Comptia

(N10-009)

CompTIA Network+

Total: **271 Questions**

Link:

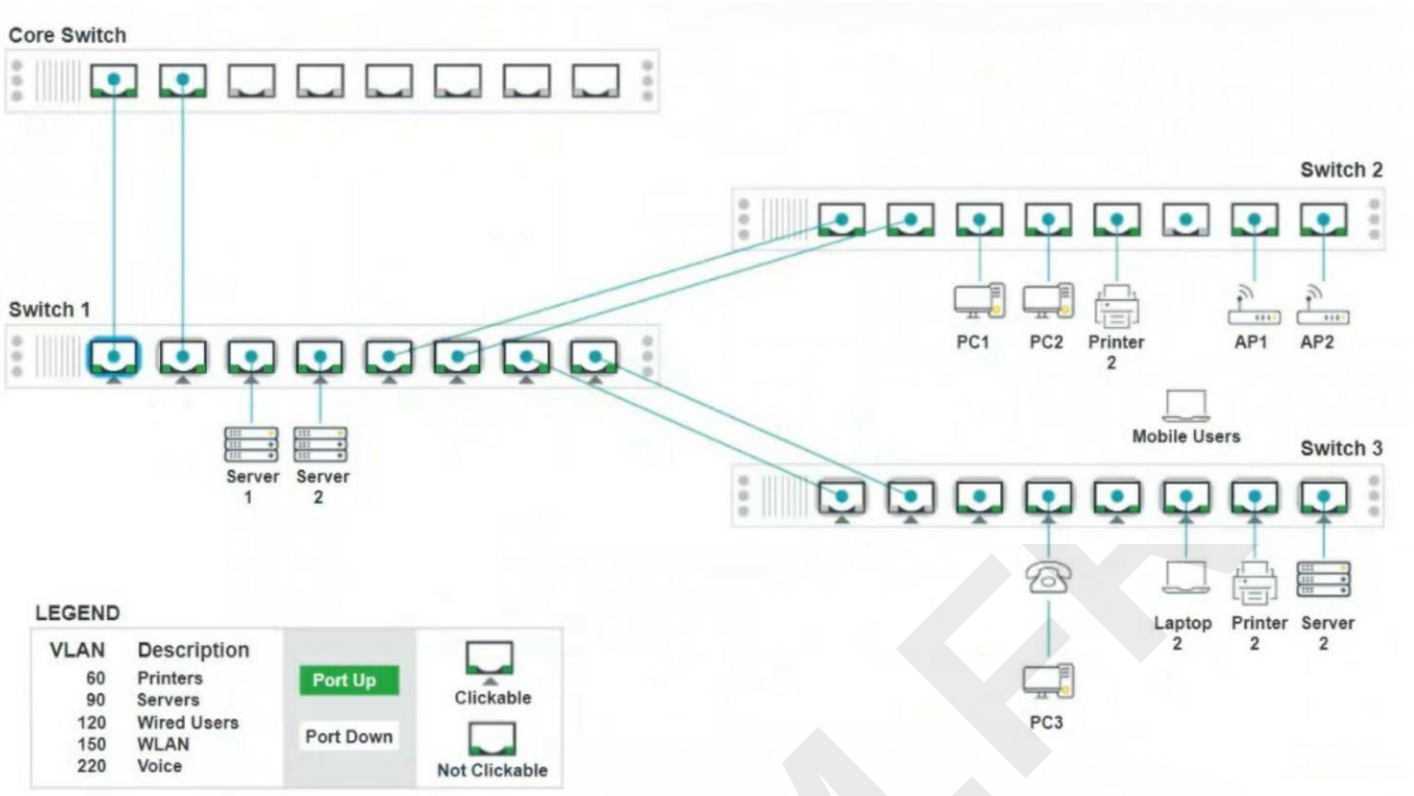
Question: 1

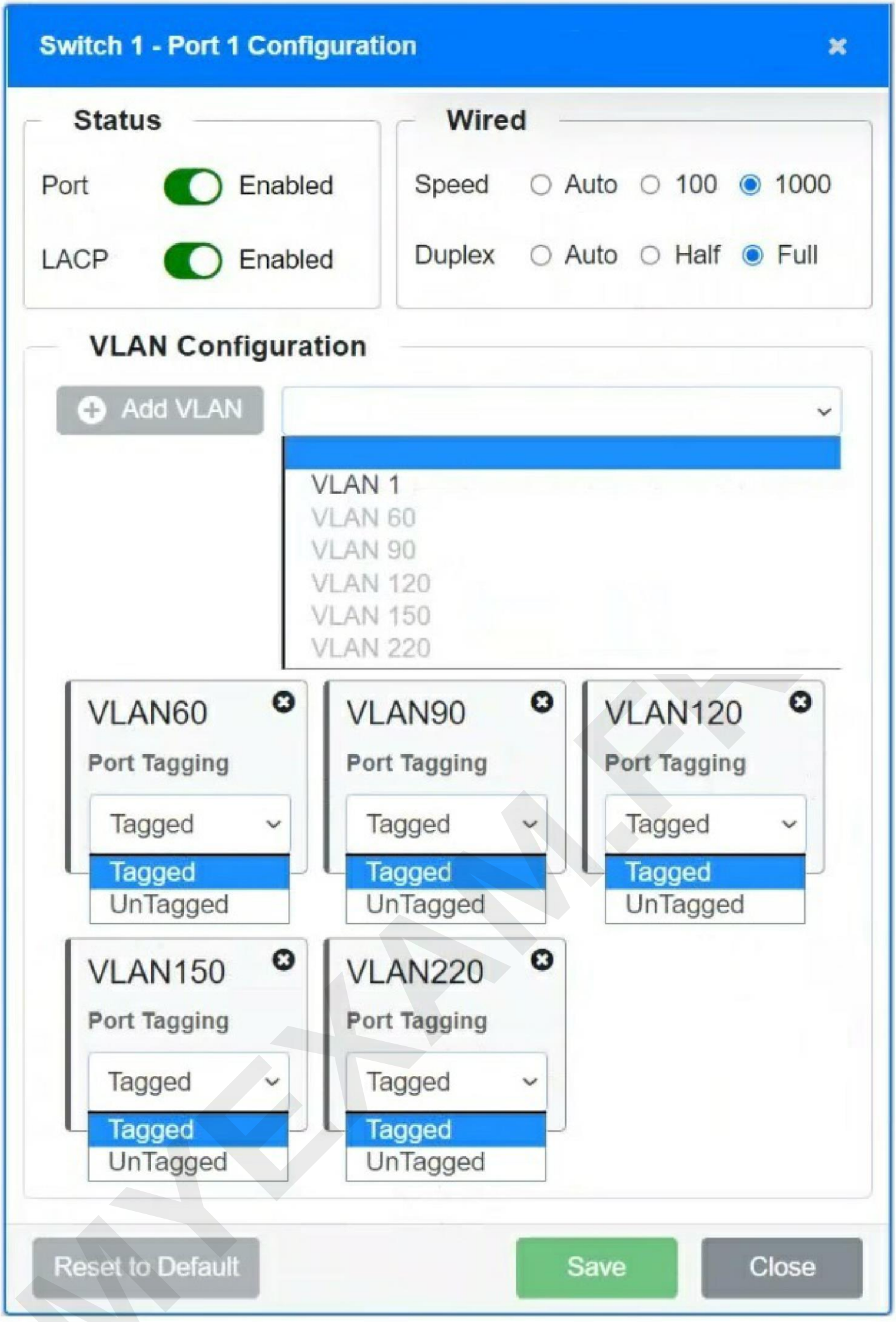
SIMULATION -

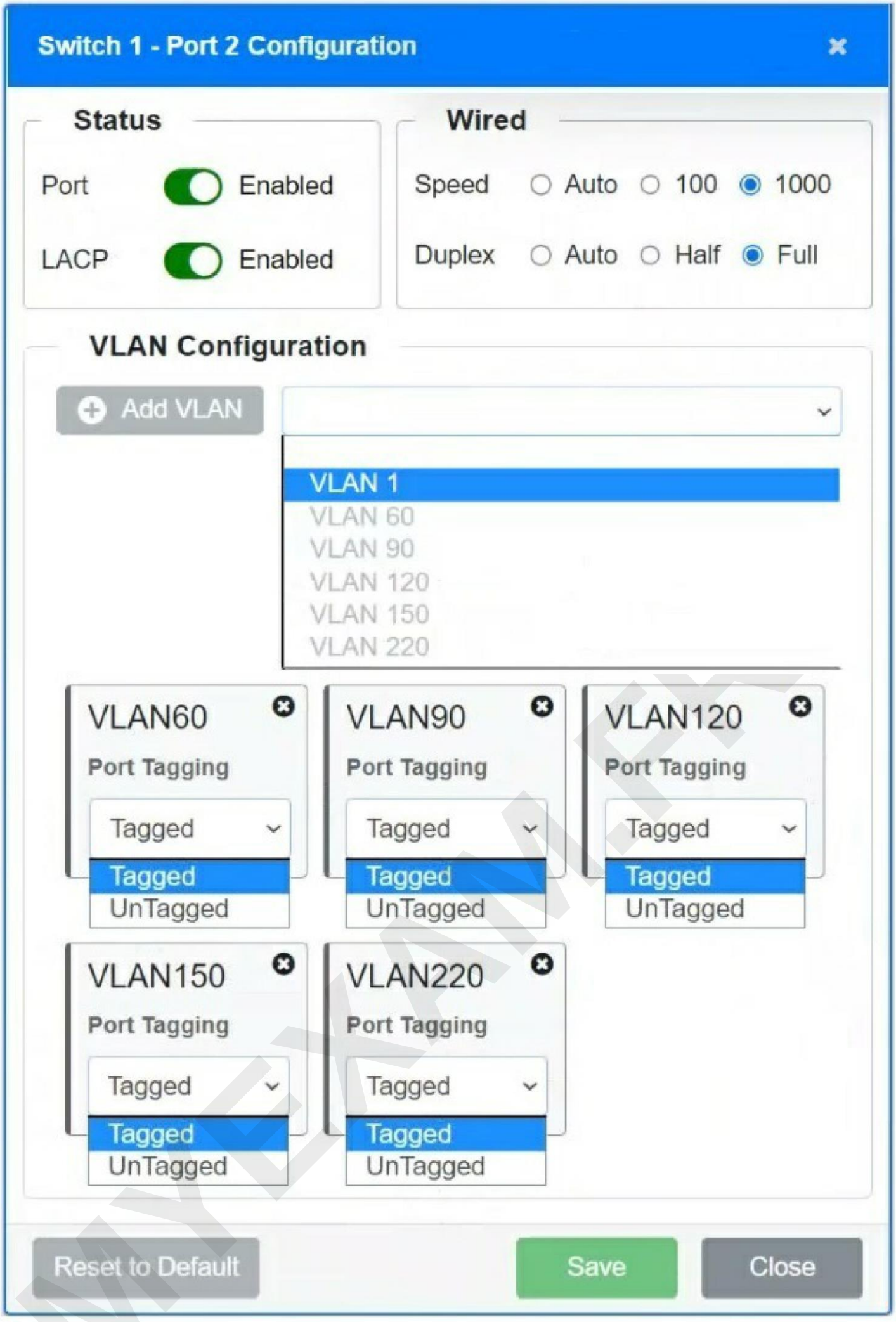
A network technician replaced an access layer switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.

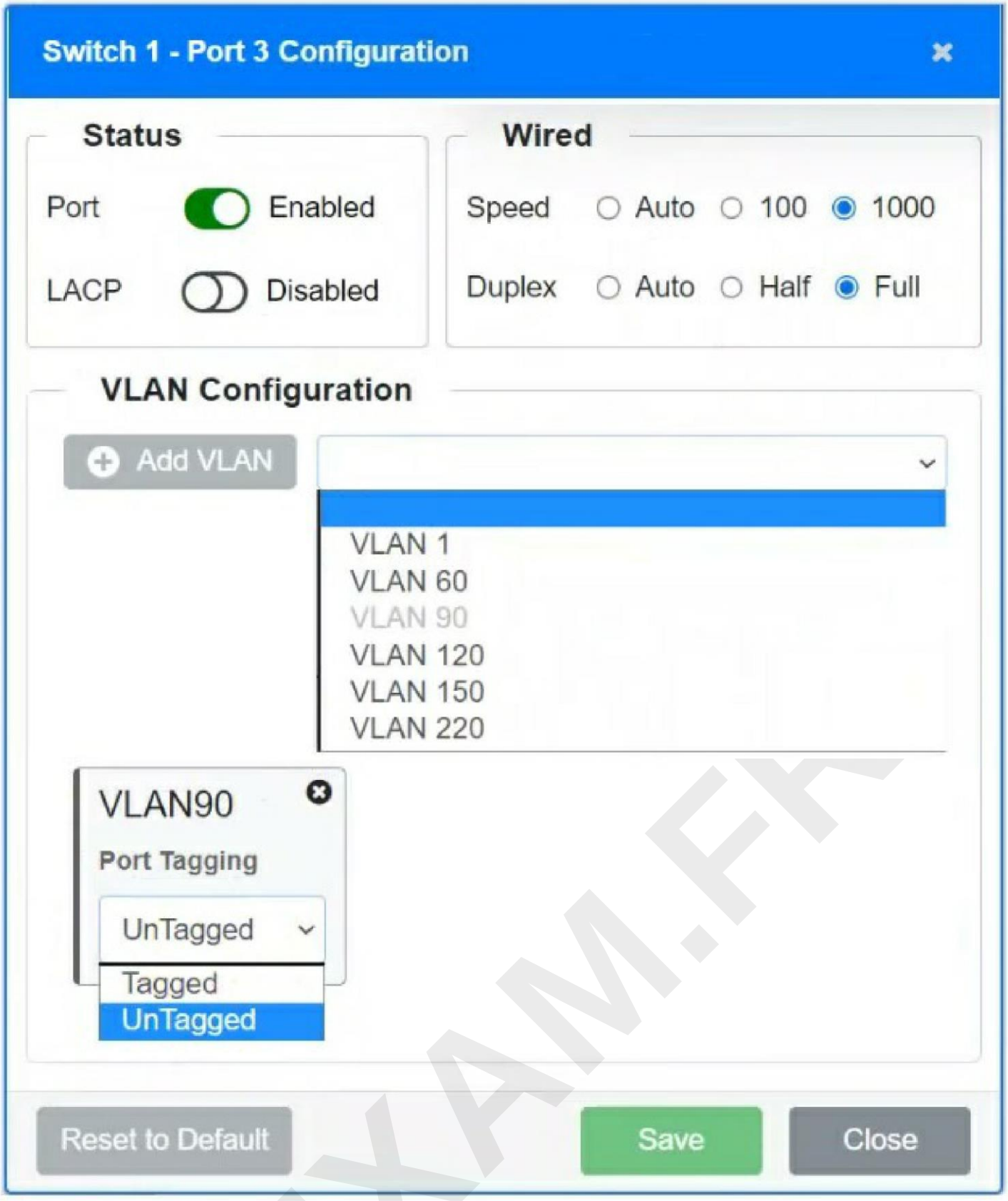
INSTRUCTIONS -

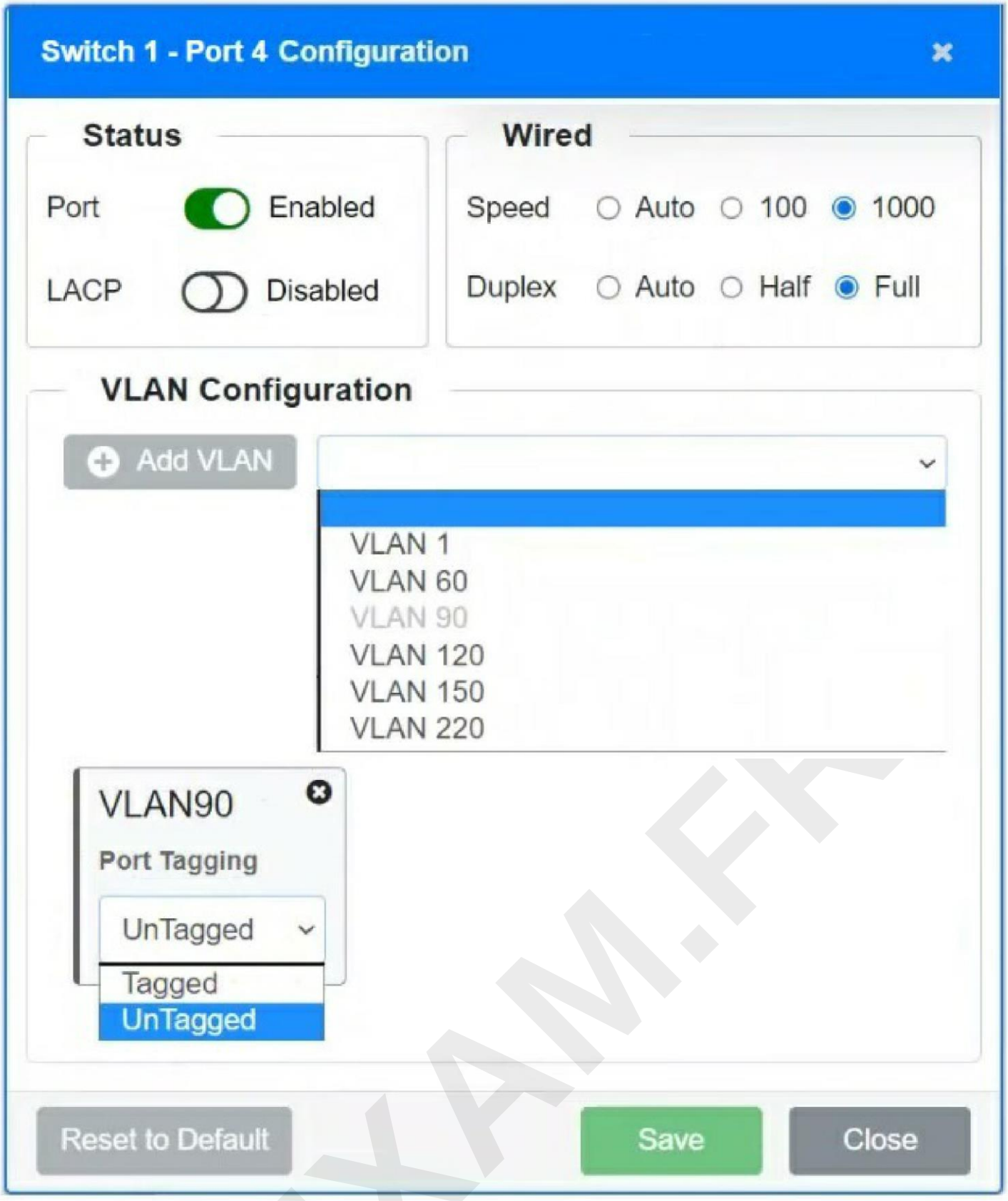
Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings: Ensure each device accesses only its correctly associated network.
Disable all unused switchports.
Require fault-tolerant connections between the switches.
Only make necessary changes to complete the above requirements.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

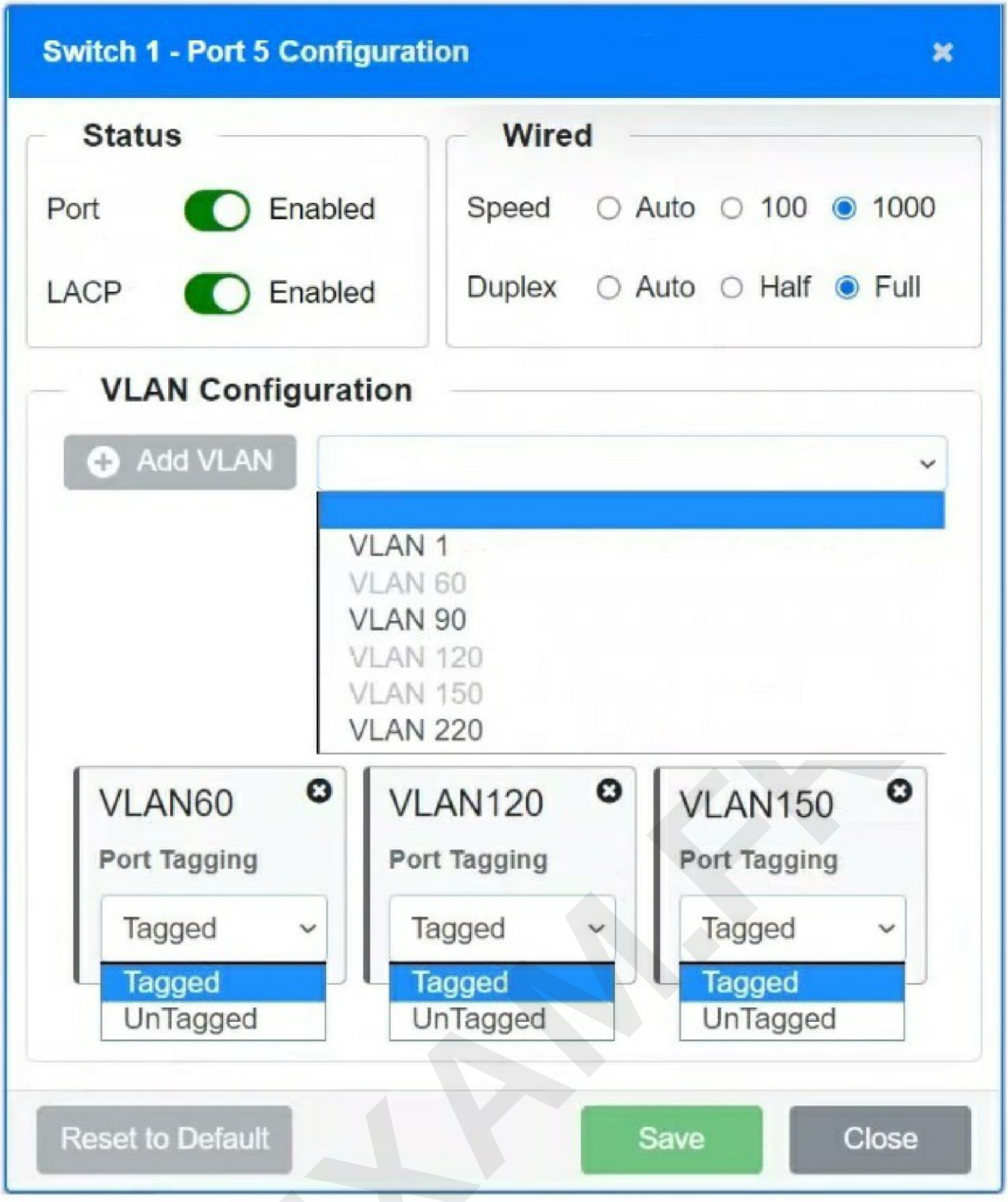


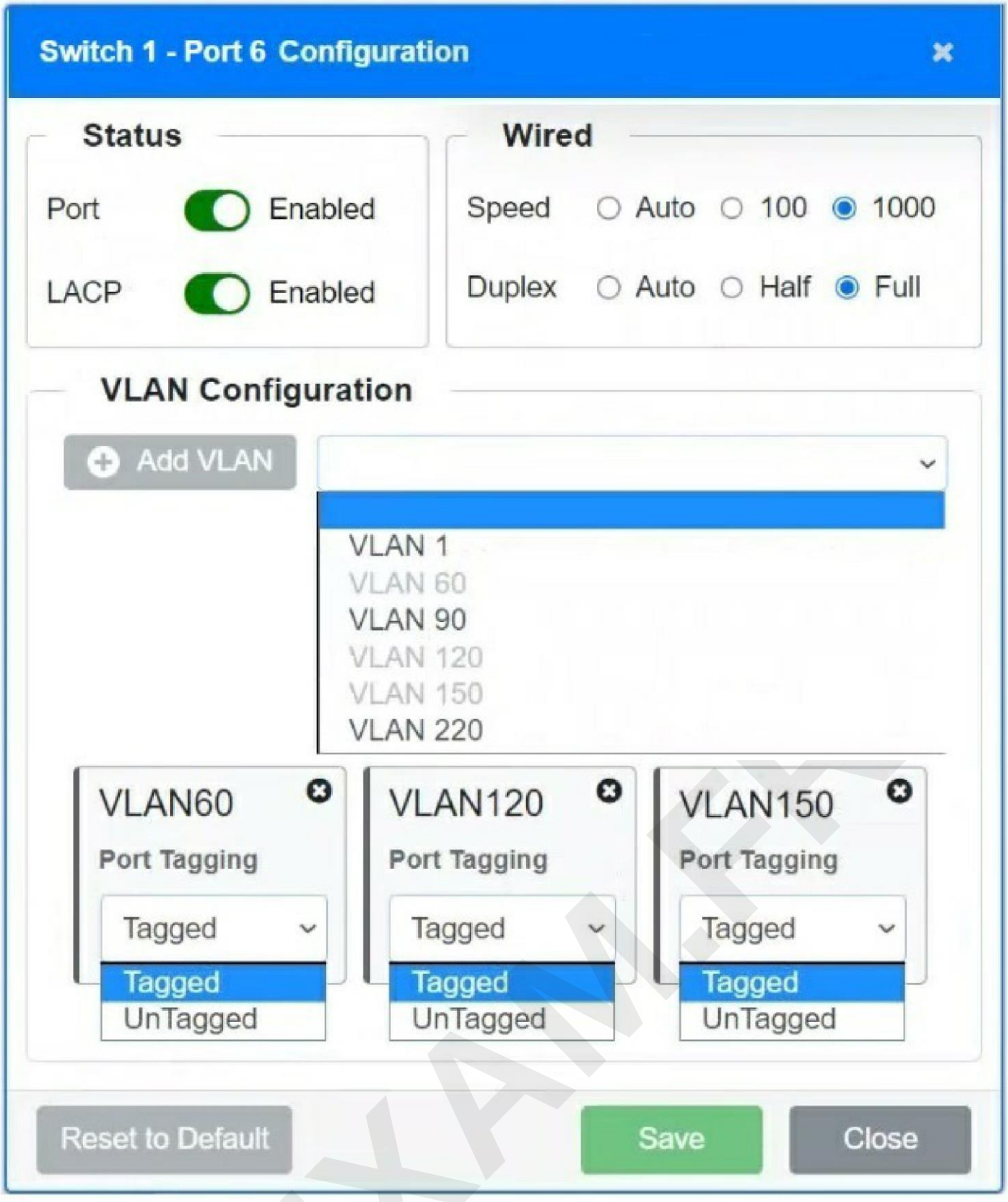

Switch 1 - Port 1 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
VLAN60
Port Tagging
Tagged
Tagged
UnTagged
VLAN90
Port Tagging
Tagged
Tagged
UnTagged
VLAN120
Port Tagging
Tagged
Tagged
UnTagged
VLAN150
Port Tagging
Tagged
Tagged
UnTagged
VLAN220
Port Tagging
Tagged
Tagged
UnTagged
Reset to Default
Save
Close

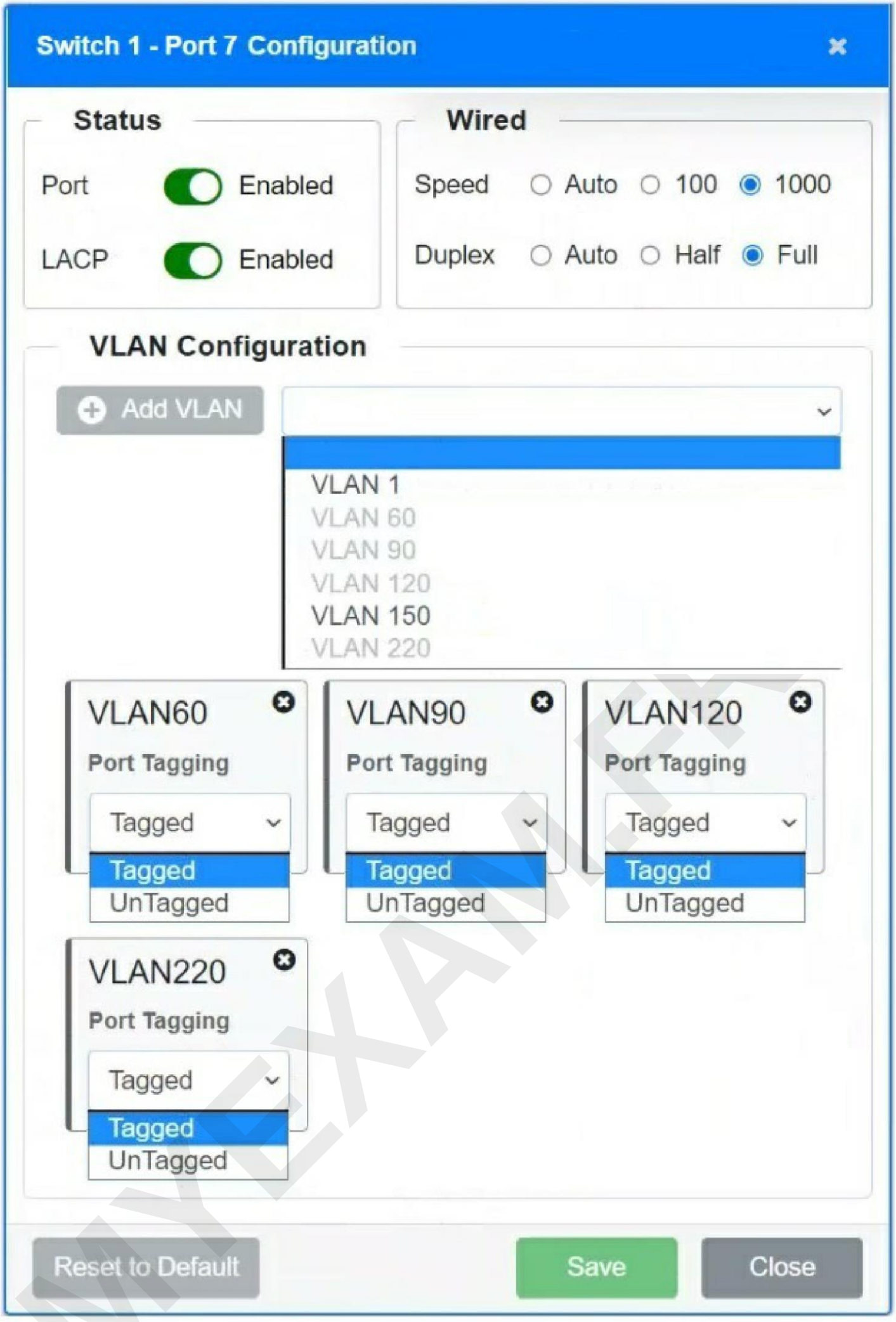

Switch 1 - Port 2 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
VLAN60
Port Tagging
Tagged
Tagged
UnTagged
VLAN90
Port Tagging
Tagged
Tagged
UnTagged
VLAN120
Port Tagging
Tagged
Tagged
UnTagged
VLAN150
Port Tagging
Tagged
Tagged
UnTagged
VLAN220
Port Tagging
Tagged
Tagged
UnTagged
Reset to Default
Save
Close

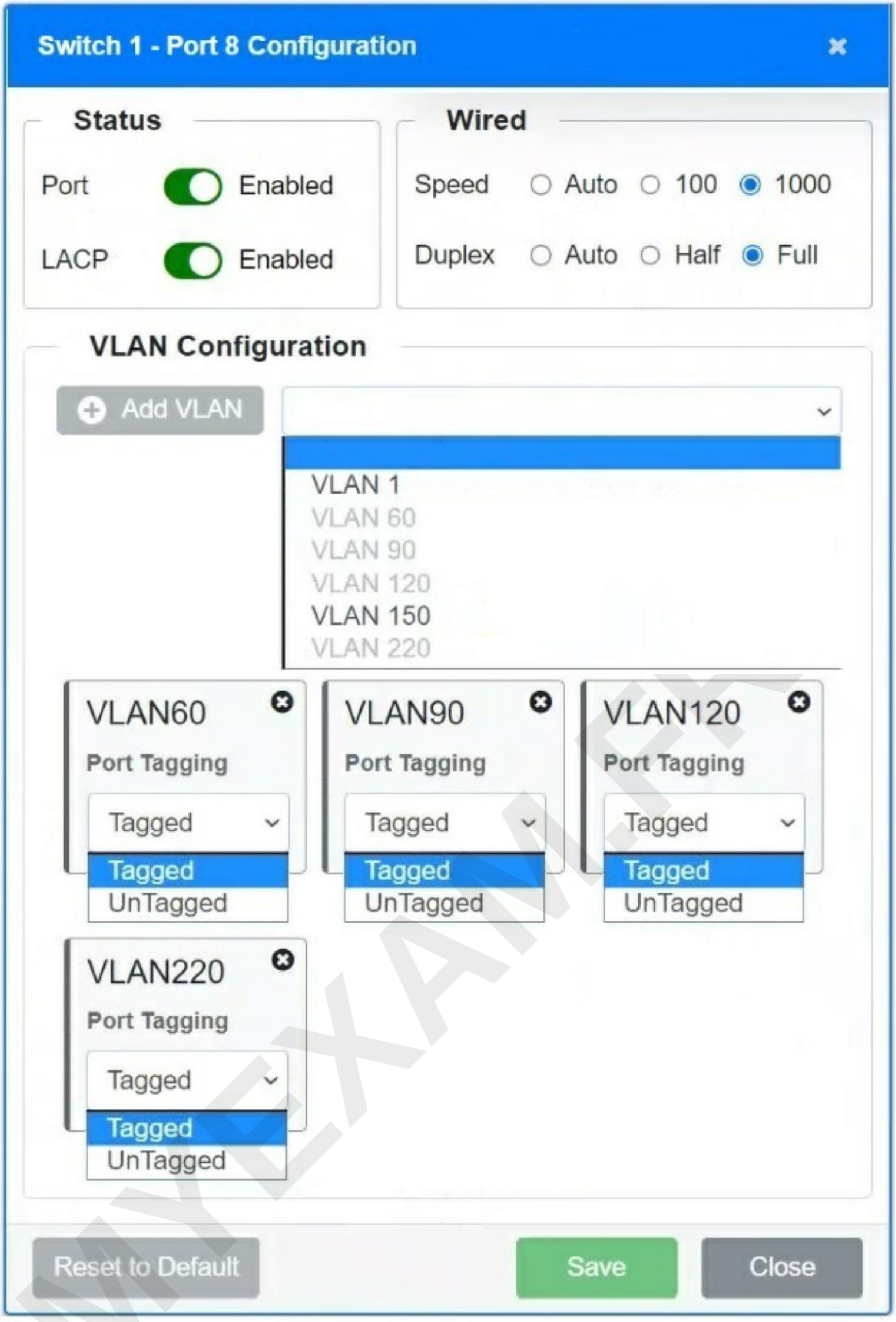

Switch 1 - Port 3 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
VLAN90
Port Tagging
UnTagged
Tagged
UnTagged
Reset to Default
Save
Close

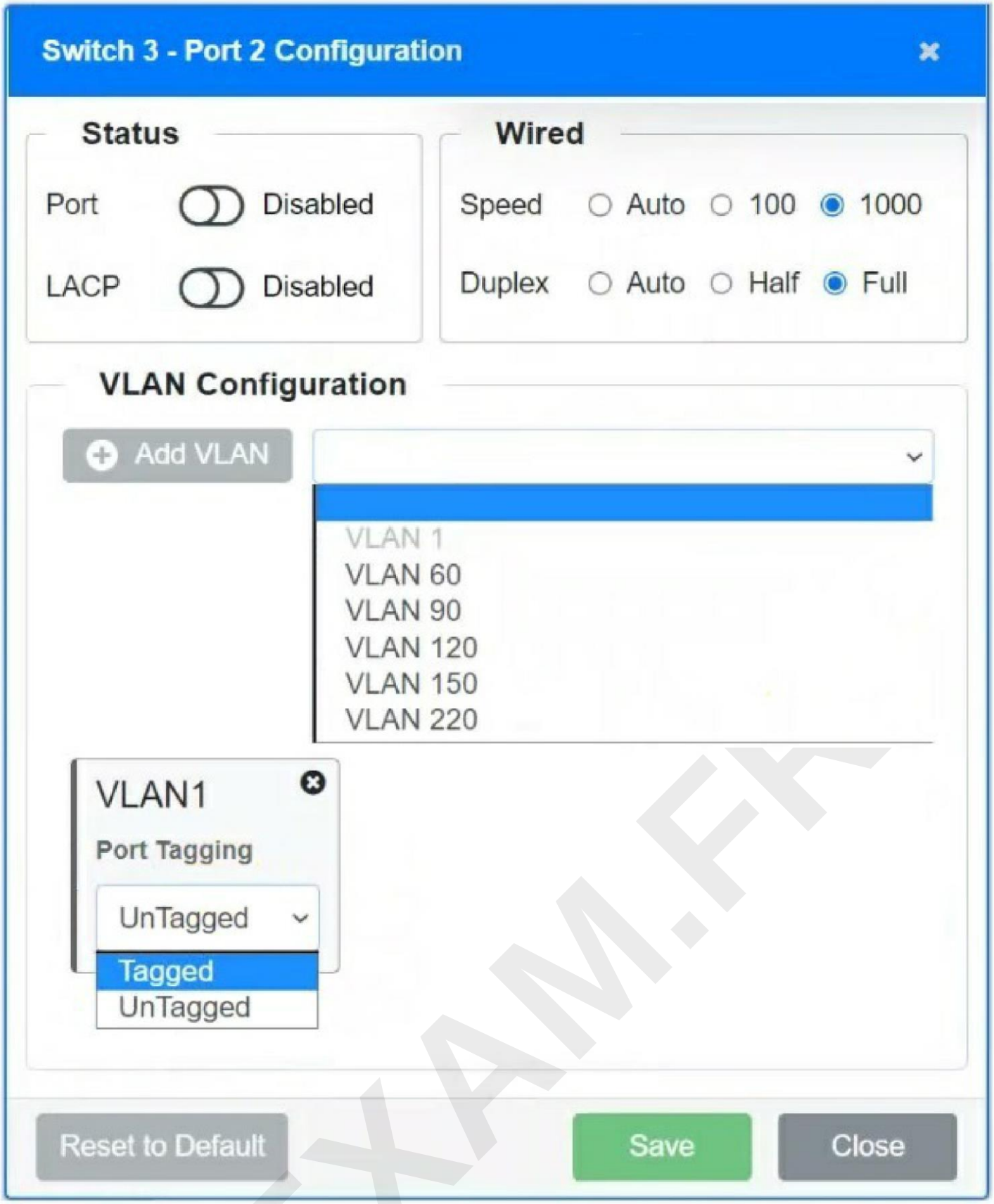

Switch 1 - Port 4 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
VLAN90
Port Tagging
UnTagged
Tagged
UnTagged
Reset to Default
Save
Close

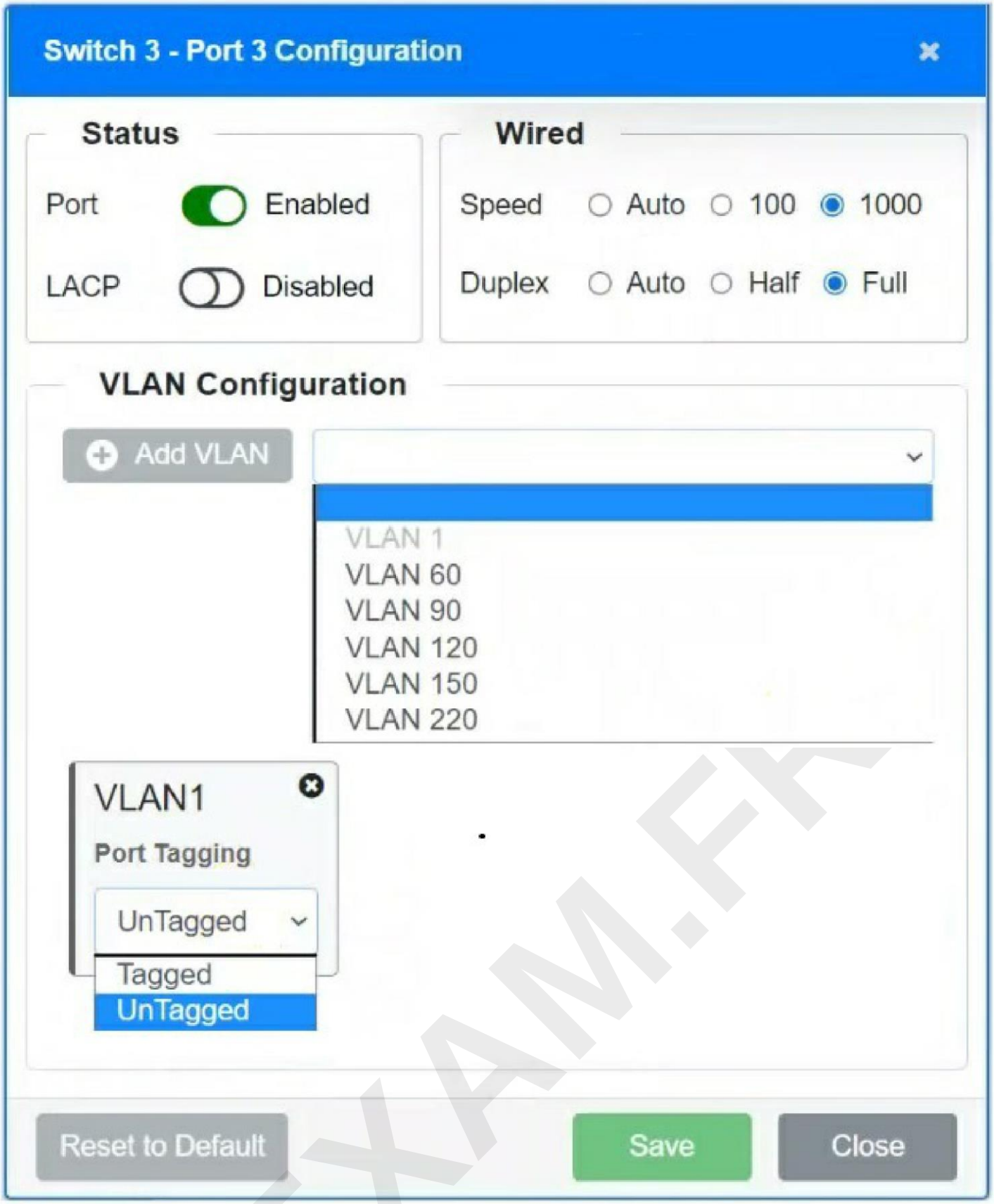

Switch 1 - Port 5 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
VLAN60
Port Tagging
Tagged
Tagged
UnTagged
VLAN120
Port Tagging
Tagged
Tagged
UnTagged
VLAN150
Port Tagging
Tagged
Tagged
UnTagged
Reset to Default
Save
Close

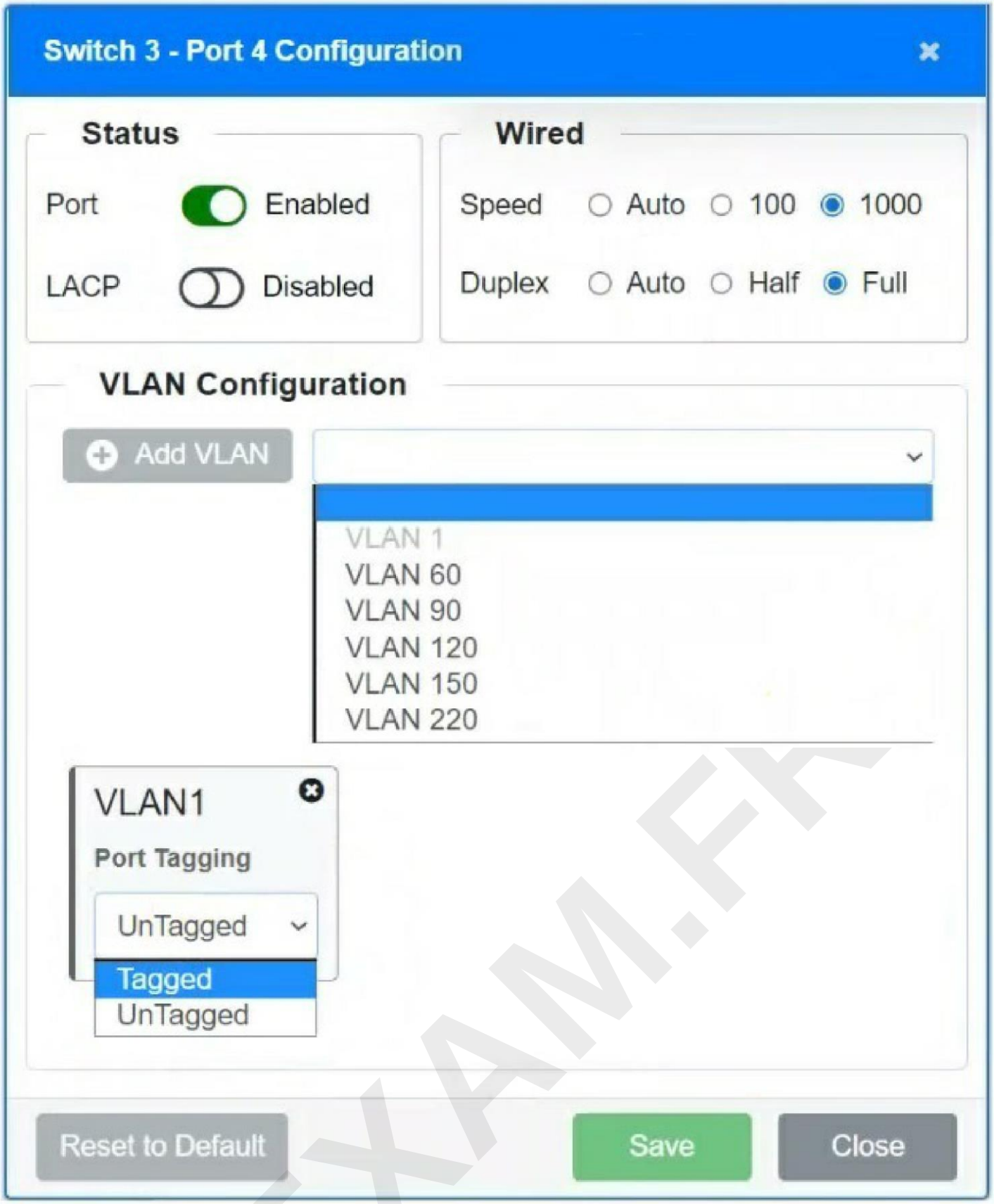

Switch 1 - Port 6 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
VLAN60
Port Tagging
Tagged
Tagged
UnTagged
VLAN120
Port Tagging
Tagged
Tagged
UnTagged
VLAN150
Port Tagging
Tagged
Tagged
UnTagged
Reset to Default
Save
Close

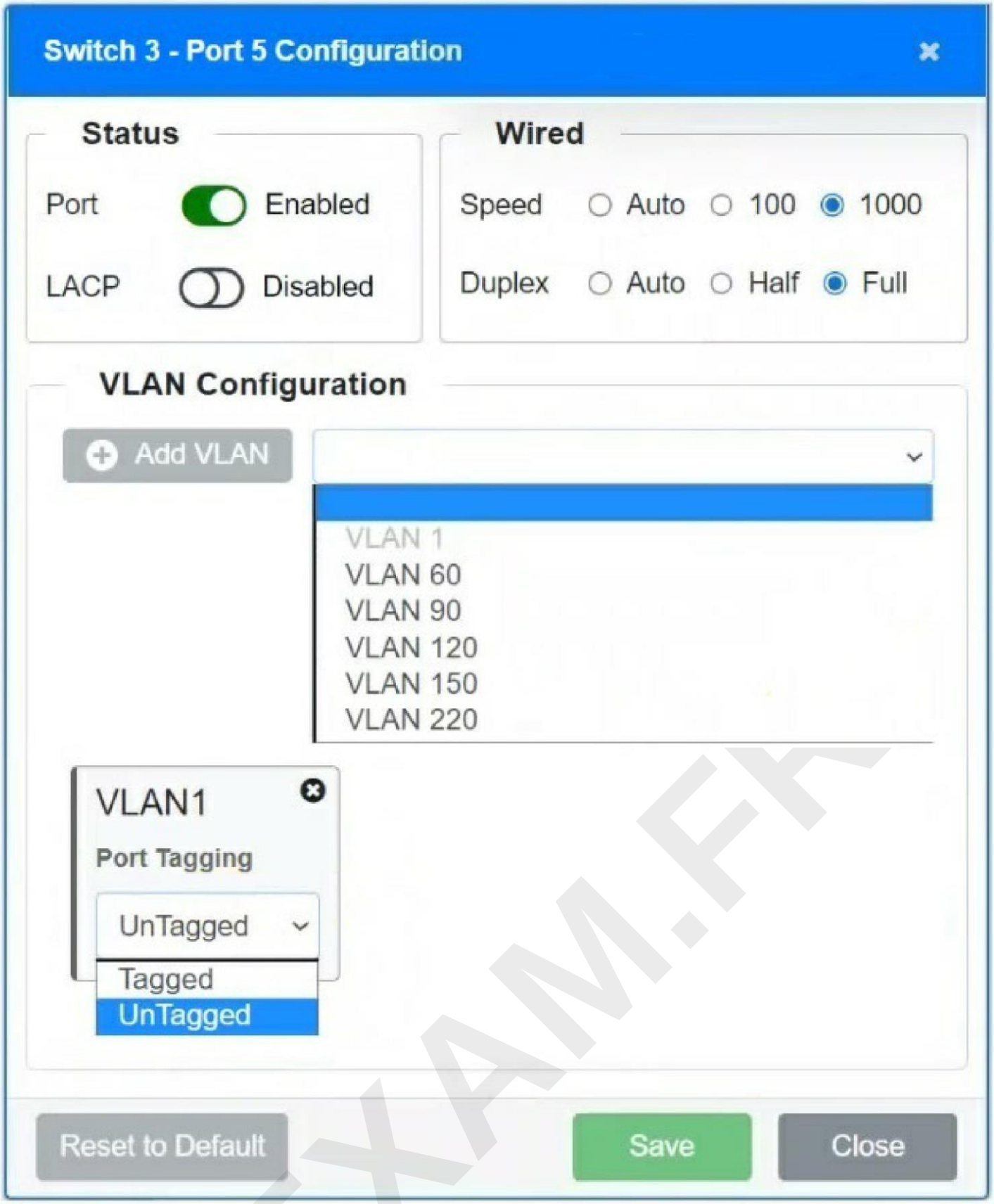

Switch 1 - Port 7 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
VLAN60
Port Tagging
Tagged
Tagged
UnTagged
VLAN90
Port Tagging
Tagged
Tagged
UnTagged
VLAN120
Port Tagging
Tagged
Tagged
UnTagged
VLAN220
Port Tagging
Tagged
Tagged
UnTagged
Reset to Default
Save
Close

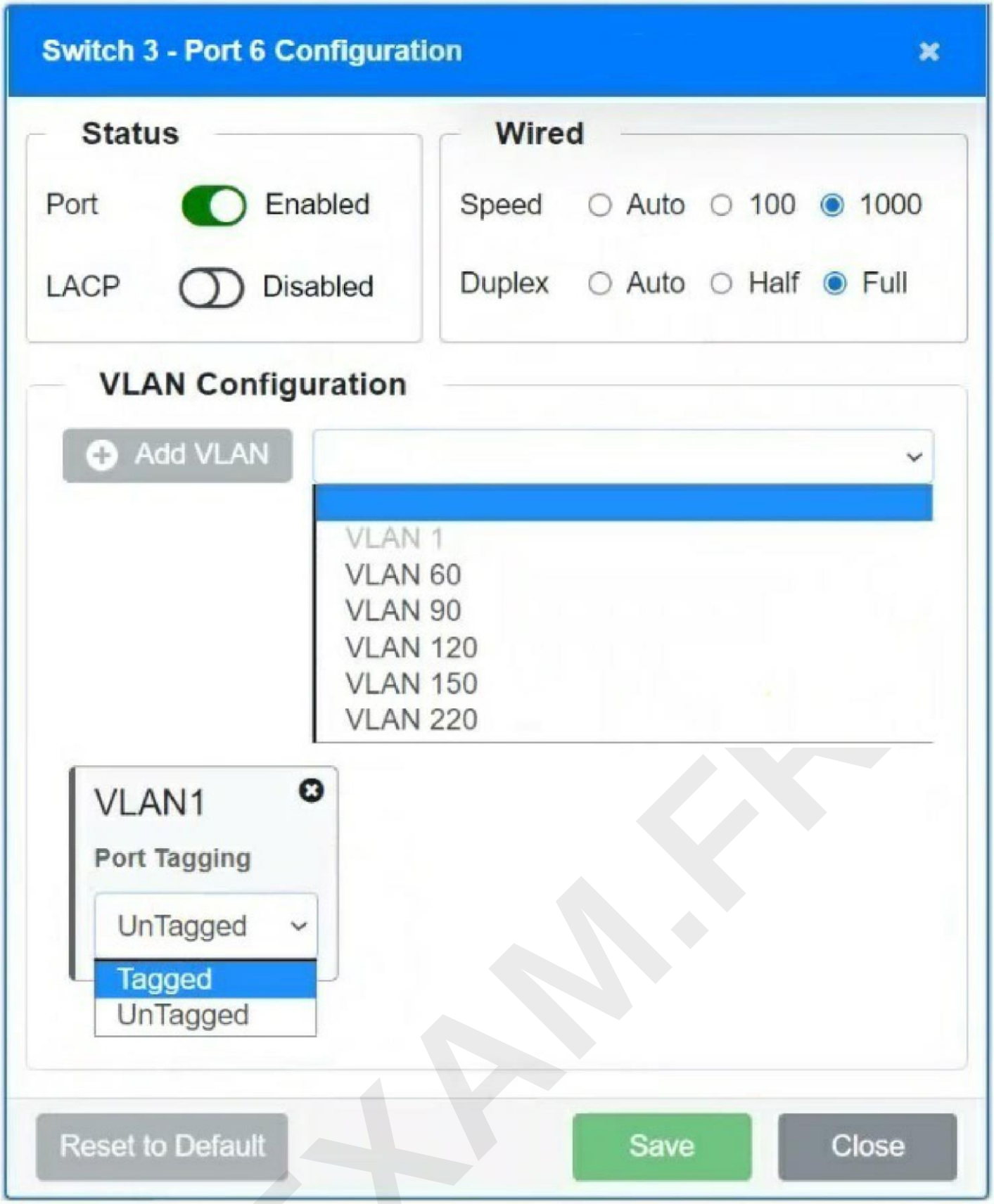

Switch 1 - Port 8 Configuration
Status
Port
Enabled
LACP
Enabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
VLAN60
Port Tagging
Tagged
Tagged
UnTagged
VLAN90
Port Tagging
Tagged
Tagged
UnTagged
VLAN120
Port Tagging
Tagged
Tagged
UnTagged
VLAN220
Port Tagging
Tagged
Tagged
UnTagged
Reset to Default
Save
Close

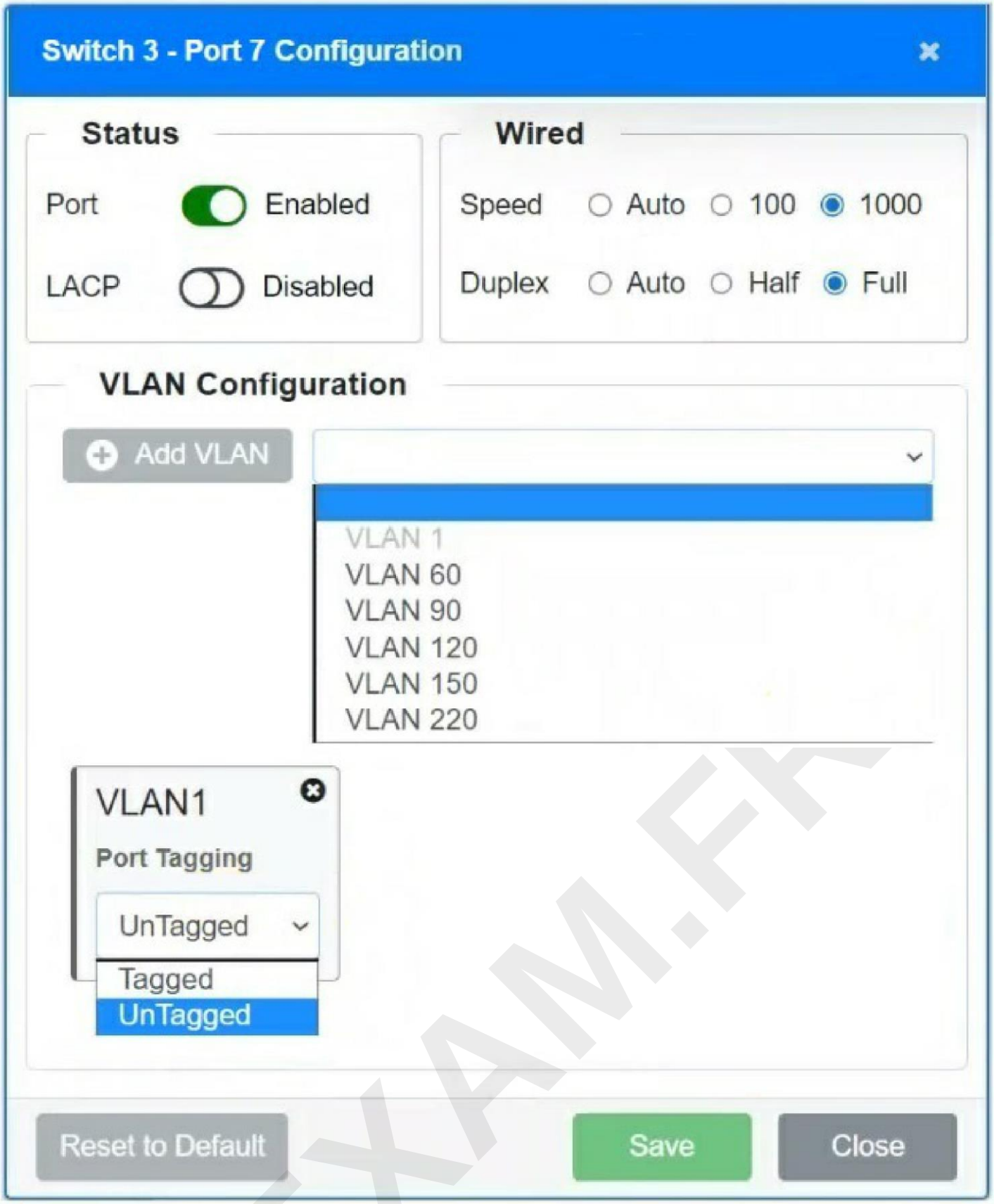

Switch 3 - Port 2 Configuration
Status
Port
Disabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
Reset to Default
Save
Close

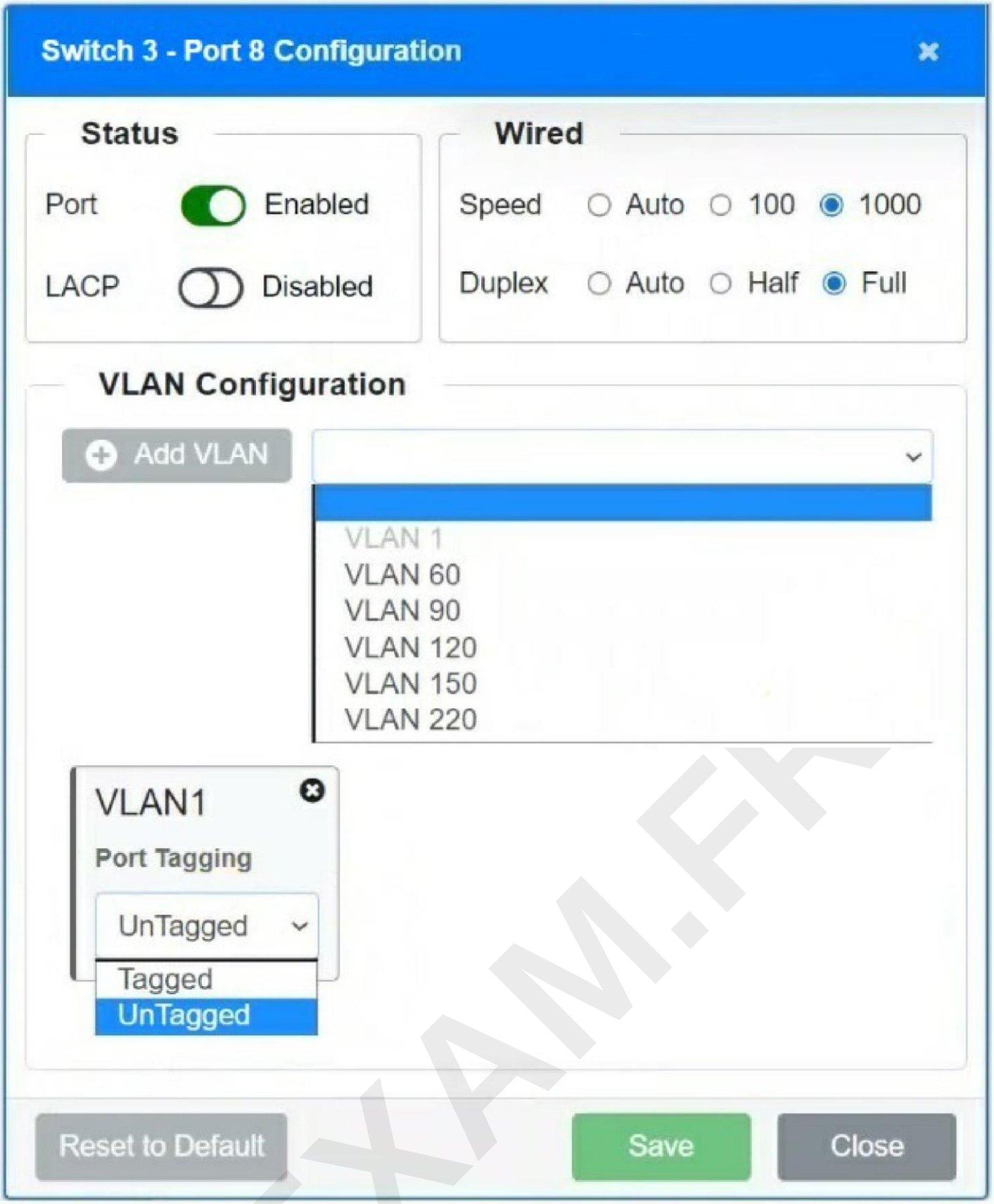

Switch 3 - Port 3 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
Reset to Default
Save
Close


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


Switch 3 - Port 5 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
Reset to Default
Save
Close


Switch 3 - Port 6 Configuration
Status
Port
Enabled
LACP
Disabled
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
VLAN Configuration
Add VLAN
VLAN 1
VLAN 60
VLAN 90
VLAN 120
VLAN 150
VLAN 220
VLAN1
Port Tagging
UnTagged
Tagged
UnTagged
Reset to Default
Save
Close


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



Answer:

Analysis and Configuration Recommendations:

Switch 1 Configurations:

- **Port 1 to Port 7**:
  - Ports should have VLANs set according to the devices they connect to. For instance, if a port is connecting to servers, only the VLAN for servers (e.g., VLAN 90) should be enabled and tagged if required.
  - Ensure unused VLANs are not active or set to untagged on these ports to prevent unauthorized network access.
- **Port 8**:
  - This port's configuration needs to align with the devices it connects to. Based on your first image, adjust the VLAN tagging accordingly. If it connects to printers, VLAN 60 should be tagged, and all other VLANs should be disabled or untagged.

Switch 3 Configurations:

- **Ports 2 to 8**:
  - The configurations here must also match the connected devices. For mobile user connections, only VLANs relevant to user access (like VLAN 150 for WLAN) should be enabled and set to tagged or untagged based on network policies.
  - Any VLAN not associated with the connected devices should be disabled to secure the network.

Fault Tolerant Connections:

- **Ensure redundancy**: If these switches are connected via multiple ports, configure Link Aggregation Control Protocol (LACP) if not already set up to provide redundancy and increased bandwidth.
- **Check duplex and speed settings**: Ensure that duplex settings are set to Auto to avoid duplex mismatch which can cause performance issues.

Disabling Unused Ports:

- Any port not connected or not planned to be used should be disabled to prevent unauthorized access or network breaches.

Final Checks:

- **Verify settings**: After configuration changes, verify all settings to ensure they adhere to network policies and the devices are performing as expected.
- **Documentation**: Update network documentation to reflect changes for future troubleshooting and audits.

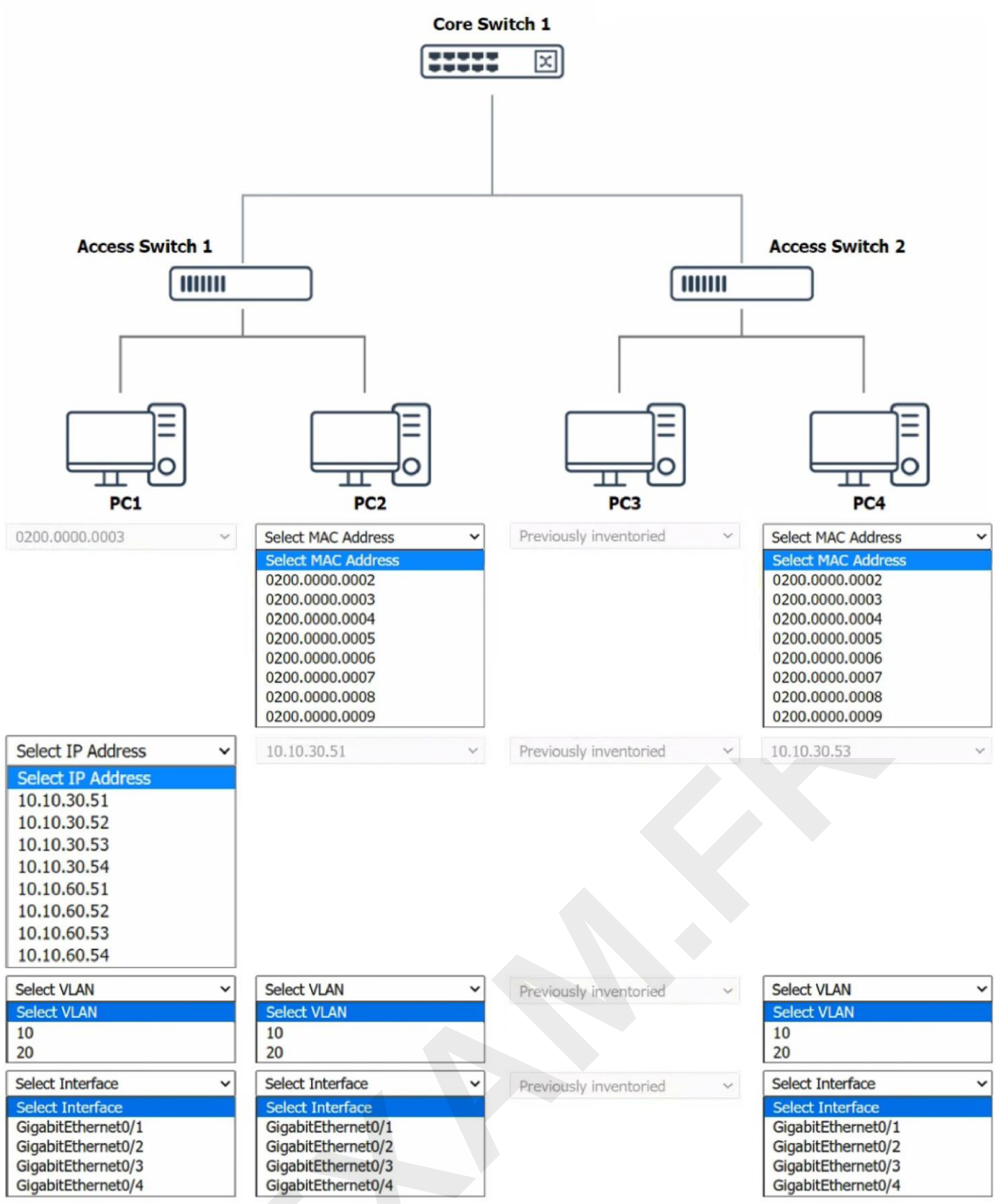
Question: 2

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. Type help to view a list of available commands.
Fill in the missing information using the drop-down menus provided.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:

Steps for Network Documentation:

1. **Network Discovery**:
   - Use discovery commands on each switch to collect data about connected devices. Common commands include show mac-address-table to view MAC addresses associated with the ports and show ip interface brief to check the IP configuration of switch interfaces.
2. **Document MAC and IP Addresses**:
   - From the MAC address table, document the MAC addresses linked to each port. In your provided image, select the appropriate MAC address for each PC (e.g., PC1, PC2, PC3, PC4) based on their connection to Access Switch 1 or 2.
   - Assign and document IP addresses for each device from the range available in the dropdown (e.g., 10.10.30.51 for PC1).
3. **VLAN Assignment**:
   - Assign and document VLANs for each PC according to network segmentation policies. It seems VLAN 10 and 20 are options; ensure each PC is assigned to the correct VLAN based on their network usage (e.g., regular users, admin, guest network).
4. **Interface Configuration**:
   - Document the interface each PC is connected to on their respective Access Switch. Ensure the interface matches the physical connection layout.

Final Verification:

- Use commands like show vlan to verify that VLAN assignments are correct across devices.
- Use show running-config to verify the overall configuration and ensure it aligns with security and operational policies.

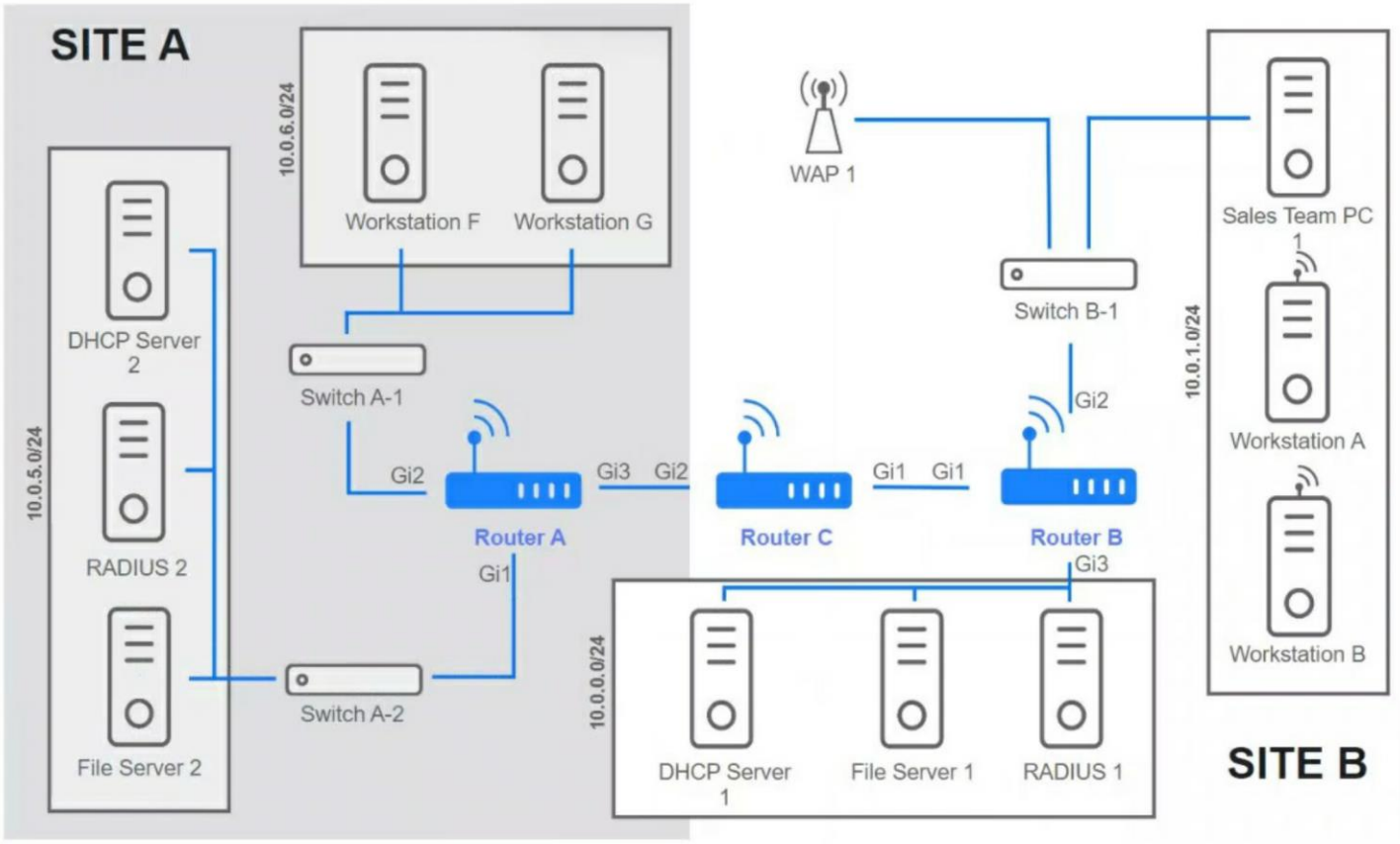
Question: 3

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.

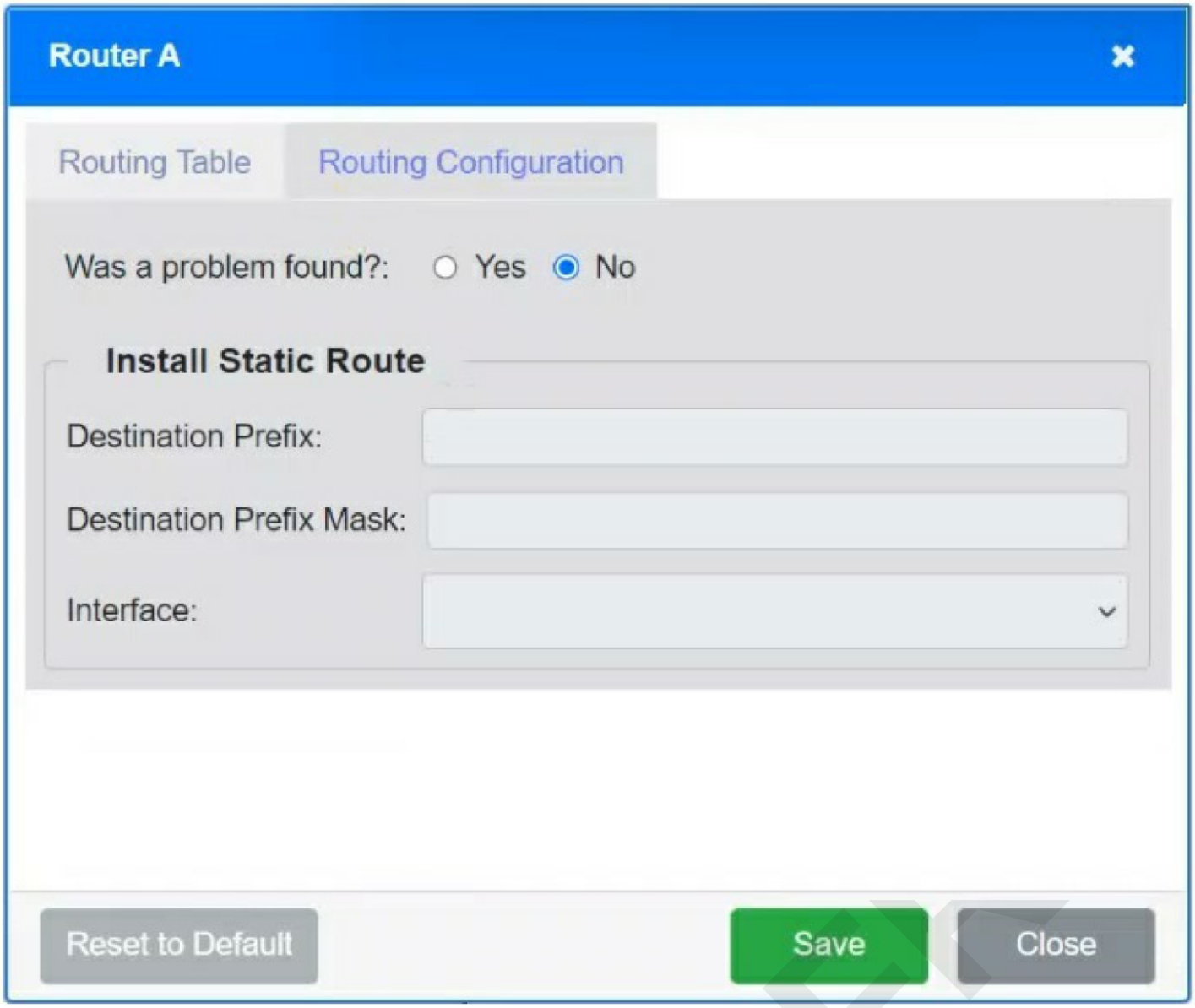

SITE A
10.0.6.0/24
Workstation F
Workstation G
WAP 1
Sales Team PC 1
Switch B-1
10.0.1.0/24
Workstation A
Workstation B
DHCP Server 2
Switch A-1
Gi2
Gi2
10.0.5.0/24
RADIUS 2
Gi3
Gi2
Gi1
Gi1
Router A
Router C
Router B
Gi3
Gi1
10.0.0.0/24
Switch A-2
File Server 2
DHCP Server 1
File Server 1
RADIUS 1
SITE B

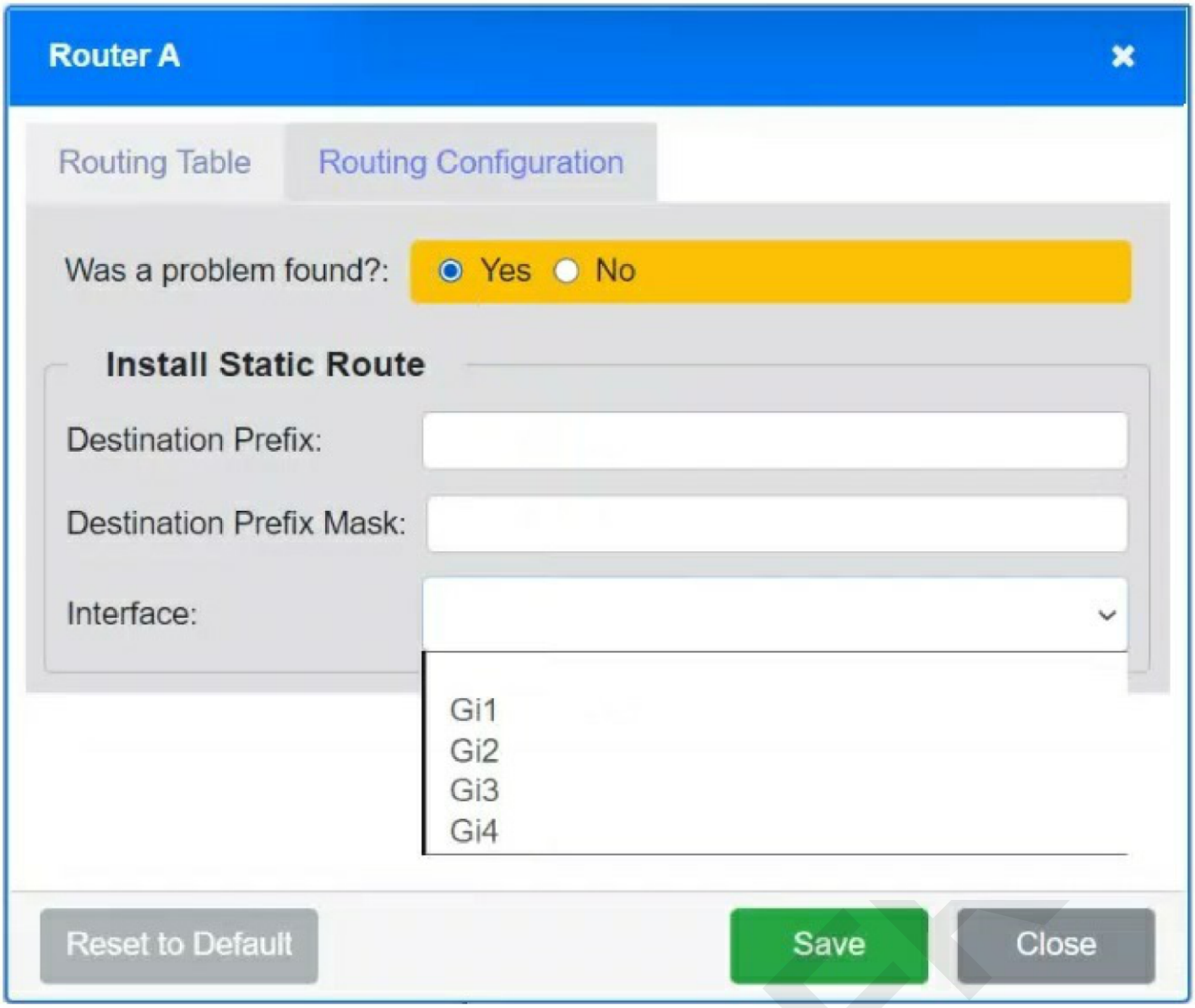
Router A

Routing Table | Routing Configuration

```
Router-A# 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, 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
```

Reset to Default | Save | Close


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

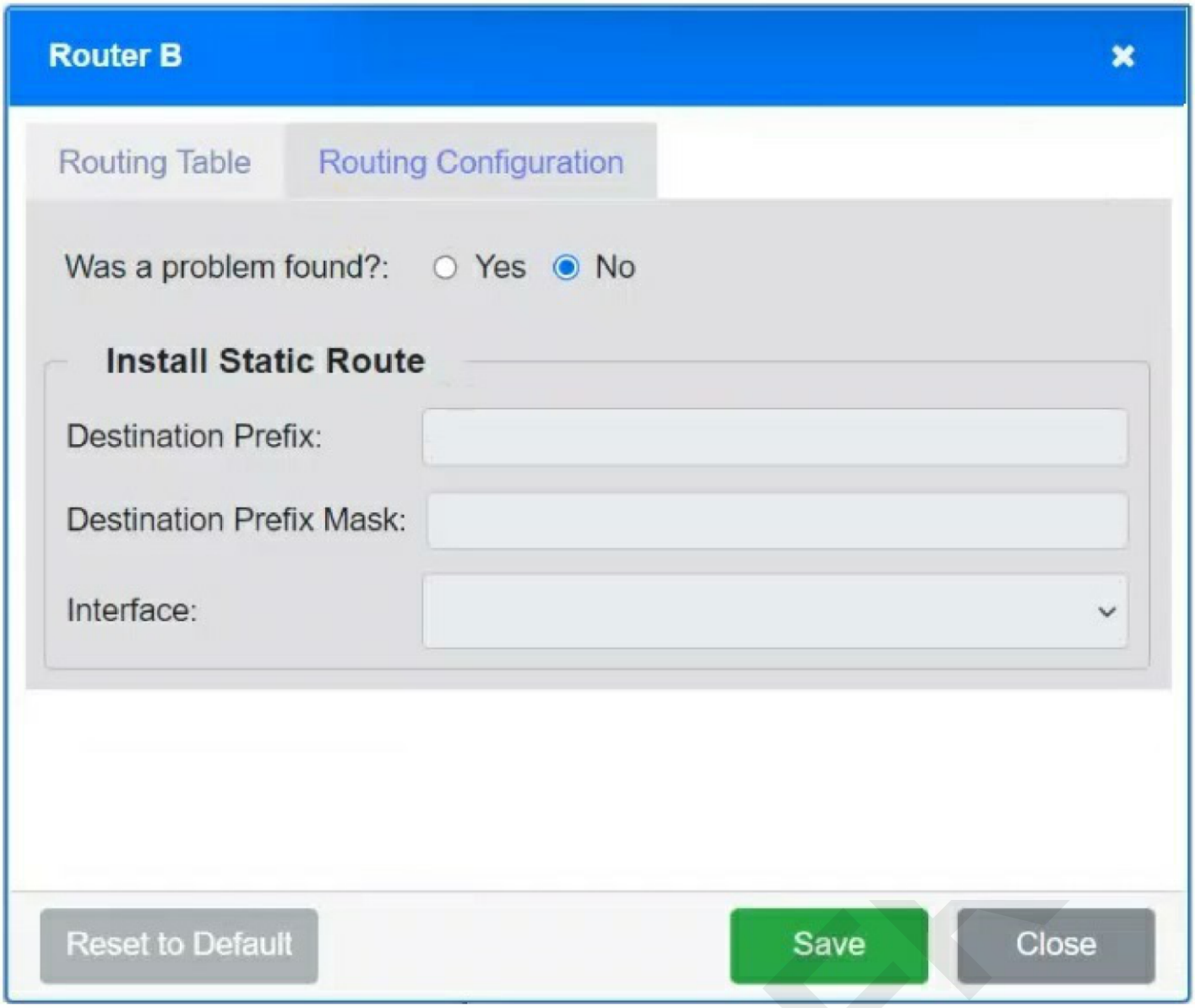

Router A
Routing Table
Routing Configuration
Was a problem found?:
Yes
No
Install Static Route
Destination Prefix:
Destination Prefix Mask:
Interface:
Gi1
Gi2
Gi3
Gi4
Reset to Default
Save
Close

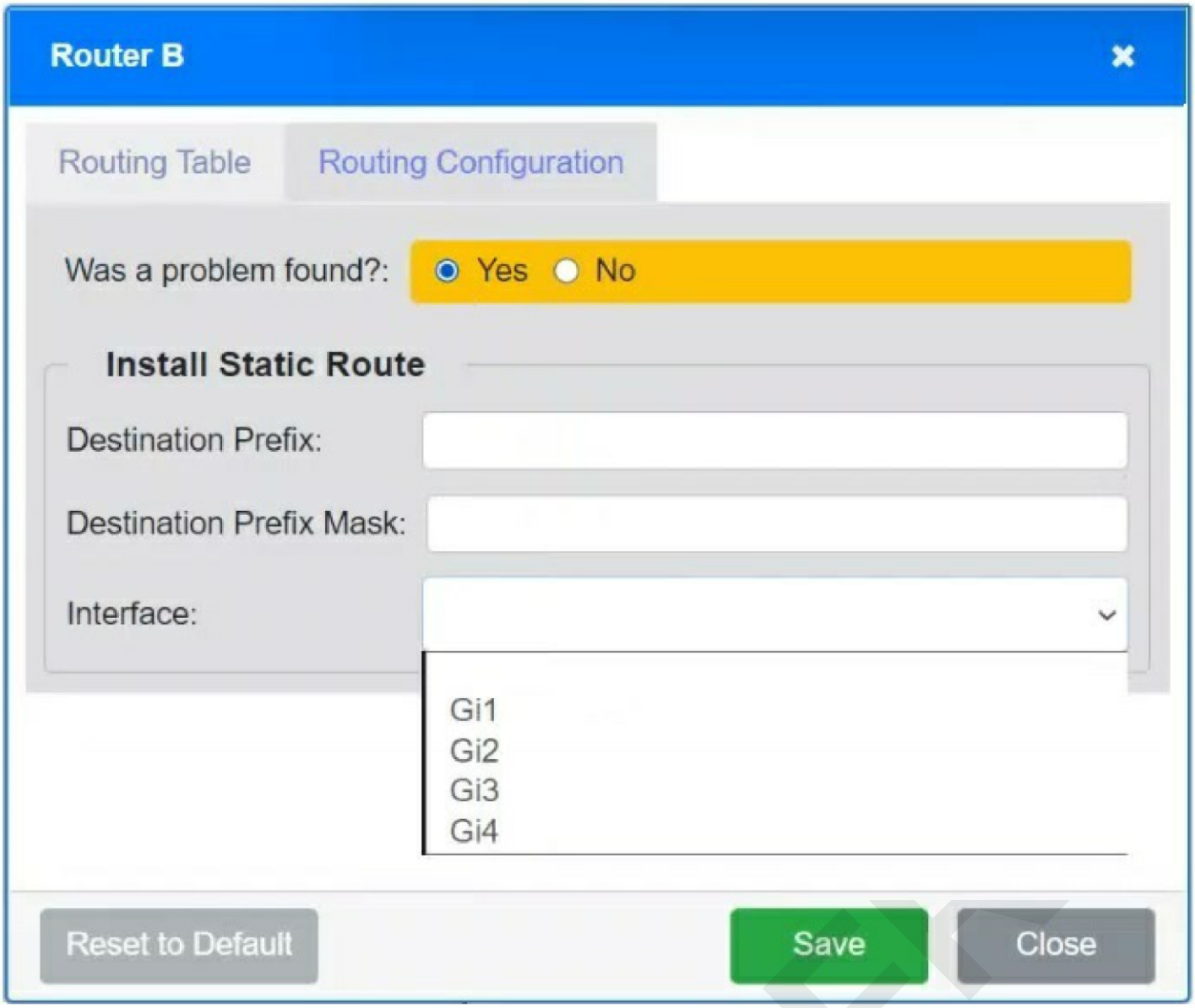
Router B

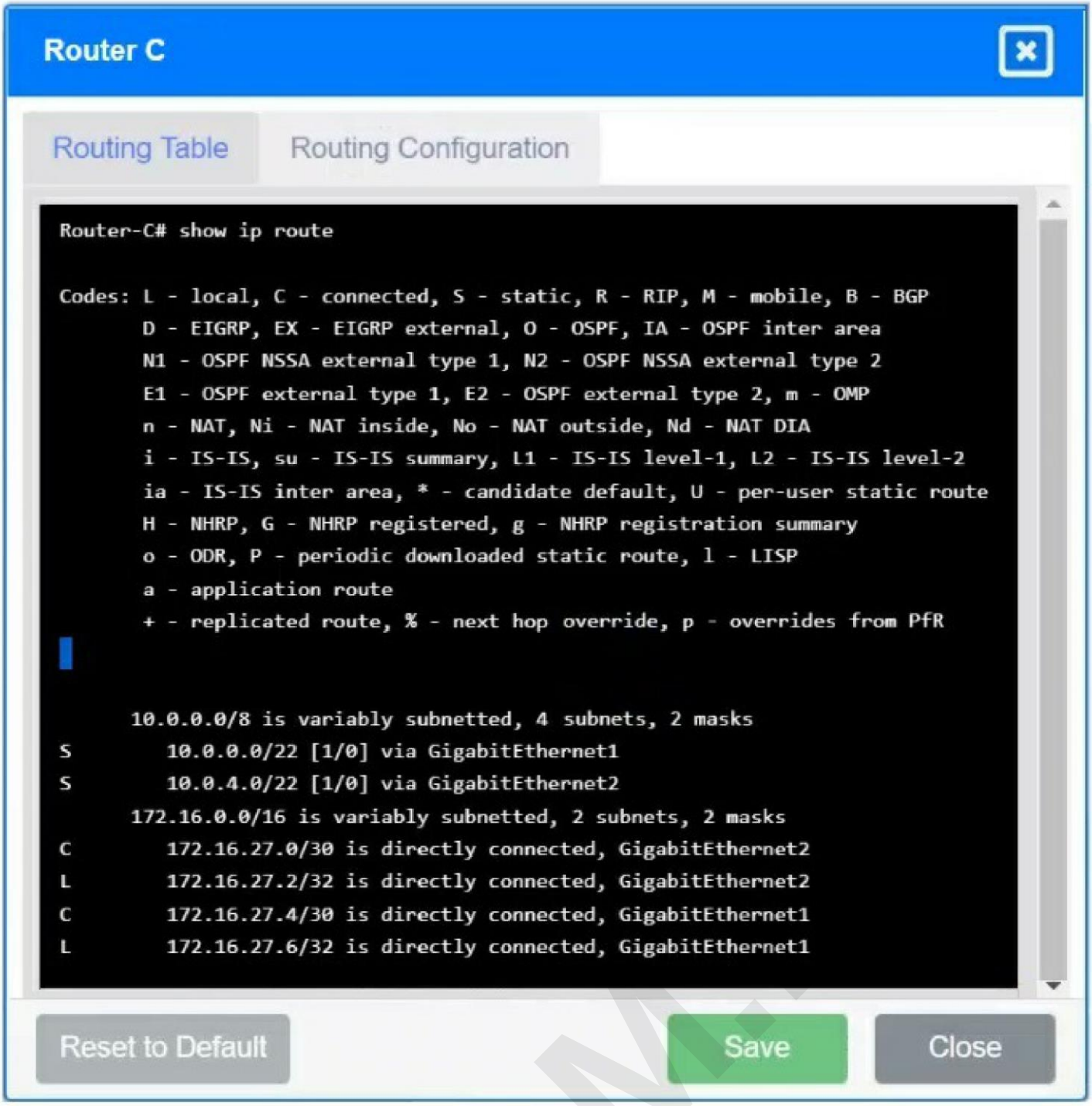
Routing Table | Routing Configuration

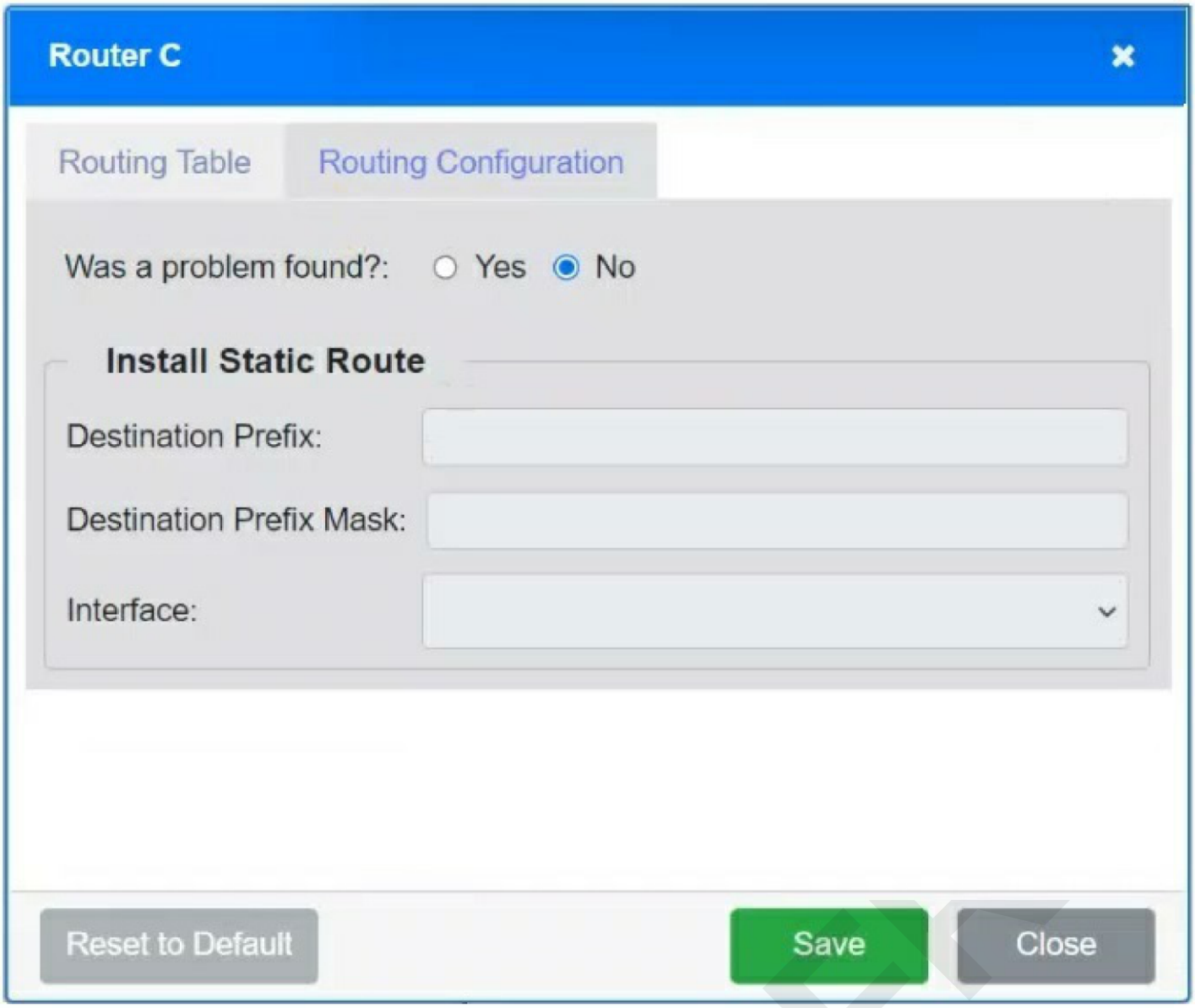
```
Router-B# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, GigabitEthernet1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/22 is directly connected, GigabitEthernet3
L        10.0.0.1/32 is directly connected, GigabitEthernet3
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.4/30 is directly connected, GigabitEthernet1
L        172.16.27.5/32 is directly connected, GigabitEthernet1
```

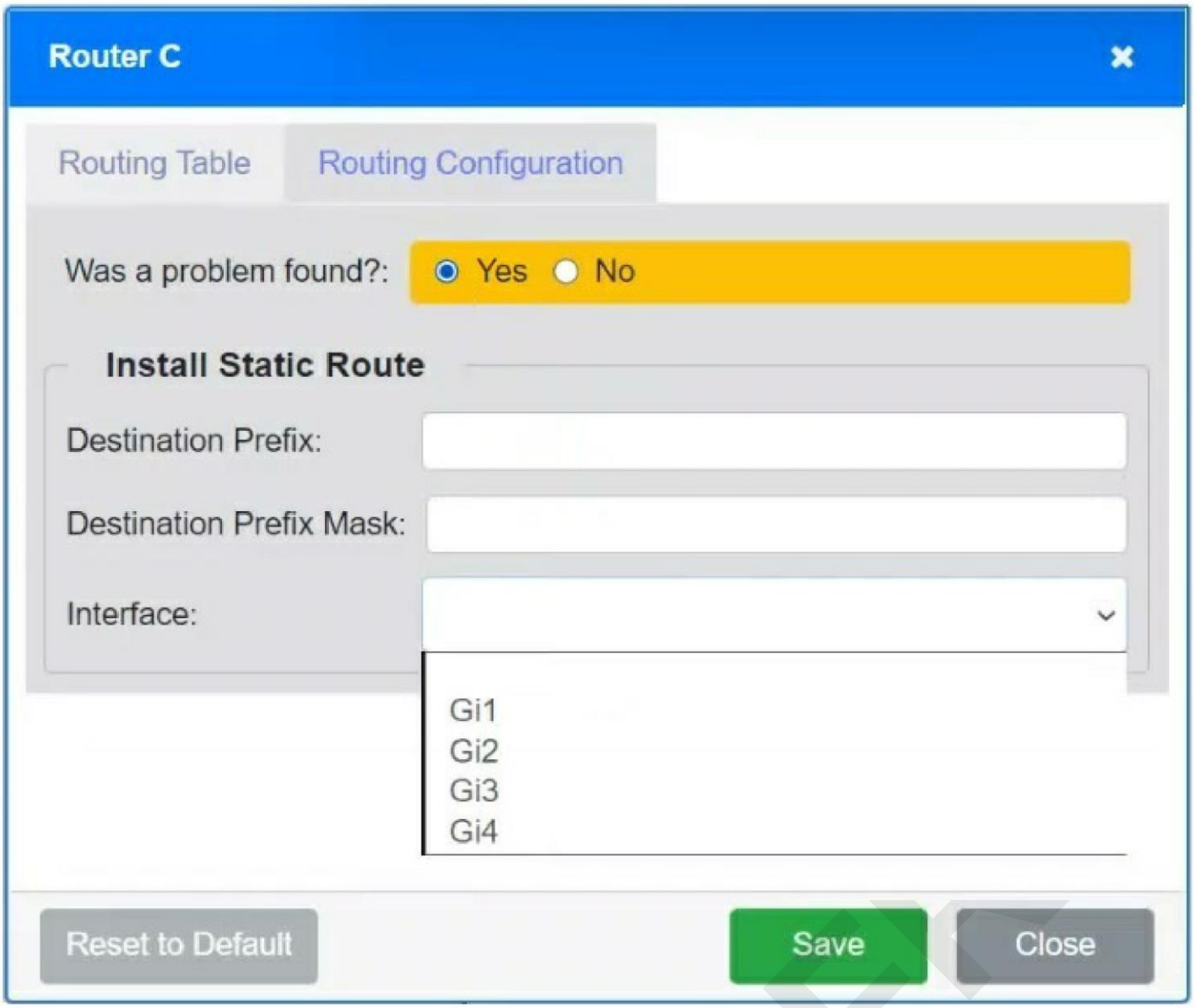
Reset to Default | Save | Close


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


Router B
Routing Table
Routing Configuration
Was a problem found?:
Yes
No
Install Static Route
Destination Prefix:
Destination Prefix Mask:
Interface:
Gi1
Gi2
Gi3
Gi4
Reset to Default
Save
Close


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


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



Answer:

Issue Identified: Workstation A cannot access File Server 2 due to missing routing information.
Solution:

1. **Review Router Configuration**:
   - Analyze the routing tables on Routers A, B, and C to confirm whether routes to the File Server 2 subnet are present.
2. **Add Static Route**:
   - Install a static route on the router that connects Workstation A's network to File Server 2's network:
     - **Destination Prefix**: Enter the network address of File Server 2.
     - **Destination Prefix Mask**: Enter the subnet mask for File Server 2's network.
     - **Interface**: Select the router interface that faces towards File Server 2's network.
3. **Action**:
   - Configure the static route using the routing configuration panel on the router that requires the update.
   - Save the changes and test connectivity from Workstation A to File Server 2 to ensure the issue is resolved.

Question: 4

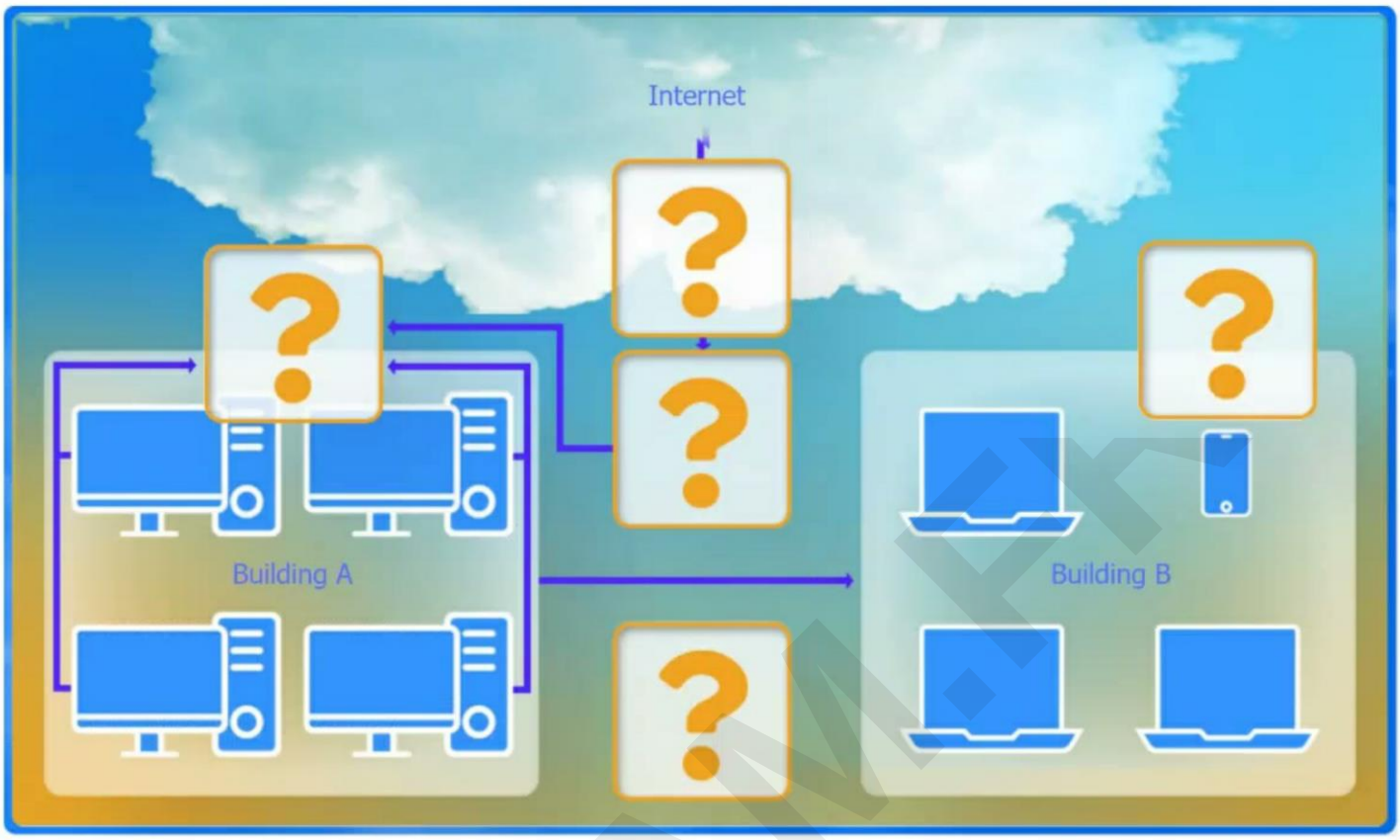
SIMULATION -

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.



Answer:

Central Device Connecting to the Internet (marked with a question mark at the top middle connecting to the Internet):

- **Device**: **Firewall**
- **Reason**: To inspect and filter all internet traffic before it enters the network, ensuring security compliance.

Device between Building A and the Internet (first question mark inside Building A):

- **Device**: **Router**
- **Reason**: To route traffic between the internal networks (Building A, Building B) and the internet via the firewall.

Devices inside Building A (two question marks linked to desktops and server infrastructure):

- **Device**: **Switch**
- **Reason**: To connect all desktops and servers within Building A, ensuring that each device can communicate with others within the building without seeing traffic destined for other devices.

Device connecting Building A to Building B (question mark between the two buildings):

- **Device**: **Wireless range extender**
- **Reason**: Given the 50 feet separation and no physical connectivity, a wireless range extender can bridge this gap by extending the wireless signal from Building A to Building B, facilitating network access across both buildings.

Device inside Building B (question mark inside Building B):

- **Device**: **Switch**
- **Reason**: To provide connectivity for the devices in Building B, allowing them to connect to the network and access resources in Building A as well as the internet.

Question: 5

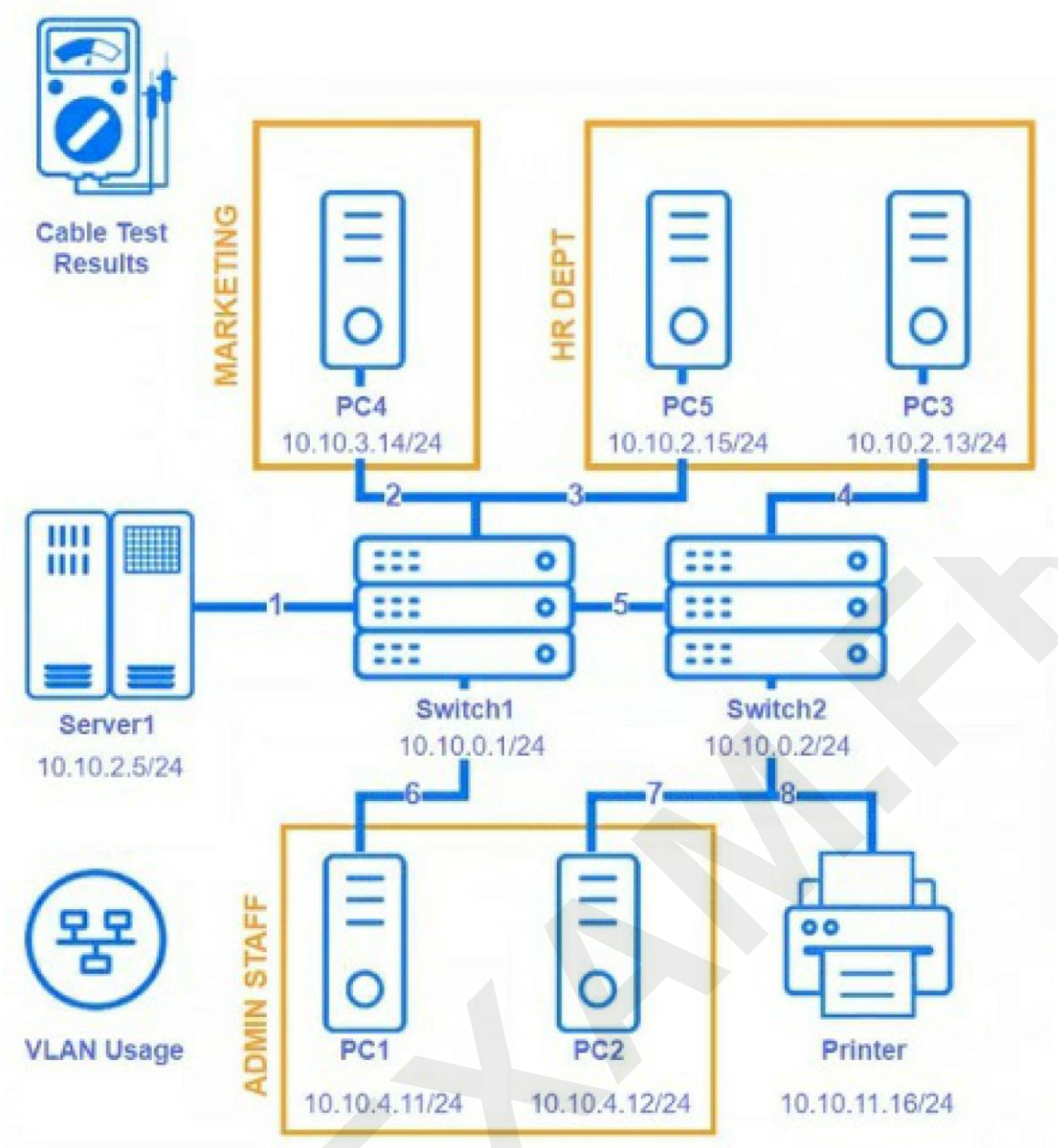
SIMULATION -

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. Type help in each terminal to view a list of available commands.

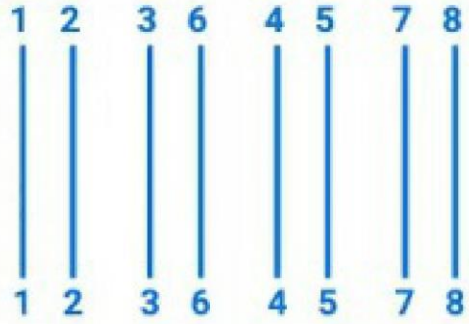
Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Cable Test Results

Cable 1 | Cable 2 | Cable 3 | Cable 4 | Cable 5 | Cable 6 | Cable 7 | Cable 8

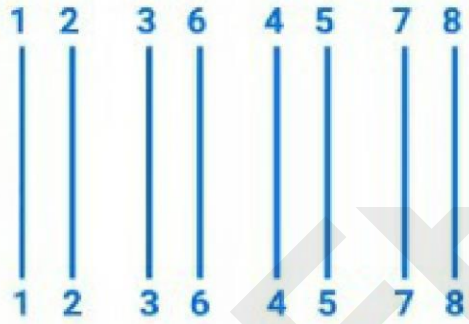
Length: 22M
VLAN: VLAN 2
Speed: 1000 FDX
Port: GigabitEthernet0/1



Cable Test Results

Cable 1 | Cable 2 | Cable 3 | Cable 4 | Cable 5 | Cable 6 | Cable 7 | Cable 8

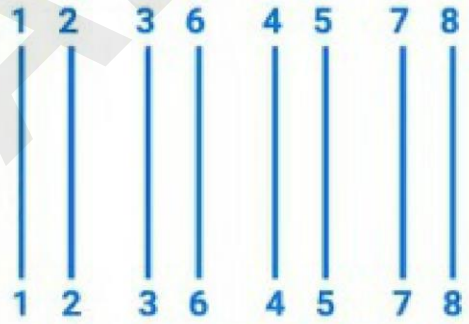
Length: 103M
VLAN: VLAN 3
Speed: 1000 FDX
Port: GigabitEthernet0/4



Cable Test Results

Cable 1 | Cable 2 | Cable 3 | Cable 4 | Cable 5 | Cable 6 | Cable 7 | Cable 8

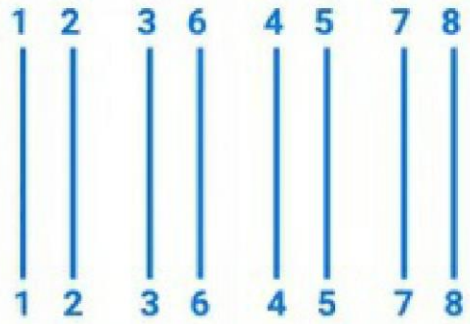
Length: 18M
VLAN: VLAN 2
Speed: 1000 FDX
Port: GigabitEthernet0/3



Cable Test Results

Cable 1 | Cable 2 | Cable 3 | Cable 4 | Cable 5 | Cable 6 | Cable 7 | Cable 8

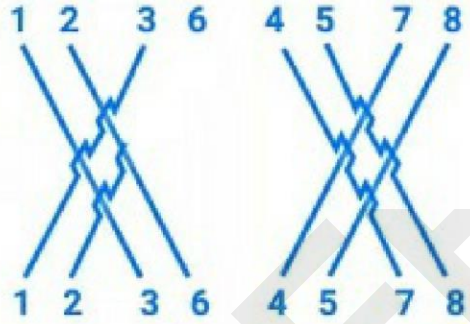
Length: 20M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/2



Cable Test Results

Cable 1 | Cable 2 | Cable 3 | Cable 4 | Cable 5 | Cable 6 | Cable 7 | Cable 8

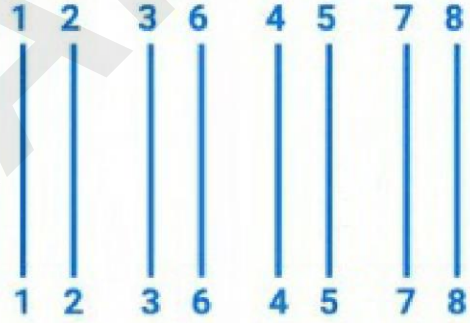
Length: 16M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/5



Cable Test Results

Cable 1 | Cable 2 | Cable 3 | Cable 4 | Cable 5 | Cable 6 | Cable 7 | Cable 8

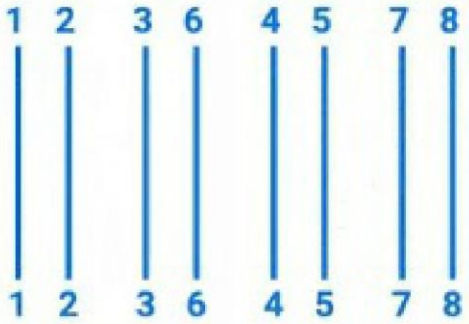
Length: 42M
VLAN: VLAN 4
Speed: 1000 FDX
Port: GigabitEthernet0/2



Cable Test Results

Cable 1 | Cable 2 | Cable 3 | Cable 4 | Cable 5 | Cable 6 | Cable 7 | Cable 8

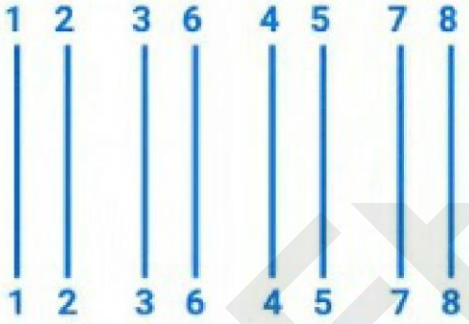
Length: 12M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/1



Cable Test Results

Cable 1 | Cable 2 | Cable 3 | Cable 4 | Cable 5 | Cable 6 | Cable 7 | Cable 8

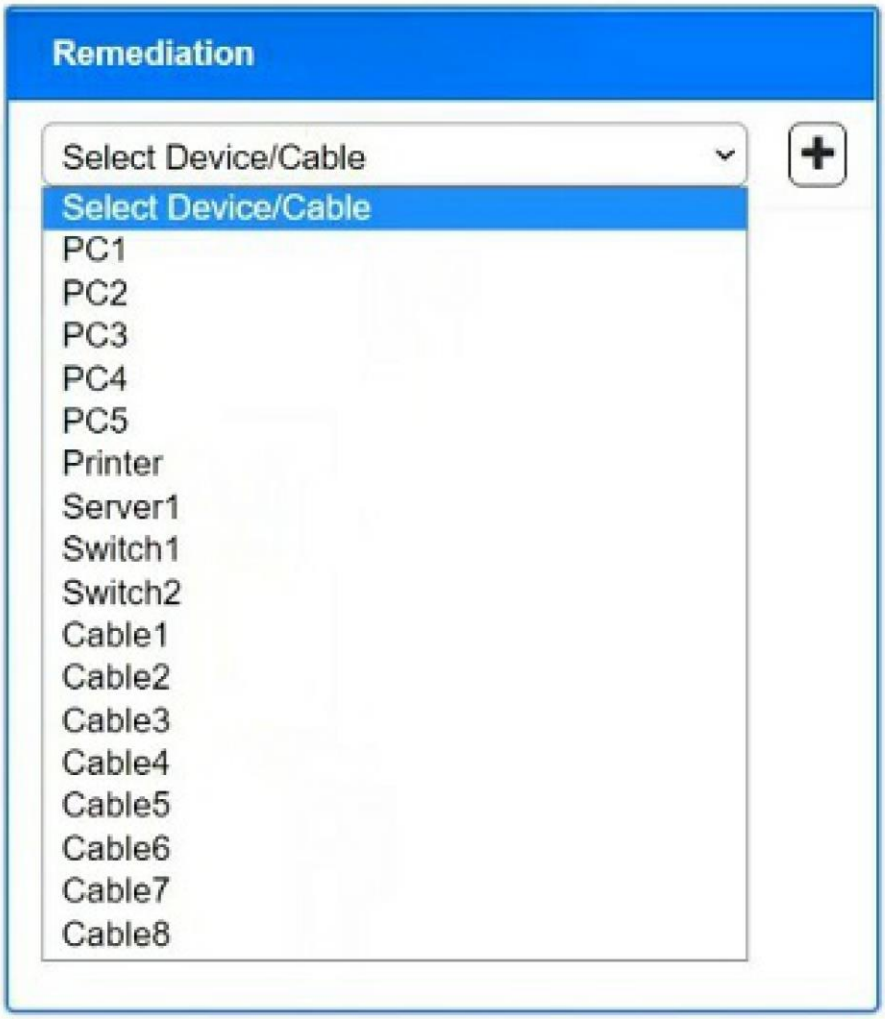
Length: 90M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/3

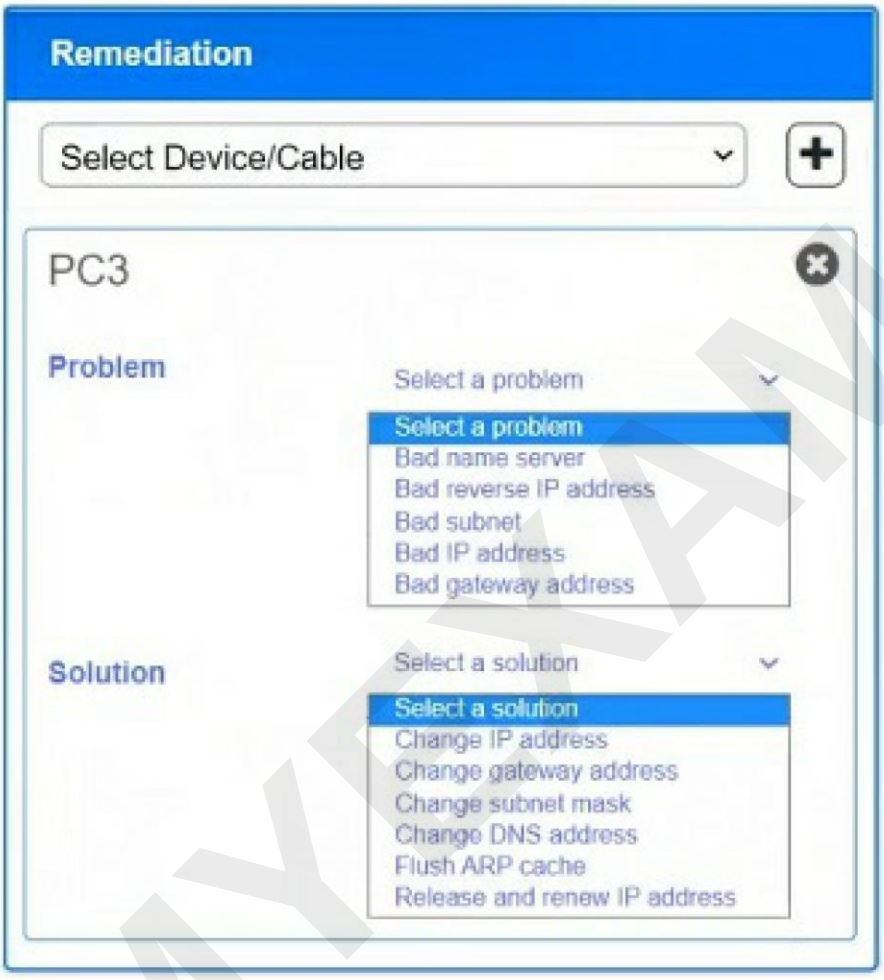


VLAN Usage

VLAN1:	Default	
VLAN2:	Server/HR	10.10.2.0/24
VLAN3:	Marketing	10.10.3.0/24
VLAN4:	Admin Staff	10.10.4.0/24
VLAN10:	PCs	10.10.10.0/24
VLAN11:	Printer	10.10.11.0/24


Printer
HP Network Configuration Page
Model: HP Officejet Pro 8610
General Information
Network Status Ready
Active Connection Type Wired
URL(s) for Embedded Web Server http://HP4D30EC, http://192.168.2.9
Firmware Revision FDP1CN1347AR
Hostname HP4D30EC
Serial Number CN3AO1KG42
Internet Not Connected
802.3 Wired
Hardware Address (MAC) 9c:b6:54:4d:30:ec
Link Configuration None
IPv4
IP Address 10.10.11.56
Subnet Mask 255.255.255.0
Default Gateway 10.10.11.1
Configuration Source DHCP
Primary DNS Server 8.8.8.8
Secondary DNS Server 8.8.4.4
Total Packets Transmitted 15655
Total Packets Received 394068





Answer:

Router and Firewall Configuration:

- Ensure that all routers are configured with correct static routes to facilitate proper network traffic routing between different VLANs and external networks.
- Install a firewall at the network's entry point to inspect and filter Internet traffic as required by the security policy.

Switch Configuration:

- Configure switches to ensure PCs in different VLANs do not see each other's traffic. Implement VLAN tagging on the switches to segregate traffic between the different departments as indicated.

Cable Test Results:

- Address any faulty cables as indicated by the test results. For example, any cable showing physical connection issues (crossed pairs, etc.) should be replaced.
- Ensure that cables are appropriately labeled and meet the length requirements to avoid potential transmission issues over long distances.

Device Specific Issues:

- For devices showing incorrect configuration details such as bad IP addresses, subnet masks, or DNS configurations, apply appropriate corrections. For instance, resetting IP configurations or updating DNS settings where mismatches are found.

Printer Configuration:

- Check the printer configuration to ensure it aligns with the network settings, particularly the IP address, subnet, and gateway to guarantee connectivity for all users needing access.

Overall Network Health:

- Continuously monitor the network for any emerging issues, perform regular updates to the firmware of network devices, and ensure compliance with the latest security standards to maintain network integrity and performance.

Question: 6

SIMULATI

ON -

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

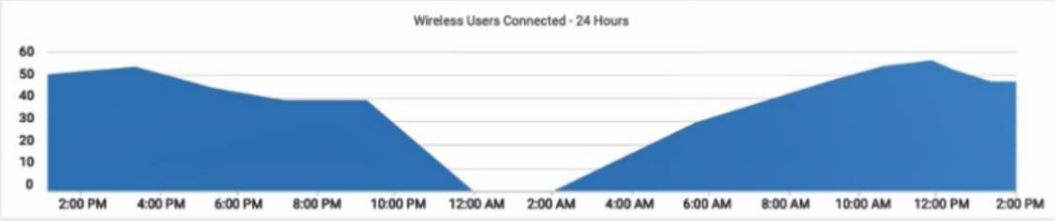
INSTRUCTIONS -

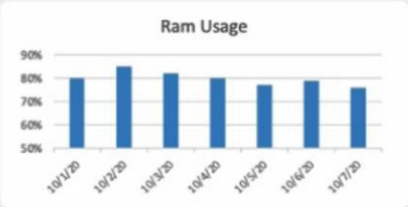
Click on each tab at the top of the screen. Select a widget to view information, then use the drop-down menus to answer the associated questions.

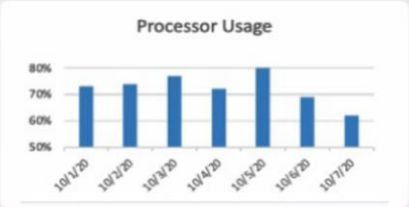
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Network Health | Device Monitoring

Show Question | Reset All Answers







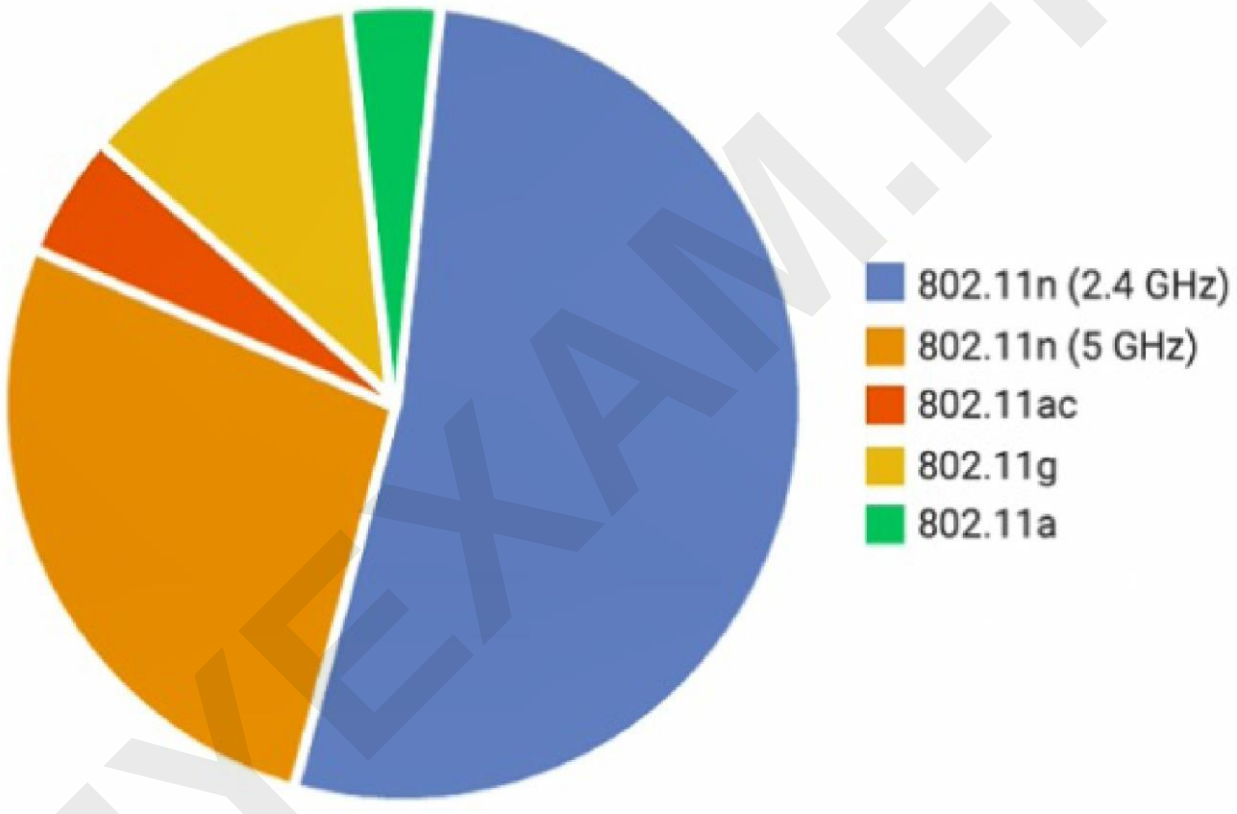
Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms

Which WAN station should be preferred for VoIP traffice?

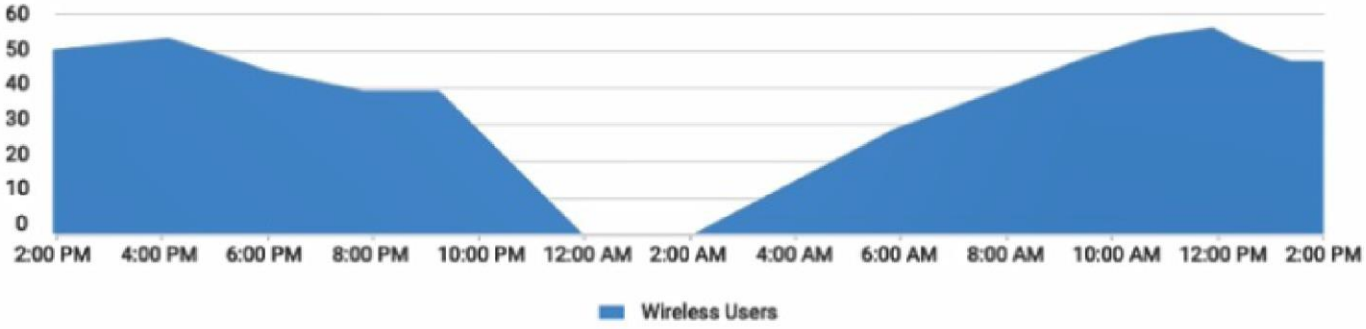
Select WAN

- Select WAN
- WAN 1
- WAN 2

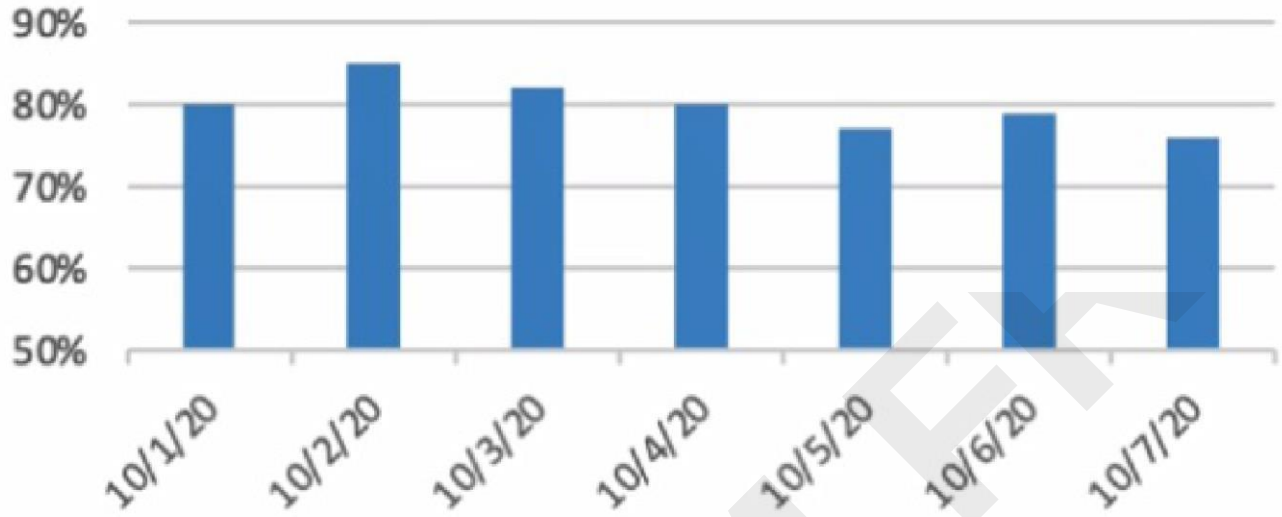
Wireless Client Distribution



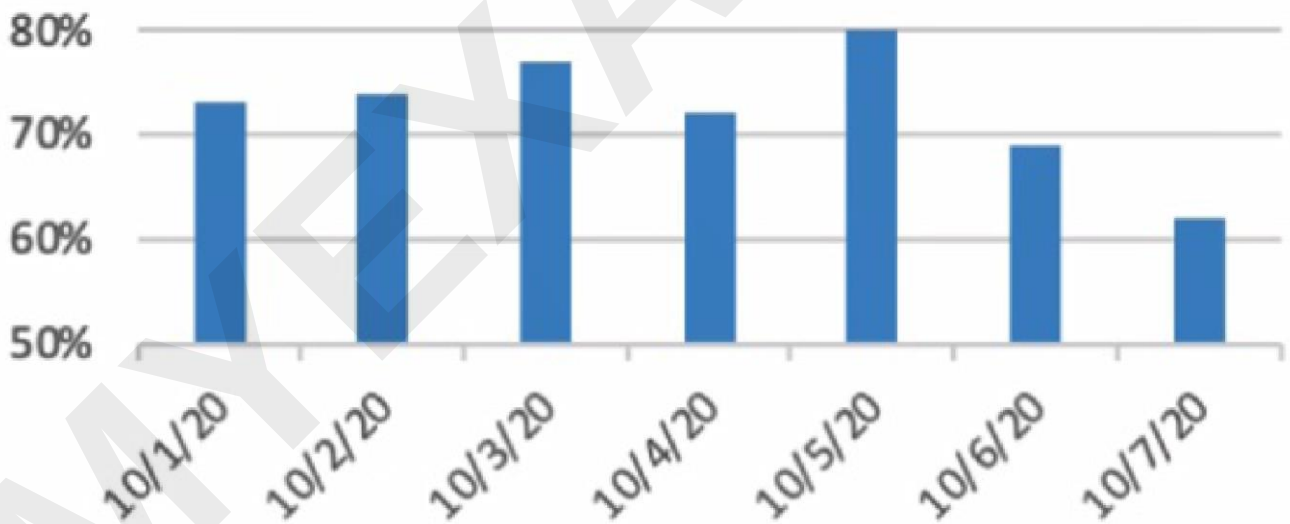
Wireless Users Connected - 24 Hours



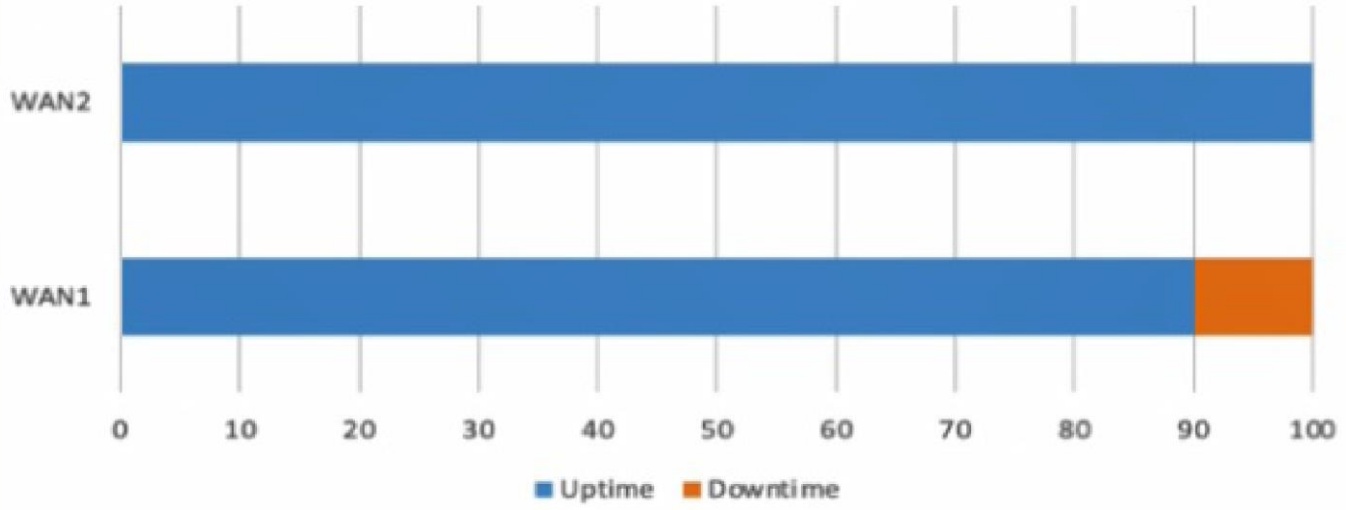
RAM Usage



Processor Usage



WAN Health



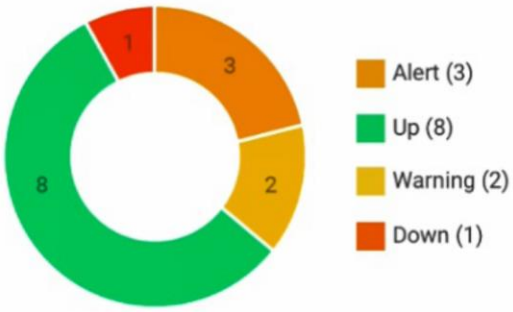
WAN Uplinks

Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms

Network Health | Device Monitoring

Show Question | Reset All Answers

Device Status



Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

Which device is experiencing connectivity issues?

Select Answer

- Select Answer
- Router A
- Router B
- WAP1
- WAP2
- WirelessController
- Switch A
- Switch B
- DHCP Server
- Web Server
- APP Server

Which workstation IP is generating the MOST traffic?

Select Answer

- Select Answer
- 10.1.99.28
- 10.1.99.14
- 10.1.99.10
- 10.1.99.22
- 10.1.99.24
- 206.208.133.10
- 206.208.133.9
- 10.1.50.14
- 10.1.50.13
- 10.1.59.81
- 10.1.90.53
- 10.1.90.55

Device Status

Status	Device Name	IP Address	Ping Time	Total Traffic
	Switch A	10.1.99.22	30msec	1Gbit/s
	Switch B	10.1.99.24	21msec	100Mbit/s
	WAP1	10.1.99.14	52msec	90Mbit/s
	WAP2	10.1.99.28	16msec	100Mbit/s
	Router A	206.208.133.10	Request timed out	0Gbit/s
	Router B	206.208.133.9	40msec	1Gbit/s
	WirelessController	10.1.99.10	17msec	10Gbit/s

Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

Answer:

WAN 1:
- Uplink Speed: 10G
- Total Usage: 26.969GB Up / 1.748GB Down
- Average Throughput: 353MBps Up / 23.42MBps Down
- Loss: 2.51%
- Average Latency: 24ms
- Jitter: 9.5ms

WAN 2:
- Uplink Speed: 1G
- Total Usage: 930GB Up / 138GB Down
- Average Throughput: 12.21MBps Up / 1.82MBps Down
- Loss: 0.01%
- Average Latency: 11ms
- Jitter: 3.9ms

Although WAN 1 offers greater bandwidth and throughput, it exhibits higher latency and jitter, which could detract from VoIP performance. In contrast, WAN 2, despite its lower bandwidth, offers much lower latency, nearly negligible packet loss, and reduced jitter. These characteristics are essential for VoIP applications, which demand consistent and quick packet delivery.

Therefore, for VoIP communications, WAN 2 is recommended due to its enhanced stability in latency and jitter handling, which are pivotal for the clarity and reliability of voice calls. WAN 1 could be better utilized for other tasks that require high bandwidth and are less affected by latency variations, such as large-scale data transfers.

Question: 7

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

A.Establish a theory.

B.Implement the solution.
C.Create a plan of action.
D.Verify functionality.

Answer: A

Question: 8

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

A.LLDP
B.IKE
C.VLAN
D.netstat

Answer: A

Question: 9

A network administrator needs to set up a file server to allow user access. The organization uses DHCP to assign IP addresses. Which of the following is the best solution for the administrator to set up?

A.A separate scope for the file server using a /32 subnet
B.A reservation for the server based on the MAC address
C.A static IP address within the DHCP IP range
D.A SLAAC for the server

Answer: B

Question: 10

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

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

Answer: A

Question: 11

A network administrator wants to implement an authentication process for temporary access to an organization's network. Which of the following technologies would facilitate this process?

A.Captive portal
B.Enterprise authentication
C.Ad hoc network
D.WPA3

Answer: A

Question: 12

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

Answer: A

Question: 13

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

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

Answer: D

Question: 14

Which of the following should be used to obtain remote access to a network appliance that has failed to start up properly?

A.Crash cart
B.Jump box
C.Secure Shell
D.Out-of-band management

Answer: D

Question: 15

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

A.MAC flooding
B.VLAN hopping
C.DNS spoofing
D.ARP poisoning

Answer: B

Question: 16

A network administrator is configuring a new switch and wants to connect two ports to the core switch to ensure redundancy. Which of the following configurations would meet this requirement?

A.Full duplex
B.802.1Q tagging
C.Native VLAN
D.Link aggregation

Answer: D

Question: 17

Which of the following ports is used for secure email?

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

Answer: D

Question: 18

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

A.Least privilege network access
B.Dynamic inventories
C.Central policy management
D.Zero-touch provisioning
E.Configuration drift prevention
F.Subnet range limits

Answer: AC

Question: 19

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

A.Web traffic is filtered through a web filler.

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

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

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

Answer: D

Question: 20

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

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

Answer: D

Question: 21

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

A.DNS poisoning
B.Denial-of-service
C.Social engineering
D.ARP spoofing

Answer: A

Question: 22

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

A.ARP spoofing
B.Evil twin
C.MAC flooding
D.DNS poisoning

Answer: C

Question: 23

A company's office has publicly accessible meeting rooms equipped with network ports. A recent audit revealed that visitors were able to access the corporate network by plugging personal laptops into open network ports. Which of the following should the company implement to prevent this in the future?

A.URL filters
B.VPN
C.ACLs
D.NAC

Answer: D

Question: 24

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

A.dig
B.nmap
C.tracert
D.nslookup

Answer: B

Question: 25

Which of the following technologies is the best choice to listen for requests and distribute user traffic across web servers?

A.Router
B.Switch
C.Firewall
D.Load balancer

Answer: D

Question: 26

A company is hosting a secure server that requires all connections to the server to be encrypted. A junior administrator needs to harden 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

Answer: B

Question: 27

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

A.Determine resolution steps.
B.Duplicate the problem in a lab.
C.Present the theory for approval.
D.Implement the solution to the problem.

Answer: A

Question: 28

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

A.Configure ACLs.
B.Implement a captive portal.
C.Enable port security.
D.Disable unnecessary services.

Answer: C

Question: 29

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

A.255.255.255.128
B.255.255.255.192
C.255.255.255.224
D.255.255.255.240

Answer: D

Question: 30

A user reports having intermittent connectivity issues to the company network. The network configuration for the user reveals the following:

IP address: 192.168.1.10 -

Subnet mask: 255.255.255.0 -

Default gateway: 192.168.1.254 -
The network switch shows the following ARP table:

MAC address	IP address	Interface	VLAN
0c00.1134.0001	192.168.1.10	eth4	10
0c00.1983.210a	192.168.2.13	eth5	11
0c00.1298.d239	192.168.1.10	eth6	10
0c00.a291.c113	192.168.2.12	eth7	11
0c00.923b.2391	192.168.1.11	eth8	10
feff.2391.1022	192.168.1.254	eth1	10

Which of the following is the most likely cause of the user's connection issues?

A.A port with incorrect VLAN assigned
B.A switch with spanning tree conflict
C.Another PC with manually configured IP
D.A router with overlapping route tables

Answer: C

Question: 31

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

A.Logical diagram
B.Layer 3 network diagram
C.Service-level agreement
D.Heat map

Answer: D

Question: 32

Which of the following cloud deployment models is most commonly associated with multitenancy and is generally offered by a service provider?

A.Private
B.Community
C.Public
D.Hybrid

Answer: C

Question: 33

A network administrator needs to create an SVI on a Layer 3-capable device to separate voice and data traffic. Which of the following best explains this use case?

A.A physical interface used for trunking logical ports
B.A physical interface used for management access
C.A logical interface used for the routing of VLANs
D.A logical interface used when the number of physical ports is insufficient

Answer: C

Question: 34

A network administrator is performing a refresh of a wireless environment. As the APs are being placed, they overlap a little bit with each other. Which of the following 2.4GHz channels should be selected to ensure that they do not conflict?

A.1, 3, 5
B.1, 6, 11
C.2, 6, 10
D.3, 6, 9

Answer: B

Question: 35

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

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

Answer: D

Question: 36

Which of the following would allow a network administrator to analyze attacks coming from the internet without affecting latency?

A.IPS
B.IDS
C.Load balancer
D.Firewall

Answer: B

Question: 37

A technician is troubleshooting wireless connectivity near a break room. Whenever a user turns on the microwave, connectivity to the user's laptop is lost. Which of the following frequency bands is the laptop most likely using?

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

Answer: A

Question: 38

A network administrator needs to implement routing capabilities in a hypervisor. Which of the following should the administrator most likely implement?

A.VPC
B.Firewall
C.NFV
D.IaaS

Answer: C

Question: 39

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

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

Answer: A

Question: 40

A network administrator received complaints of intermittent network connectivity issues. The administrator

investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?

A.Enable spanning tree.
B.Configure port security.
C.Change switch port speed limits.
D.Enforce 802.1Q tagging.

Answer: A

Question: 41

Which of the following routing technologies uses a successor and a feasible successor?

A.IS-IS
B.OSPF
C.BGP
D.EIGRP

Answer: D

Question: 42

Which of the following best describes what an organization would use port address translation for?

A.VLANs on the perimeter
B.Public address on the perimeter router
C.Non-routable address on the perimeter router
D.Servers on the perimeter

Answer: C

Question: 43

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

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

Answer: B

Question: 44

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

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

Answer: B

Question: 45

Which of the following cable types provides the highest possible transmission speed?

A.Plenum
B.Ethernet
C.Fiber-optic
D.DAC

Answer: C

Question: 46

Which of the following layers of the OSI model is responsible for end-to-end encryption?

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

Answer: D

Question: 47

A network security administrator needs to monitor the contents of data sent between a secure network and the rest of the company. Which of the following monitoring methods will accomplish this task?

A.Port mirroring
B.Flow data
C.Syslog entries
D.SNMP traps

Answer: A

Question: 48

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

A.Lower bandwidth requirements
B.The ability to reset local computer passwords

C.Corporate inspection of all network traffic
D.Access to blocked sites

Answer: C

Question: 49

Which of the following does a hash provide?

A.Non-repudiation
B.Integrity
C.Confidentiality
D.Availability

Answer: B

Question: 50

A company wants to implement a disaster recovery site for non-critical applications, which can tolerate a short period of downtime. Which of the following types of sites should the company implement to achieve this goal?

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

Answer: C

Question: 51

Which of the following is an XML-based security concept that works by passing sensitive information about users, such as log-in information and attributes, to providers?

A.IAM
B.MFA
C.RADIUS
D.SAML

Answer: D

Question: 52

Which of the following routing technologies uses unequal cost load balancing and port 88?

A.EIGRP
B.BGP
C.RIP

D.OSPF

Answer: A

Question: 53

A wireless network consultant is deploying a large number of WAPs and wants to centrally control them from one wireless LAN controller. Which of the following network types should the consultant employ?

A.Mesh
B.Infrastructure
C.Point-to-point
D.Ad hoc

Answer: B

Question: 54

Which of the following network topologies involves sending all traffic through a single point?

A.Mesh
B.Hybrid
C.Hub-and-spoke
D.Point-to-point

Answer: C

Question: 55

Which of the following functions is used to prioritize network traffic based on the type of traffic?

A.QoS
B.VPN
C.CDN
D.TTL

Answer: A

Question: 56

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

A.KVM size
B.Switch depth
C.Hard drive size
D.Cooling fan speed
E.Outlet amperage

F.Server height

Answer: BF

Question: 57

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

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

Answer: D

Question: 58

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

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

Answer: A

Question: 59

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 modem has a signal power of -97dB. Which of the following should the support agent recommend to troubleshoot the issue?

A.Removing any splitters connected to the line
B.Switching the devices to wireless
C.Moving the devices closer to the modem
D.Lowering the network speed

Answer: A

Question: 60

Which of the following does OSPF use to communicate routing updates?

A.Unicast
B.Anycast

C.Multicast
D.Broadcast

Answer: D

Question: 61

A storage network requires reduced overhead and increased efficiency for the amount of data being sent. Which of the following should an engineer most likely configure to meet these requirements?

A.Link speed
B.Jumbo frames
C.QoS
D.802.1q tagging

Answer: B

Question: 62

A security administrator is creating a new firewall object for a device with IP address 192.168.100.1/25. However, the firewall software only uses dotted decimal notation in configuration fields. Which of the following is the correct subnet mask to use?

A.255.255.254.0
B.255.255.255.1
C.255.255.255.128
D.255.255.255.192

Answer: C

Question: 63

Which of the following disaster recovery metrics describes the average length of time a piece of equipment can be expected to operate normally?

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

Answer: D

Question: 64

A network administrator logs on to a router and sees an interface with an IP address of 10.61.52.34 255.255.255.252. Which of the following best describes how this interface IP address is being used?

A.As a point-to-point connection

B.To connect to the internet
C.As a virtual address for redundancy
D.For out-of-band management

Answer: A

Question: 65

A network technician is troubleshooting a faulty NIC and tests the theory. Which of the following should the technician do next?

A.Develop a theory.
B.Establish a plan of action.
C.Implement the solution.
D.Document the findings.

Answer: B

Question: 66

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

A.11MHz
B.20MHz
C.40MHz
D.80MHz
E.160MHz

Answer: B

Question: 67

A network manager wants to view network traffic for devices connected to a switch. A network engineer connects an appliance to a free port on the switch and needs to configure the switch port connected to the appliance. Which of the following is the best option for the engineer to enable?

A.Trunking
B.Port mirroring
C.Full duplex
D.SNMP

Answer: B

Question: 68

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

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

Answer: B

Question: 69

A network administrator is troubleshooting an application issue after a firewall change. The administrator has confirmed that the port and protocol are accessible to the user, but the application is still having issues. Which of the following tools allows the administrator to look at traffic on the application layer of the OSI model?

A.ifconfig
B.tcpdump
C.nslookup
D.traceroute

Answer: B

Question: 70

Which of the following ports should a network administrator enable for encrypted log-in to a network switch?

A.22
B.23
C.80
D.123

Answer: A

Question: 71

Which of the following is used to stage copies of a website closer to geographically dispersed users?

A.VPN
B.CDN
C.SAN
D.SDN

Answer: B

Question: 72

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

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

Answer: C

Question: 73

An administrator is configuring a switch that will be placed in an area of the office that is accessible to customers. Which of the following is the best way for the administrator to mitigate unknown devices from connecting to the network?

A.SSE
B.ACL
C.Perimeter network
D.802.1X

Answer: D

Question: 74

Which of the following diagrams would most likely include specifications about fiber connector types?

A.Logical
B.Physical
C.Rack
D.Routing

Answer: B

Question: 75

Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?

A.To encrypt sensitive data in transit
B.To secure the endpoints
C.To maintain contractual agreements
D.To comply with data retention requirements

Answer: A

Question: 76

An organization moved its DNS servers to new IP addresses. After this move, customers are no longer able to access the organization's website. Which of the following DNS entries should be updated?

A.AAA
B.CNAME
C.MX
D.NS

Answer: D

Question: 77

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

A.Fire suppression system
B.UPS location
C.Humidity control
D.Power load
E.Floor construction type
F.Proximity to nearest MDF

Answer: AC

Question: 78

A customer lost the connection to the telephone system. The administration console is configured with multiple network interfaces and is connected to multiple switches. The network administrator troubleshoots and verifies the following:
The support team is able to connect remotely to the administration console.
Rebooting the switch shows solid link and activity lights even on unused ports.
Rebooting the telephone system does not bring the system back online.
The console is able to connect directly to individual modules successfully.
Which of the following is the most likely reason the customer lost the connection?

A.A switch failed.
B.The console software needs to be reinstalled.
C.The cables to the modules need to be replaced.
D.A module failed.

Answer: D

Question: 79

A systems administrator is configuring a new device to be added to the network. The administrator is planning to perform device hardening prior to connecting the device. Which of the following should the administrator do first?

A.Update the network ACLs.
B.Place the device in a screened subnet.
C.Enable content filtering.

D.Change the default admin passwords.

Answer: D

Question: 80

A network administrator needs to connect two network closets that are 492ft (150m) away from each other. Which of the following cable types should the administrator install between the closets?

A.Single-mode fiber
B.Coaxial
C.DAC
D.STP

Answer: A