CompTIA.N10-009.vAug-2024.by.Enys.40q

Number: N10-009
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: N10-009

Exam Name: CompTIA Network+ Certification

Exam A

QUESTION 1

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

Correct Answer: A
Section:
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.
CompTIA Network+ study materials and system administration documentation.

QUESTION 2

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

Correct Answer: A
Section:
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.
CompTIA Network+ course materials and networking solution guides.

QUESTION 3
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

Correct Answer: A
Section:
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

QUESTION 4
Which of the following technologies are X.509 certificates most commonly associated with?

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

Correct Answer: A
Section:
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 5
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.

Correct Answer: A
Section:
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.
CompTIA Network+ study materials and structured cabling installation guides.

QUESTION 6
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

Correct Answer: B
Section:
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.

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

QUESTION 7
Which of the following is the most closely associated with segmenting compute resources within a single cloud account?

A. Network security group
B. IaaS
C. VPC
D. Hybrid cloud

Correct Answer: C
Section:
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 8
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

Correct Answer: A
Section:
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 9
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.

Correct Answer: D
Section:
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 10
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

Correct Answer: A
Section:
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 11
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

Correct Answer: D
Section:
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 12
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.

Correct Answer: C
Section:
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

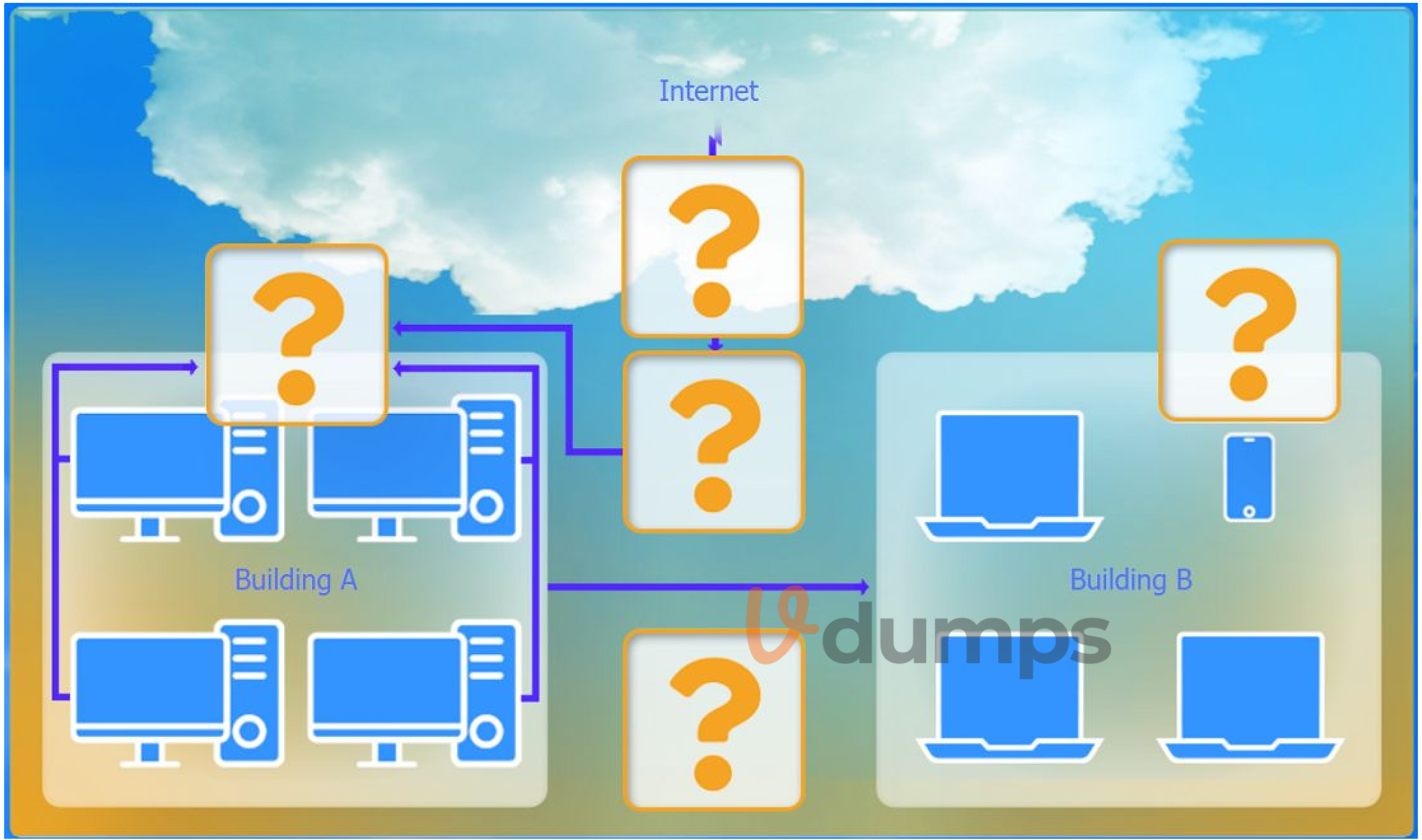
security purposes and do not directly restrict physical port access based on device identity.
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

QUESTION 13
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?

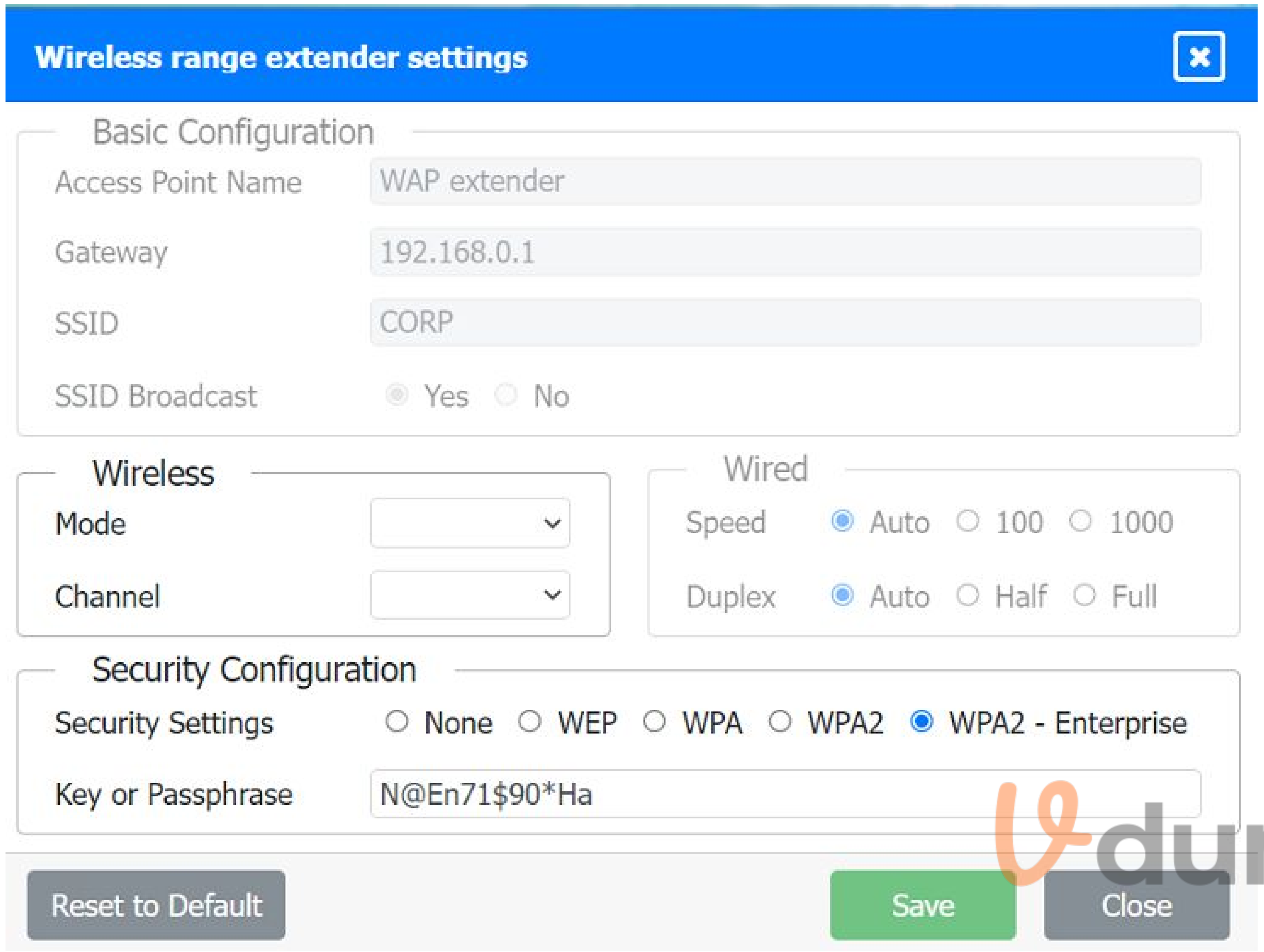
A. Implementing enterprise authentication
B. Requiring the use of PSKs
C. Configuring a captive portal for users
D. Enforcing wired equivalent protection

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

QUESTION 14
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

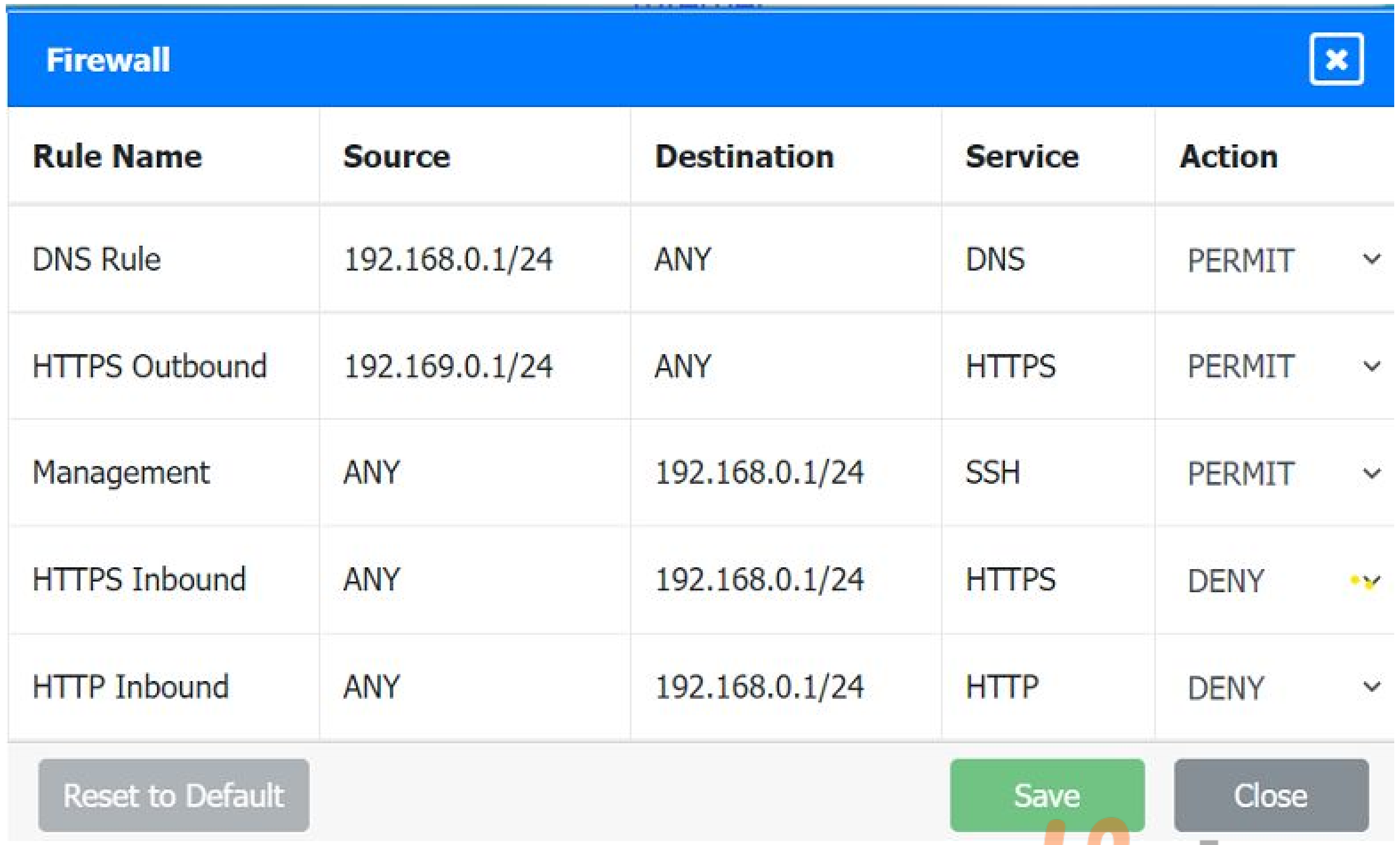
Speed: ● Auto ○ 100 ○ 1000

Duplex: ● Auto ○ Half ○ Full

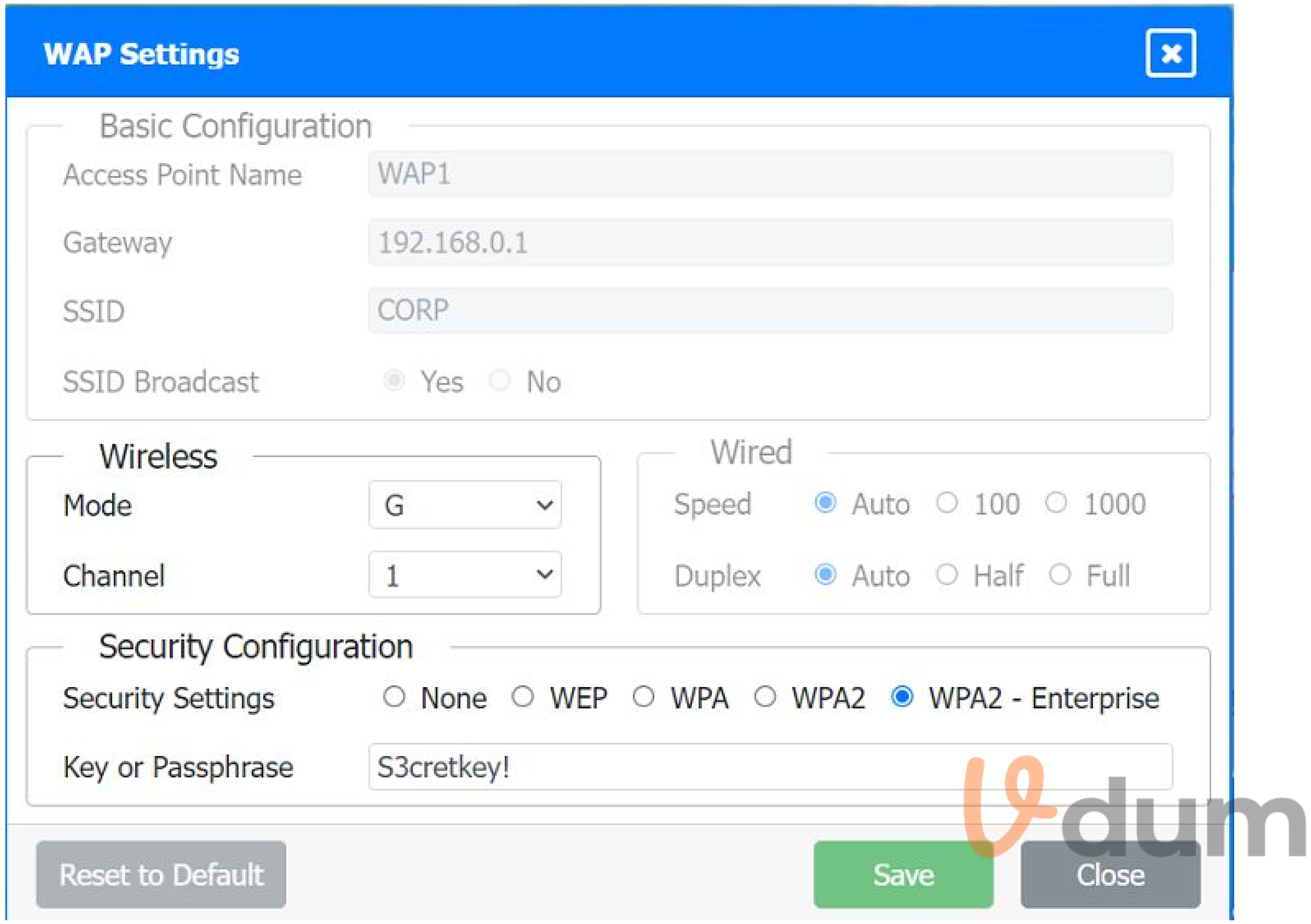
Security Configuration

Security Settings: ○ None ○ WEP ○ WPA ○ WPA2 ● WPA2 - Enterprise

Key or Passphrase: N@En71$90*Ha



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



WAP Settings

Basic Configuration

Access Point Name	WAP1
Gateway	192.168.0.1
SSID	CORP
SSID Broadcast	● Yes ○ No

Wireless

Mode	G
Channel	1

Wired

Speed	● Auto ○ 100 ○ 1000
Duplex	● Auto ○ Half ○ Full

Security Configuration

Security Settings	○ None ○ WEP ○ WPA ○ WPA2 ● WPA2 - Enterprise
Key or Passphrase	S3cretkey!

A. See the step by step complete solution below

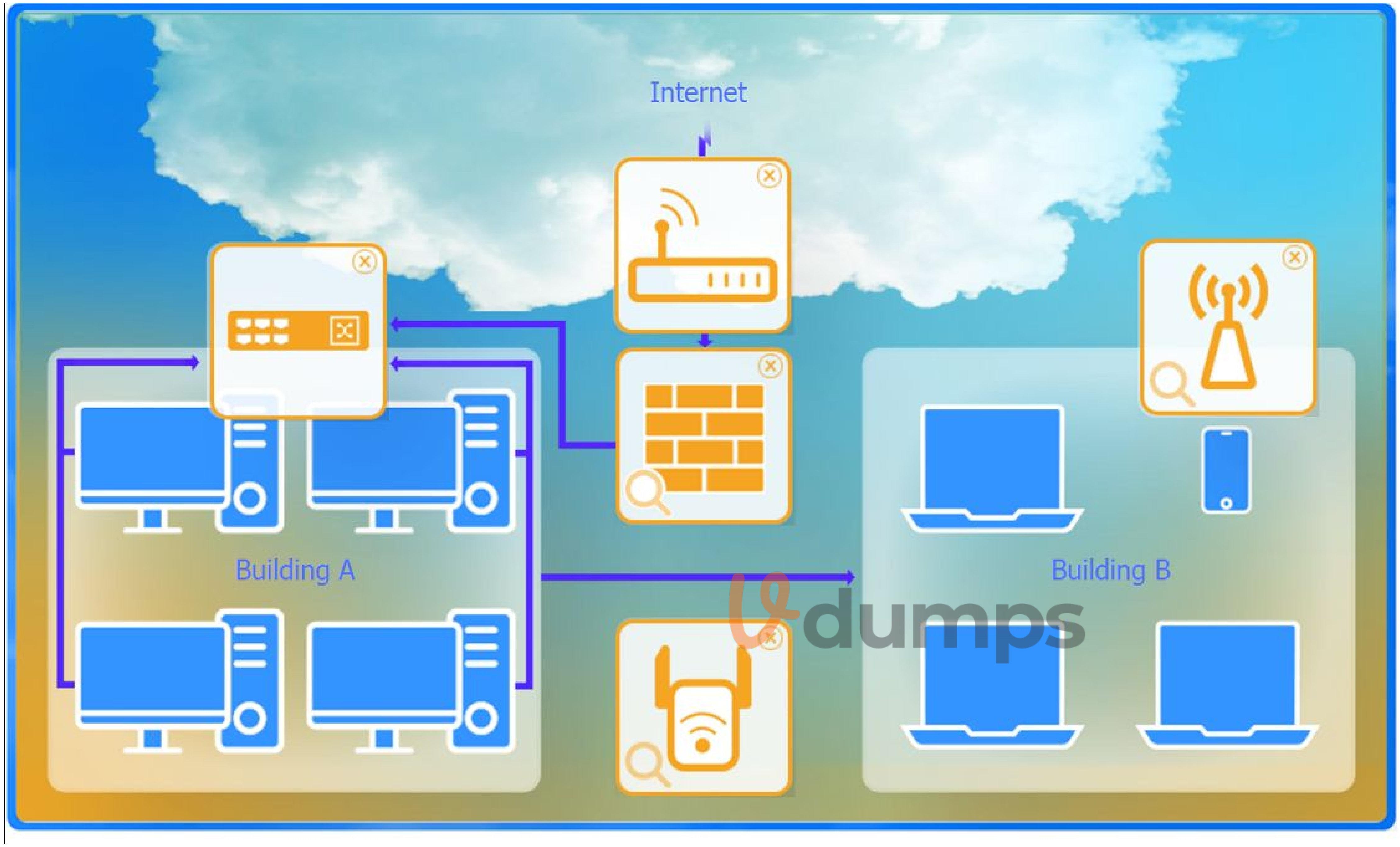
Correct Answer: A
Section:
Explanation:
Devices in both buildings should be able to access the Internet.
Security insists that all Internet traffic be inspected before entering the network.
Desktops should not see traffic destined for other devices.
Here is the corrected layout with explanation:
Building 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

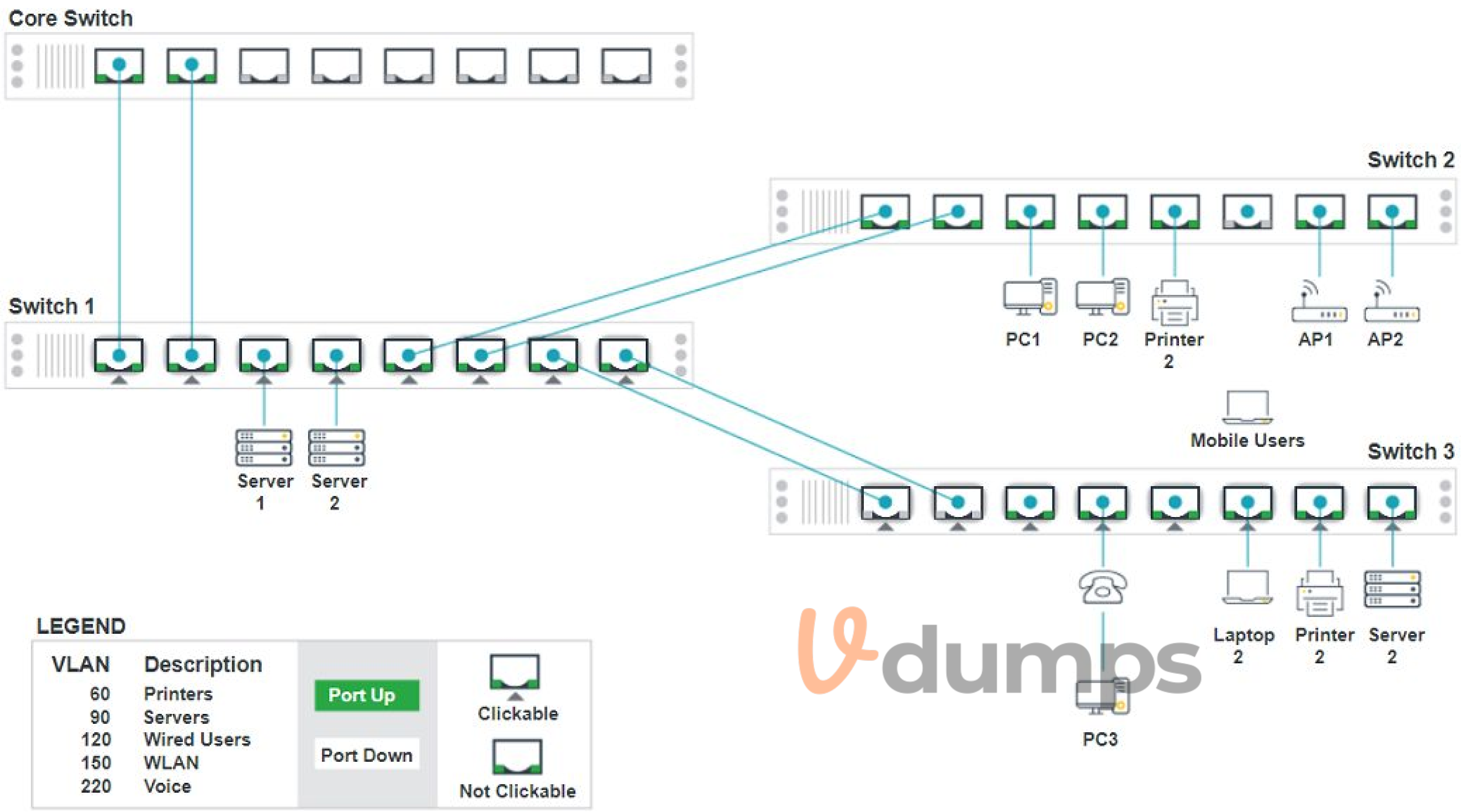
HTTPS

PERMIT

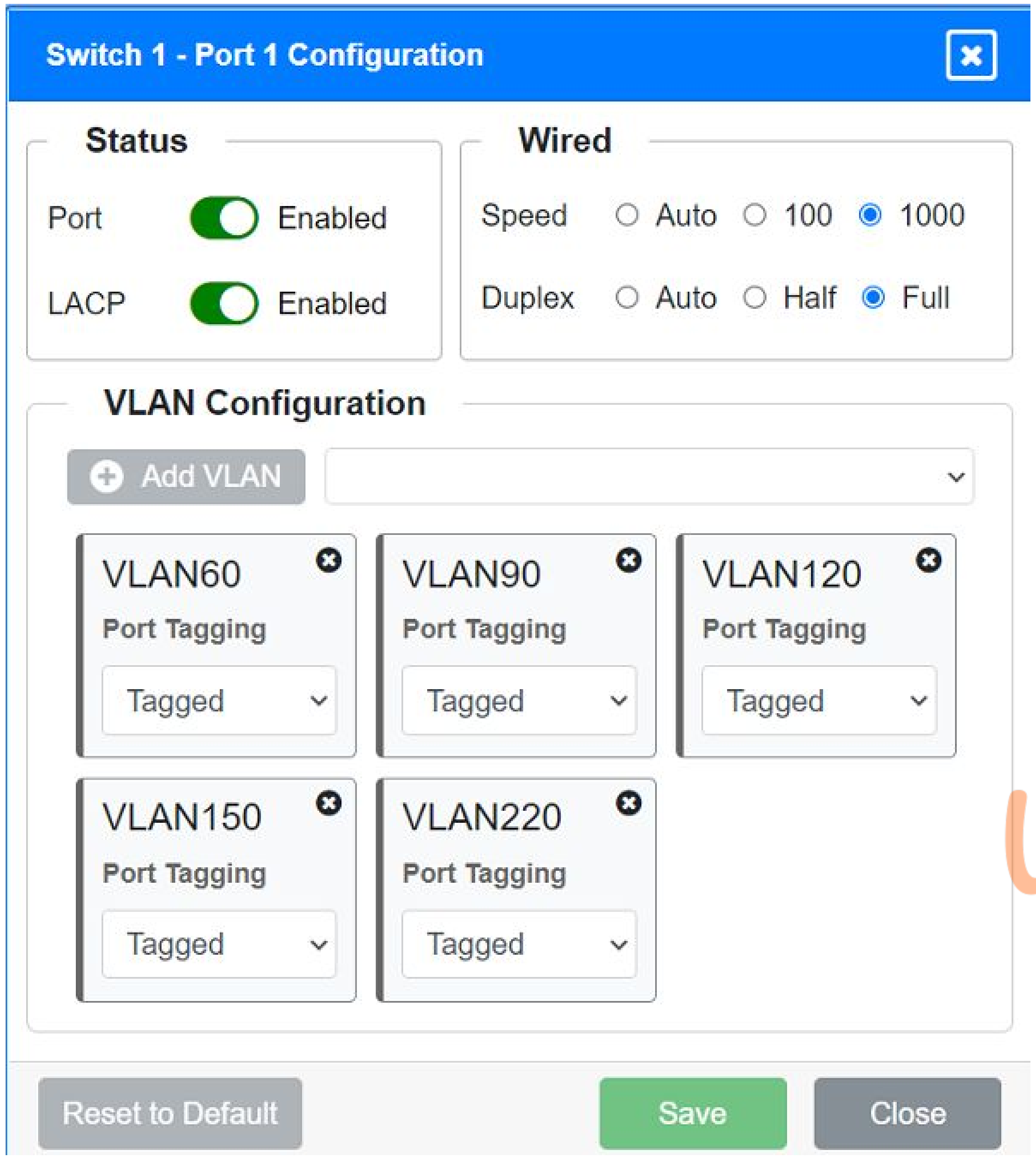
Management

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 15
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.



VLAN	Description
60	Printers
90	Servers
120	Wired Users
150	WLAN
220	Voice



Switch 1 - Port 1 Configuration

Status

Port: Enabled

LACP: Enabled

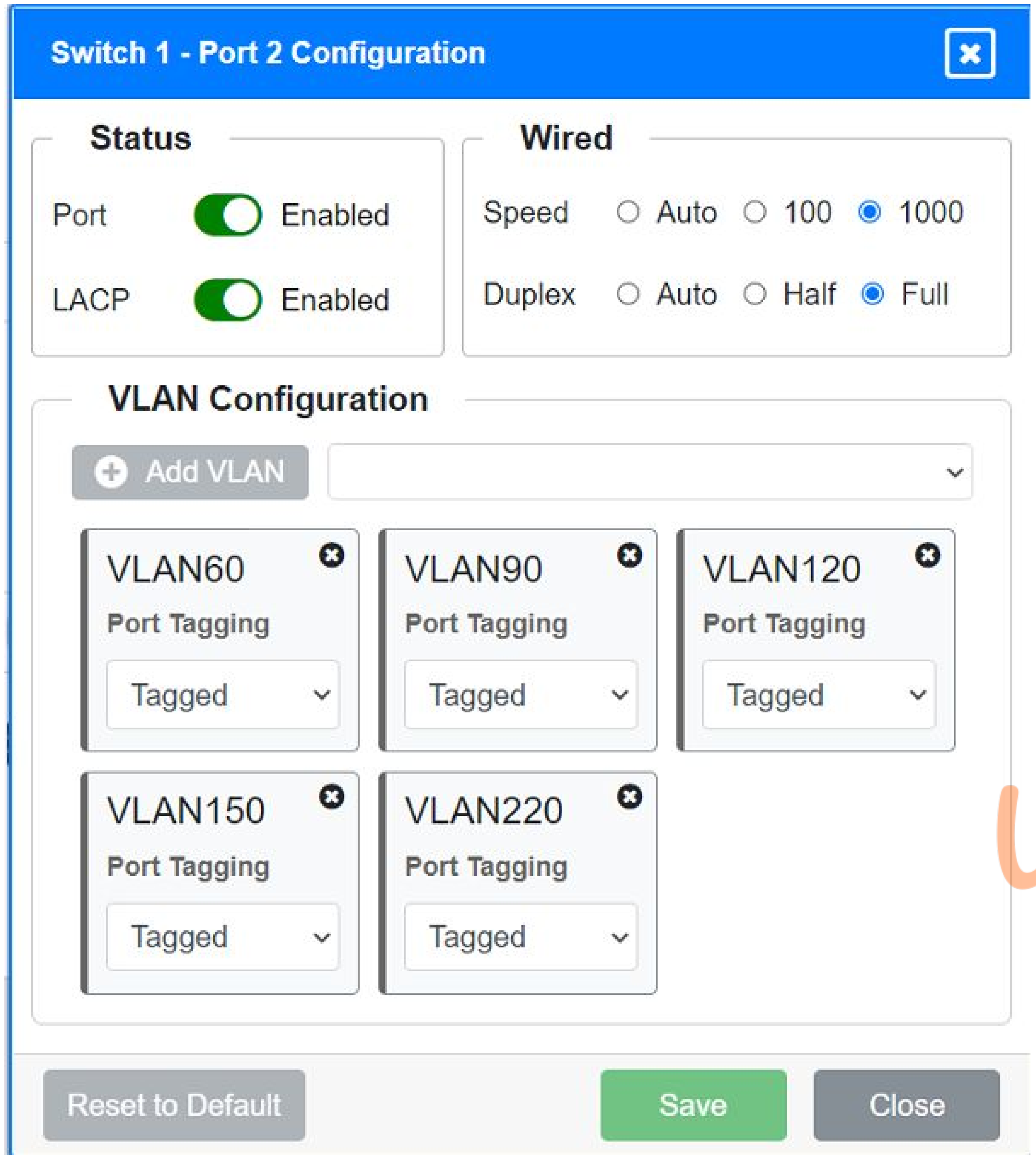
Wired

Speed: ○ Auto ○ 100 ● 1000

Duplex: ○ Auto ○ Half ● Full

VLAN Configuration

VLAN	Port Tagging
VLAN60	Tagged
VLAN90	Tagged
VLAN120	Tagged
VLAN150	Tagged
VLAN220	Tagged



Switch 1 - Port 2 Configuration

Status

Port: Enabled

LACP: Enabled

Wired

Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

VLAN Configuration

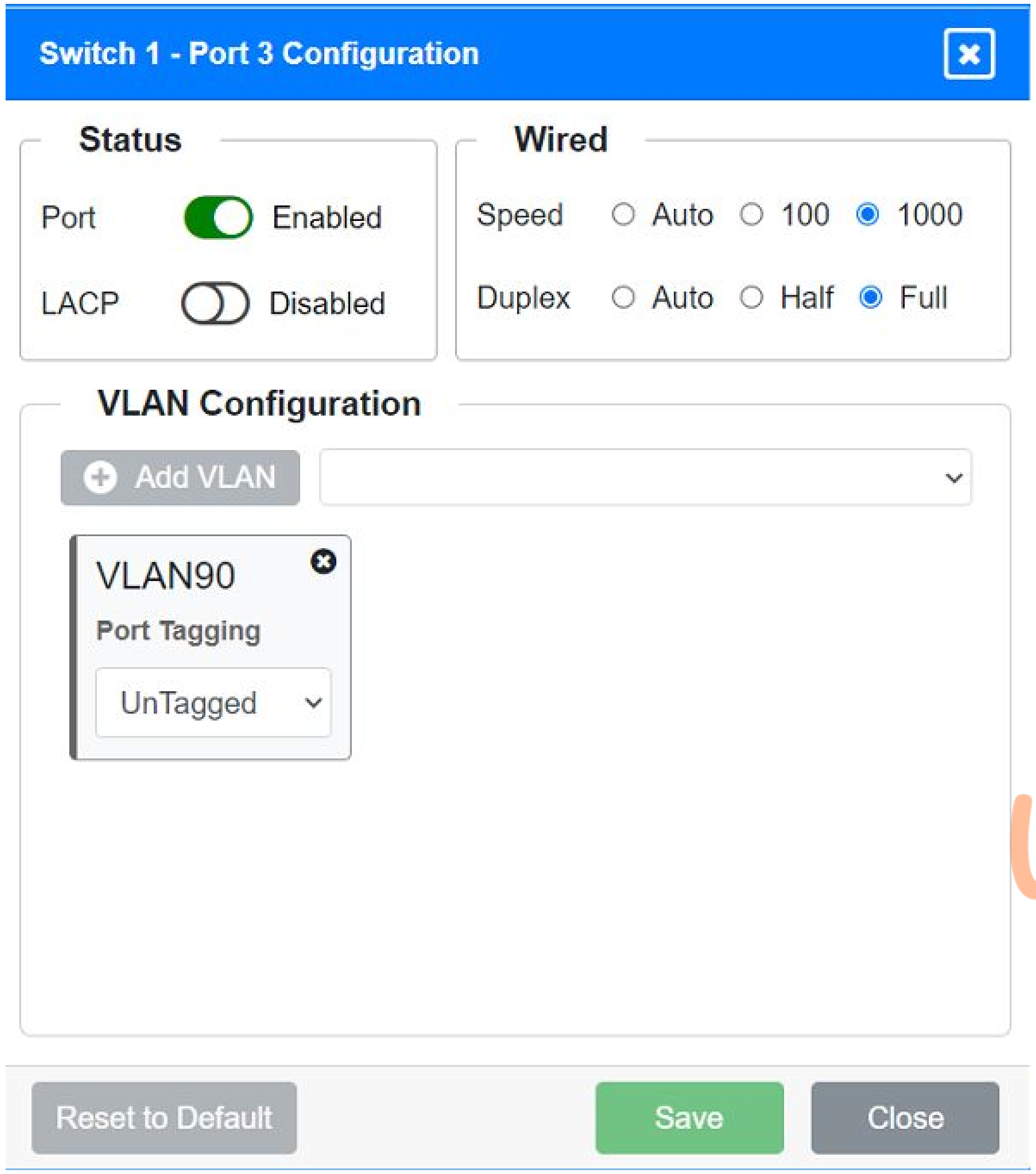
VLAN60
Port Tagging: Tagged

VLAN90
Port Tagging: Tagged

VLAN120
Port Tagging: Tagged

VLAN150
Port Tagging: Tagged

VLAN220
Port Tagging: Tagged



Switch 1 - Port 3 Configuration

Status

Port: Enabled

LACP: Disabled

Wired

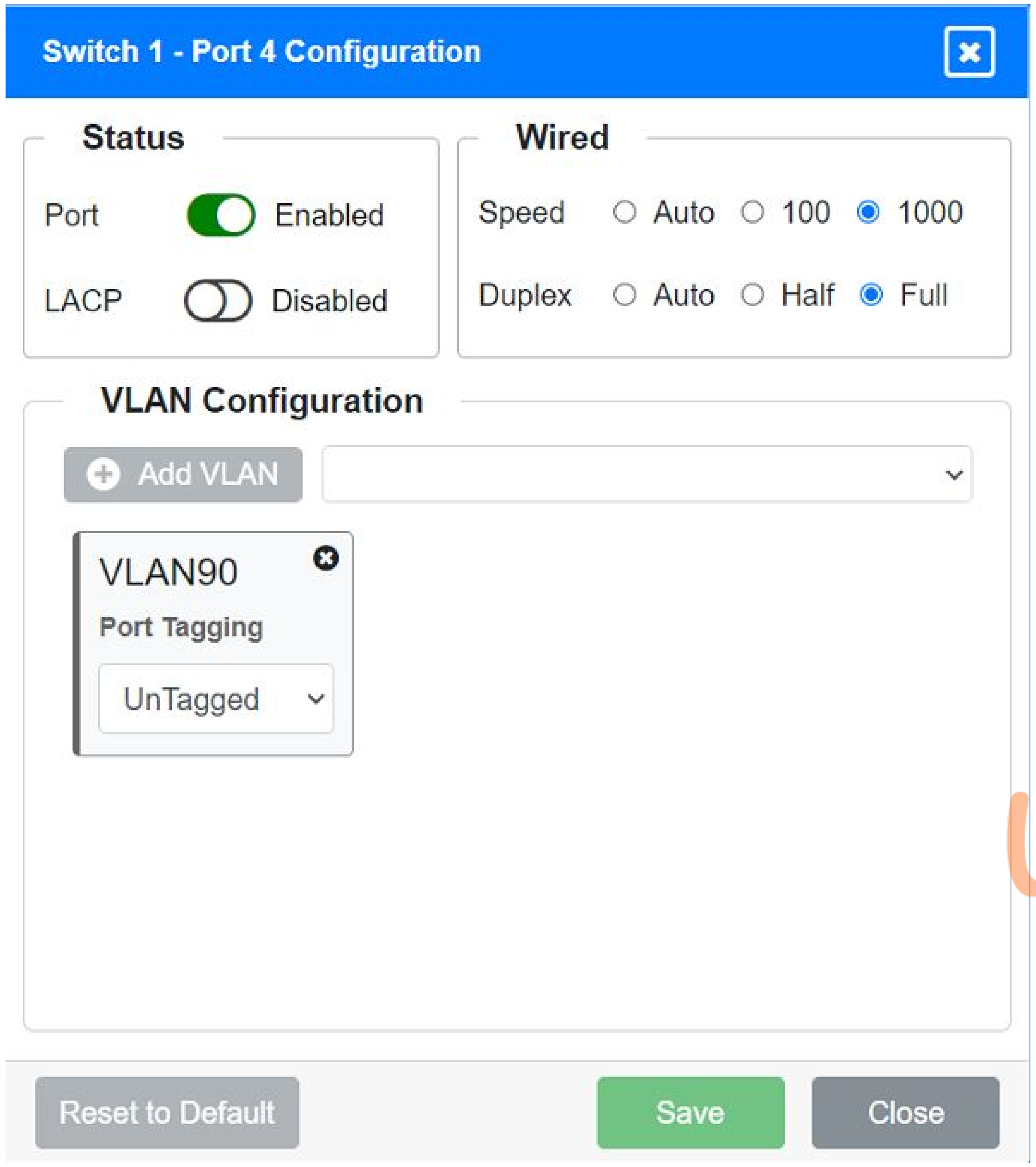
Speed: ○ Auto ○ 100 ● 1000

Duplex: ○ Auto ○ Half ● Full

VLAN Configuration

VLAN90

Port Tagging: UnTagged



Switch 1 - Port 4 Configuration

Status

Port: Enabled

LACP: Disabled

Wired

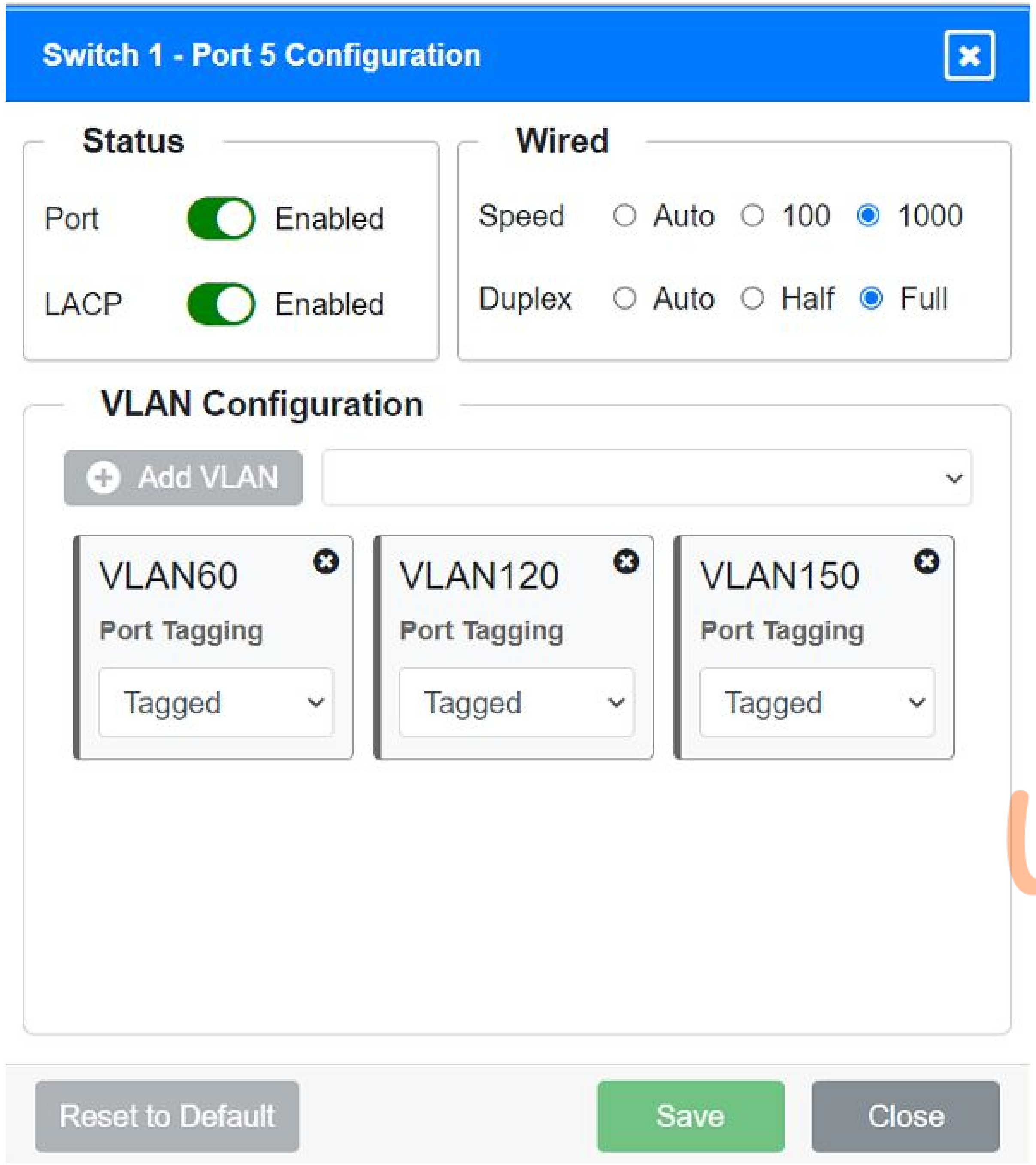
Speed: ○ Auto ○ 100 ● 1000

Duplex: ○ Auto ○ Half ● Full

VLAN Configuration

VLAN90

Port Tagging: UnTagged



Switch 1 - Port 5 Configuration

Status

Port: Enabled

LACP: Enabled

Wired

Speed ○ Auto ○ 100 ● 1000

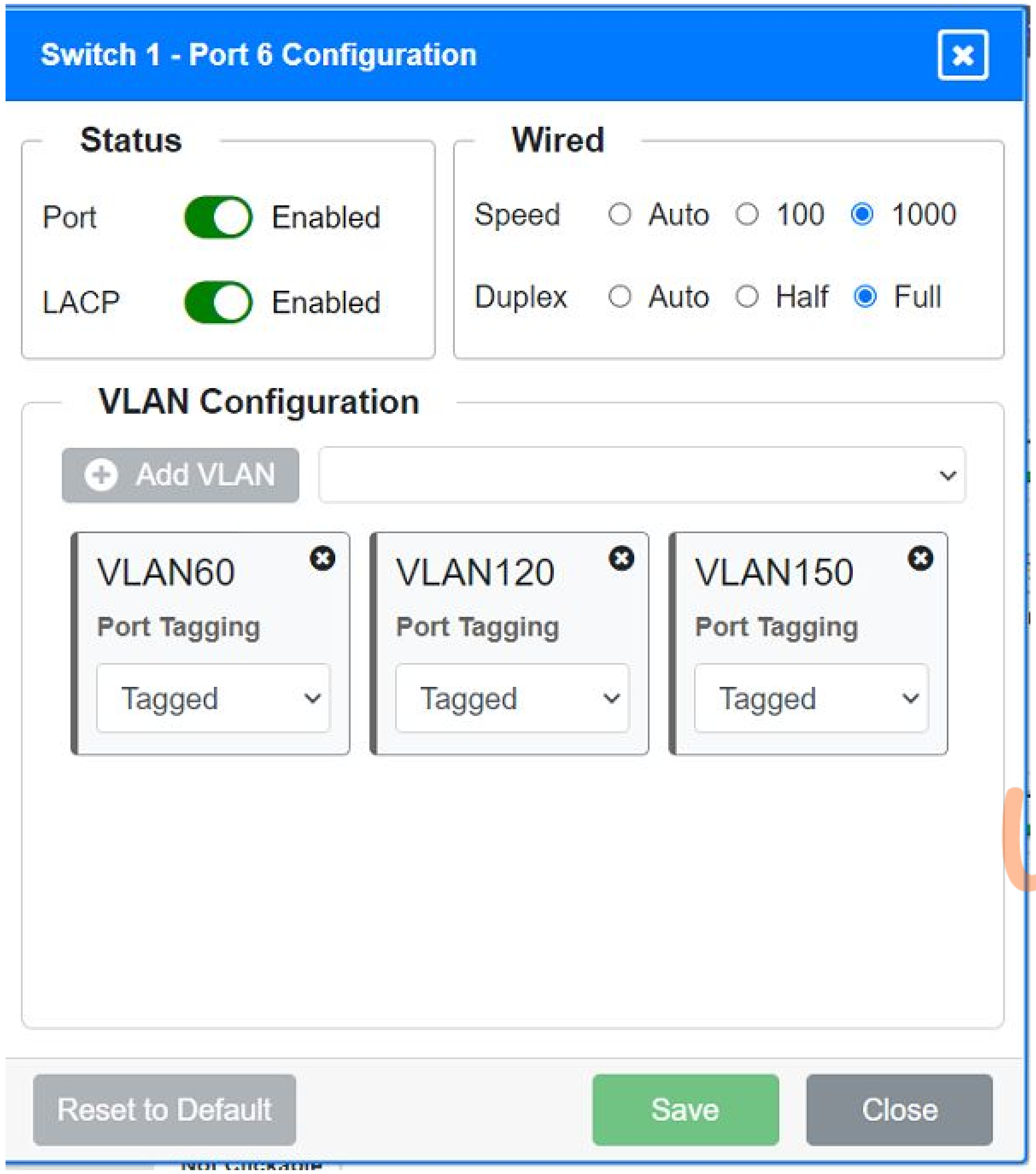
Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN60 Port Tagging: Tagged

VLAN120 Port Tagging: Tagged

VLAN150 Port Tagging: Tagged



Switch 1 - Port 6 Configuration

Status

Port: Enabled

LACP: Enabled

Wired

Speed ○ Auto ○ 100 ● 1000

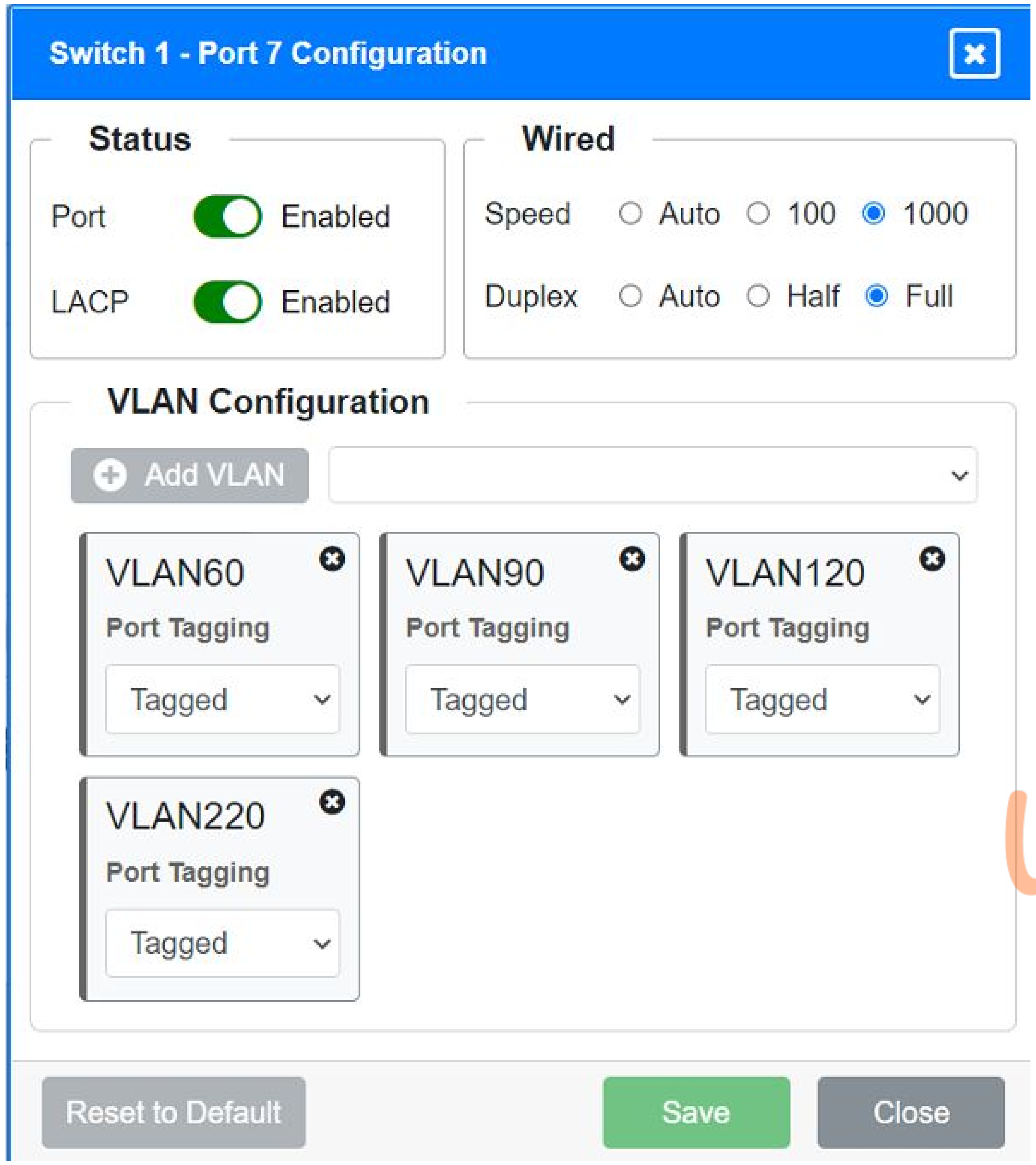
Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN60 — Port Tagging: Tagged

VLAN120 — Port Tagging: Tagged

VLAN150 — Port Tagging: Tagged



Switch 1 - Port 7 Configuration ☒

Status

Port — Enabled

LACP — Enabled

Wired

Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

VLAN Configuration

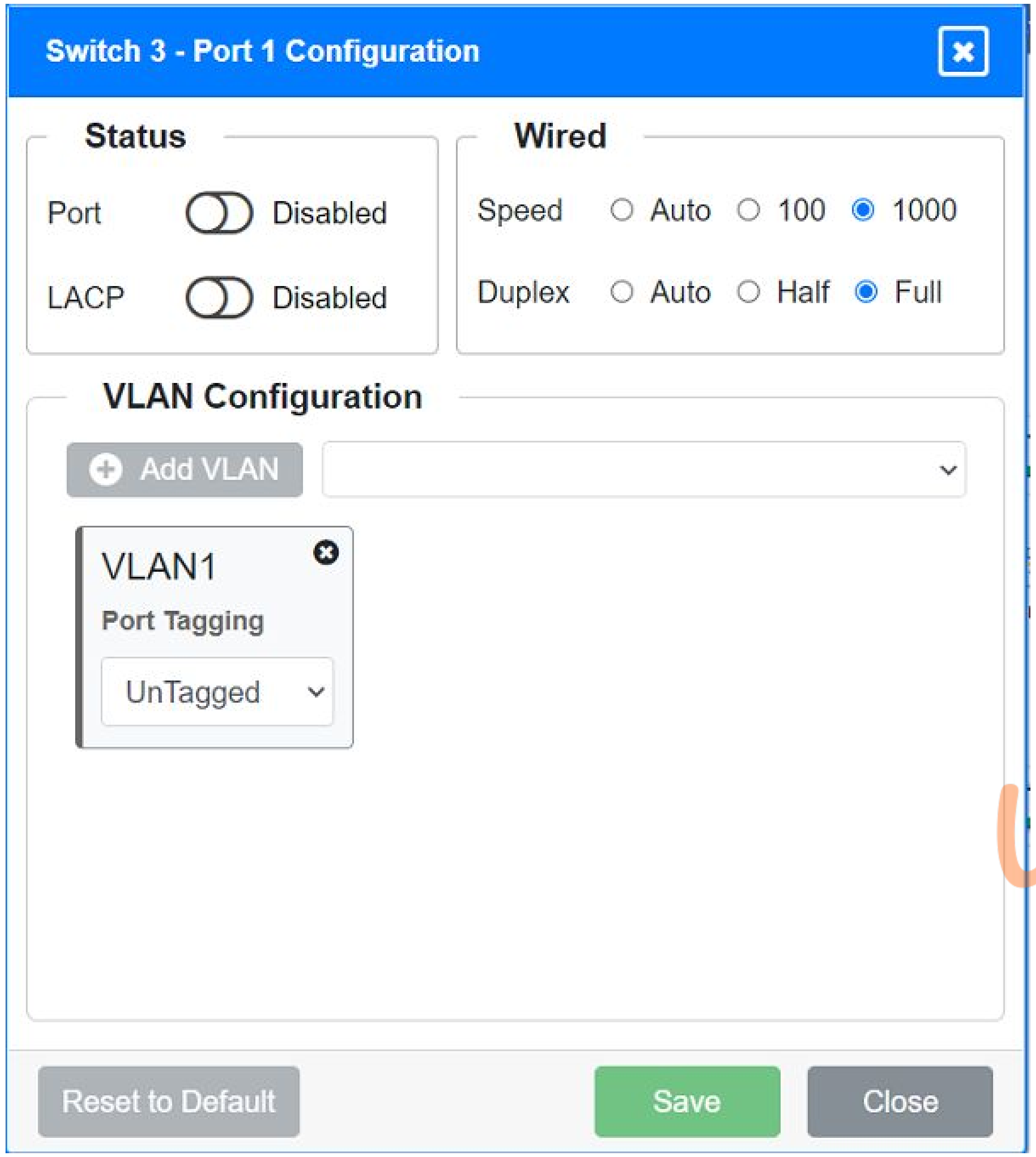
⊕ Add VLAN

VLAN60 — Port Tagging: Tagged

VLAN90 — Port Tagging: Tagged

VLAN120 — Port Tagging: Tagged

VLAN220 — Port Tagging: Tagged



Switch 3 - Port 1 Configuration

Status

Port: Disabled

LACP: Disabled

Wired

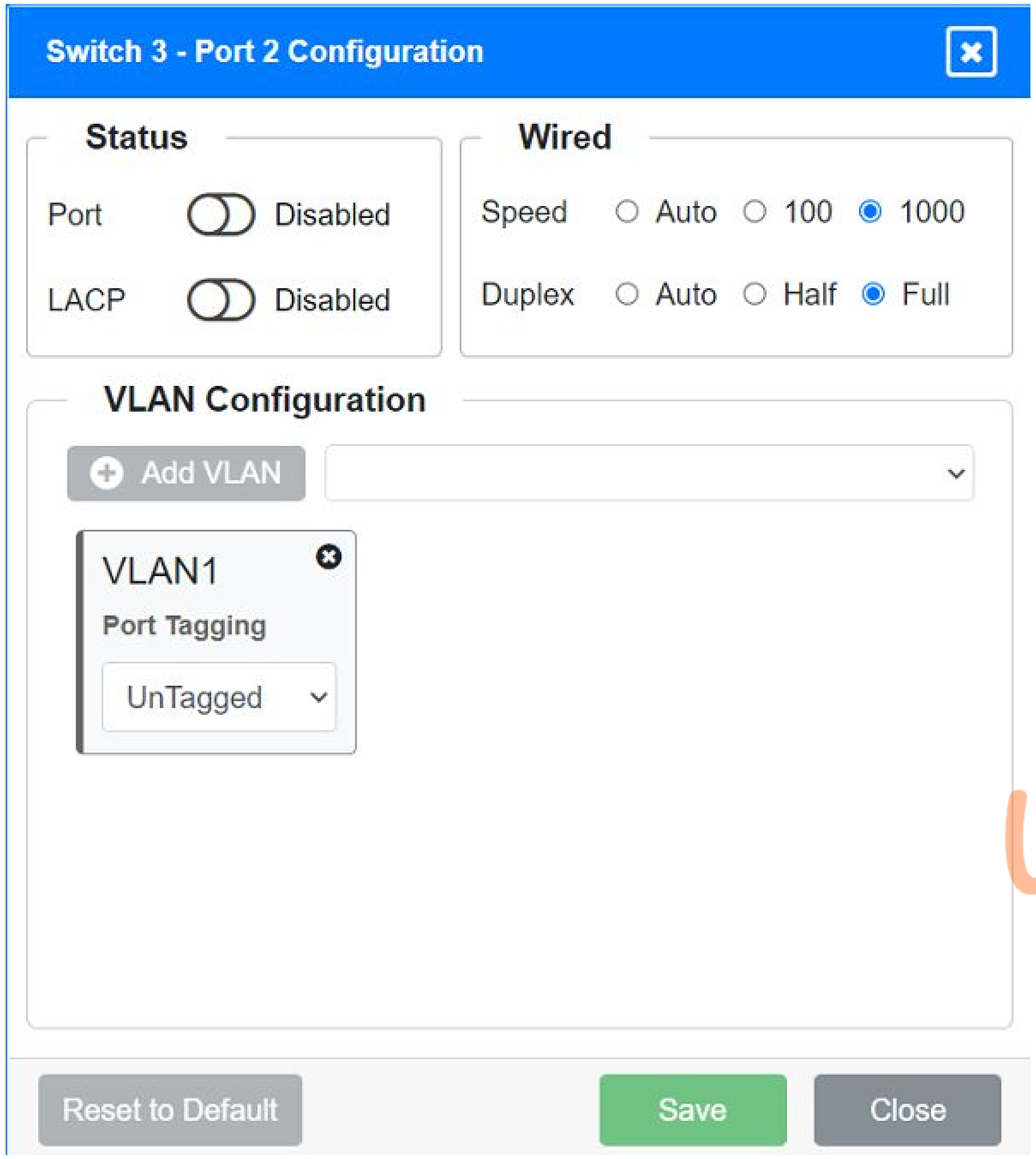
Speed: ○ Auto ○ 100 ● 1000

Duplex: ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging: UnTagged



Switch 3 - Port 2 Configuration

Status

Port: Disabled

LACP: Disabled

Wired

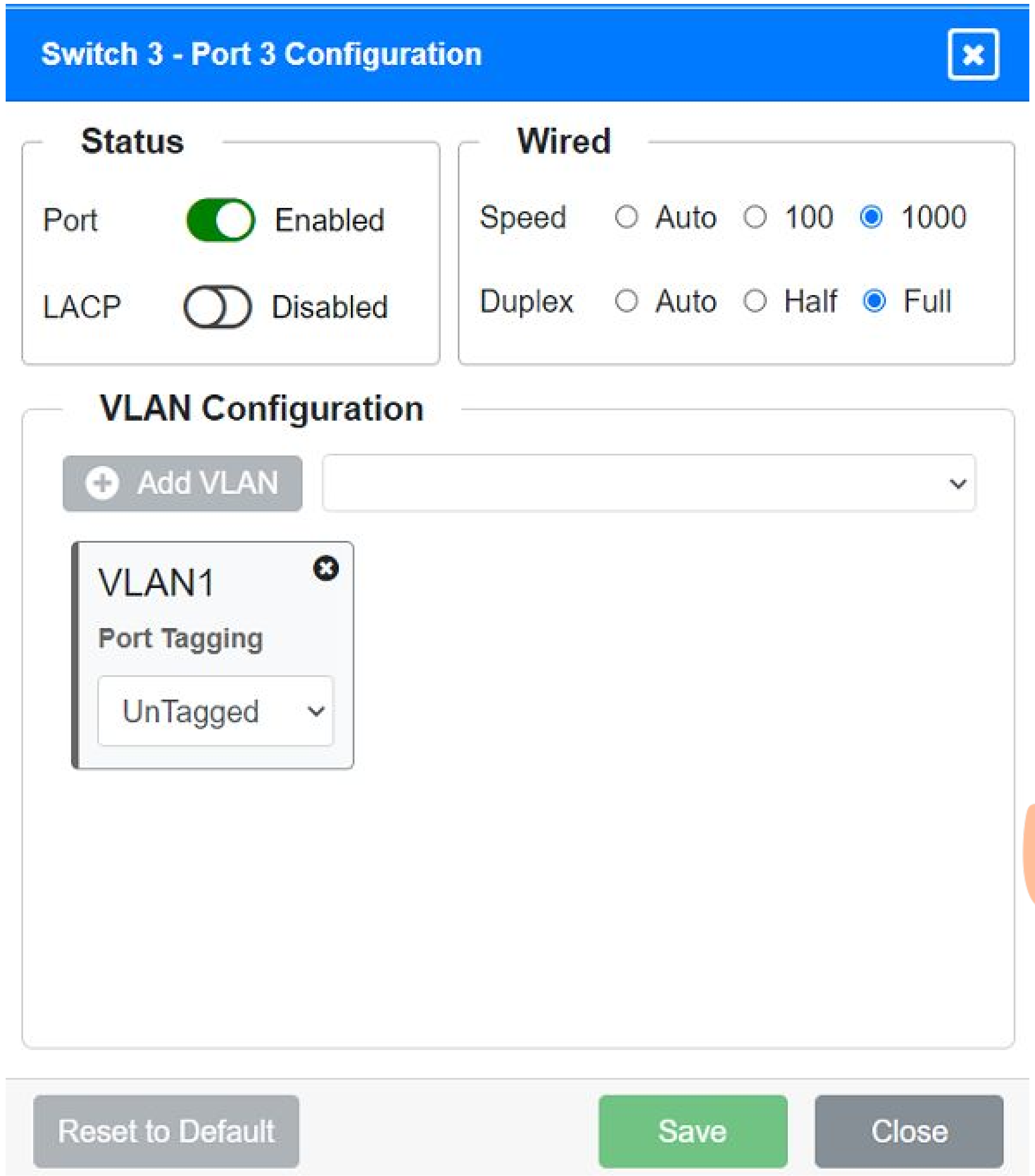
Speed: ○ Auto ○ 100 ● 1000

Duplex: ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging: UnTagged



Switch 3 - Port 3 Configuration

Status

Port: Enabled

LACP: Disabled

Wired

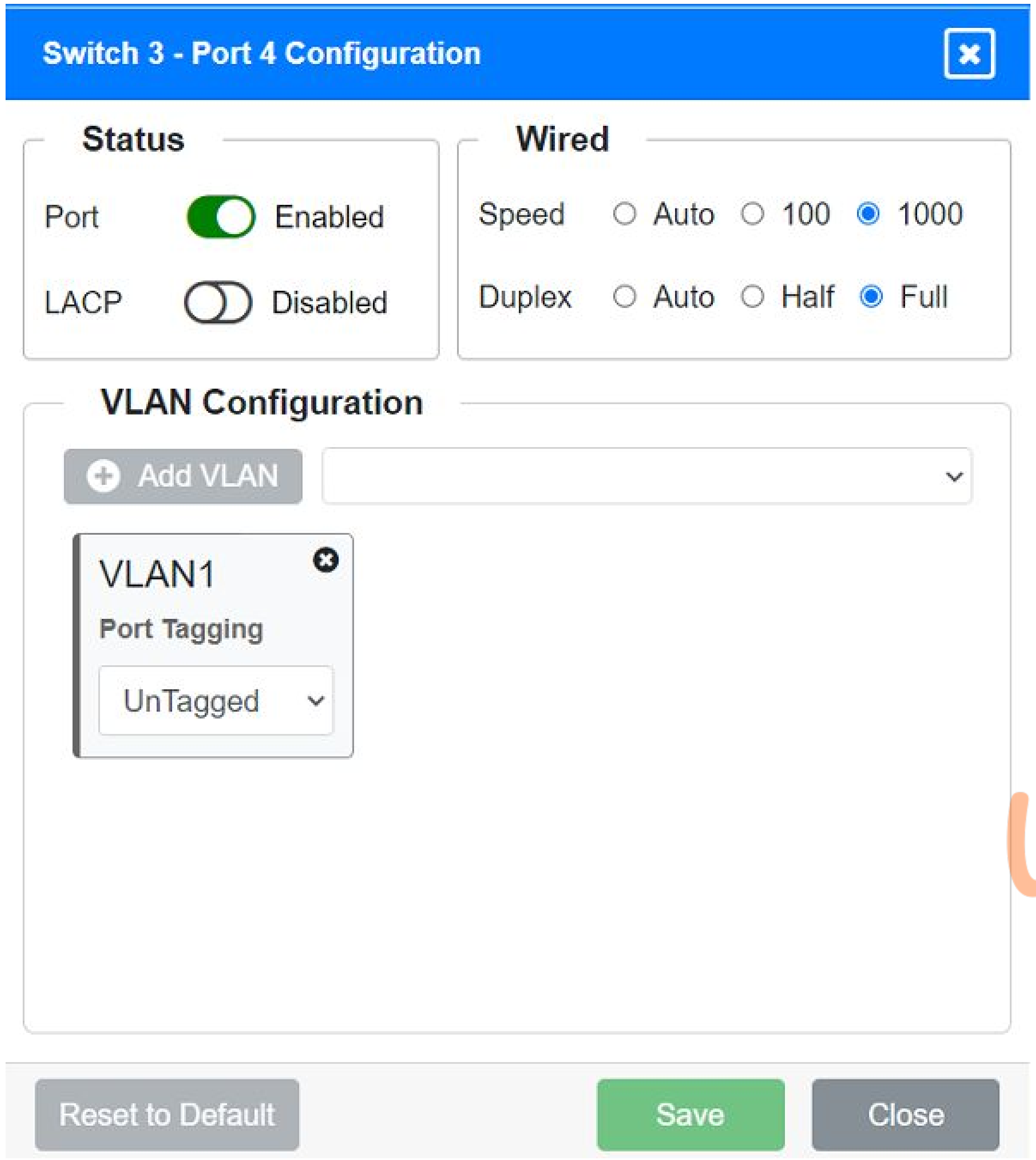
Speed: ○ Auto ○ 100 ● 1000

Duplex: ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging: UnTagged



Switch 3 - Port 4 Configuration

Status

Port: Enabled

LACP: Disabled

Wired

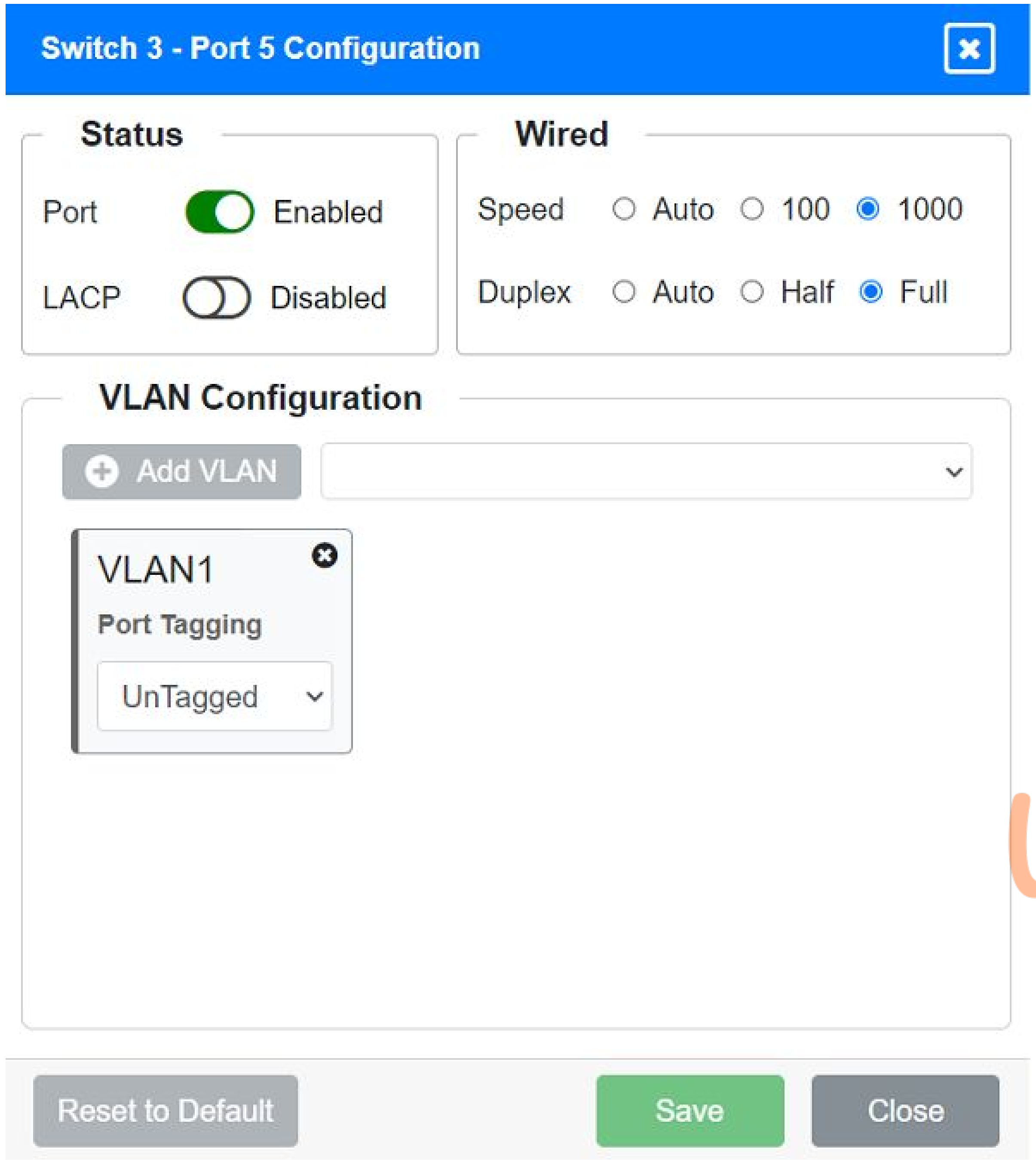
Speed: ○ Auto ○ 100 ● 1000

Duplex: ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging: UnTagged



Switch 3 - Port 5 Configuration

Status

Port: Enabled

LACP: Disabled

Wired

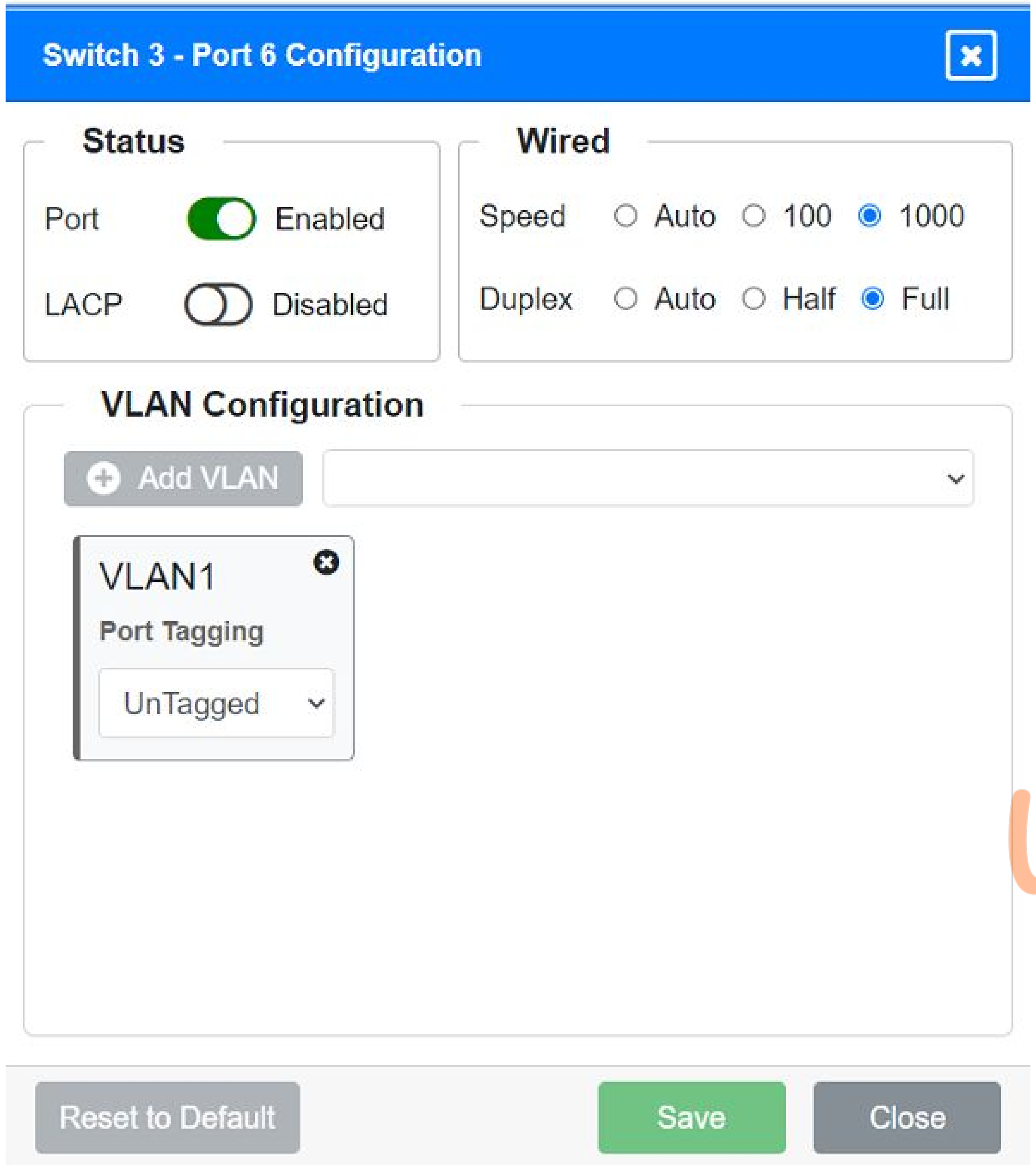
Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging: UnTagged



Switch 3 - Port 6 Configuration

Status

Port: Enabled

LACP: Disabled

Wired

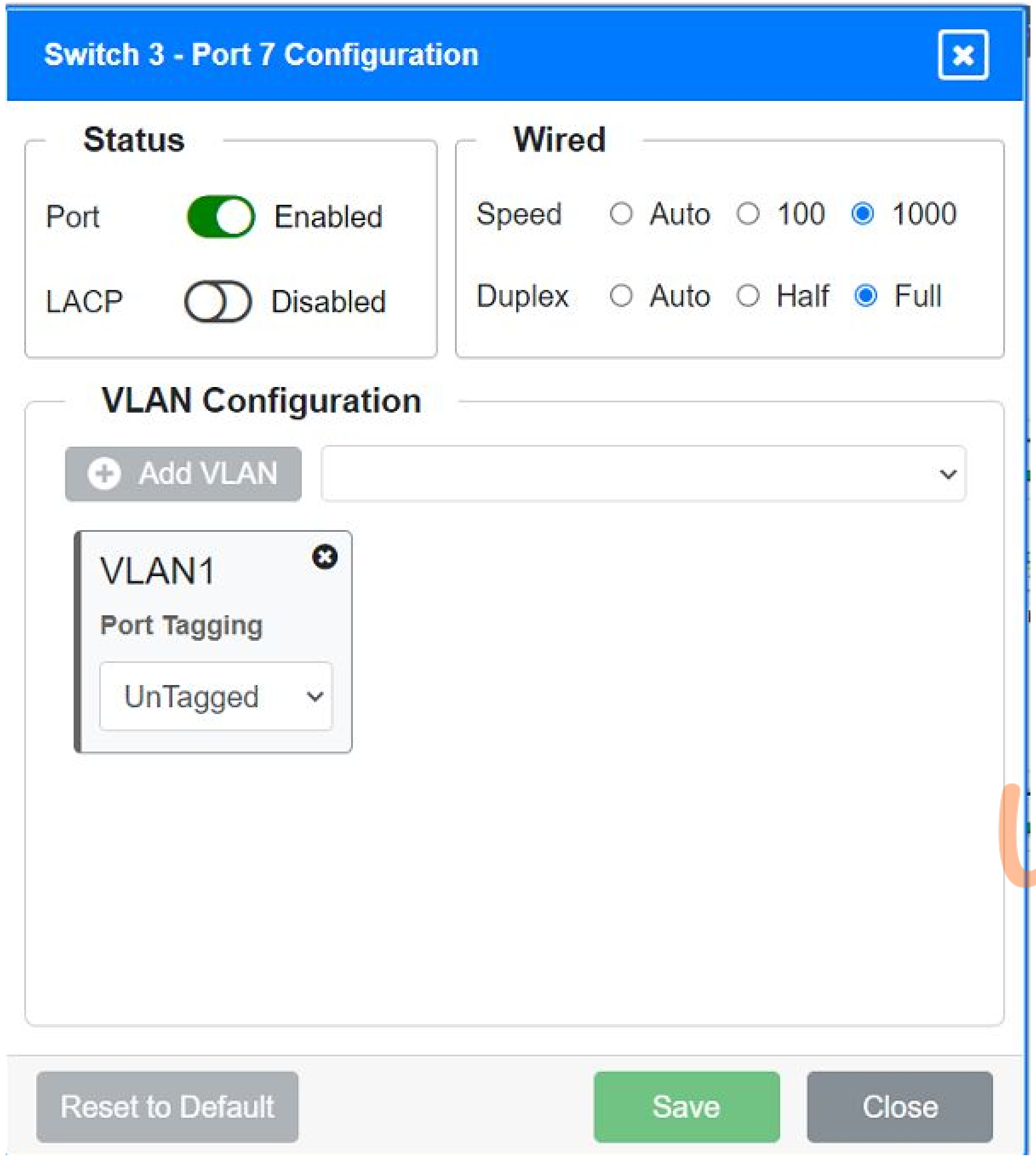
Speed: ○ Auto ○ 100 ● 1000

Duplex: ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging: UnTagged



Switch 3 - Port 7 Configuration

Status

Port: Enabled

LACP: Disabled

Wired

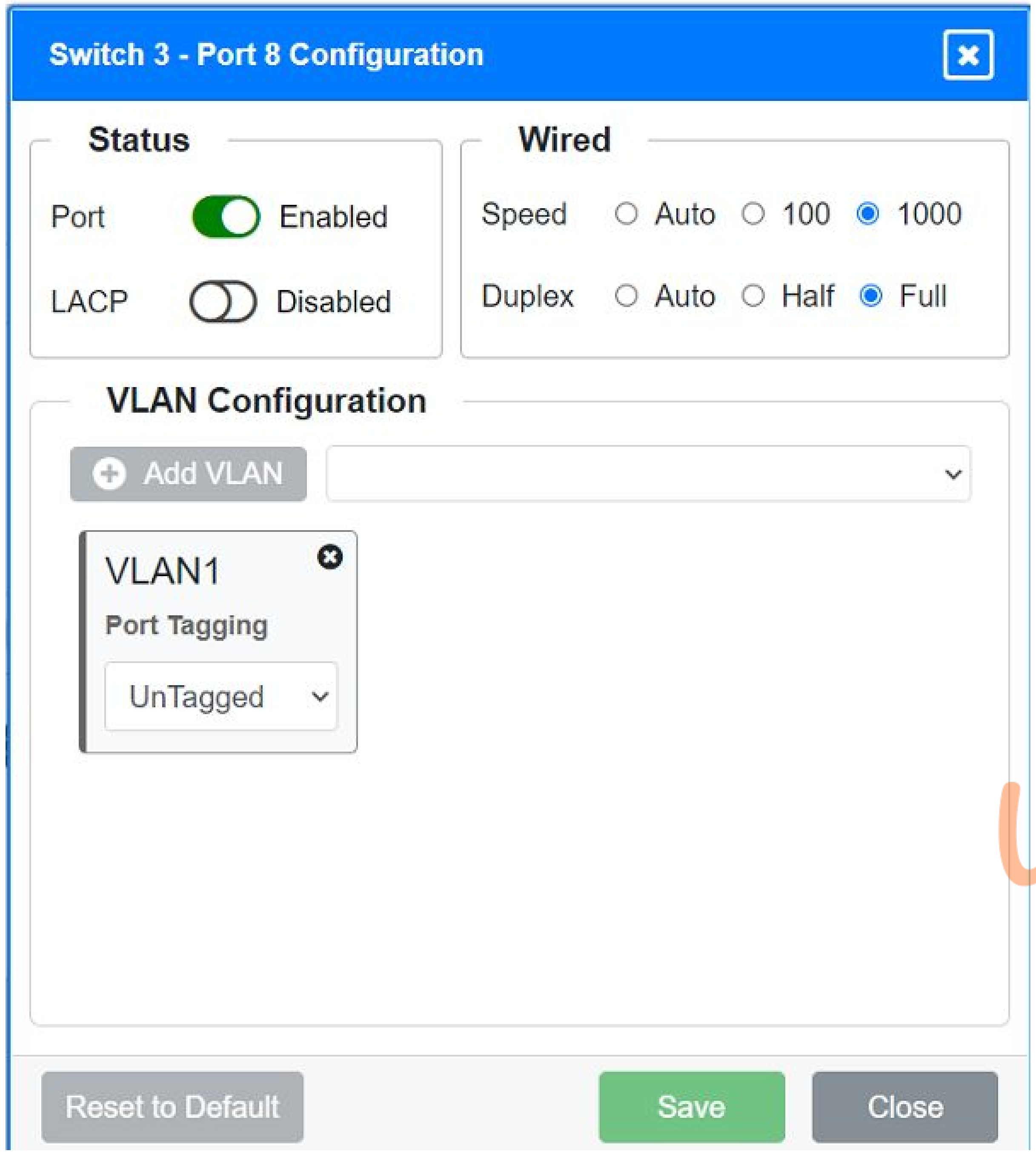
Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging: UnTagged



Switch 3 - Port 8 Configuration

Status

Port: Enabled

LACP: Disabled

Wired

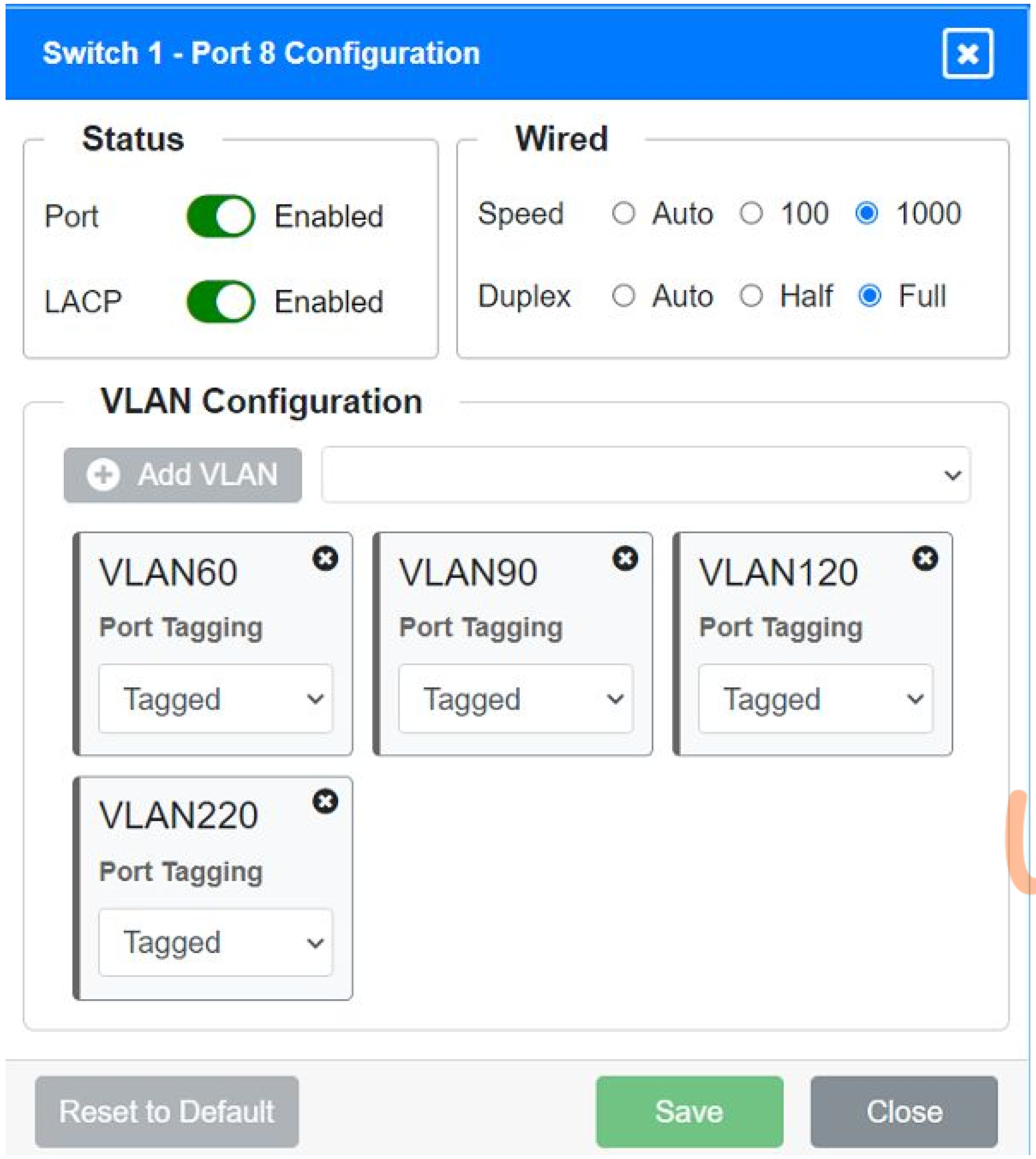
Speed: ○ Auto ○ 100 ● 1000

Duplex: ○ Auto ○ Half ● Full

VLAN Configuration

VLAN1

Port Tagging: UnTagged


Switch 1 - Port 8 Configuration

Status

Port: Enabled

LACP: Enabled

Wired

Speed ○ Auto ○ 100 ● 1000

Duplex ○ Auto ○ Half ● Full

VLAN Configuration

VLAN60 Port Tagging: Tagged

VLAN90 Port Tagging: Tagged

VLAN120 Port Tagging: Tagged

VLAN220 Port Tagging: Tagged

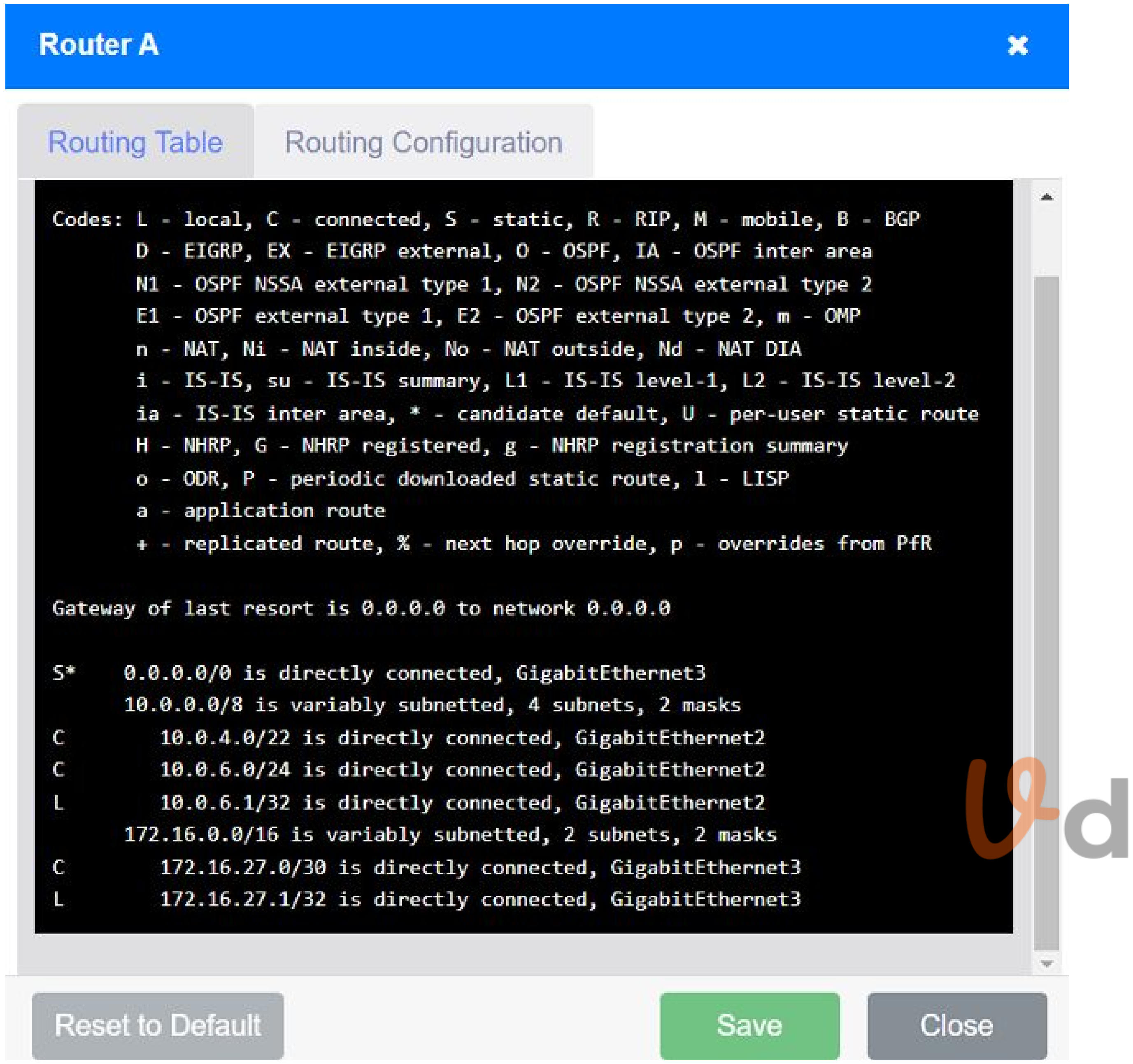
A. See the solution below in Explanation

Correct Answer: A
Section:
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.

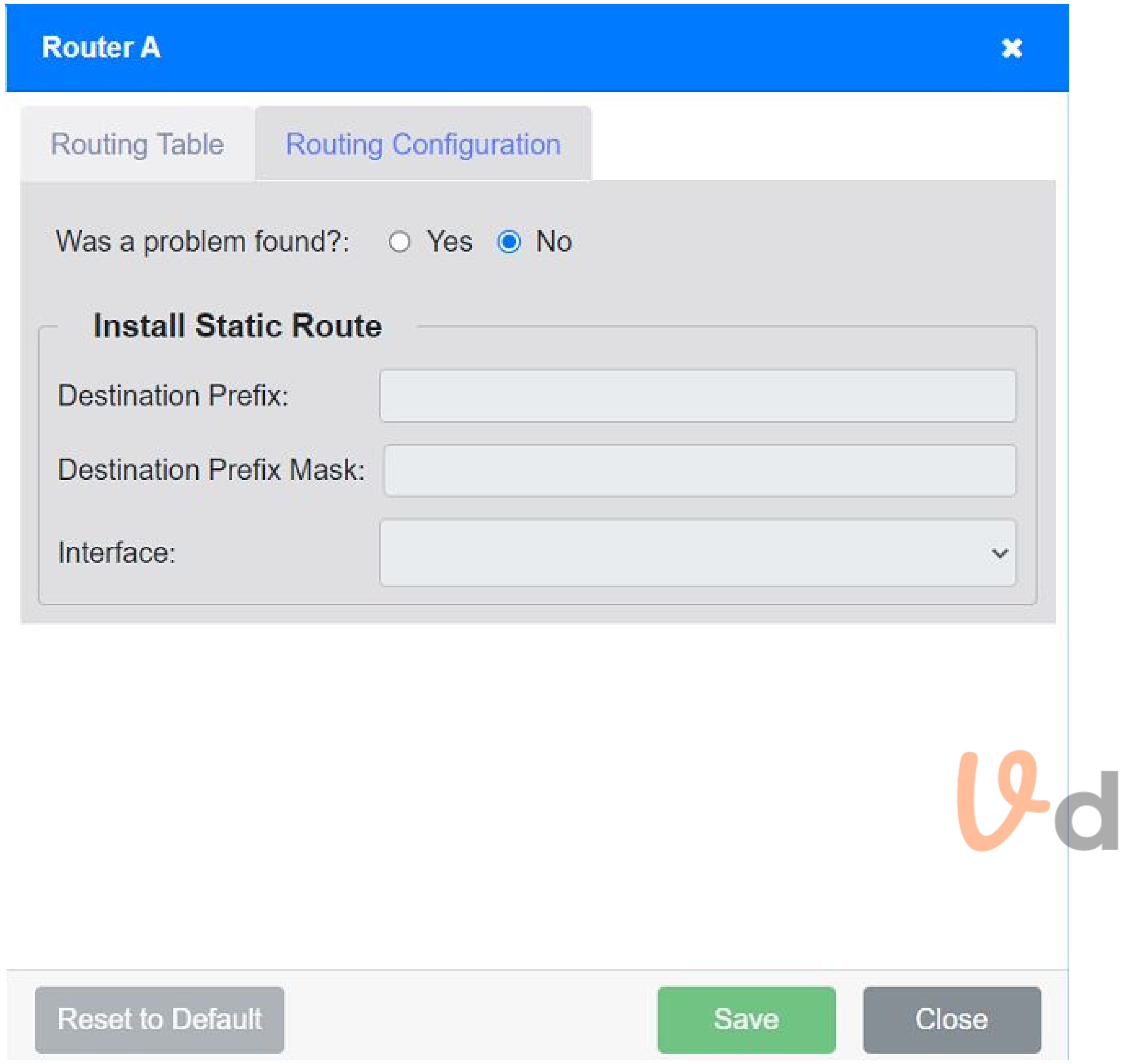
QUESTION 16
SIMULATION
Users are unable to access files on their department share located on file server 2.
The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.
INSTRUCTIONS
Click on each router to review output, identify any issues, 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.



```
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, 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
```



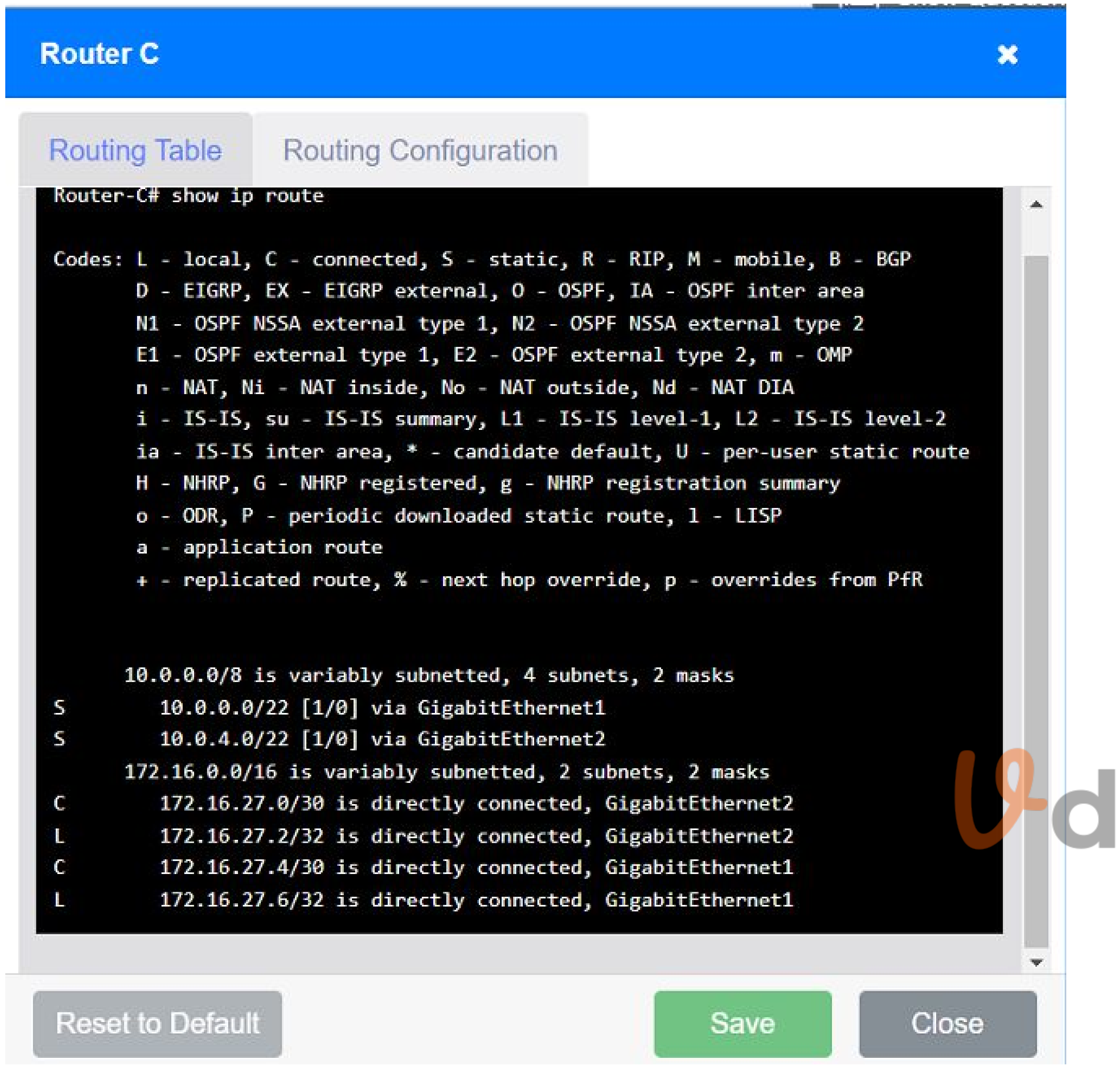
Was a problem found?: ○ Yes ● No

Install Static Route

Destination Prefix:

Destination Prefix Mask:

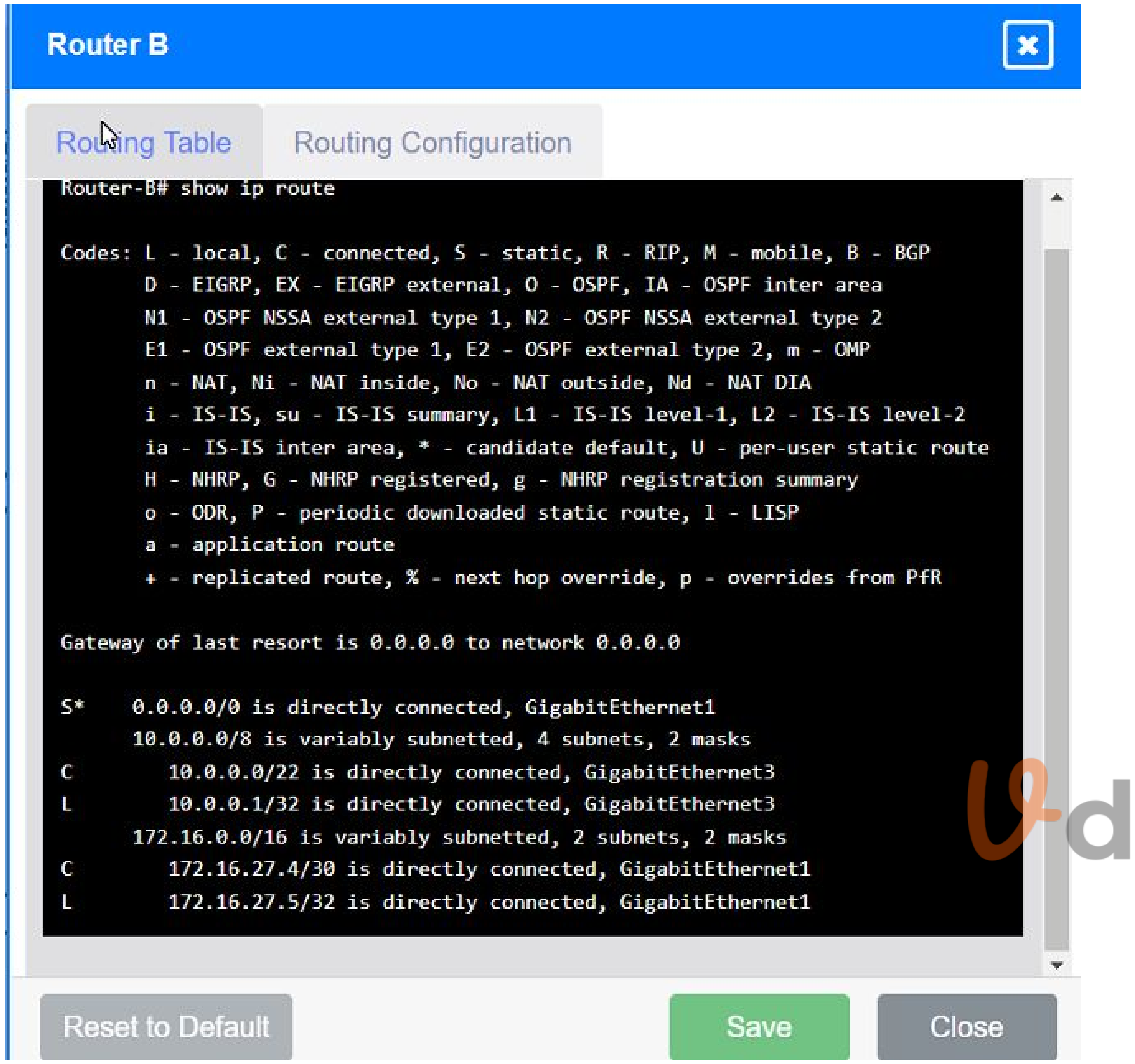
Interface:



```
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
```

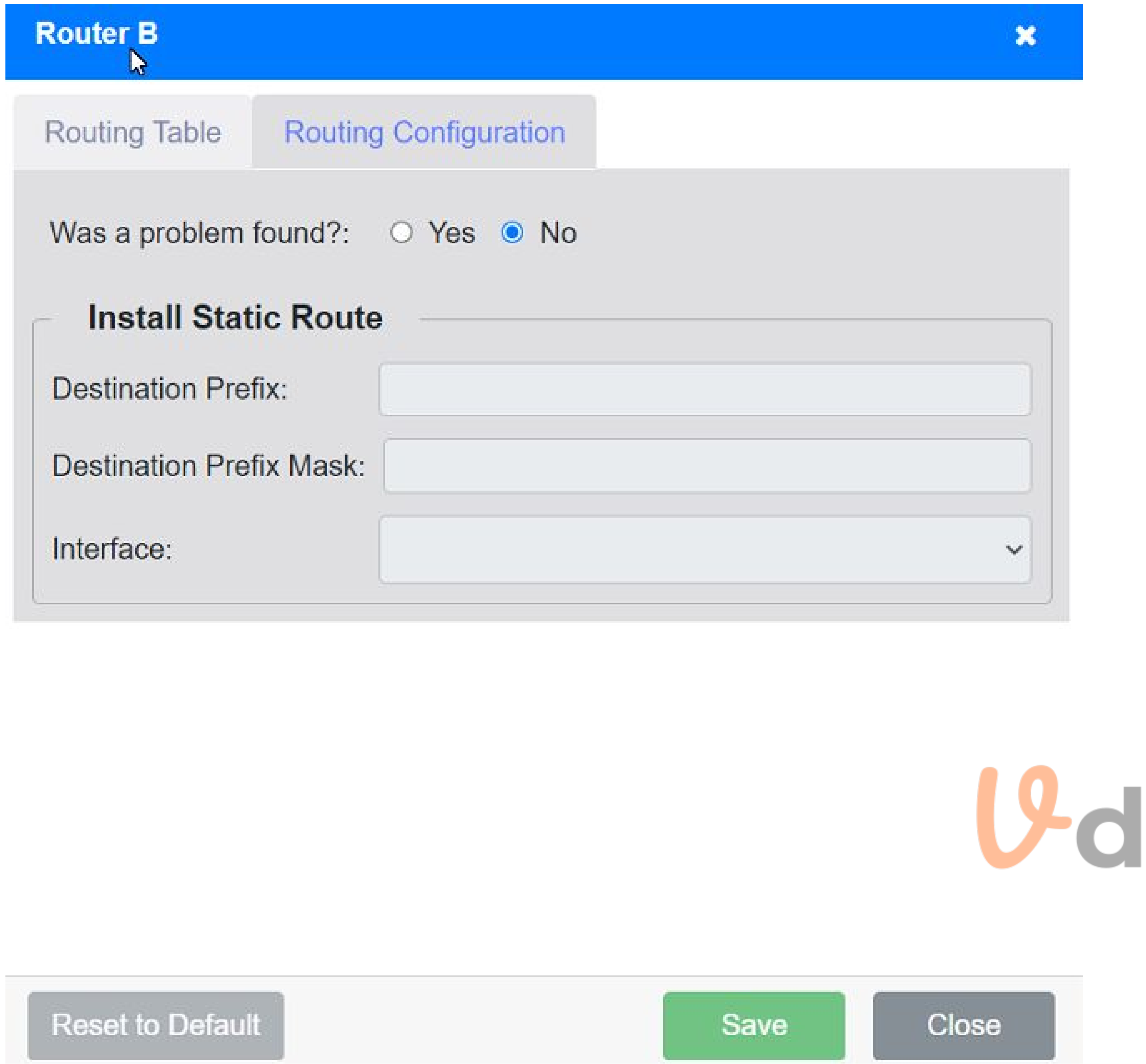


```
Router-B# show ip route

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
```



Router B

Routing Table | Routing Configuration

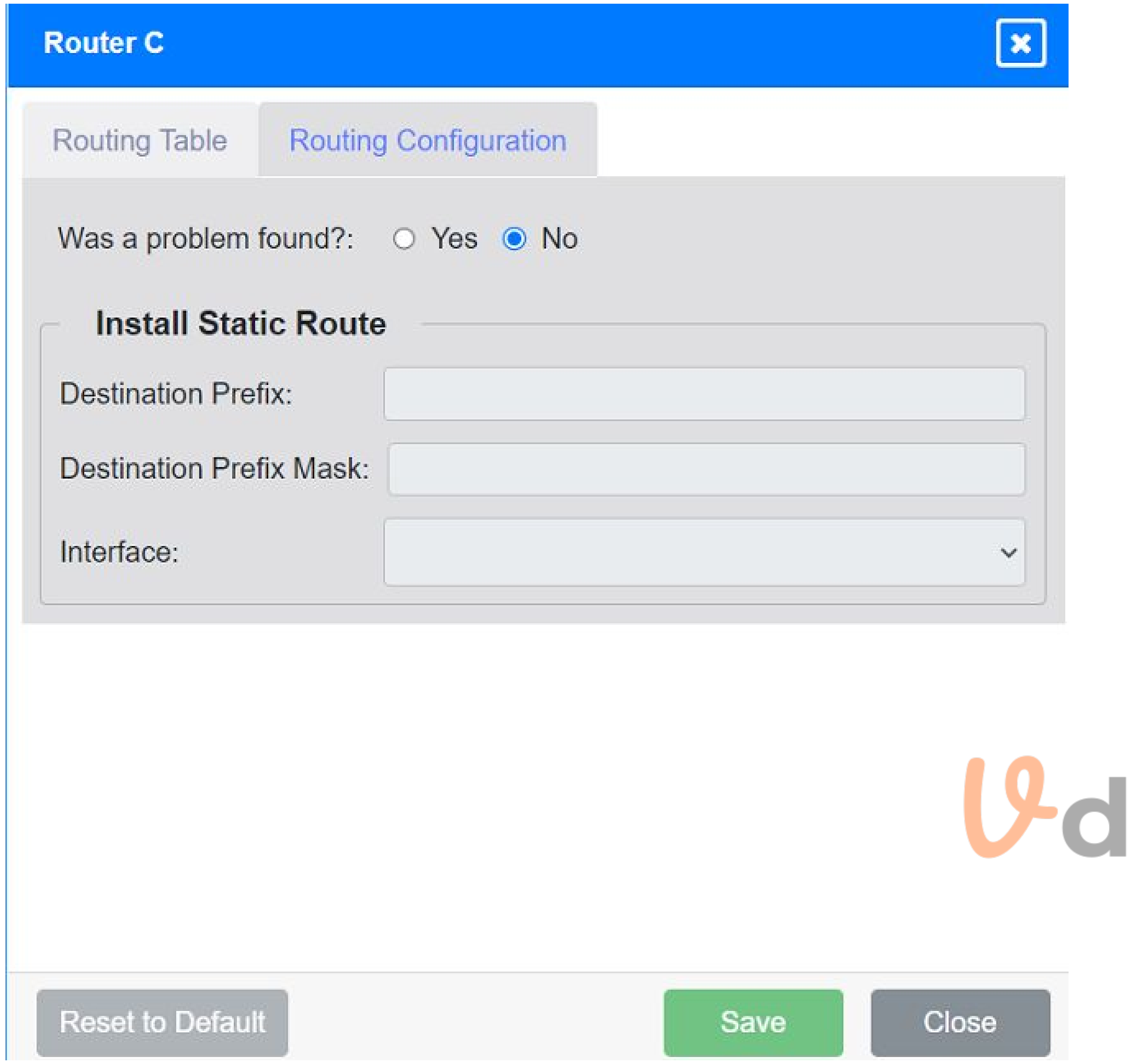
Was a problem found?: ○ Yes ● No

Install Static Route

Destination Prefix:

Destination Prefix Mask:

Interface:



Was a problem found?: ○ Yes ● No

Install Static Route

Destination Prefix:

Destination Prefix Mask:

Interface:

A. See the solution in Explanation

Correct Answer: A
Section:
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 17

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

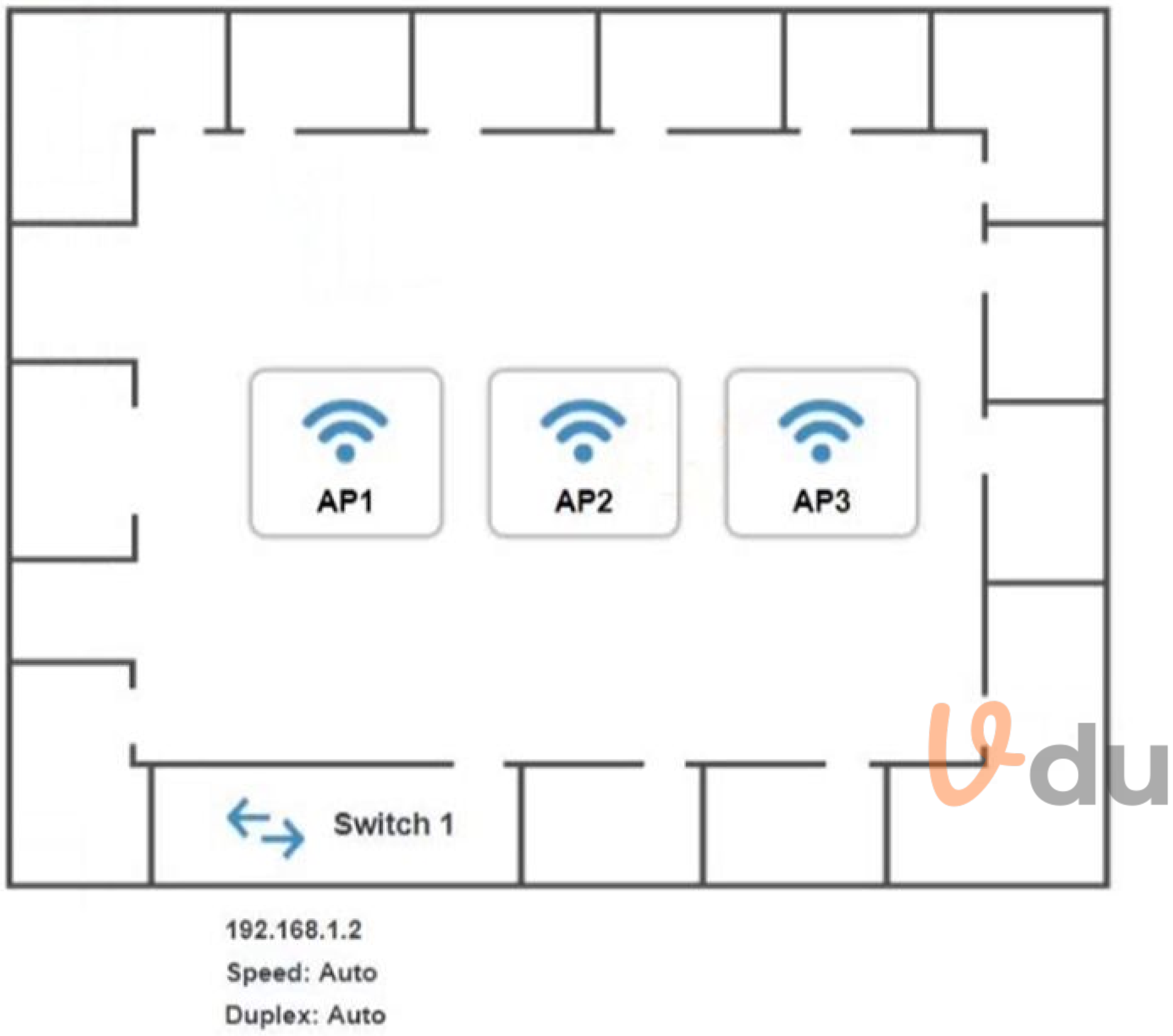
The subnet the Access Points and switch are on should only support 30 devices maximum

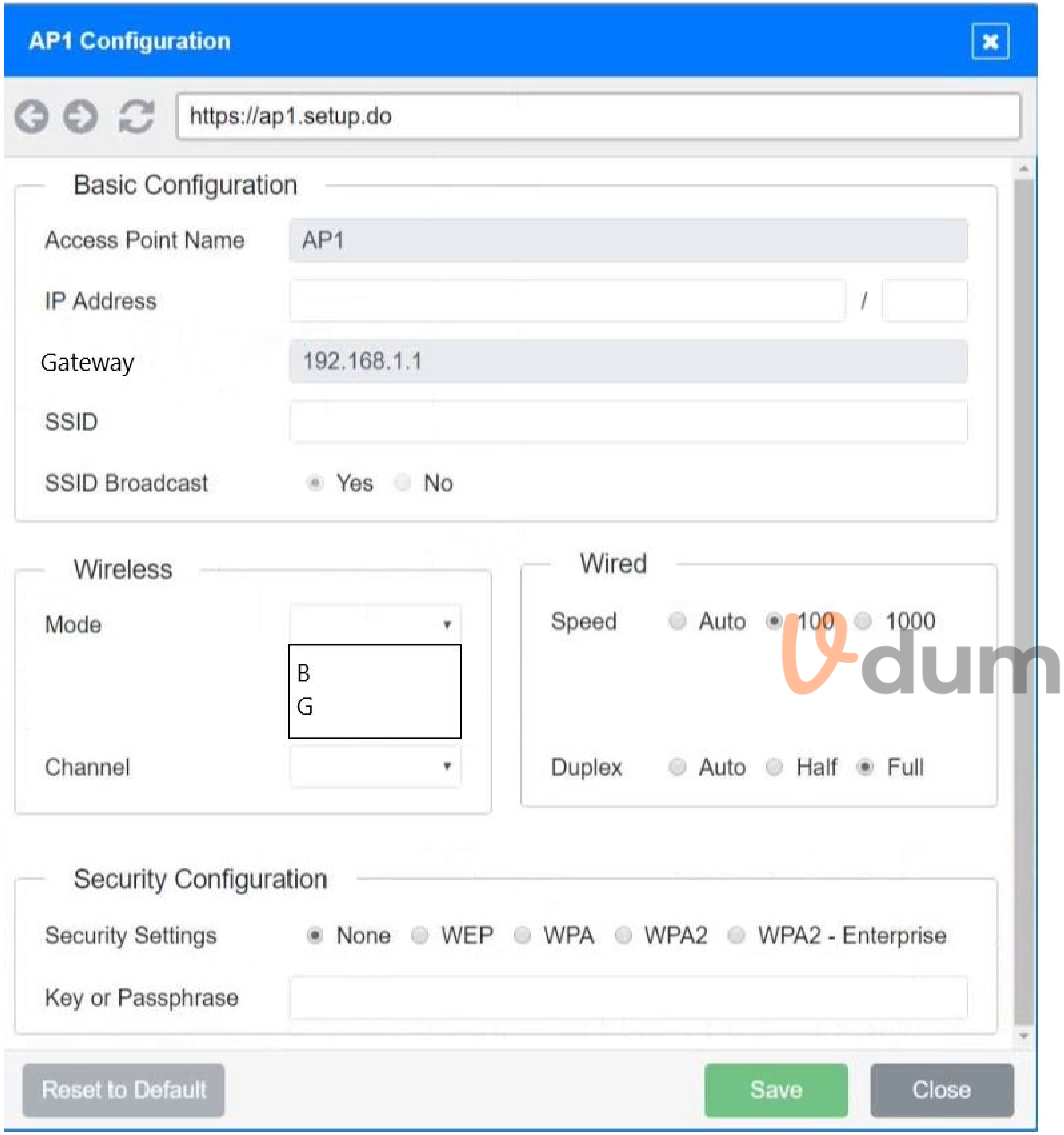
The Access Points should be configured to only support TKIP clients at a maximum speed

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



Basic Configuration

Access Point Name	AP1
IP Address	/
Gateway	192.168.1.1
SSID	
SSID Broadcast	● Yes ○ No

Wireless

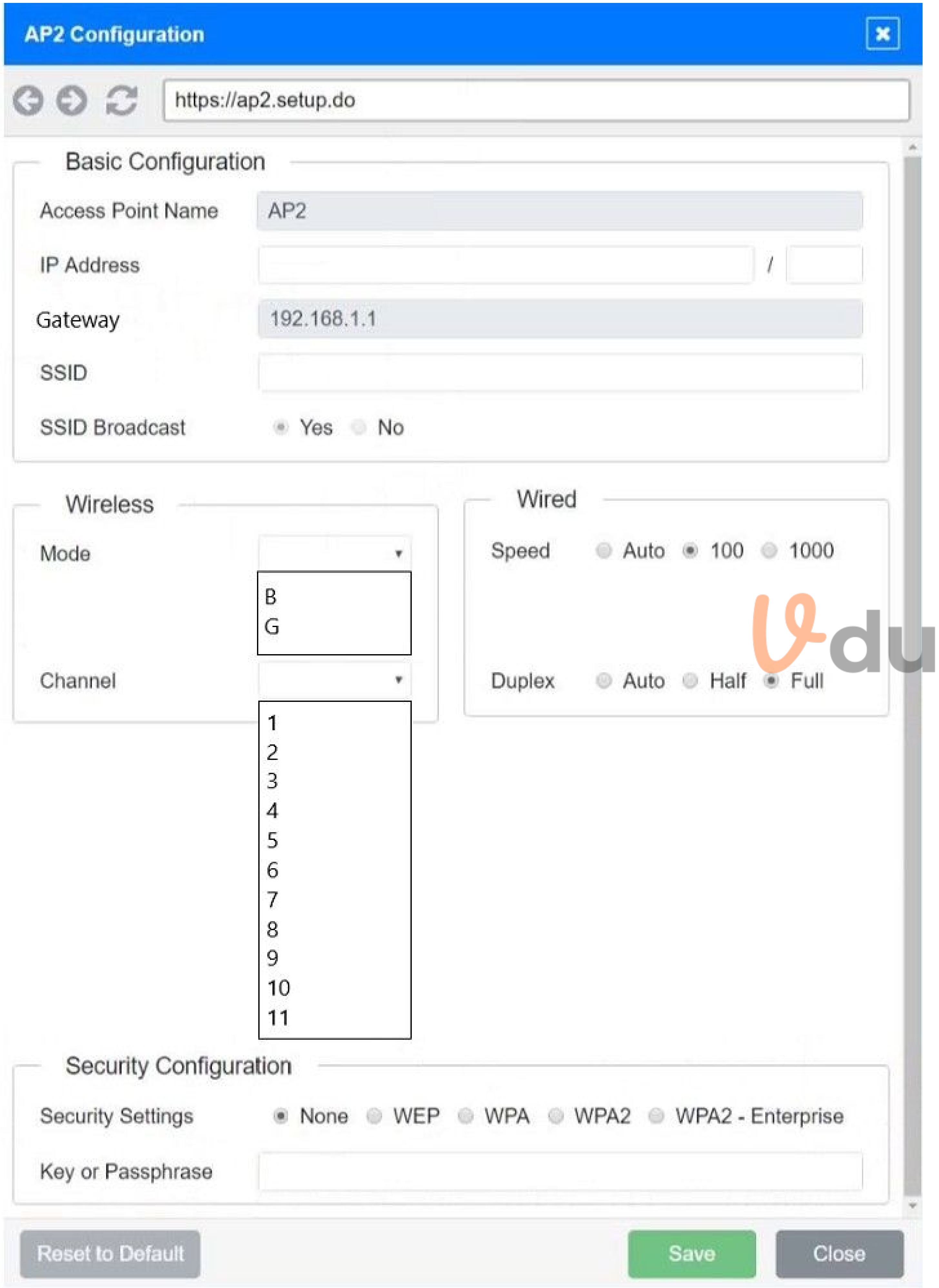
Mode	B G
Channel	

Wired

Speed	○ Auto ● 100 ○ 1000
Duplex	○ Auto ○ Half ● Full

Security Configuration

Security Settings	● None ○ WEP ○ WPA ○ WPA2 ○ WPA2 - Enterprise
Key or Passphrase	



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

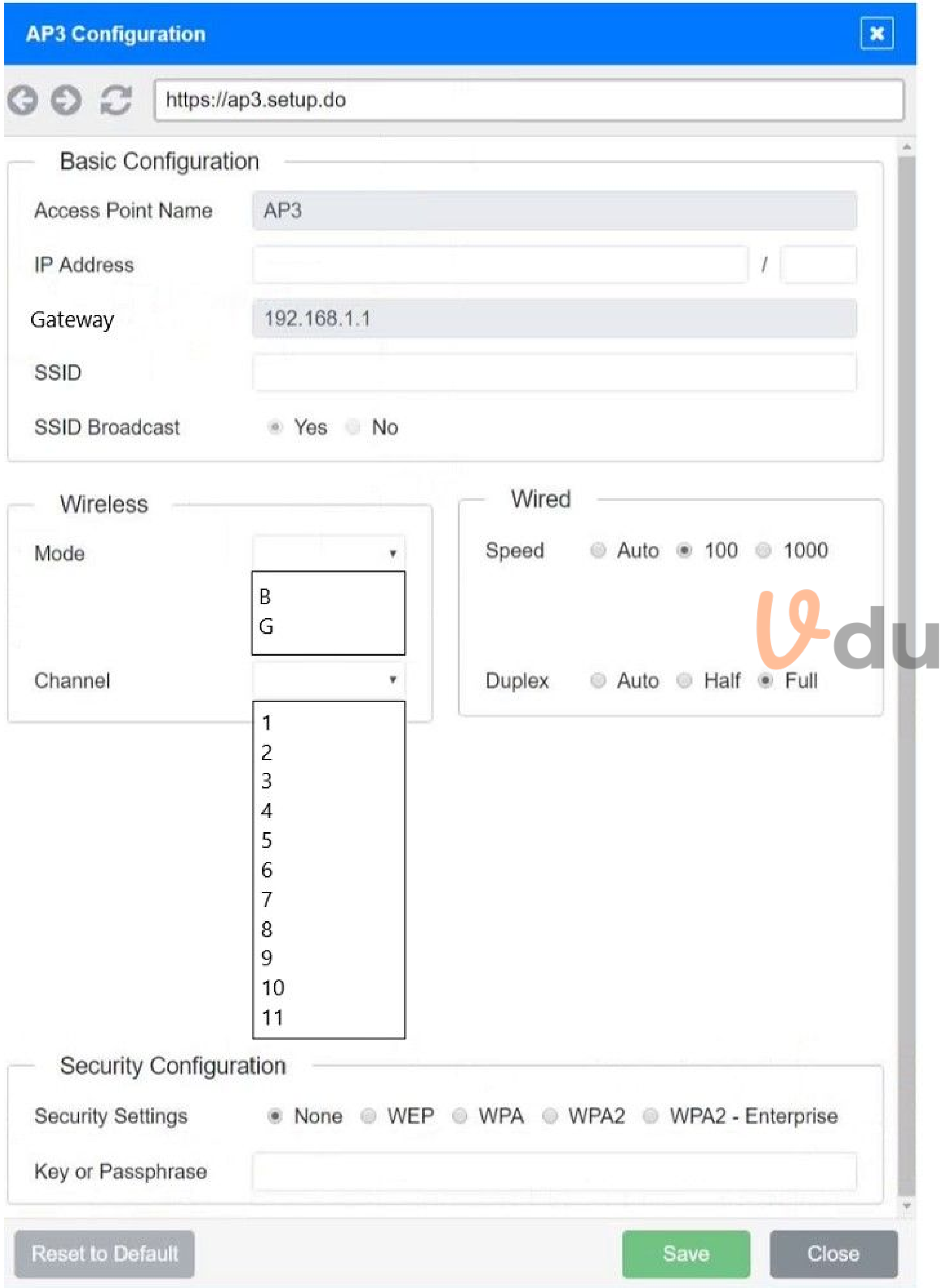
Speed ○ Auto ● 100 ○ 1000

Duplex ○ Auto ○ Half ● Full

Security Configuration

Security Settings ● None ○ WEP ○ WPA ○ WPA2 ○ WPA2 - Enterprise

Key or Passphrase


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

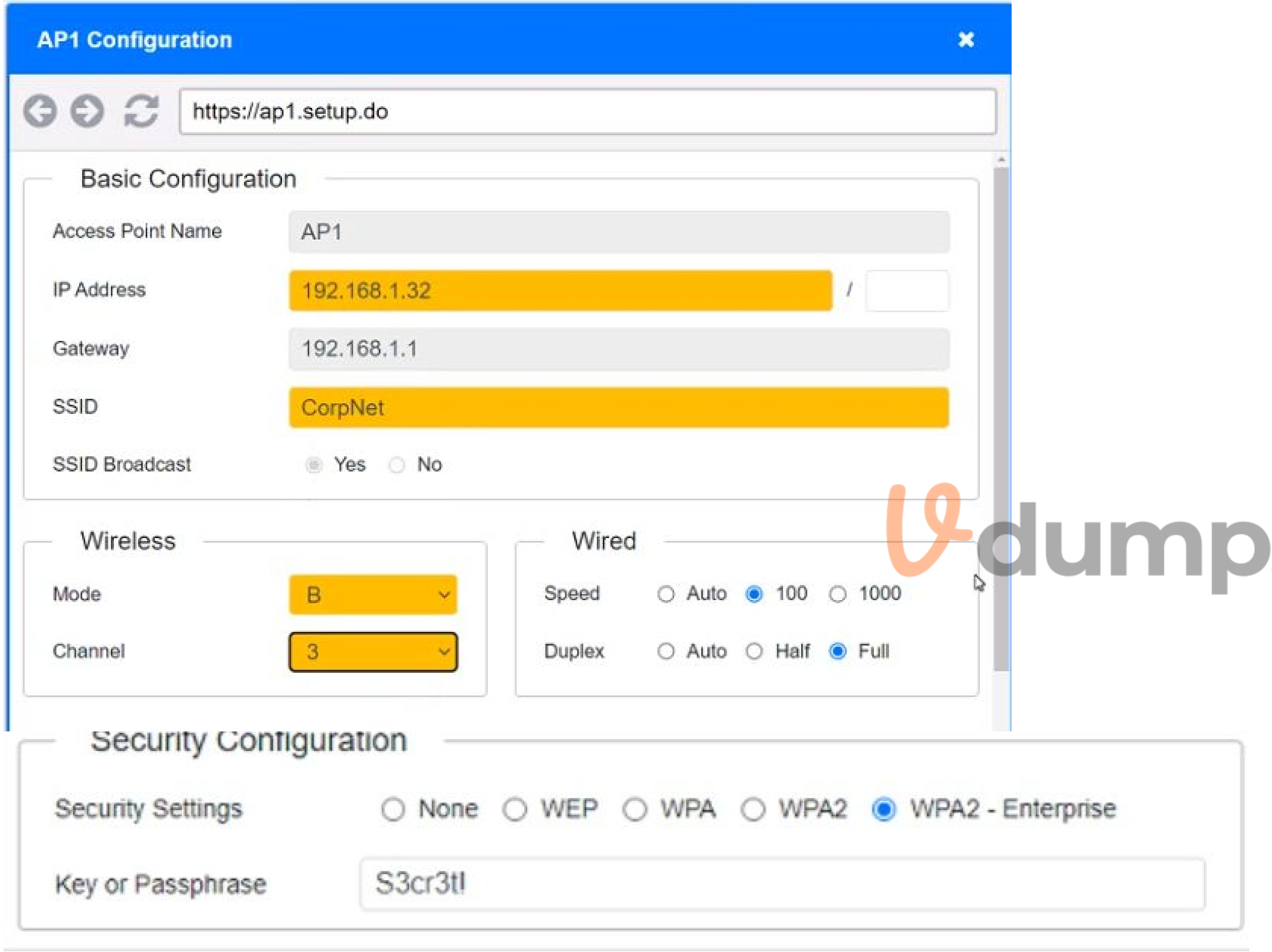
Security Configuration

Security Settings: ● None ○ WEP ○ WPA ○ WPA2 ○ WPA2 - Enterprise

Key or Passphrase:

A. See explanation below

Correct Answer: A
Section:
Explanation:
On the first exhibit, the layout should be as follows



AP1 Configuration ✖

https://ap1.setup.do

Basic Configuration

Access Point Name	AP1
IP Address	192.168.1.32 /
Gateway	192.168.1.1
SSID	CorpNet
SSID Broadcast	● Yes ○ No

Wireless

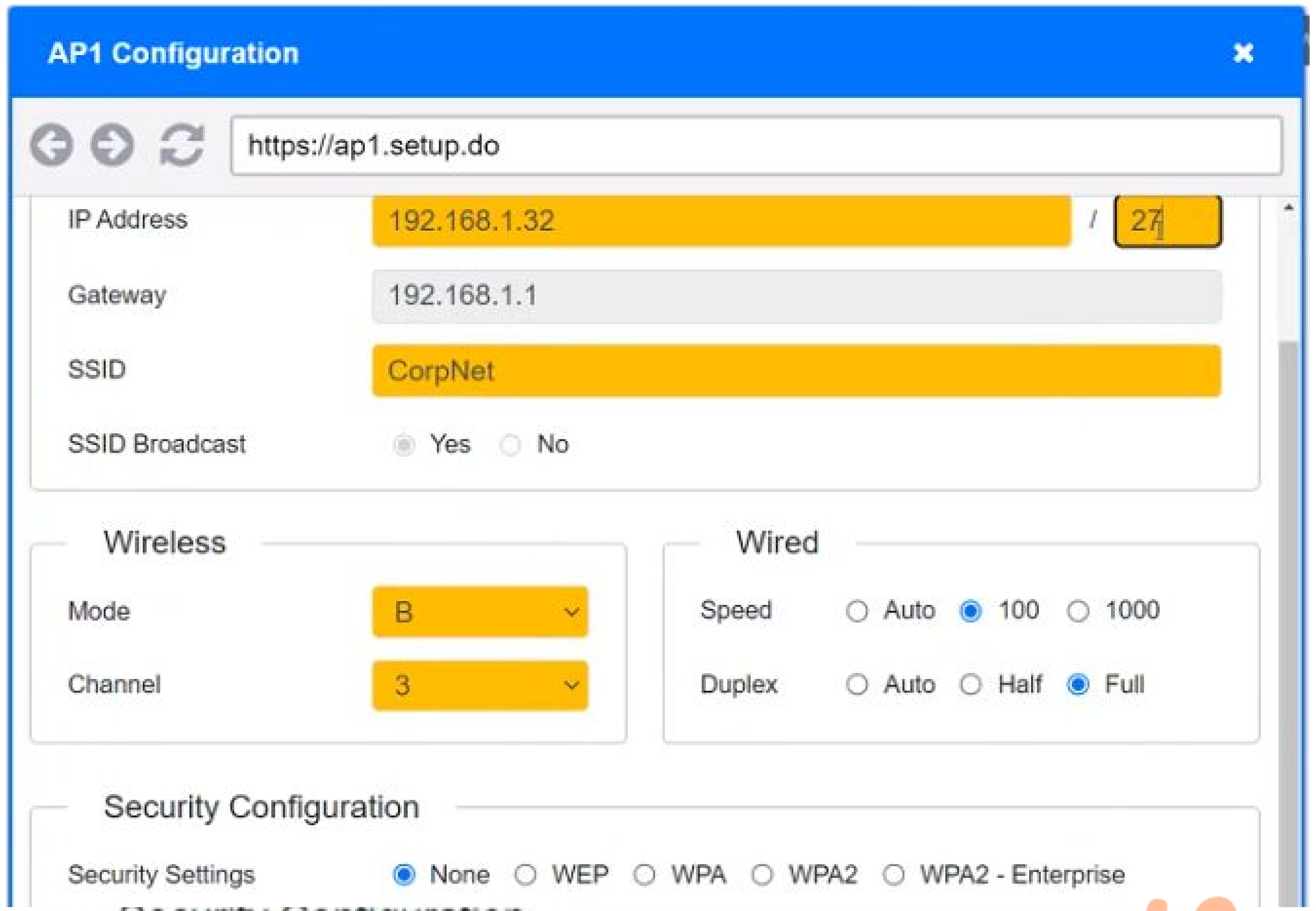
Mode	B
Channel	3

Wired

Speed	○ Auto ● 100 ○ 1000
Duplex	○ Auto ○ Half ● Full

Security Configuration

Security Settings	○ None ○ WEP ○ WPA ○ WPA2 ● WPA2 - Enterprise
Key or Passphrase	S3cr3t!



IP Address: 192.168.1.32 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ● Yes ○ No

Wireless

Mode: B

Channel: 3

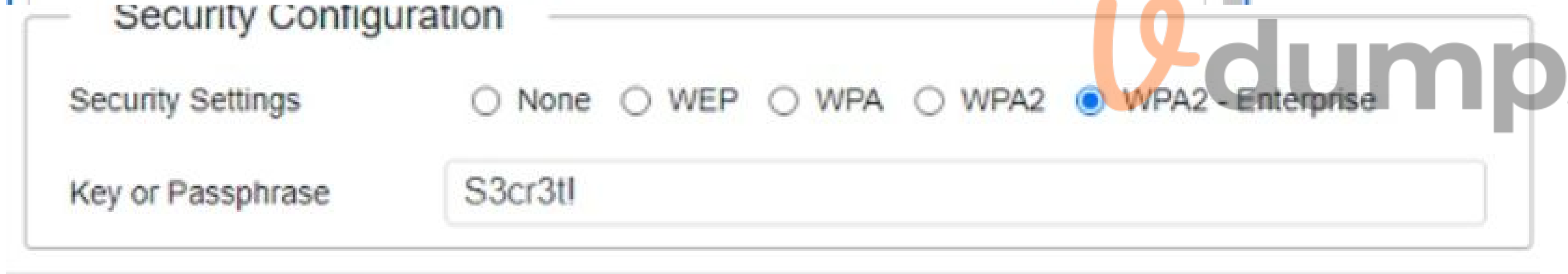
Wired

Speed: ○ Auto ● 100 ○ 1000

Duplex: ○ Auto ○ Half ● Full

Security Configuration

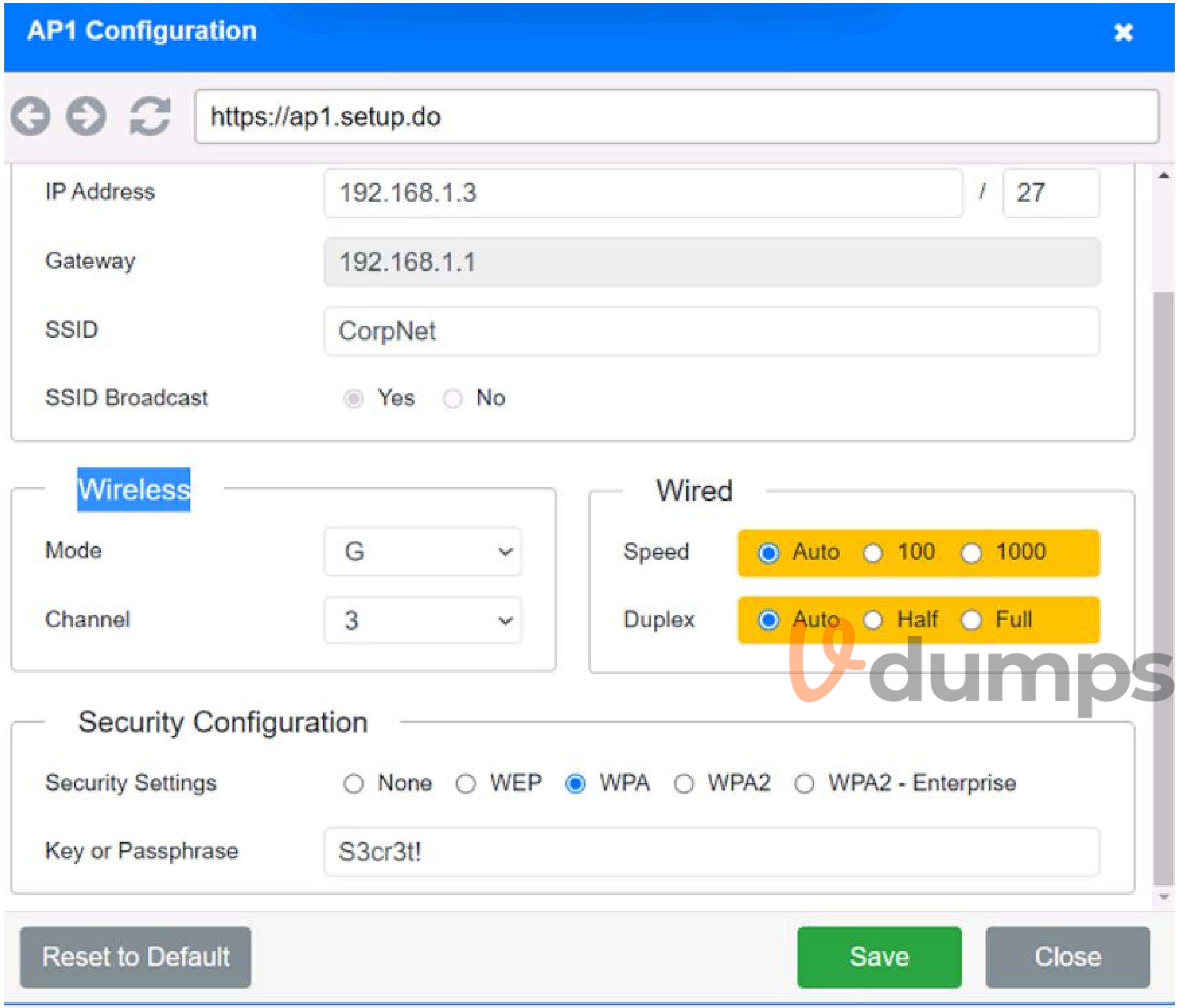
Security Settings: ● None ○ WEP ○ WPA ○ WPA2 ○ WPA2 - Enterprise



Security Configuration

Security Settings: ○ None ○ WEP ○ WPA ○ WPA2 ● WPA2 - Enterprise

Key or Passphrase: S3cr3t!



AP1 Configuration

https://ap1.setup.do

IP Address	192.168.1.3 / 27
Gateway	192.168.1.1
SSID	CorpNet
SSID Broadcast	● Yes ○ No

Wireless

Mode	G
Channel	3

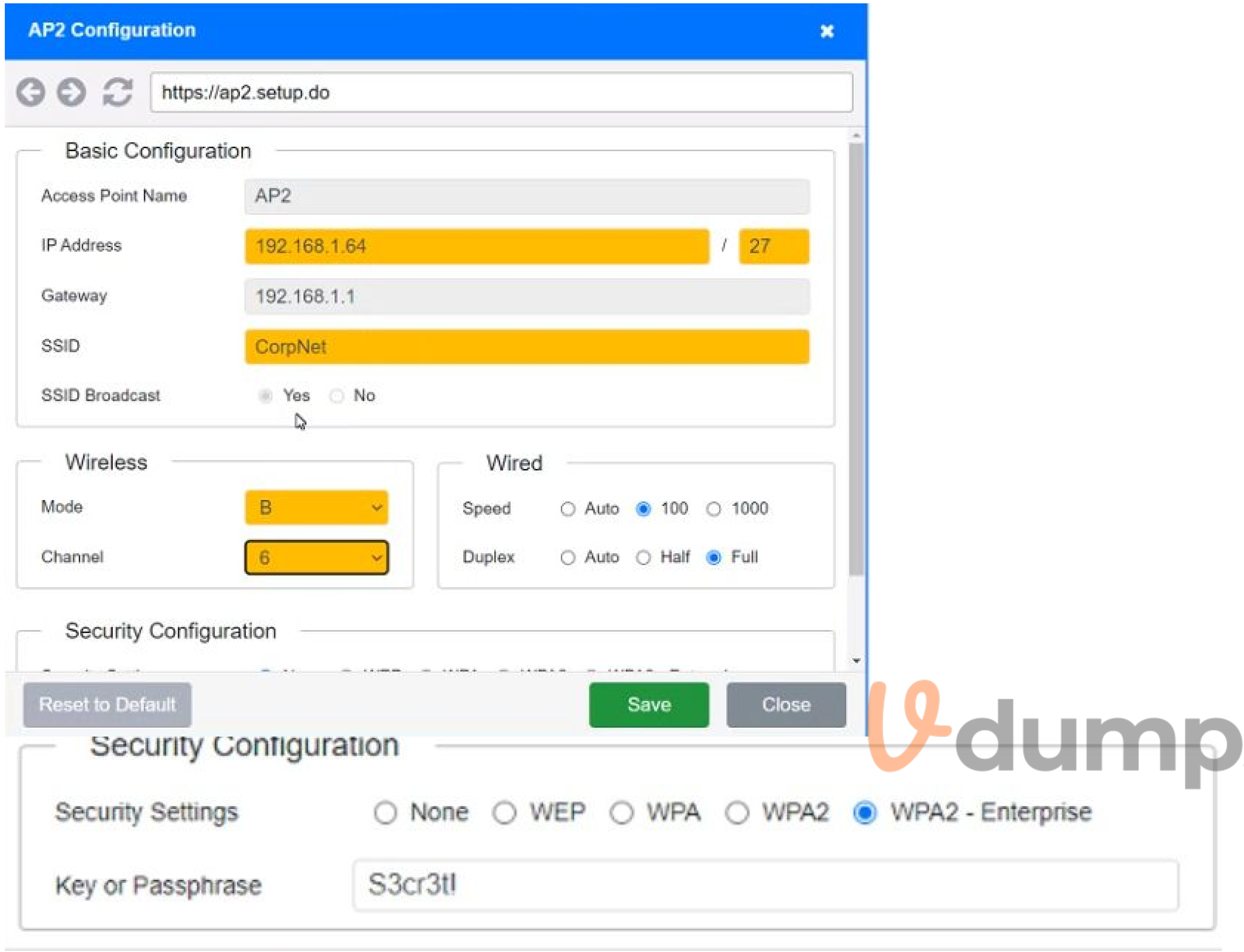
Wired

Speed	● Auto ○ 100 ○ 1000
Duplex	● Auto ○ Half ○ Full

Security Configuration

Security Settings	○ None ○ WEP ● WPA ○ WPA2 ○ WPA2 - Enterprise
Key or Passphrase	S3cr3t!

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

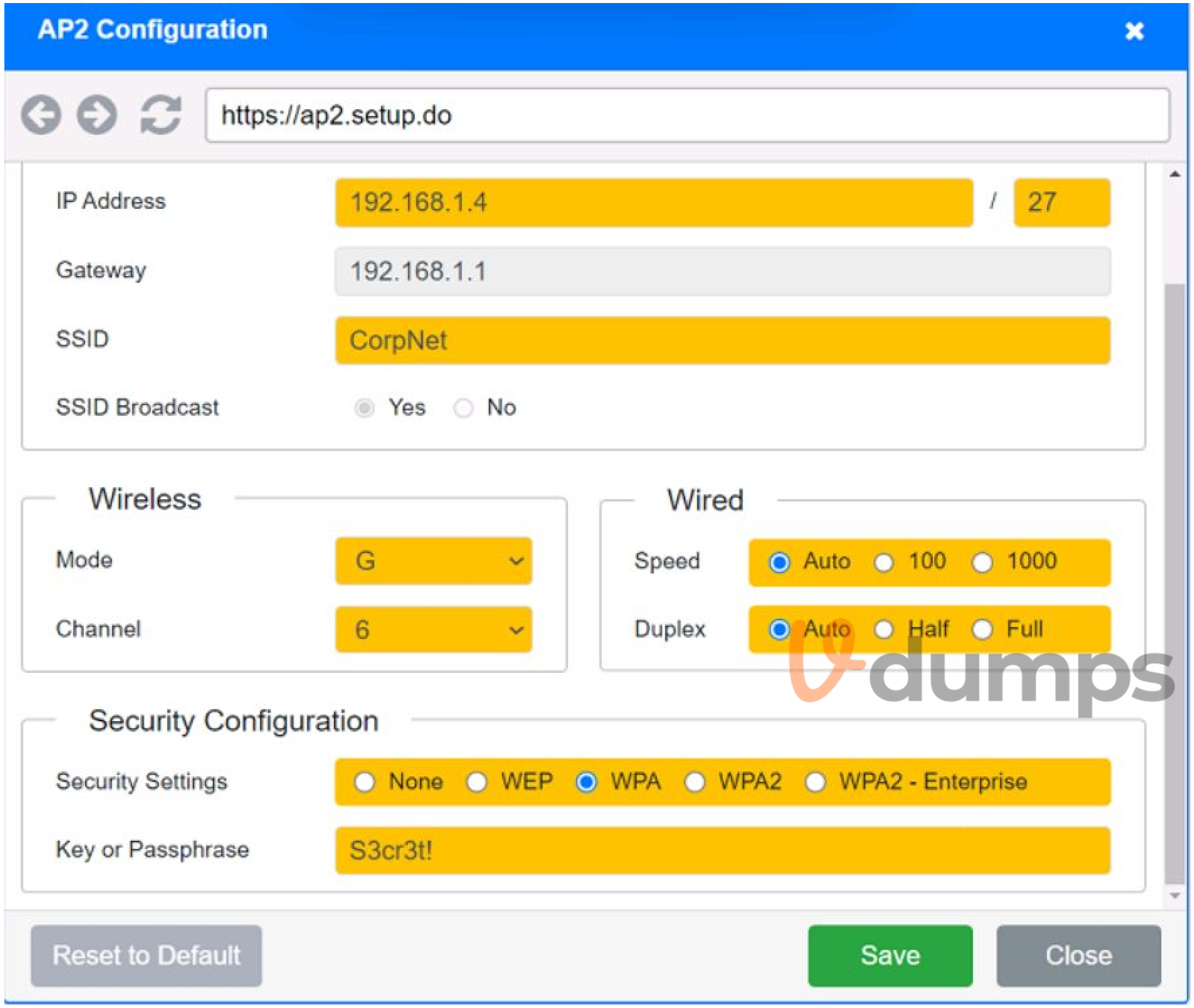
Wired

Speed	○ Auto ● 100 ○ 1000
Duplex	○ Auto ○ Half ● Full

Security Configuration

Security Configuration

Security Settings	○ None ○ WEP ○ WPA ○ WPA2 ● WPA2 - Enterprise
Key or Passphrase	S3cr3t!



AP2 Configuration

https://ap2.setup.do

IP Address	192.168.1.4 / 27
Gateway	192.168.1.1
SSID	CorpNet
SSID Broadcast	● Yes ○ No

Wireless

Mode	G
Channel	6

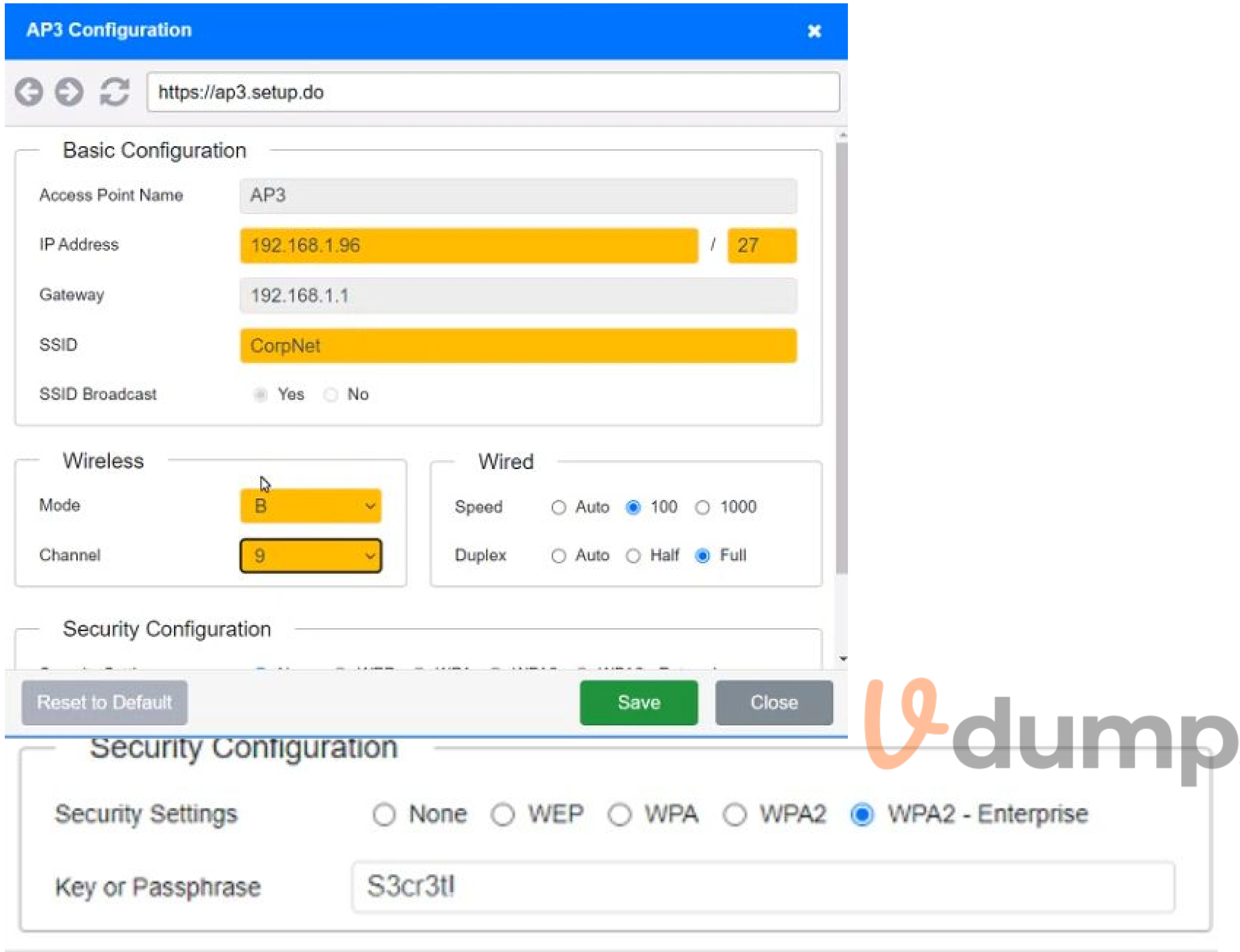
Wired

Speed	● Auto ○ 100 ○ 1000
Duplex	● Auto ○ Half ○ Full

Security Configuration

Security Settings	○ None ○ WEP ● WPA ○ WPA2 ○ WPA2 - Enterprise
Key or Passphrase	S3cr3t!

Exhibit 3 as follows
Access Point Name AP3



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

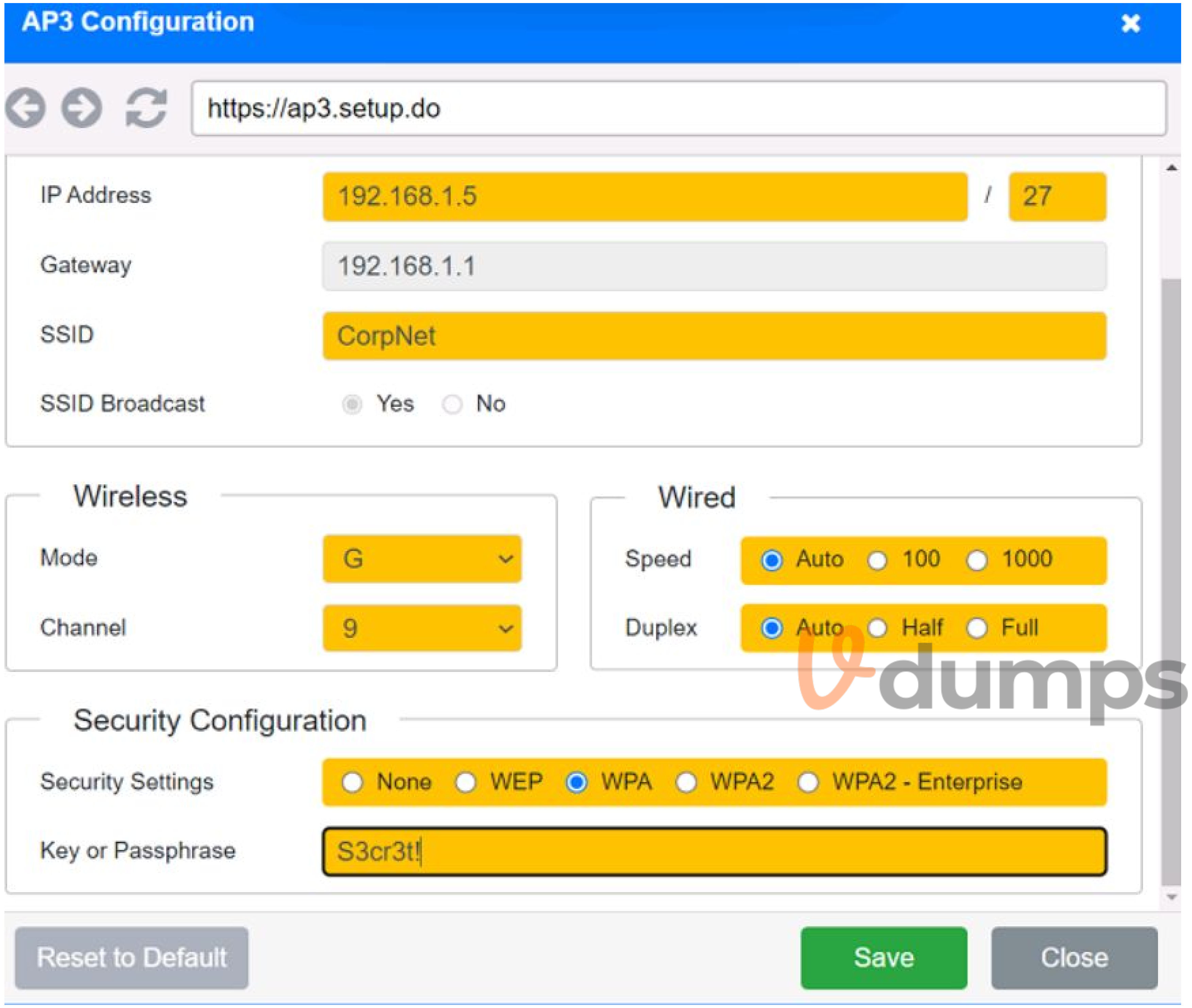
Mode	B
Channel	9

Wired

Speed	○ Auto ● 100 ○ 1000
Duplex	○ Auto ○ Half ● Full

Security Configuration

Security Settings	○ None ○ WEP ○ WPA ○ WPA2 ● WPA2 - Enterprise
Key or Passphrase	S3cr3t!



AP3 Configuration

https://ap3.setup.do

IP Address: 192.168.1.5 / 27

Gateway: 192.168.1.1

SSID: CorpNet

SSID Broadcast: ● Yes ○ No

Wireless

Mode: G

Channel: 9

Wired

Speed: ● Auto ○ 100 ○ 1000

Duplex: ● Auto ○ Half ○ Full

Security Configuration

Security Settings: ○ None ○ WEP ● WPA ○ WPA2 ○ WPA2 - Enterprise

Key or Passphrase: S3cr3t!

QUESTION 18

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

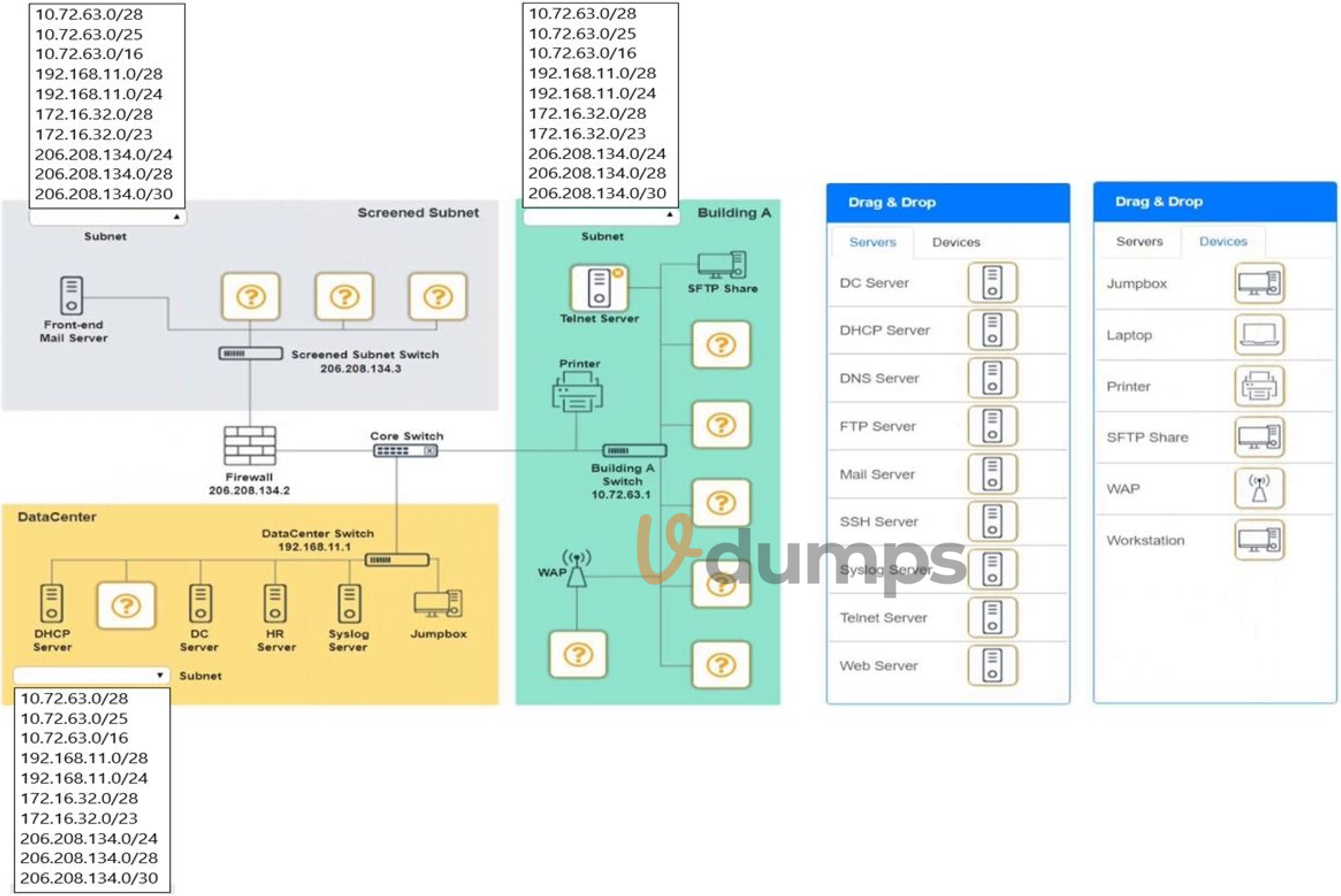
Provide a server to handle port 20/21 traffic

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.



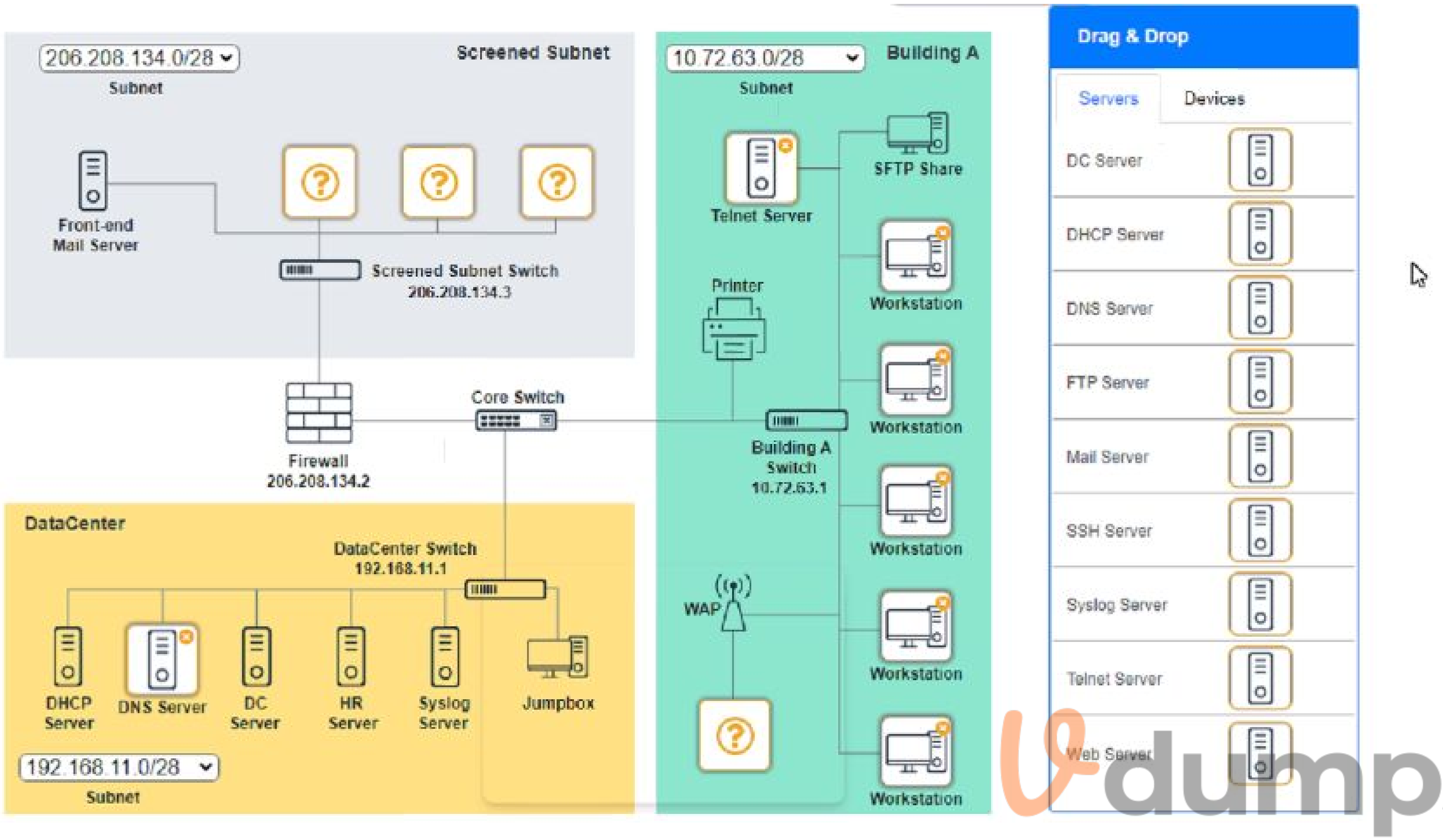
A. See explanation below

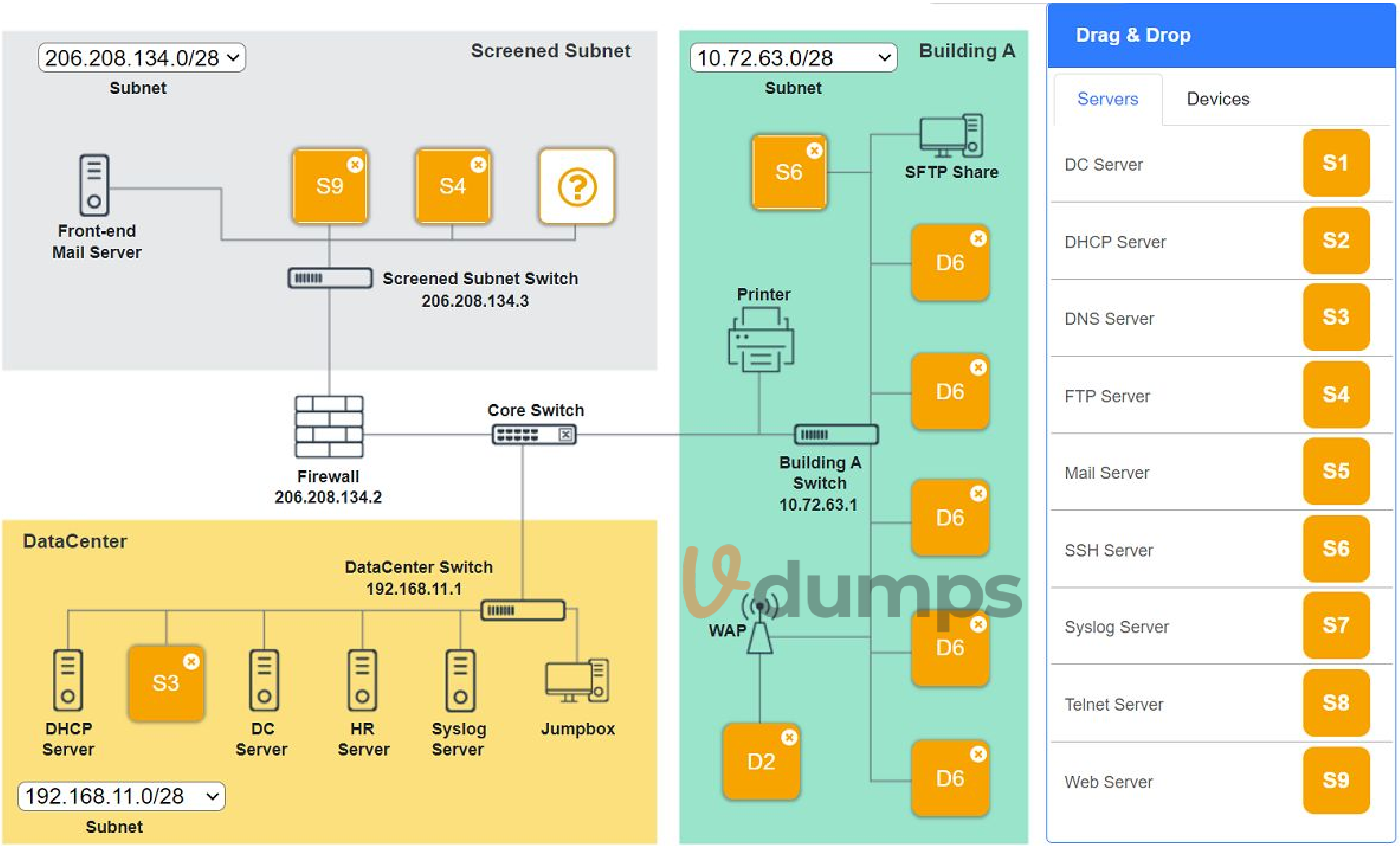
Correct Answer: A
Section:
Explanation:

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.

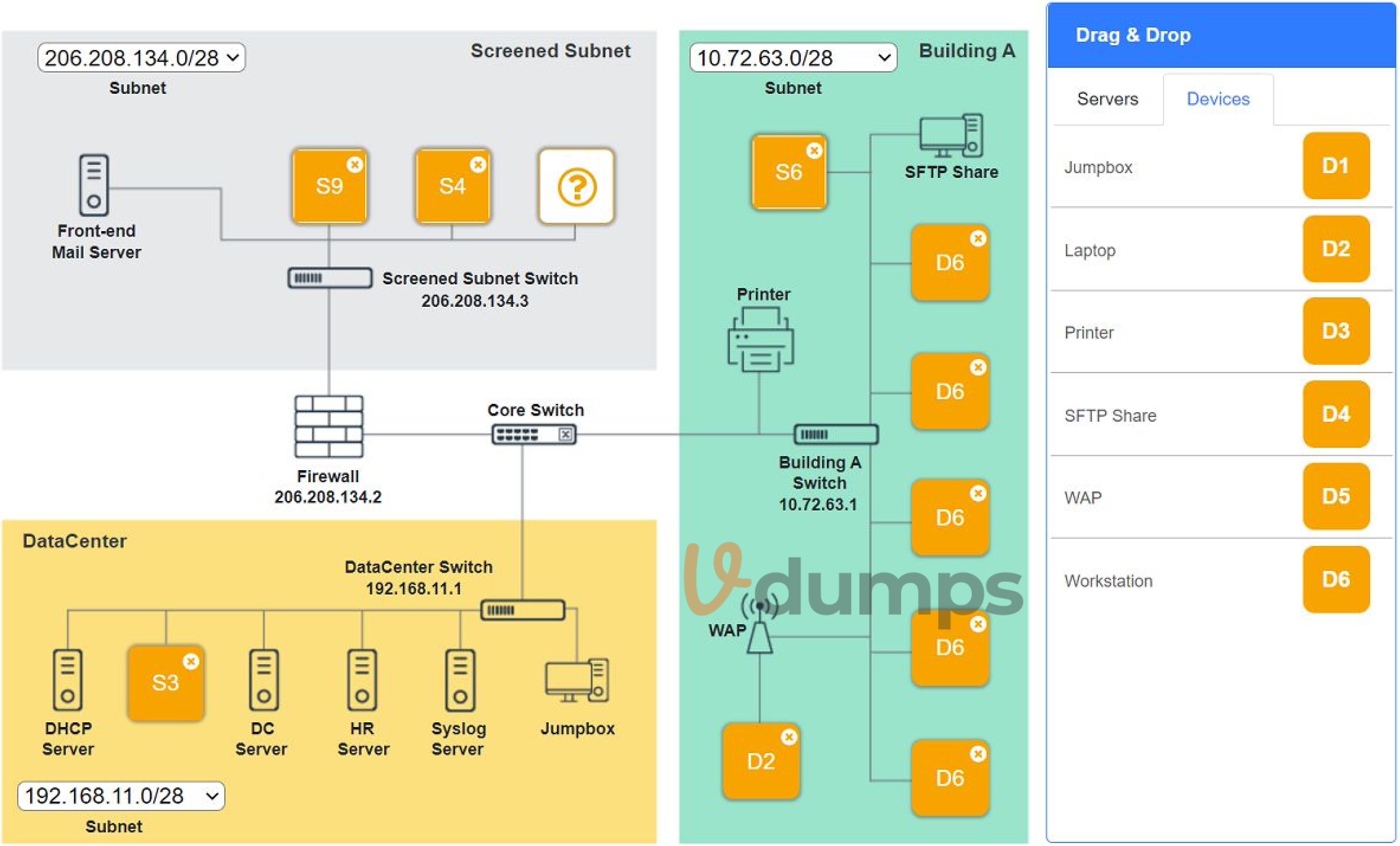




Drag & Drop

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



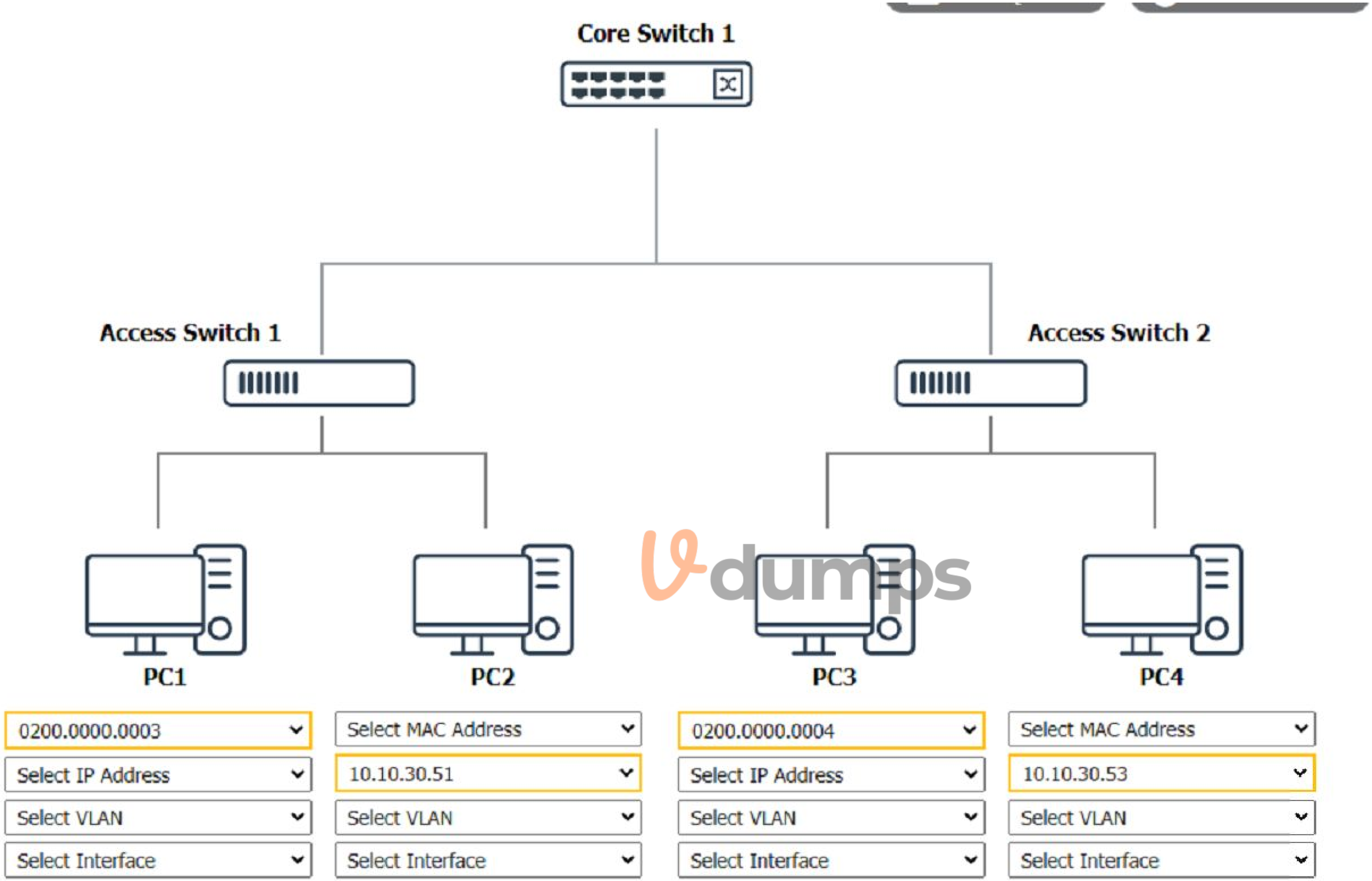
QUESTION 19

SIMULATION

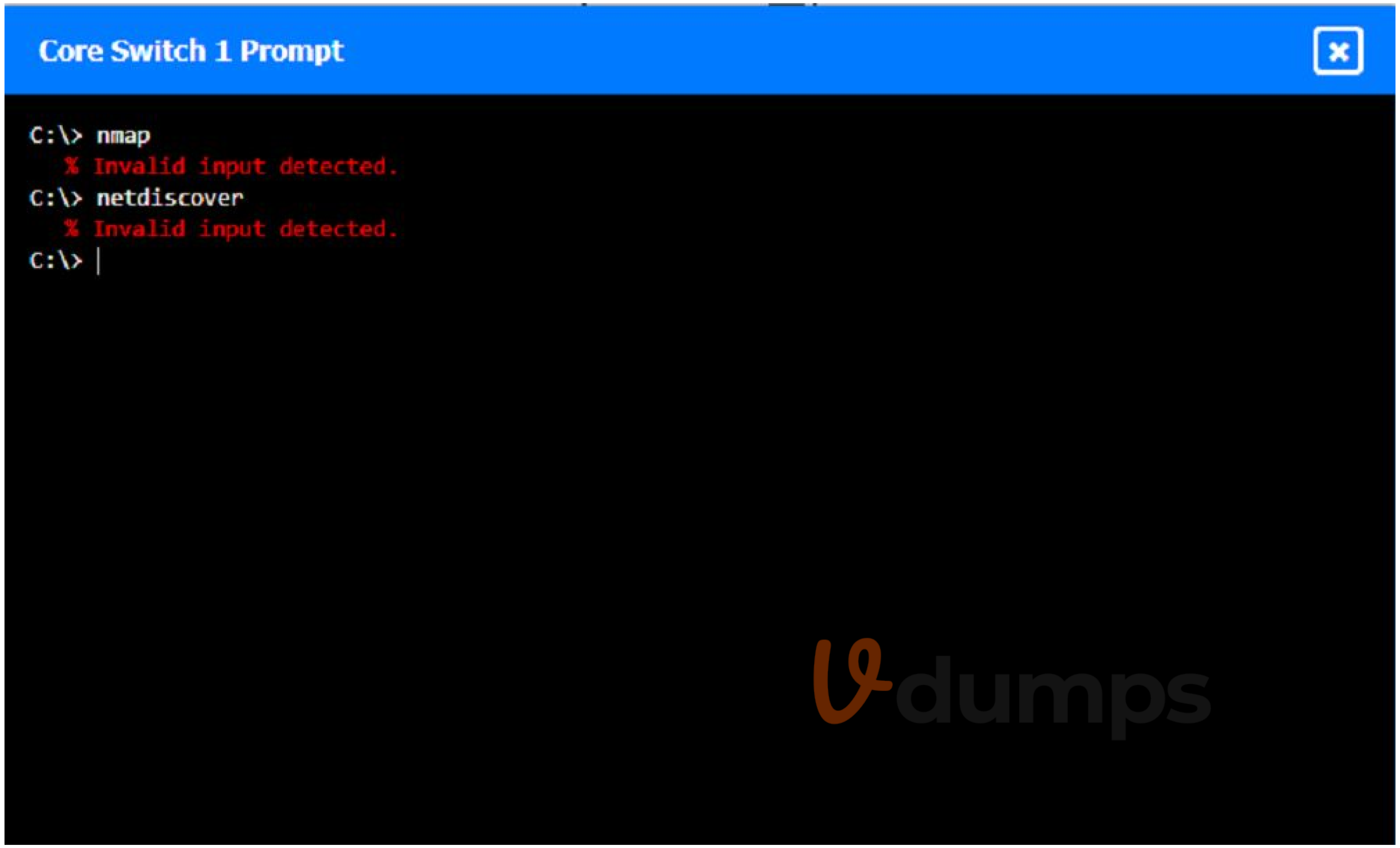
A network technician was recently onboarded to a company. A manager has tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.

Instructions:

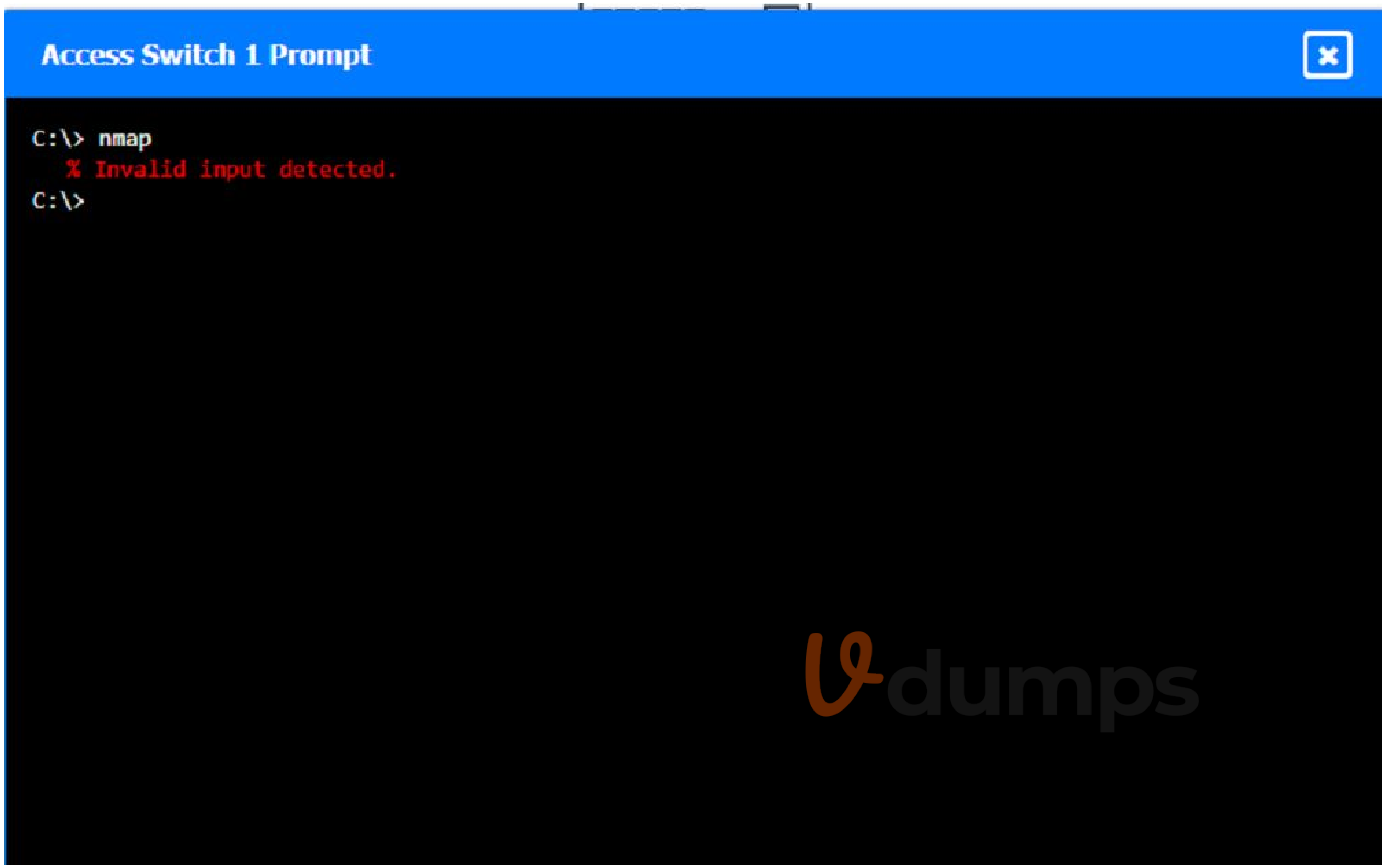
Click on each switch to perform a network discovery by entering commands into the terminal. Fill in the missing information using drop-down menus provided.



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

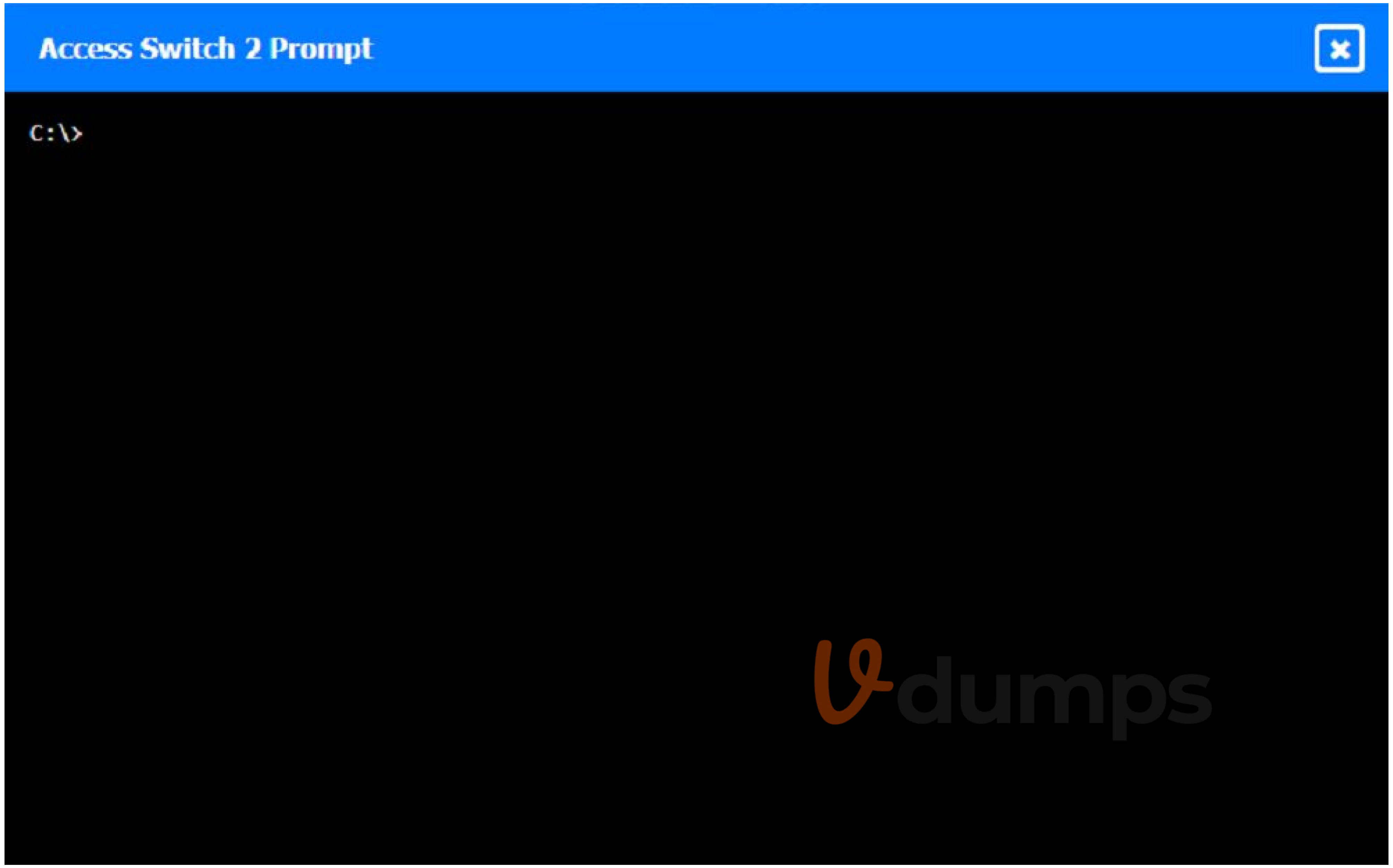


```
C:\> nmap
   % Invalid input detected.
C:\> netdiscover
   % Invalid input detected.
C:\> |
```



Access Switch 1 Prompt

```
C:\> nmap
   % Invalid input detected.
C:\>
```



Access Switch 2 Prompt

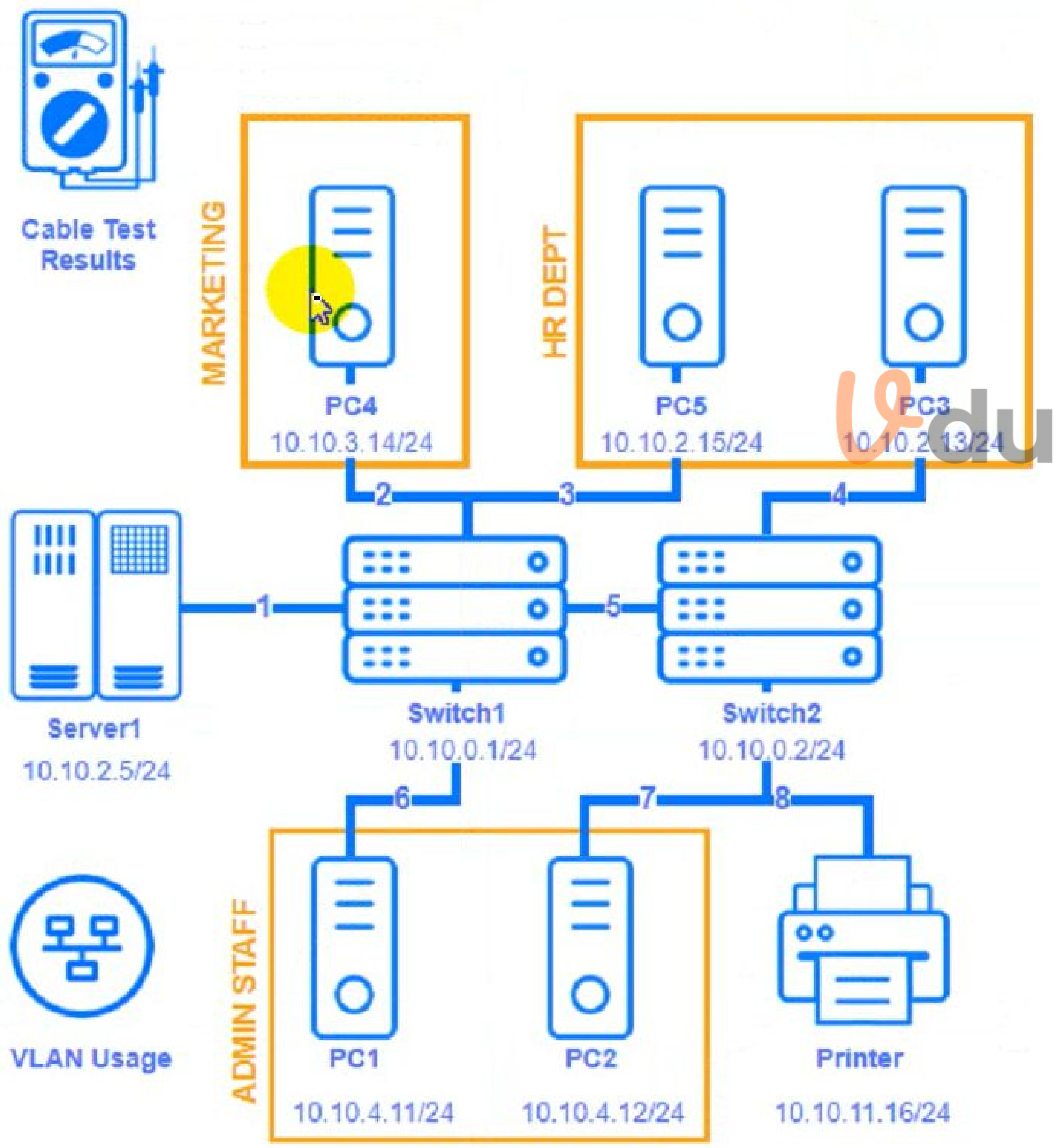
```
C:\>
```

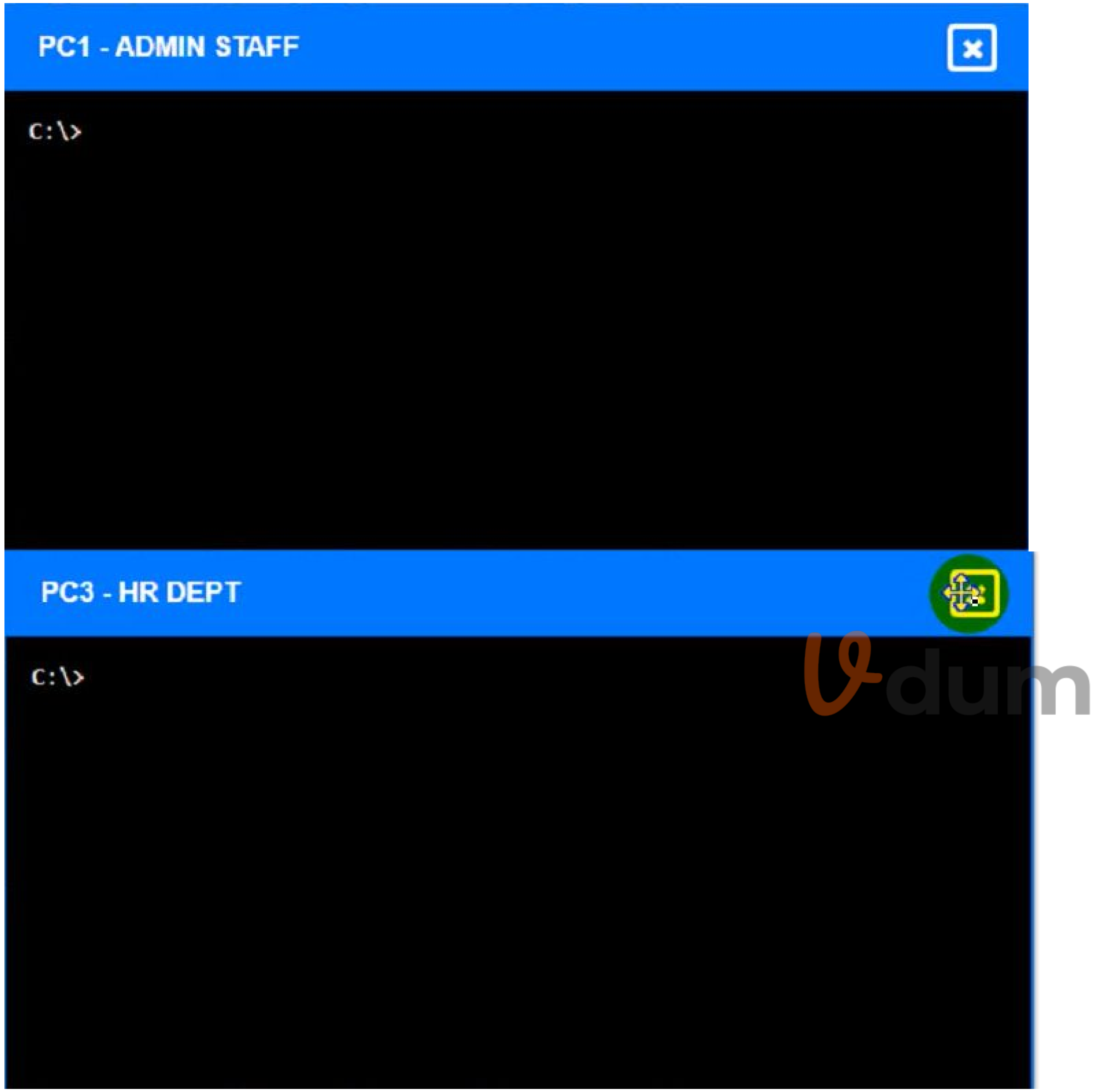
A. See the Explanation for detailed information on this simulation

Correct Answer: A
Section:
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 commandshow ip interface briefto display the IP addresses and statuses of the switch interfaces.
Enter the commandshow vlan briefto display the VLAN configurations and assignments of the switch interfaces.
Enter the commandshow cdp neighborsto 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 is192.168.1.1.
The VLAN configuration of Core Switch 1 isVLAN 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 areAccess Switch 1 and Access Switch 2.
The interfaces that connect Core Switch 1 to Access Switch 1 areGigabitEthernet0/1 and GigabitEthernet0/2.

The interfaces that connect Core Switch 1 to Access Switch 2 areGigabitEthernet0/3 and GigabitEthernet0/4.
You can use the same steps to fill in the missing information for Access Switch 1 and Access Switch 2.

QUESTION 20
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.

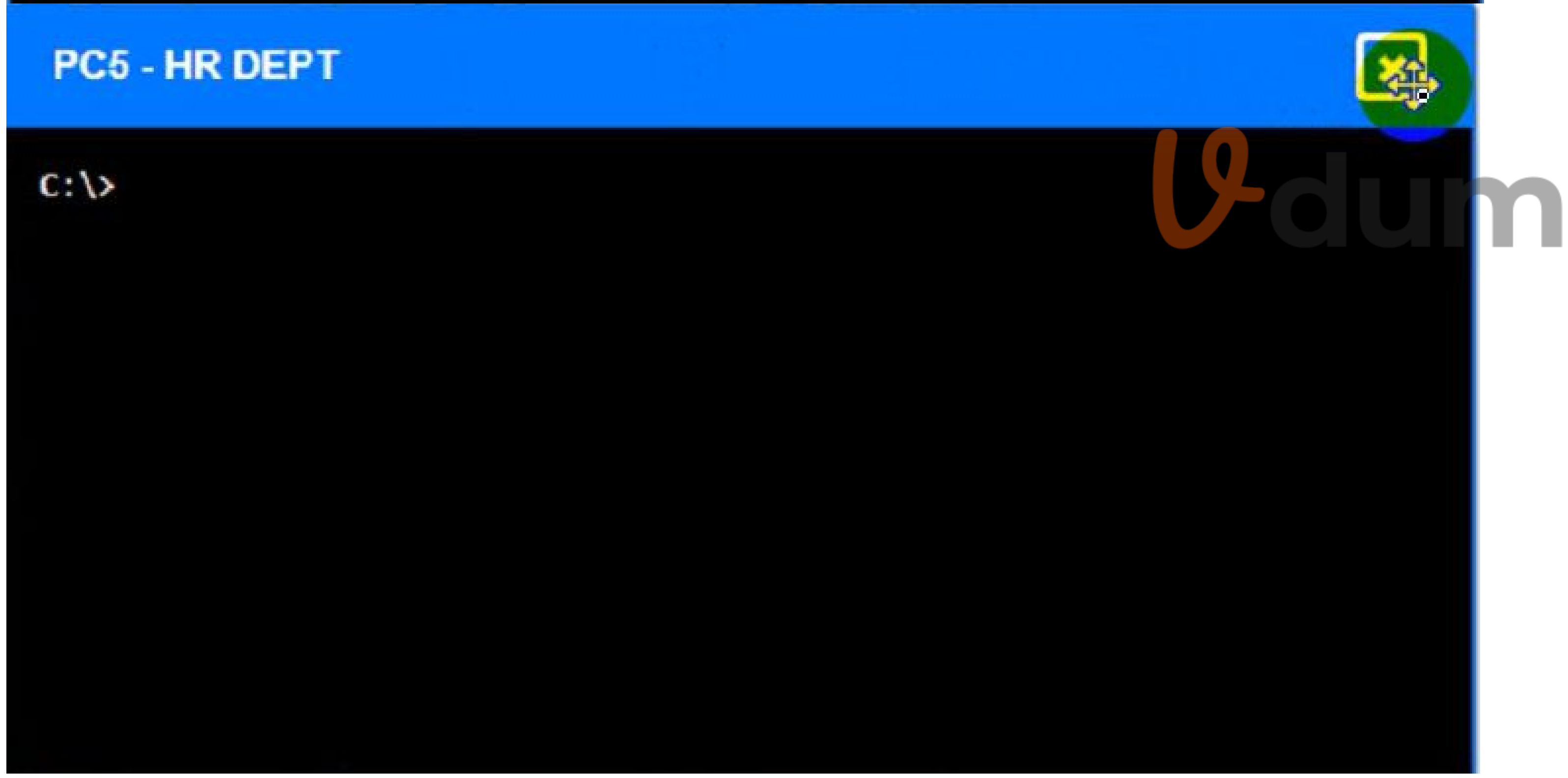




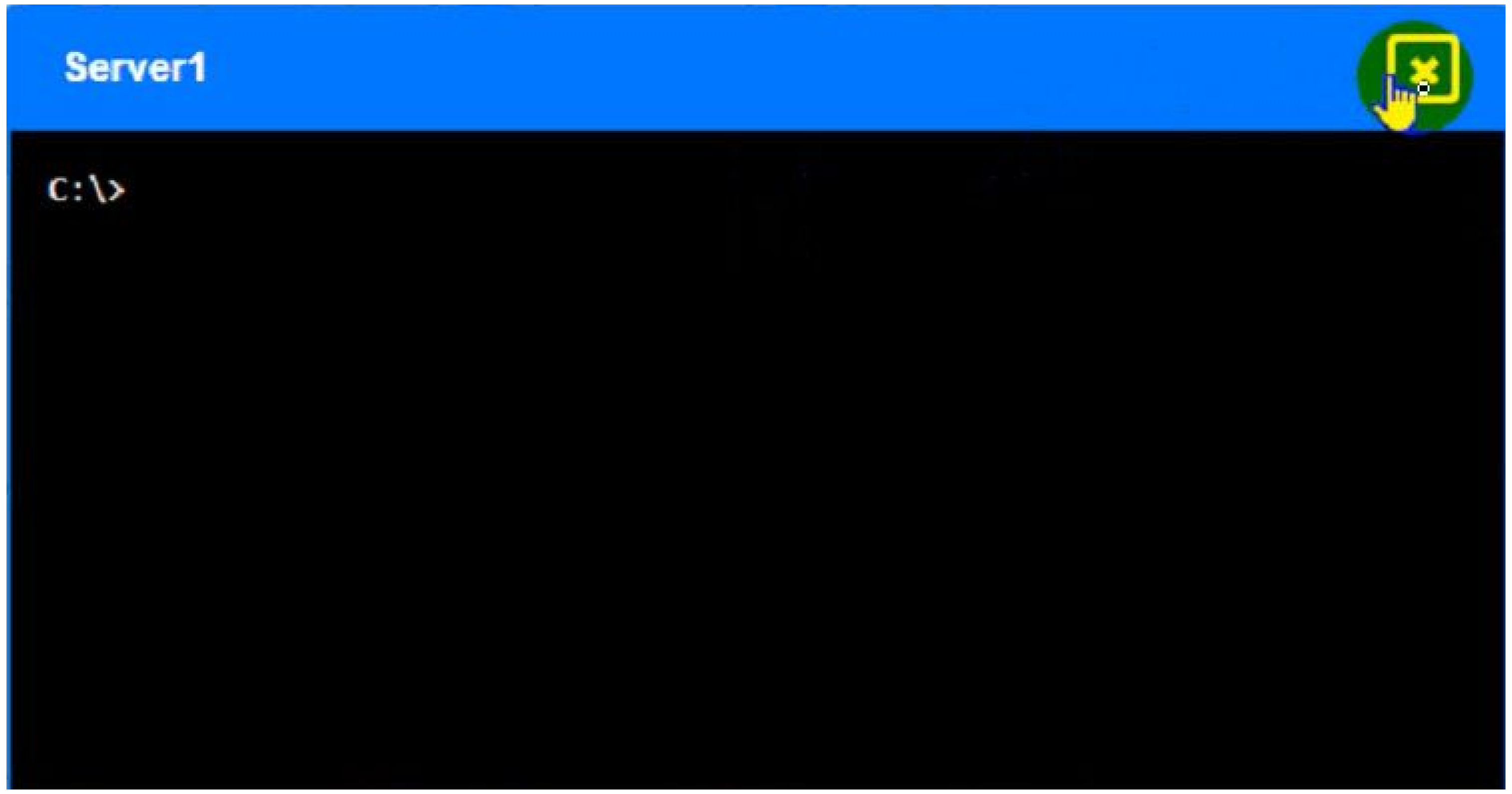
```
C:\>
```

```
C:\>
```

```
C:\>
```



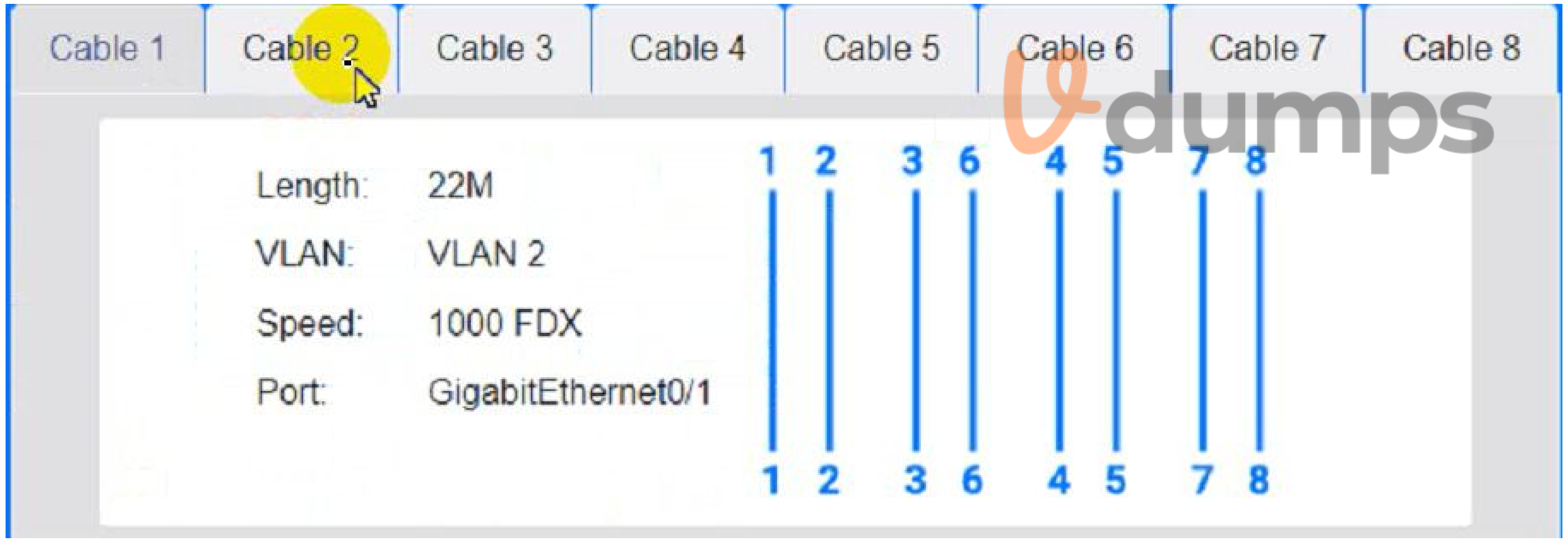
```
C:\>
```



```
C:\>
```

Cable Test Results:

Cable 1:



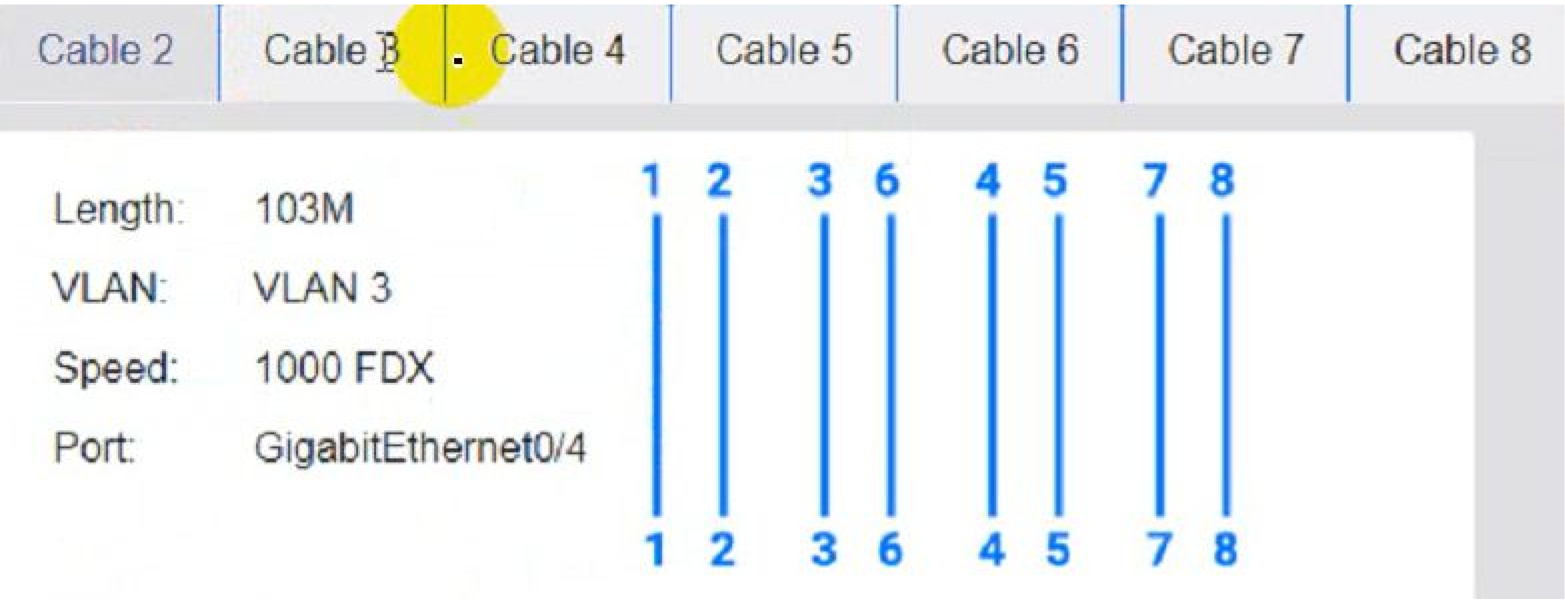
Length: 22M

VLAN: VLAN 2

Speed: 1000 FDX

Port: GigabitEthernet0/1

Cable 2:



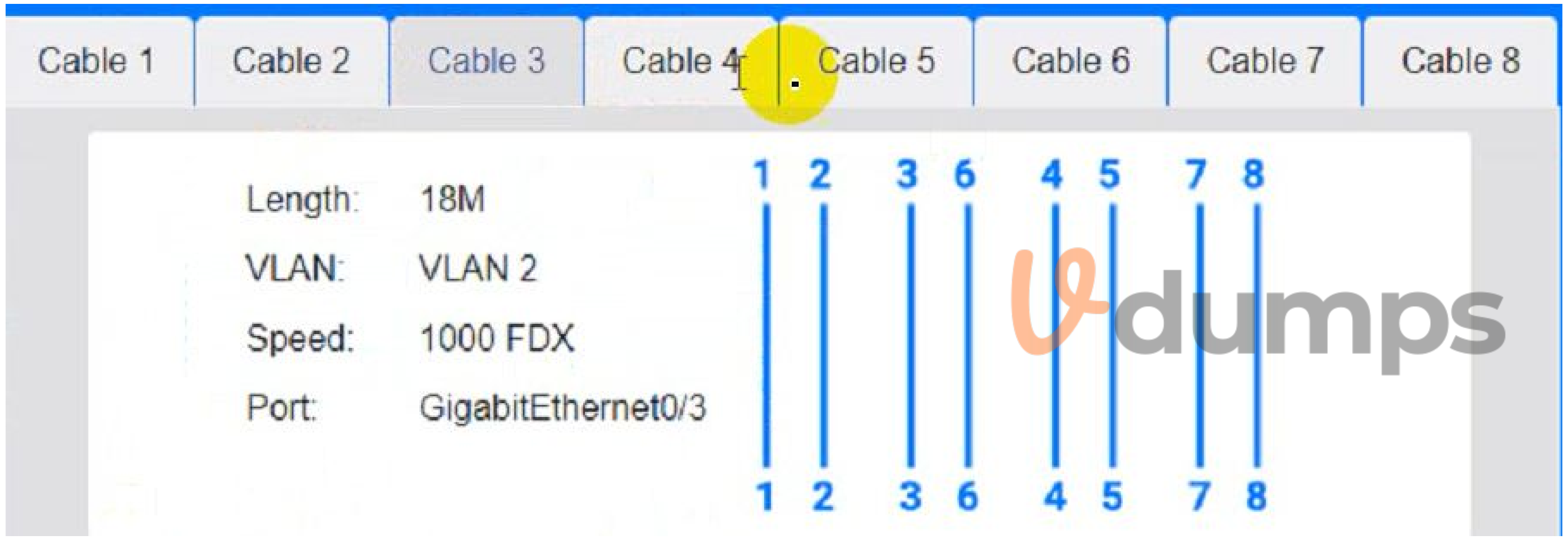
Length: 103M

VLAN: VLAN 3

Speed: 1000 FDX

Port: GigabitEthernet0/4

Cable 3:



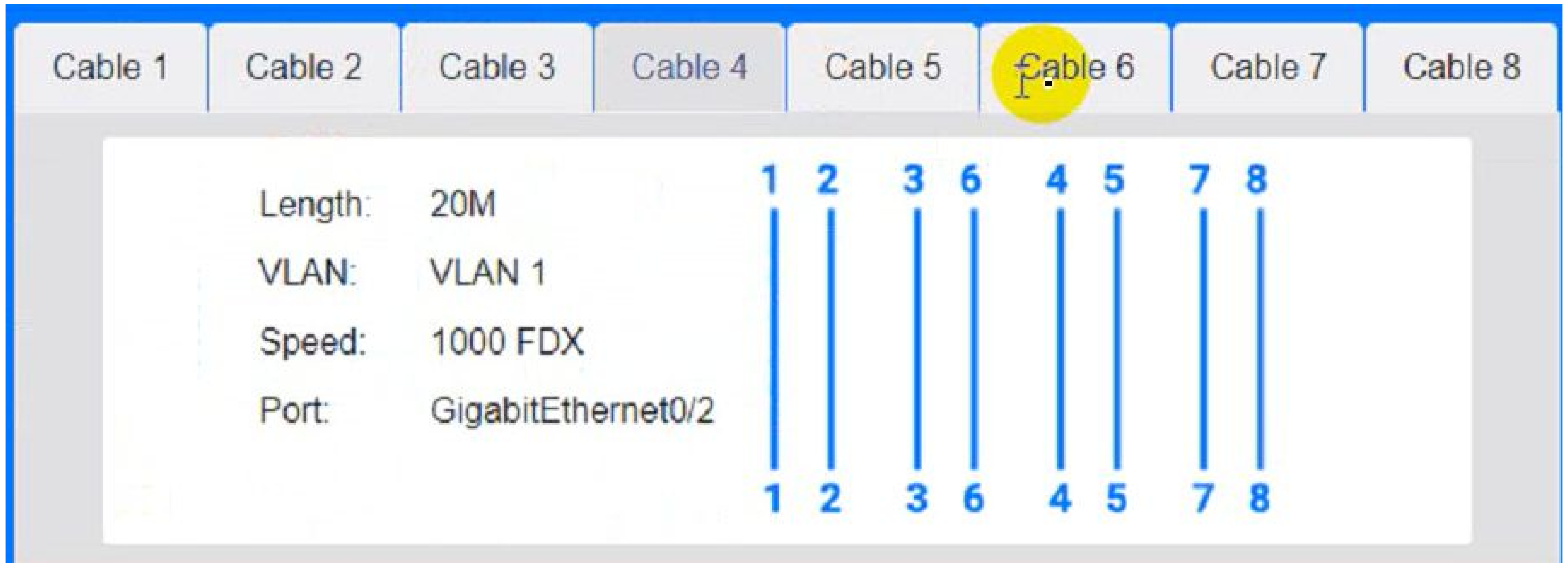
Length: 18M

VLAN: VLAN 2

Speed: 1000 FDX

Port: GigabitEthernet0/3

Cable 4:

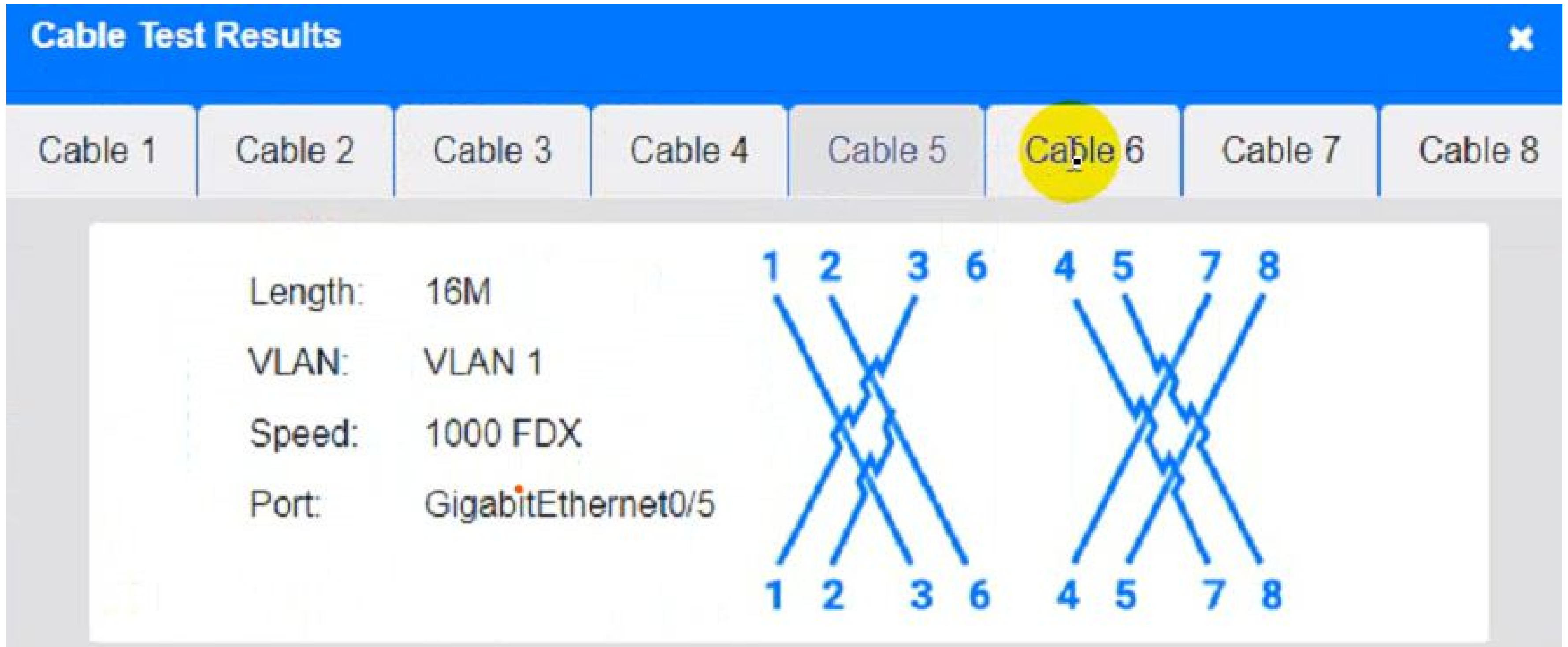


Length: 20M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/2



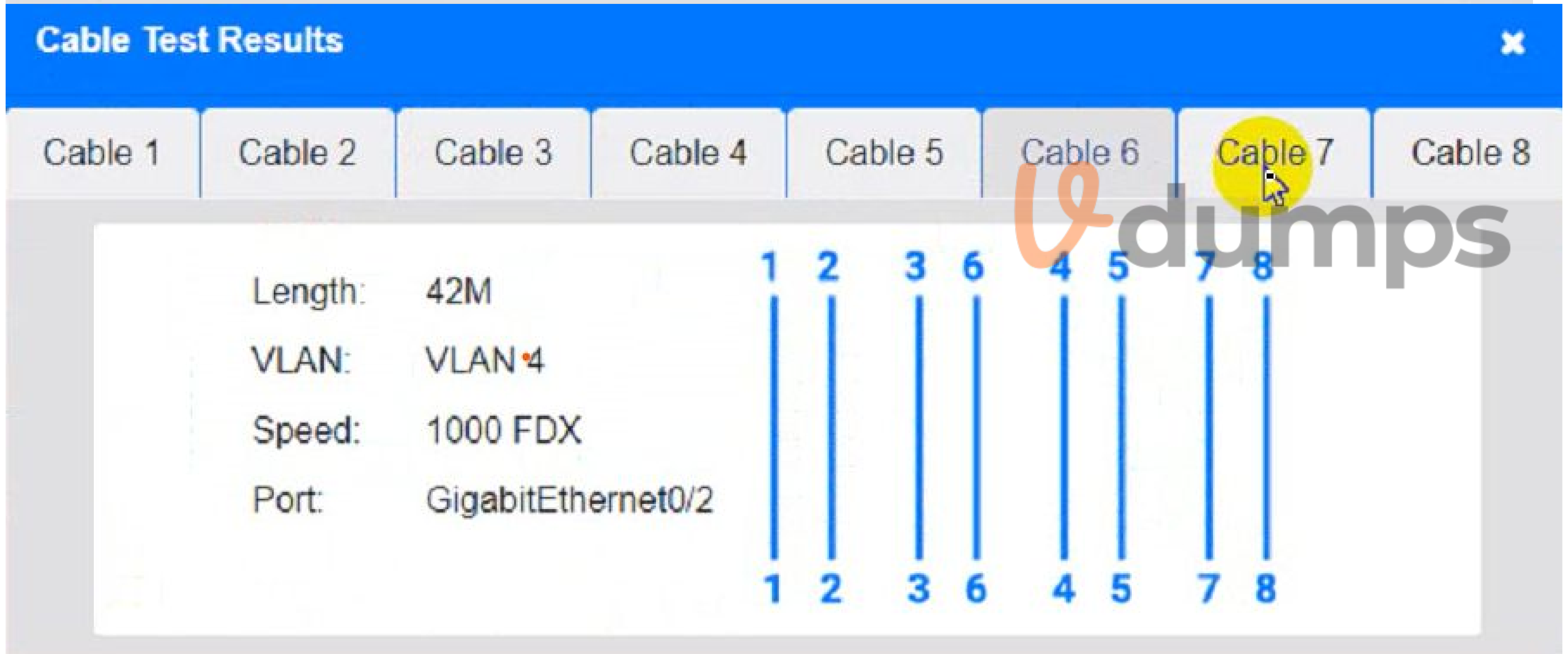
Cable Test Results

Length: 16M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/5



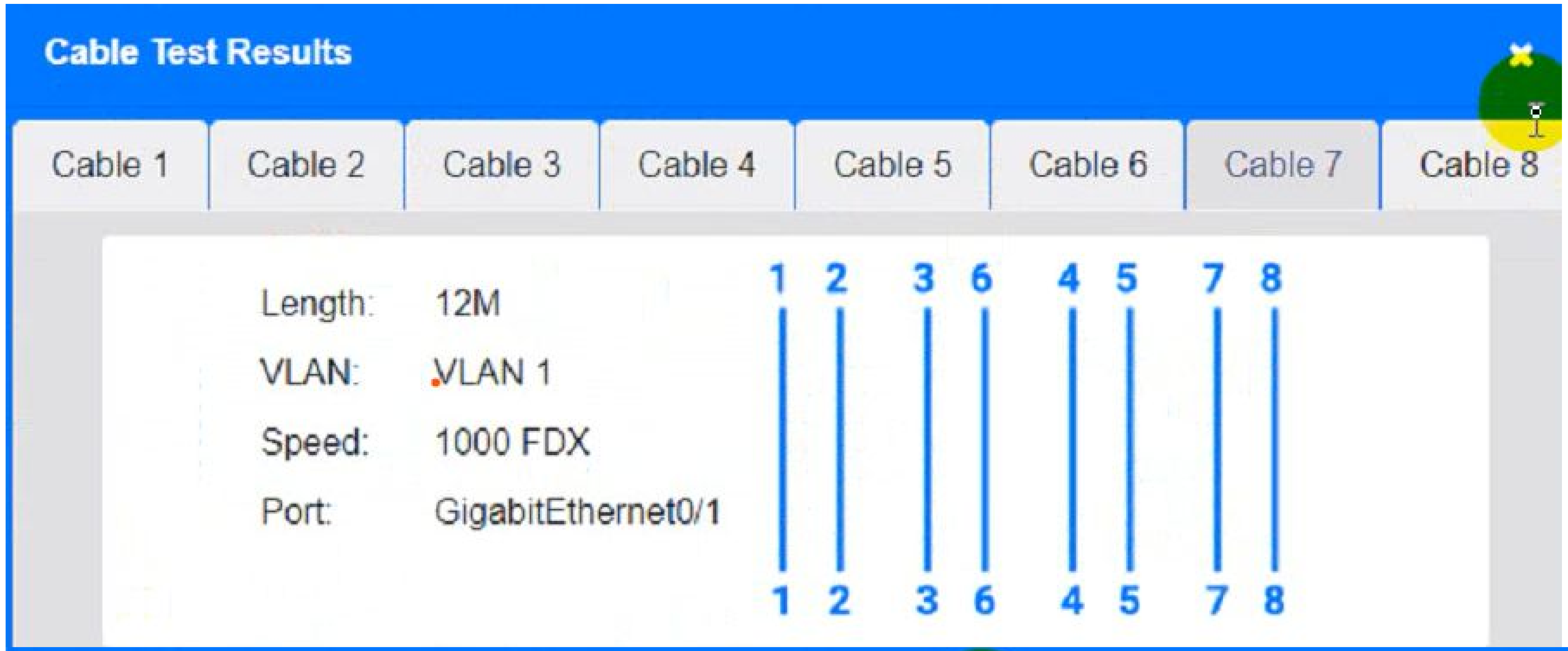
Cable Test Results

Length: 42M

VLAN: VLAN 4

Speed: 1000 FDX

Port: GigabitEthernet0/2



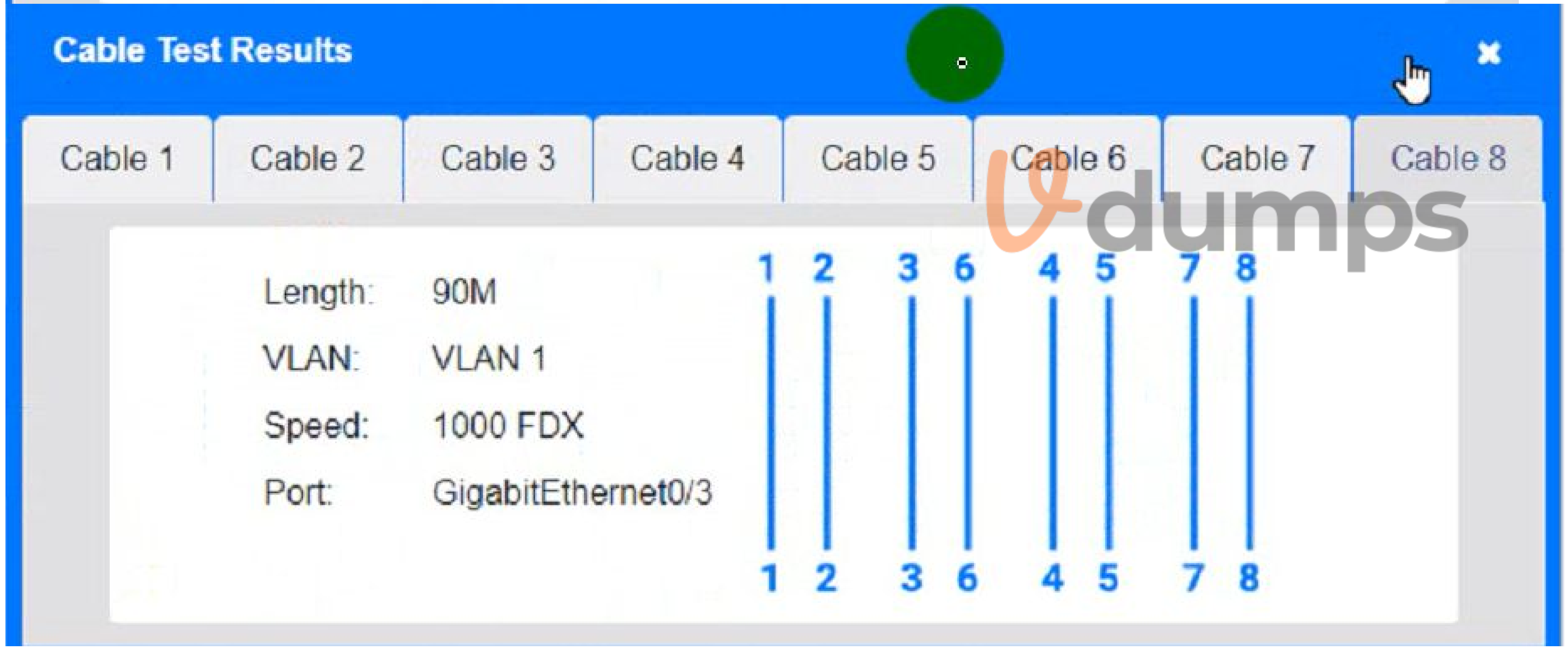
Cable Test Results

Length: 12M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/1



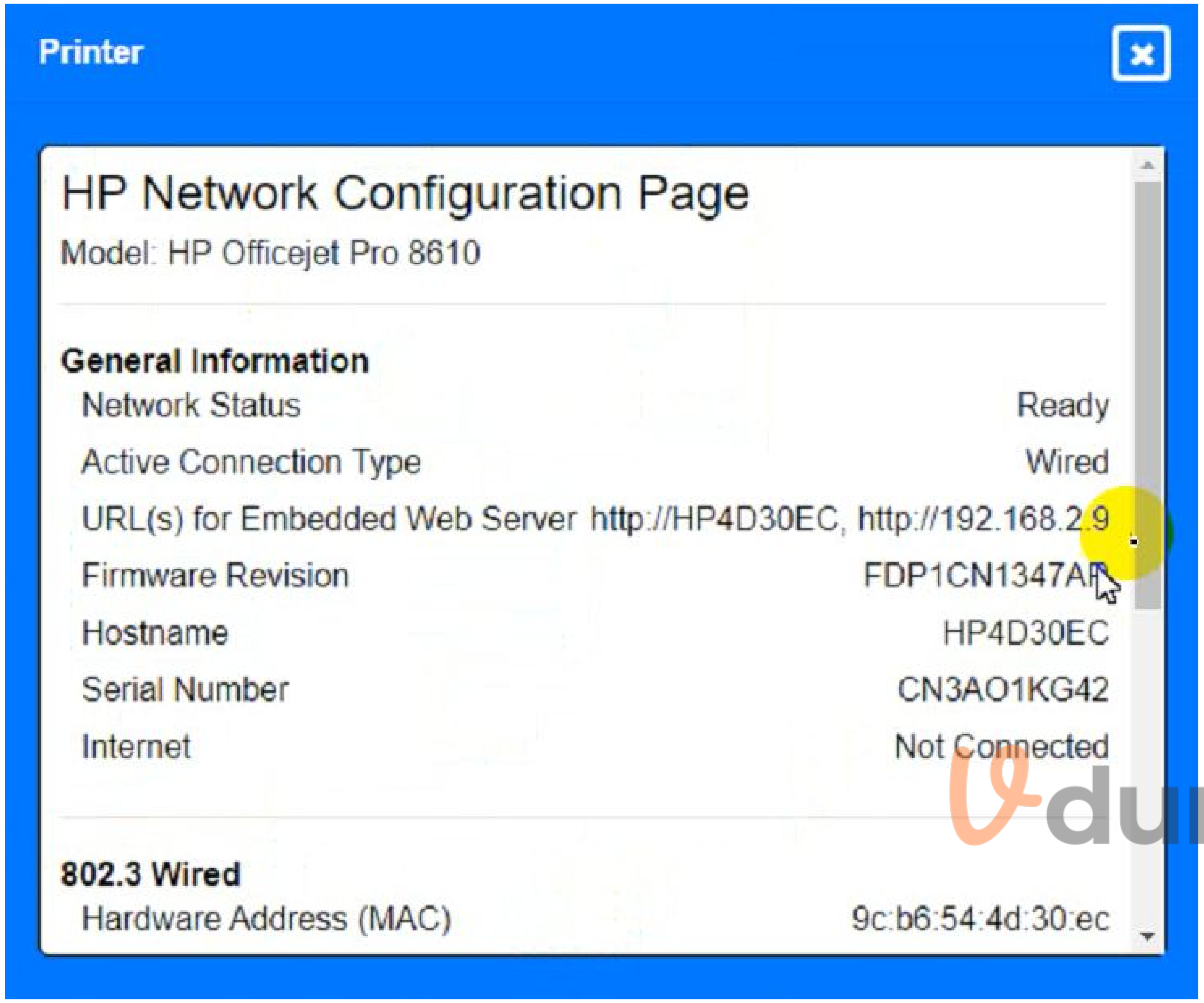
Cable Test Results

Length: 90M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/3



HP Network Configuration Page

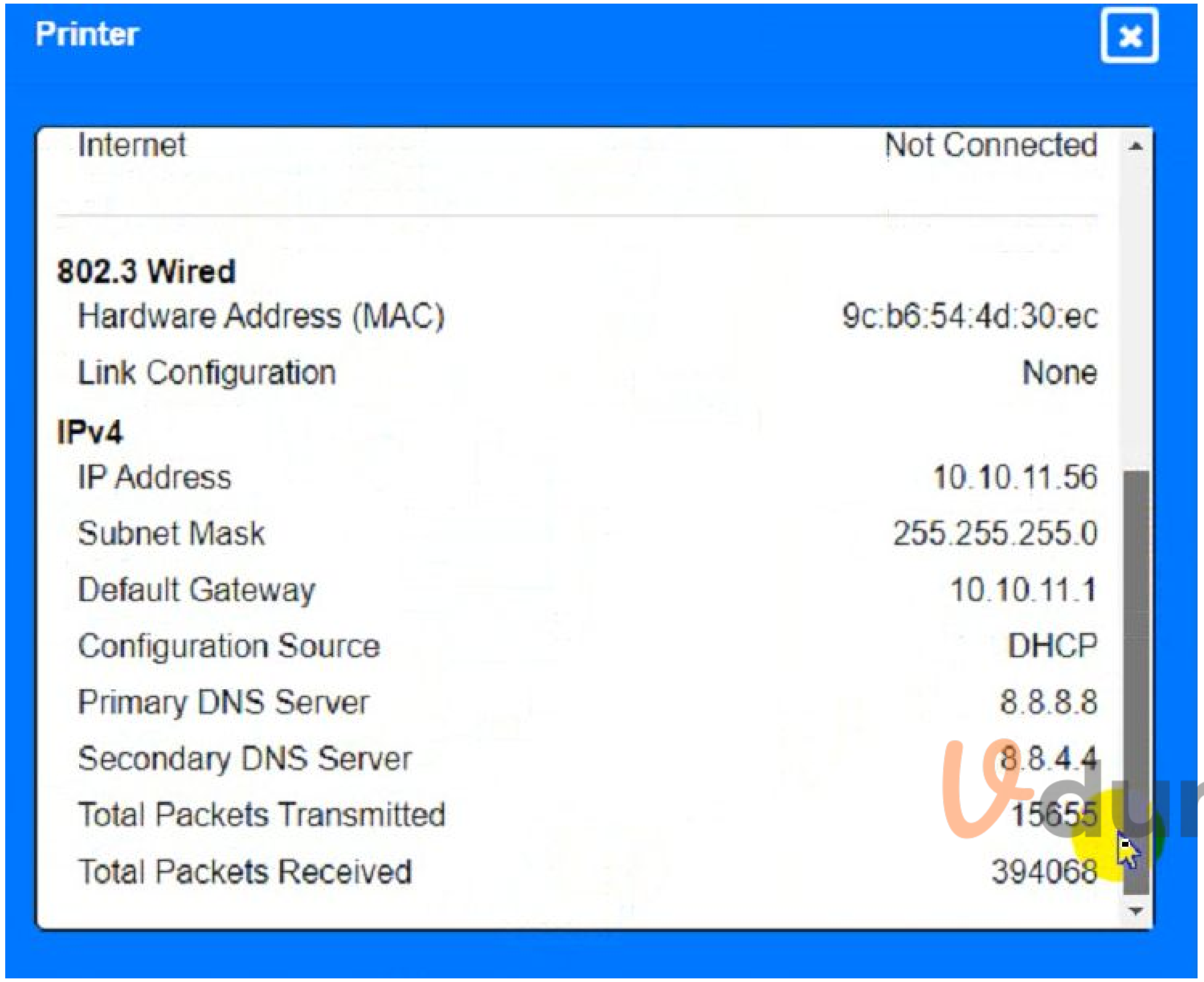
Model: HP Officejet Pro 8610

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

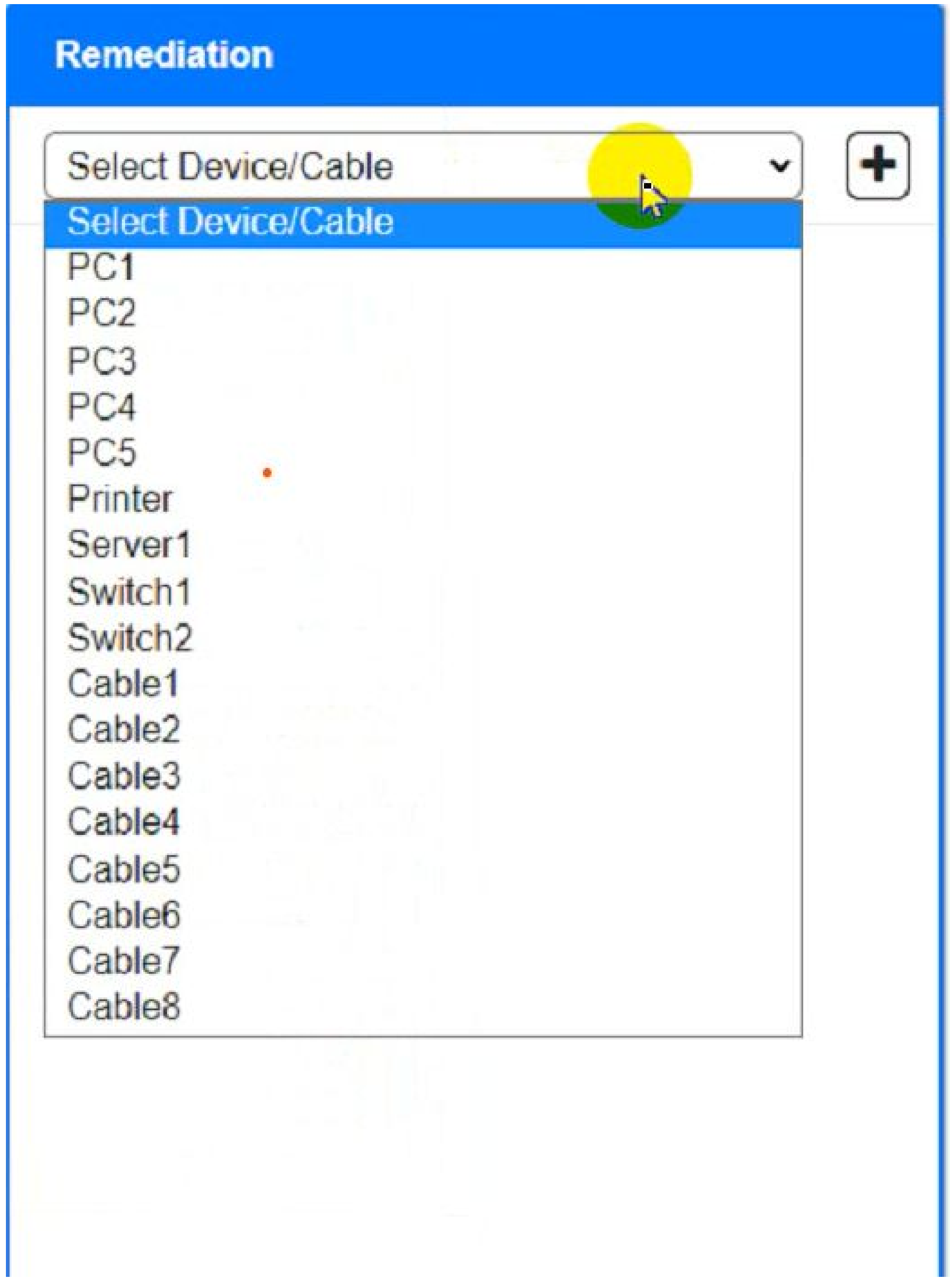
Internet	Not Connected

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



A. See the Explanation for detailed information on this simulation

Correct Answer: A
Section:
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 isPC1.

The problem isIncorrect IP address.
The solution isChange 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 commandipconfig /allto display the IP configuration of the device, including its IP address, subnet mask, default gateway, and DNS servers.
Enter the commandping <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 commandtracert <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 commandipconfig /allto 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 commandping 192.168.1.1to 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 commandtracert 192.168.1.1to 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 21
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.

Correct Answer: D
Section:
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.
CompTIA Network+ guide explaining the troubleshooting methodology and the importance of verifying functionality (see page Ref 9Basic Configuration Commands).

QUESTION 22

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

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

QUESTION 23
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

Correct Answer: B
Section:
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=TotalOperationalTimeNumberofFailures\text{MTBF} = \frac{\text{Total Operational Time}}{\text{Number of Failures}}MTBF=NumberofFailuresTotalOperationalTime

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=1000hours2=500hours\text{MTBF} = \frac{1000 \text{ hours}}{2} = 500 \text{ hours}MTBF=21000hours=500hours
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.
CompTIA Network+ guide explaining MTBF, MTTR, RPO, and RTO concepts and their calculations (see page Ref 10How to Use Cisco Packet Tracer).

QUESTION 24
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.

Correct Answer: C
Section:
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.

QUESTION 25
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

Correct Answer: C
Section:
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).

QUESTION 26
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.

Correct Answer: C
Section:
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.

QUESTION 27
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.

Correct Answer: B
Section:
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.
CompTIA Network+ study materials and DNS best practices.

QUESTION 28
Which of the following IP transmission types encrypts all of the transmitted data?

A. ESP
B. AH
C. GRE
D. UDP
E. TC P

Correct Answer: A
Section:
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.
CompTIA Network+ study materials on IPsec and encryption.

QUESTION 29
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

Correct Answer: B
Section:
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.
CompTIA Network+ study materials on wireless networking and interference mitigation.

QUESTION 30
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

Correct Answer: C
Section:
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.
CompTIA Network+ study materials and certification guides.

QUESTION 31
Which of the following can support a jumbo frame?

A. Access point
B. Bridge
C. Hub
D. Switch

Correct Answer: D
Section:
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.
CompTIA Network+ course materials and networking hardware documentation.

QUESTION 32
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

Correct Answer: D
Section:
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.
CompTIA Network+ certification materials and wireless network planning guides.

QUESTION 33
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.

Correct Answer: C
Section:
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.
CompTIA Network+ study materials on VLAN configuration and VoIP implementation.

QUESTION 34
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

Correct Answer: C
Section:
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.
CompTIA Network+ study materials on network security threats and mitigation techniques.

QUESTION 35
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

Correct Answer: A
Section:
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.
CompTIA Network+ study materials on network protocols and SIEM systems.

QUESTION 36
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

Correct Answer: C
Section:
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.
CompTIA Network+ study materials on IPsec and secure communication protocols.

QUESTION 37
Which of the following network traffic type is sent to all nodes on the network?

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

Correct Answer: B
Section:
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.

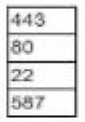
IPv4 Broadcast: An IPv4 broadcast address (e.g., 255.255.255.255) ensures the packet is sent to all devices on the network.
Network

QUESTION 38
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

Correct Answer: A, C
Section:
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

QUESTION 39
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:



443
80
22
587

Which of the following ports should be disabled?

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

Correct Answer: B
Section:
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

QUESTION 40

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

Correct Answer: D
Section:
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