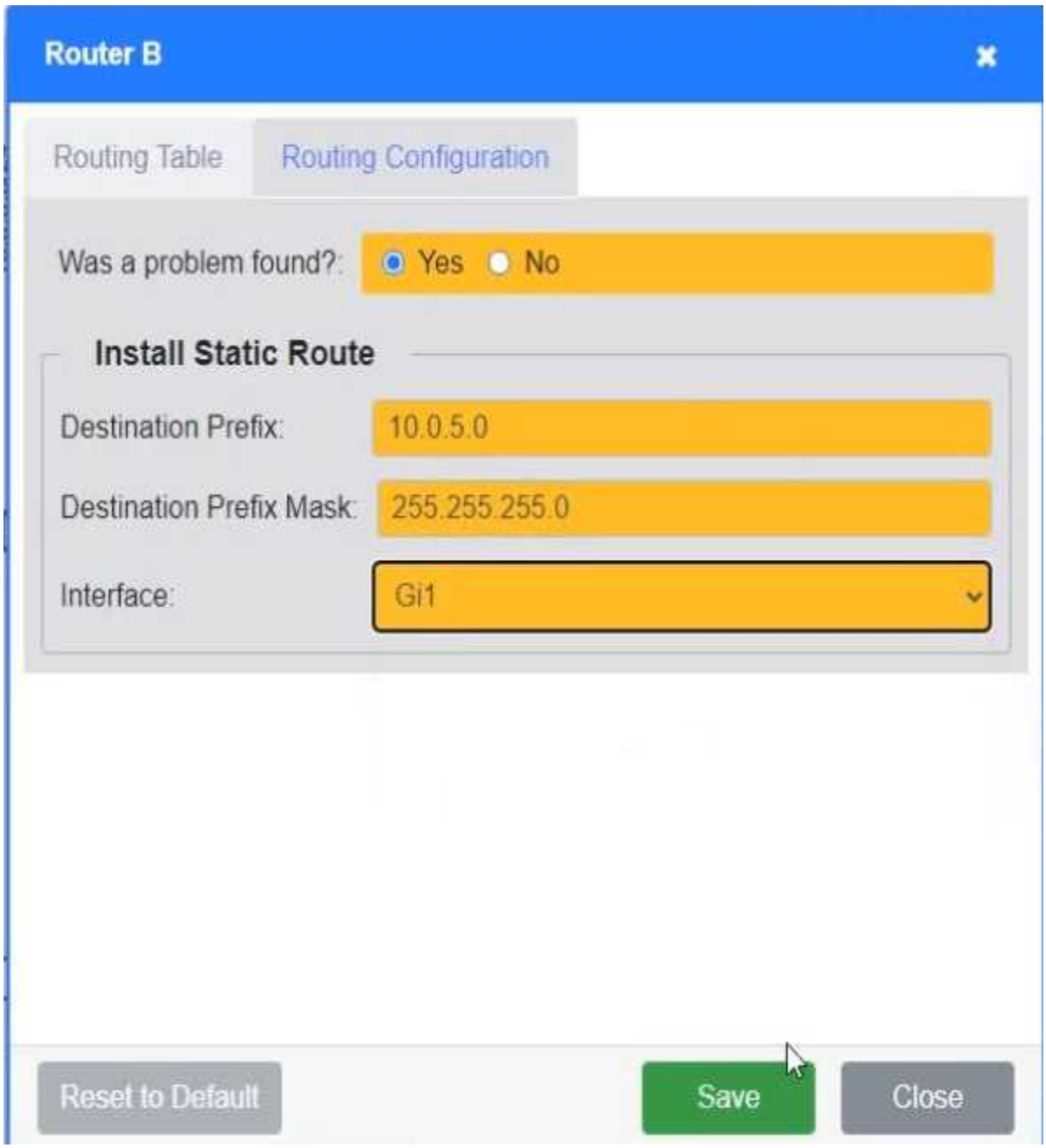
If at any time you would like to bring back the initial state of trie simulation, please click the reset All button;

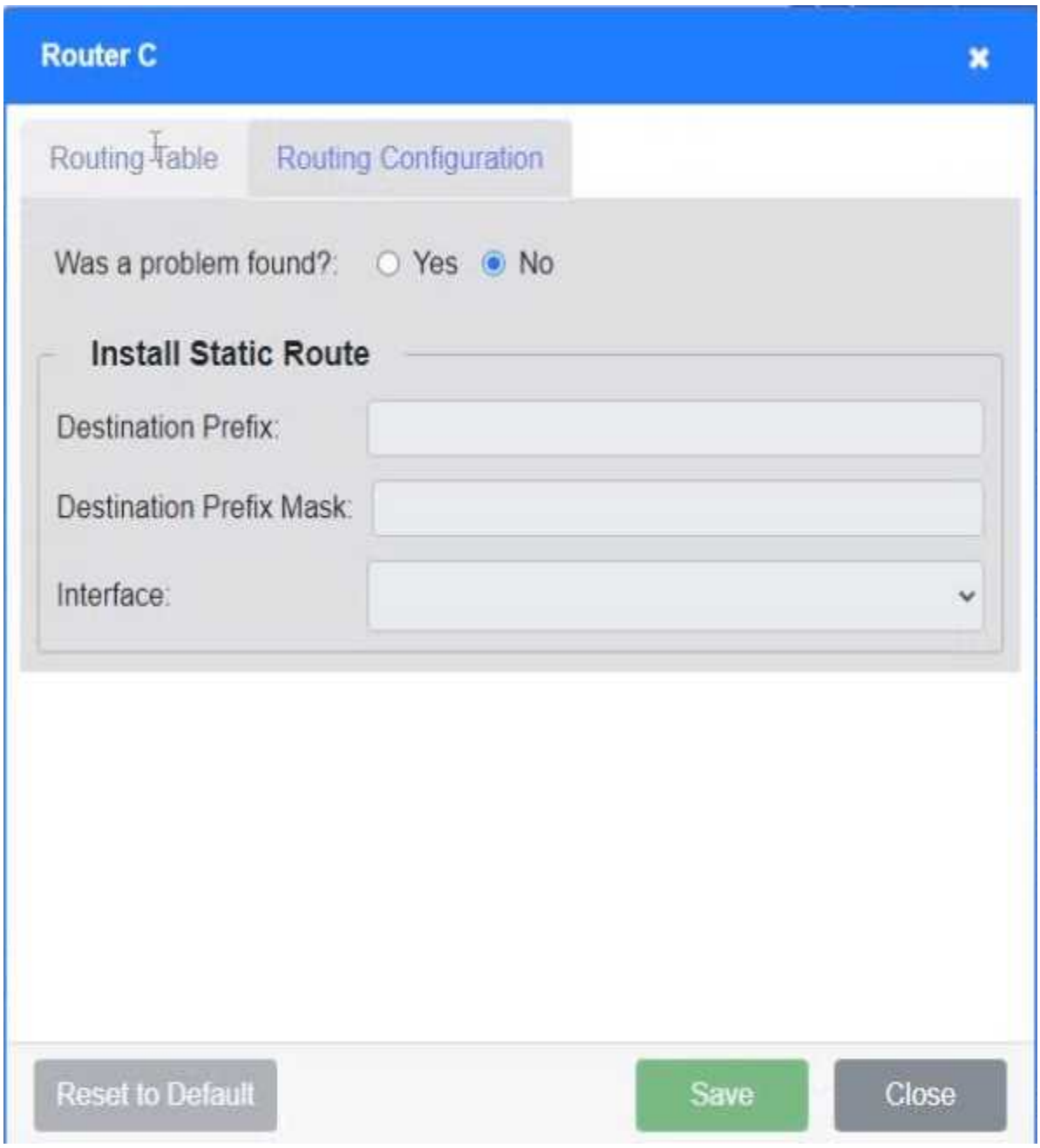


Answer: See the solution configuration below in Explanation.

Explanation:


Router A
Routing Table
Routing Configuration
Was a problem found?:
Yes
No
Install Static Route
Destination Prefix:
10.0.5.0
Destination Prefix Mask:
255.255.255.0
Interface:
Gi1
Reset to Default
Save
Close


Router B
Routing Table
Routing Configuration
Was a problem found?:
Yes
No
Install Static Route
Destination Prefix:
10.0.5.0
Destination Prefix Mask:
255.255.255.0
Interface:
Gi1
Reset to Default
Save
Close


Router C
Routing Table
Routing Configuration
Was a problem found?: Yes No
Install Static Route
Destination Prefix:
Destination Prefix Mask:
Interface:
Reset to Default
Save
Close