Free Questions for N10-009 by certsdeals

Shared by Lyons on 22-07-2024

Question 1

Question Type: **MultipleChoice**

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?

Options:

A- Use a network tap.

B- Use Nmap software.

C- Use a protocol analyzer.

D- Use a port mirror.

Answer:

D

Explanation:

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

Question 2

Question Type: MultipleChoice

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?

Options:

A- Clientless

B- Client-to-site

C- Full tunnel

D- Site-to-site

Answer:

A

Explanation:

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

Question 3

Question Type: MultipleChoice

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

Options:

A- Network security group

B- laaS

C- VPC

D- Hybrid cloud

Answer:

C

Explanation:

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

Question 4

Question Type: MultipleChoice

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

Options:

A- Identify the problem.

B- Document the findings and outcomes.

C- Test the theory to determine cause.

D- Establish a plan of action.

Answer:

A

Explanation:

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

Question 5

Question Type: MultipleChoice

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

Options:

A- Infrastructure as a service

B- Software as a service

C- Platform as a service

D- Network as a service

Answer:

A

Explanation:

Infrastructure as a Service (IaaS) typically requires the greatest up-front expense by the customer when migrating a data center to the cloud. IaaS provides virtualized computing resources over the internet, where customers rent virtual machines, storage, and networks.

The customer is responsible for managing the operating systems, applications, and data. This model often necessitates significant initial investment in planning, migration, and configuring the infrastructure. In contrast, Software as a Service (SaaS) and Platform as a Service (PaaS) models usually involve lower up-front costs because they offer more managed services. Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

Question 6

Question Type: **MultipleChoice**

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?

Options:

A- 11MHz

B- 20MHz

C- 40MHz

D- 80MHz

E- 160MHz

Answer:

B

Explanation:

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

Question 7

Question Type: MultipleChoice

SIMULATION

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

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

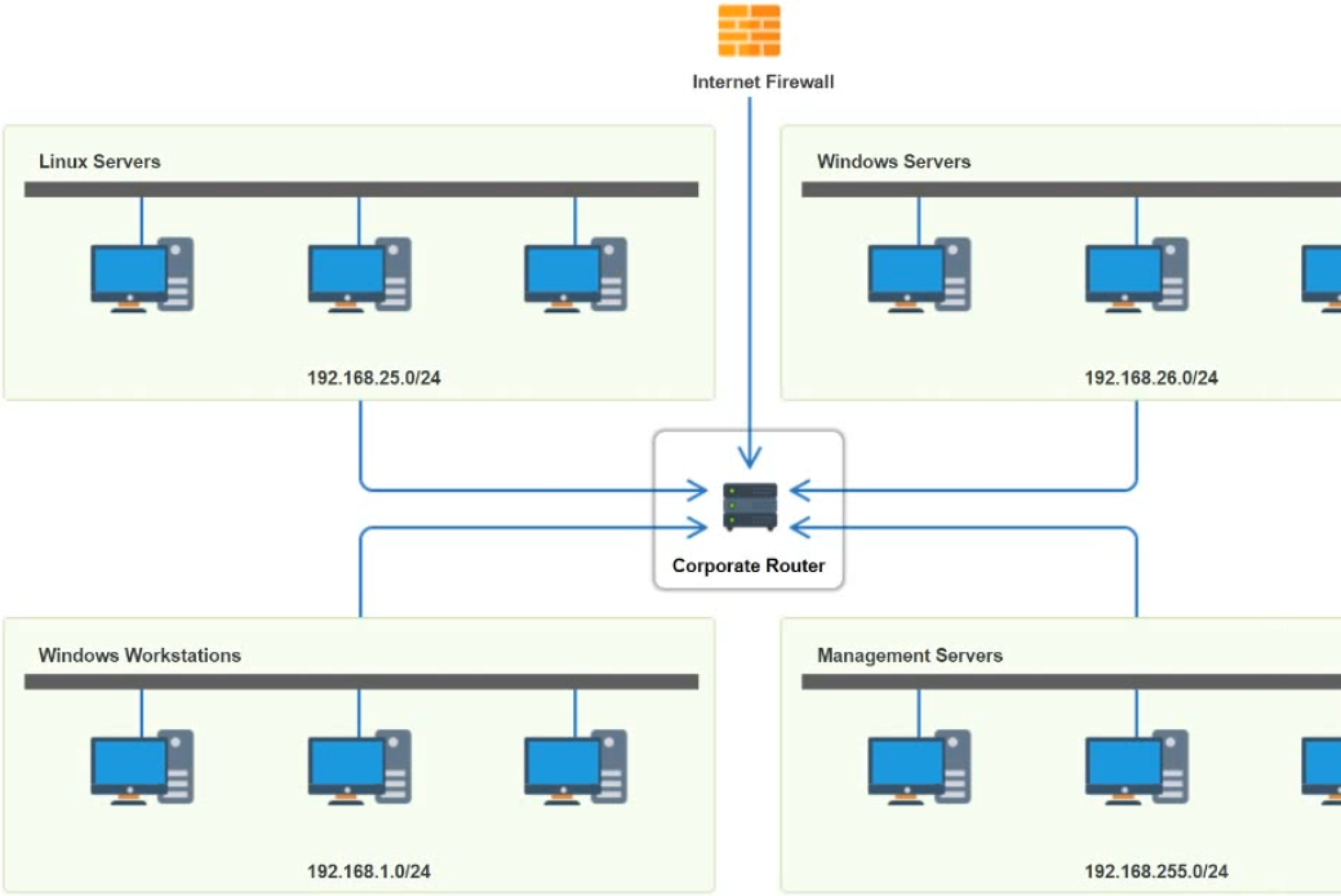
2. Ensure the user subnet cannot use the most commonly used remote access technologies in the Linux and Windows Server segments.

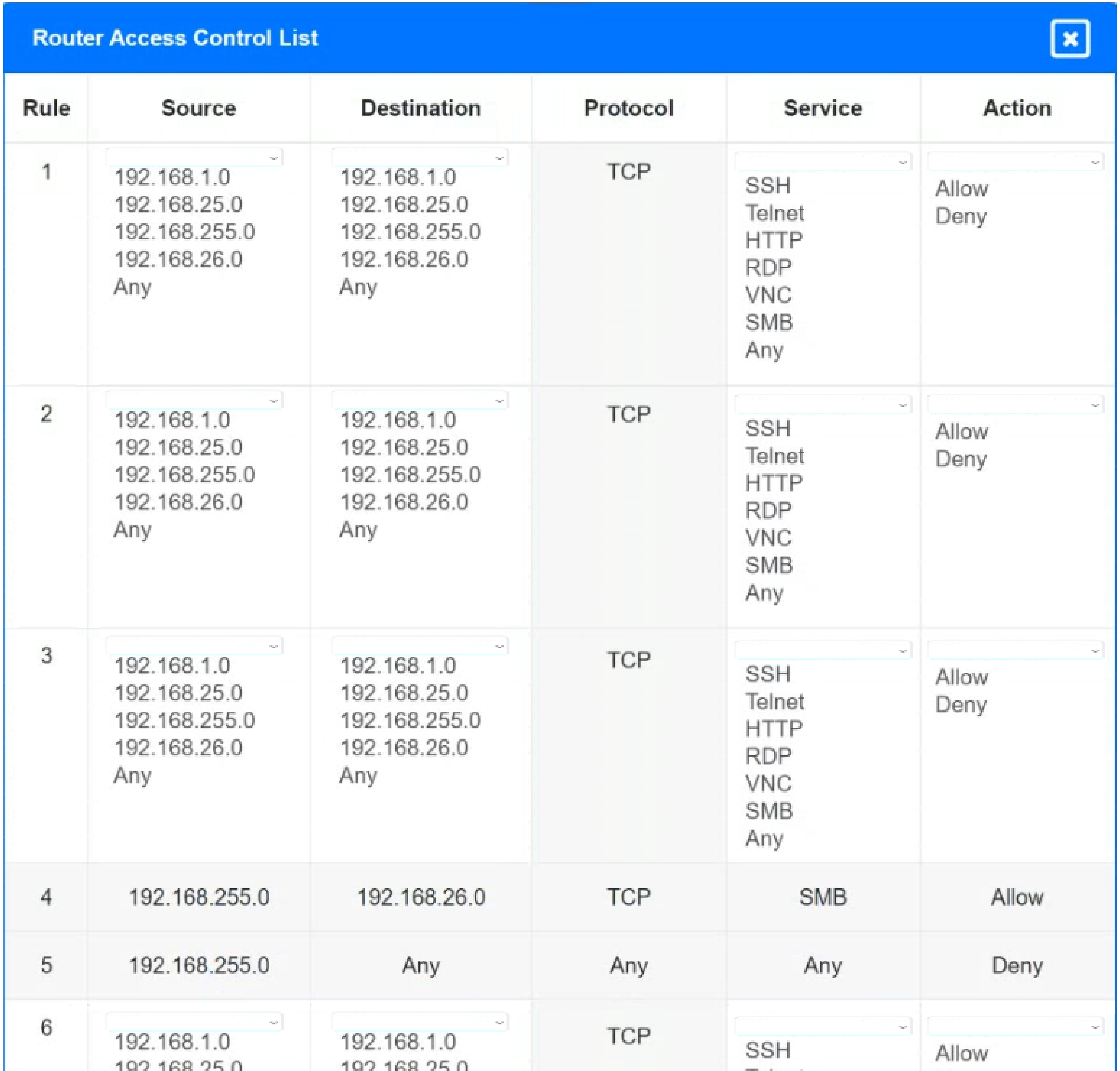
3. Prohibit any traffic that has not been specifically allowed.

INSTRUCTIONS

Use the drop-downs to complete the ACL

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


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



Router Access Control List

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

Options:

A- See the answer and solution below

Answer:

A

Question 8

Question Type: **MultipleChoice**

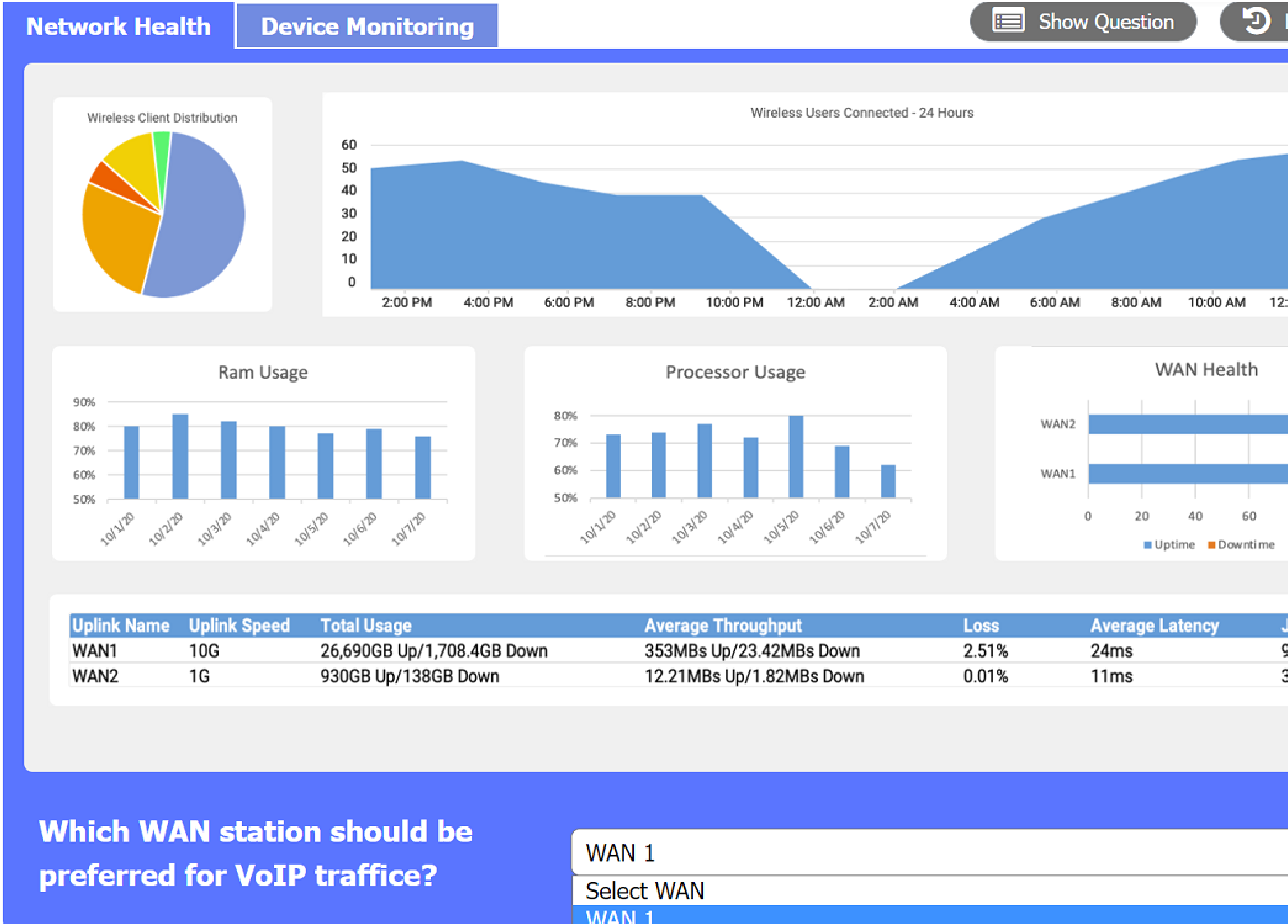
SIMULATION

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

INSTRUCTIONS

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

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



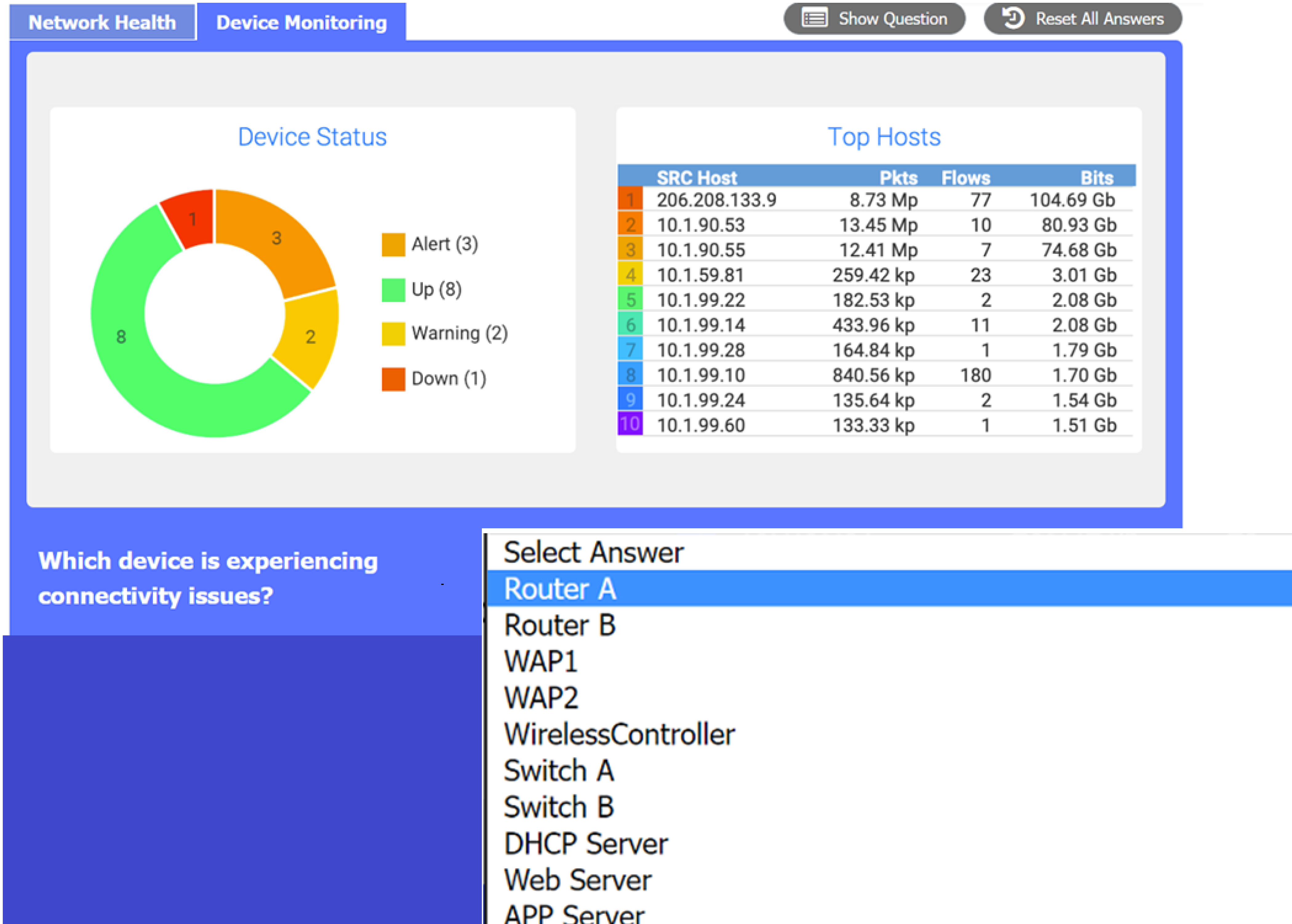
Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	J
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3

Which WAN station should be preferred for VoIP traffice?

WAN 1

Select WAN

WAN 1



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
Router A
Router B
WAP1
WAP2
WirelessController
Switch A
Switch B
DHCP Server
Web Server
APP Server

Options:

A- See the answer and solution below

Answer:

A

Explanation:

Network Health:

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

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

WAN 1:

Uplink Speed: 10G

Total Usage: 26.969GB Up / 1.748GB Down

Average Throughput: 353MBps Up / 23.42MBps Down

Loss: 2.51%

Average Latency: 24ms

Jitter: 9.5ms

WAN 2:

Uplink Speed: 1G

Total Usage: 930GB Up / 138GB Down

Average Throughput: 12.21MBps Up / 1.82MBps Down

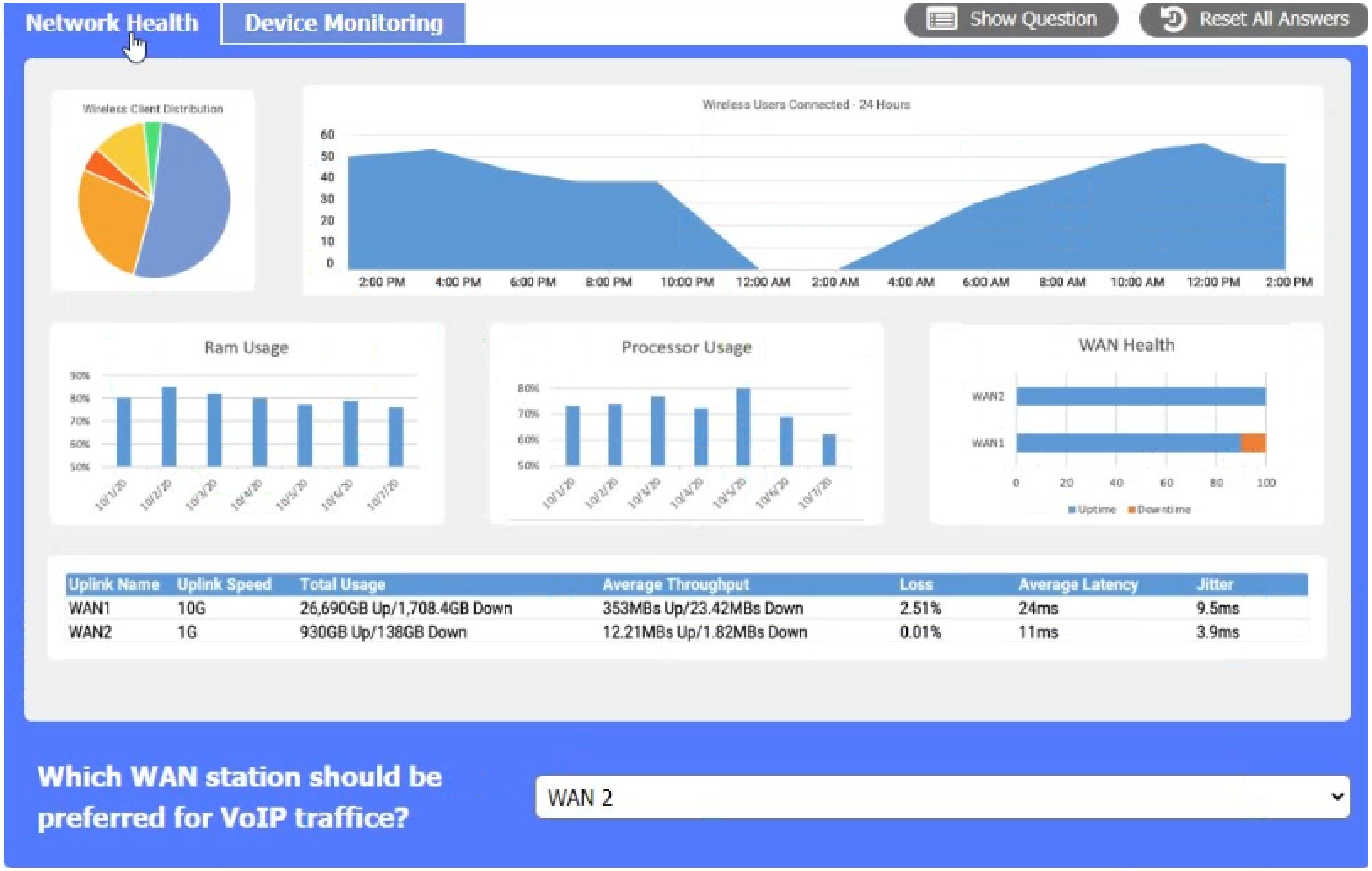
Loss: 0.01%

Average Latency: 11ms

Jitter: 3.9ms

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

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



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

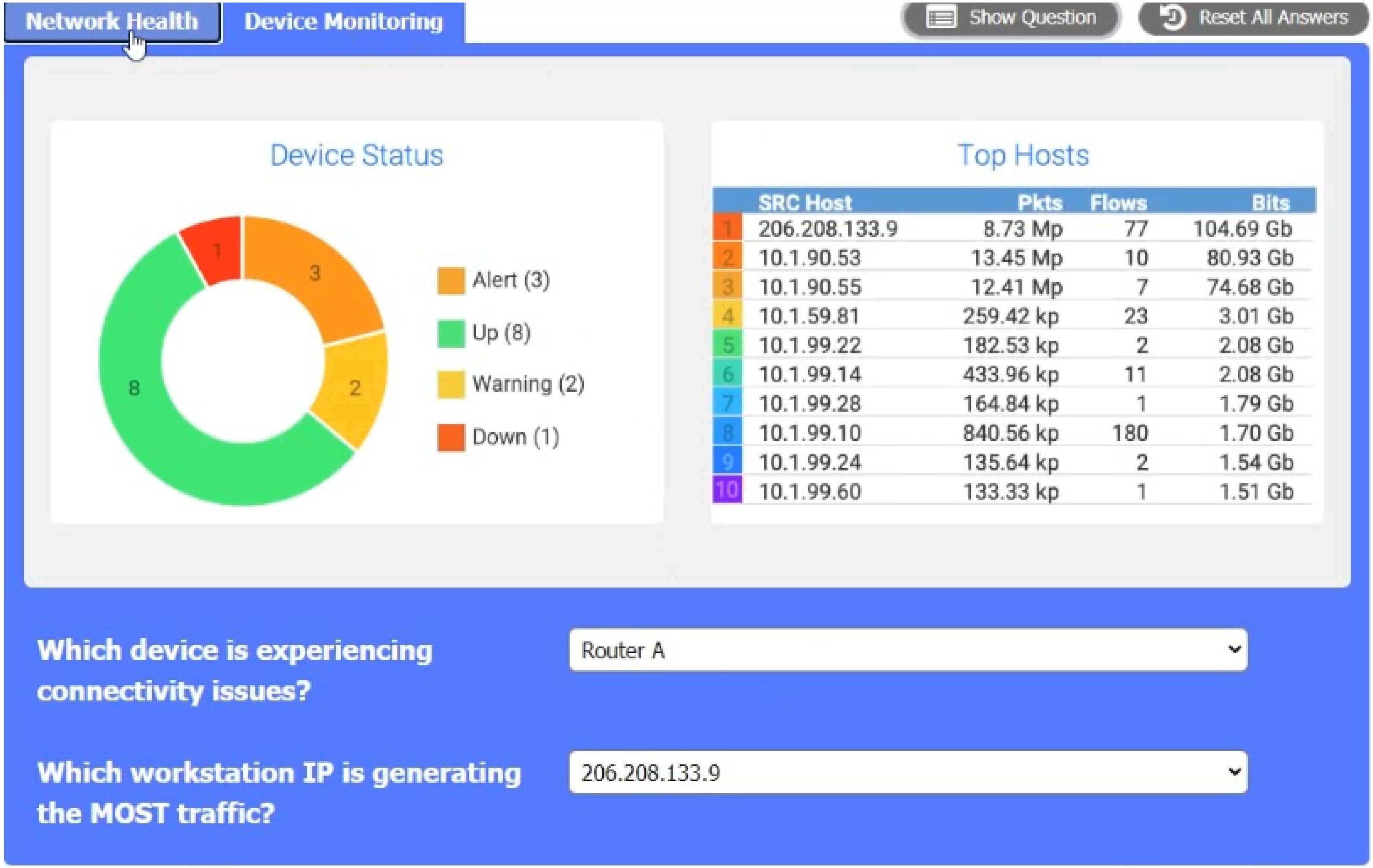
Which WAN station should be preferred for VoIP traffice?

WAN 2

Device Monitoring:

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

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



Device Status

🟧 Alert (3)

🟩 Up (8)

🟨 Warning (2)

🟥 Down (1)

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? Router A

Which workstation IP is generating the MOST traffic? 206.208.133.9

Question 9

Question Type: **MultipleChoice**

SIMULATION

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

INSTRUCTIONS

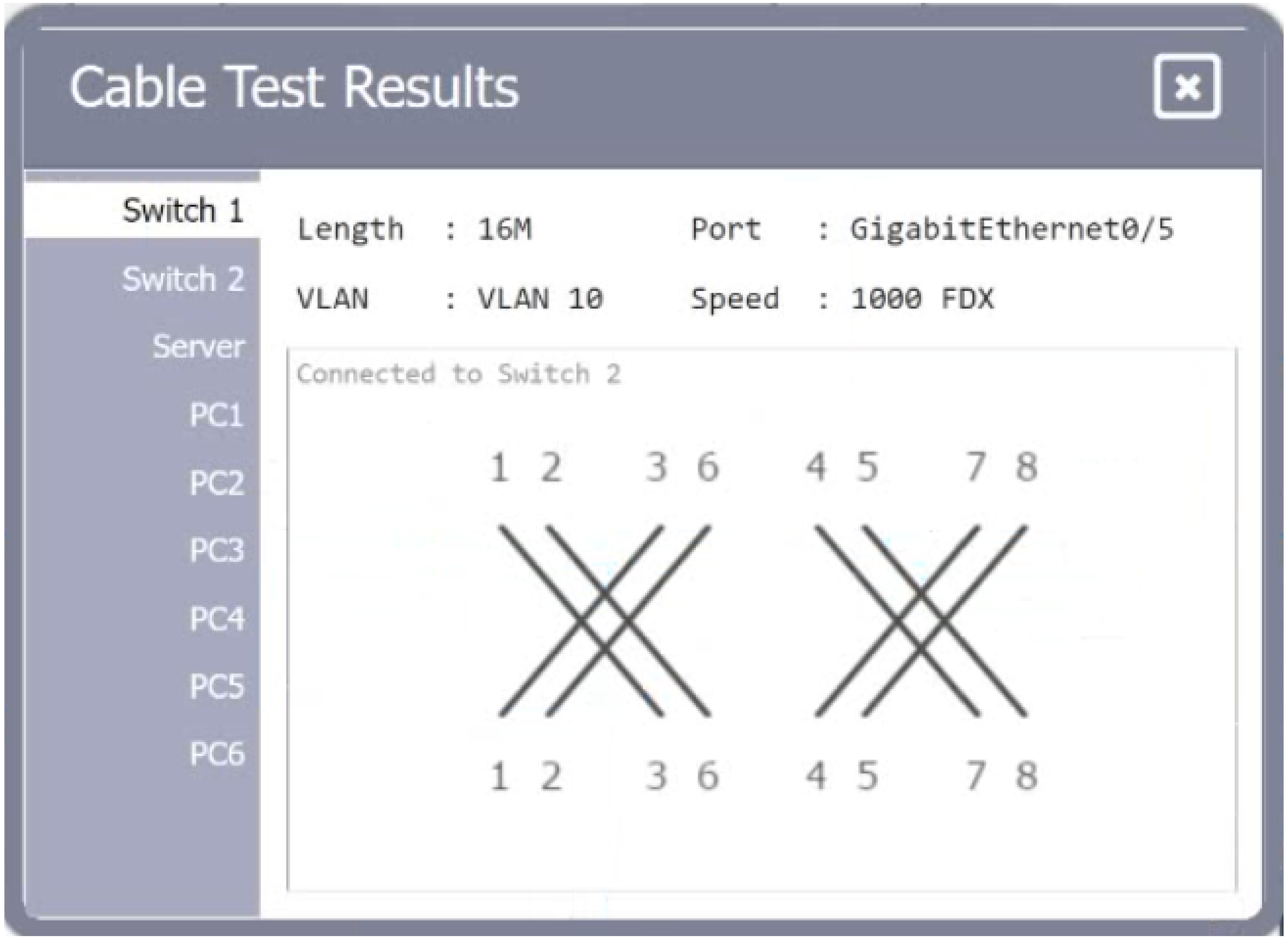
Troubleshoot all the network components.

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

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

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

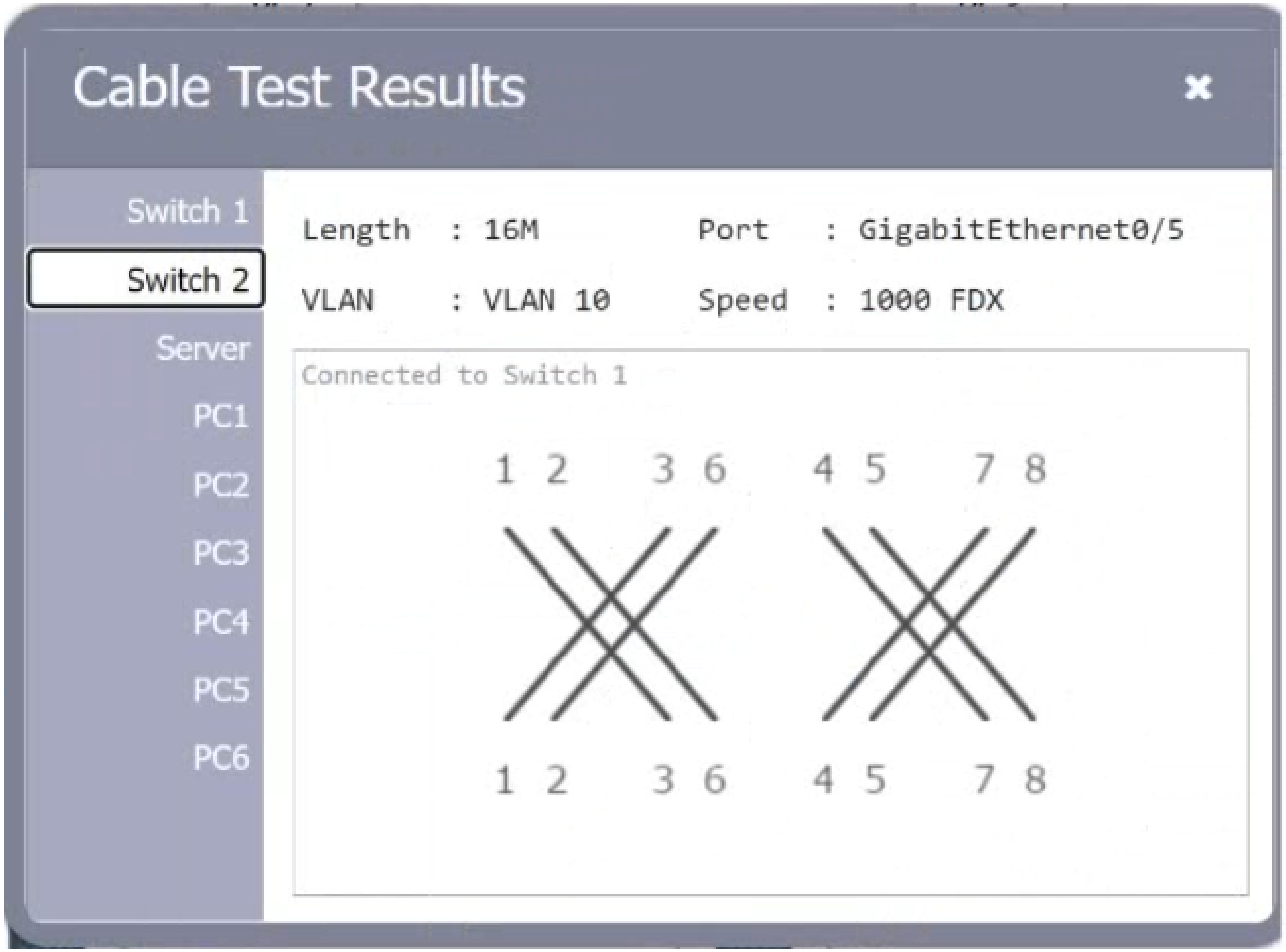
click the Reset All button.



Cable Test Results

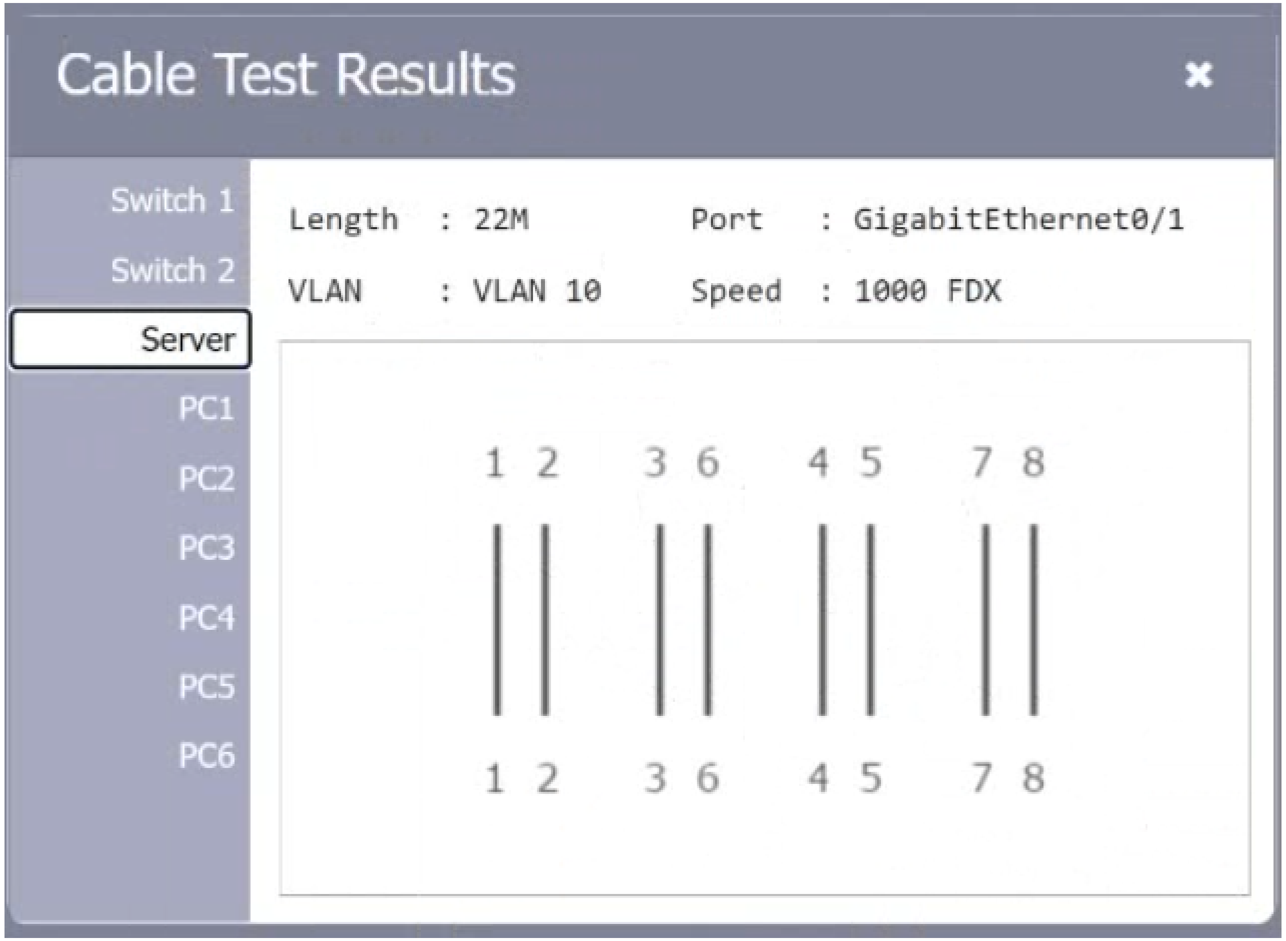
```
Length   : 16M          Port    : GigabitEthernet0/5
VLAN     : VLAN 10      Speed   : 1000 FDX
```

Connected to Switch 2



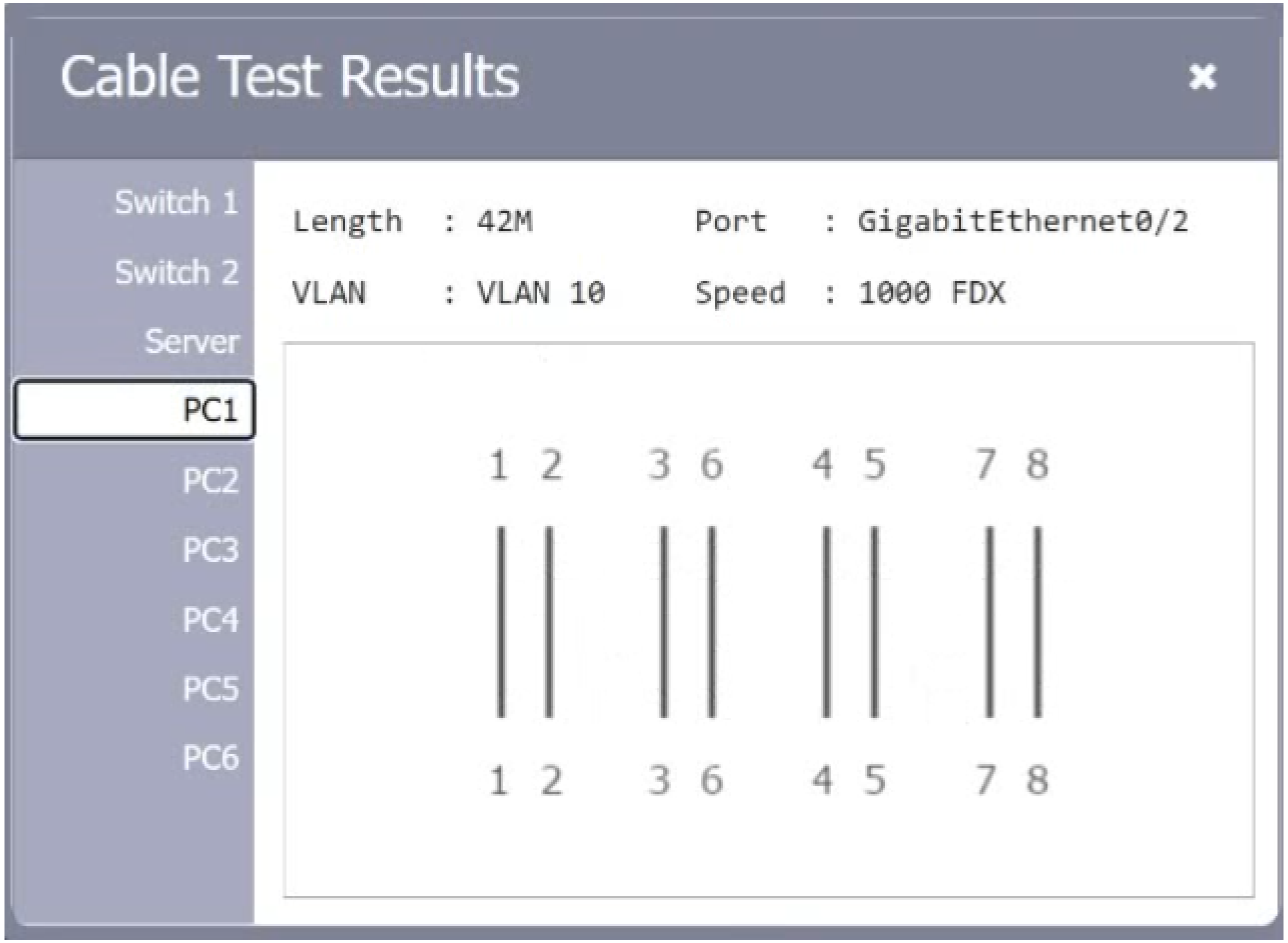
```
Length   : 16M          Port   : GigabitEthernet0/5
VLAN     : VLAN 10      Speed  : 1000 FDX
```

Connected to Switch 1



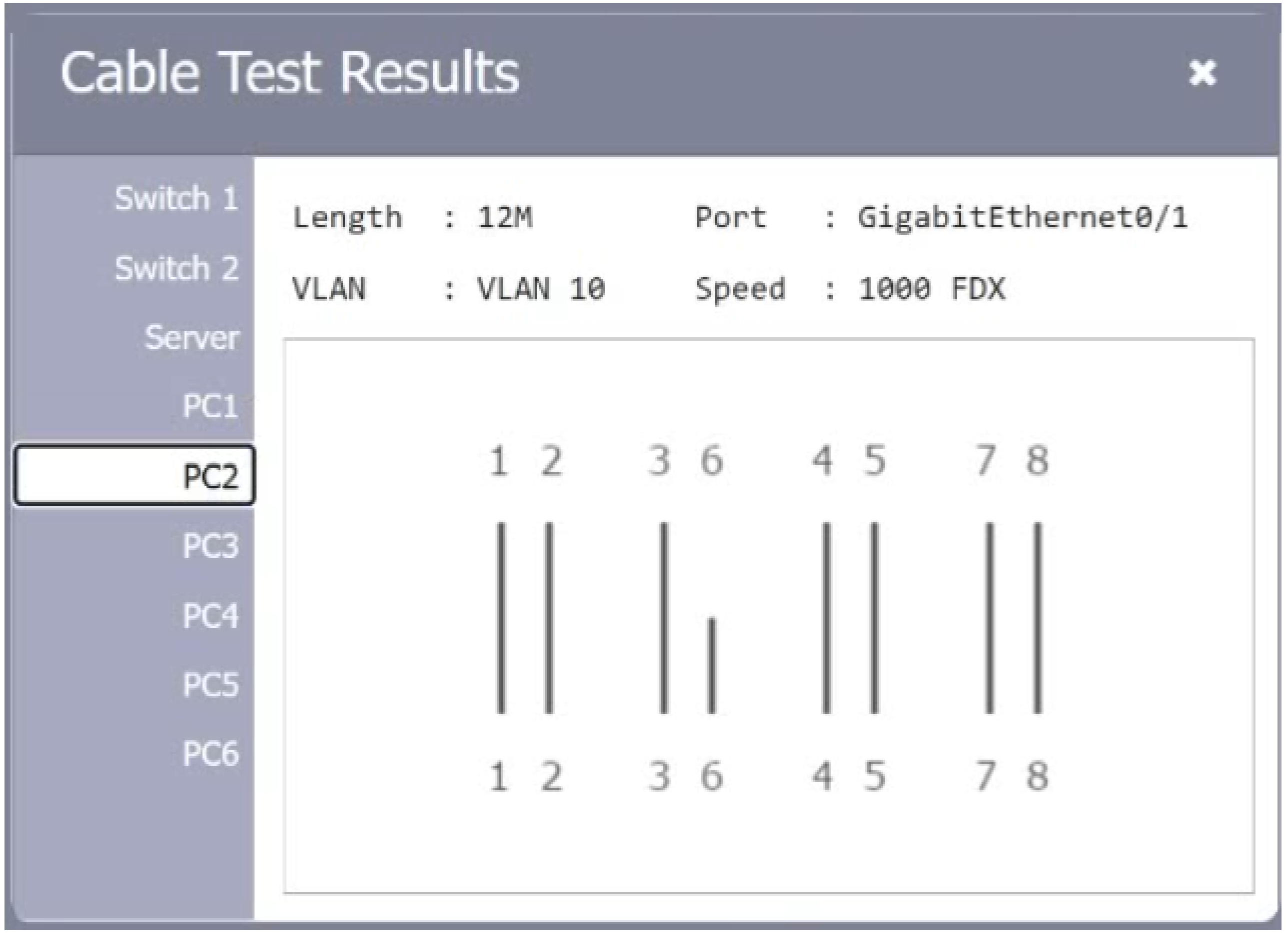
Cable Test Results

```
Length   : 22M          Port   : GigabitEthernet0/1
VLAN     : VLAN 10      Speed  : 1000 FDX
```



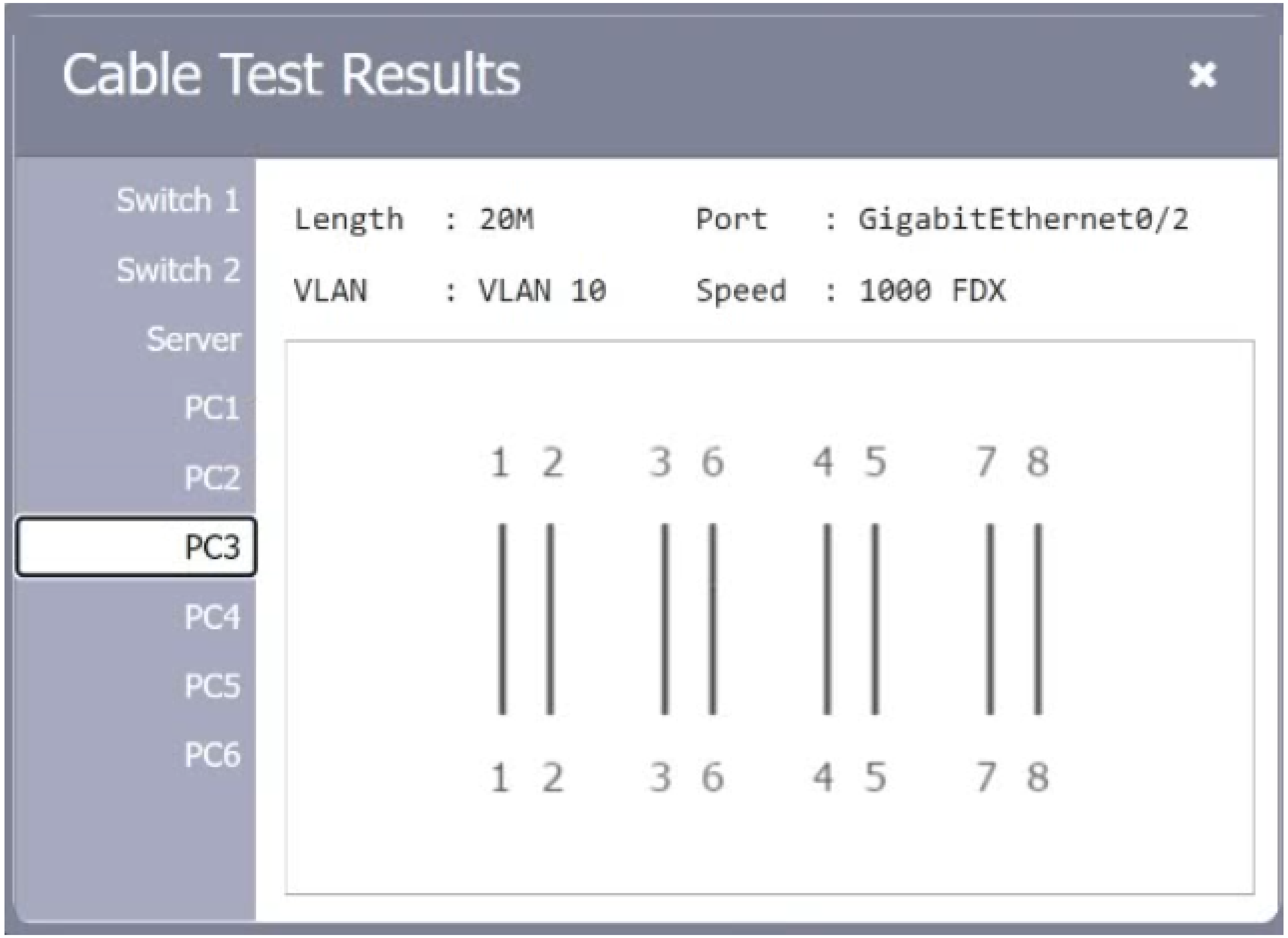
Cable Test Results

```
Length  : 42M        Port   : GigabitEthernet0/2
VLAN    : VLAN 10    Speed  : 1000 FDX
```

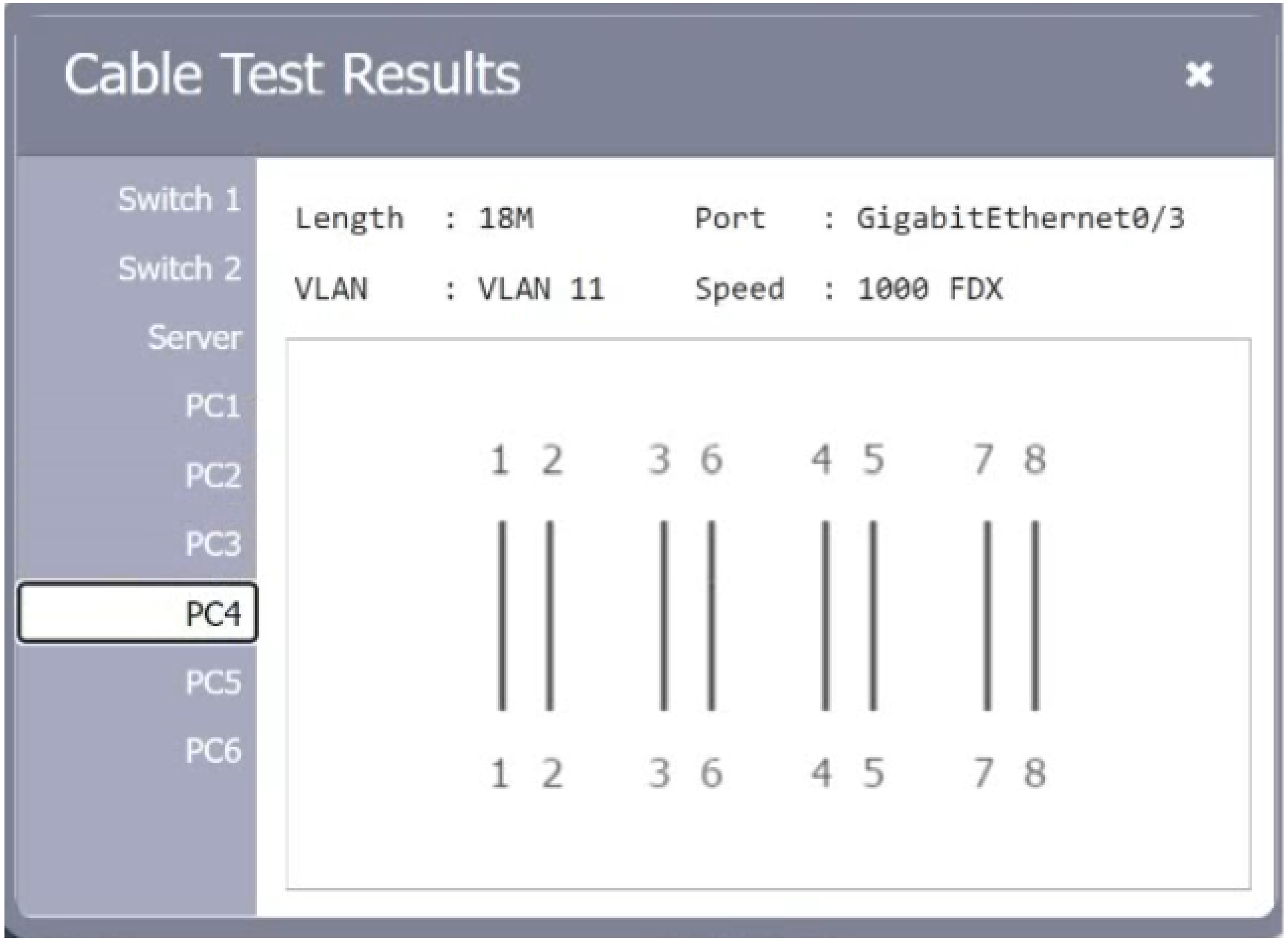


Cable Test Results

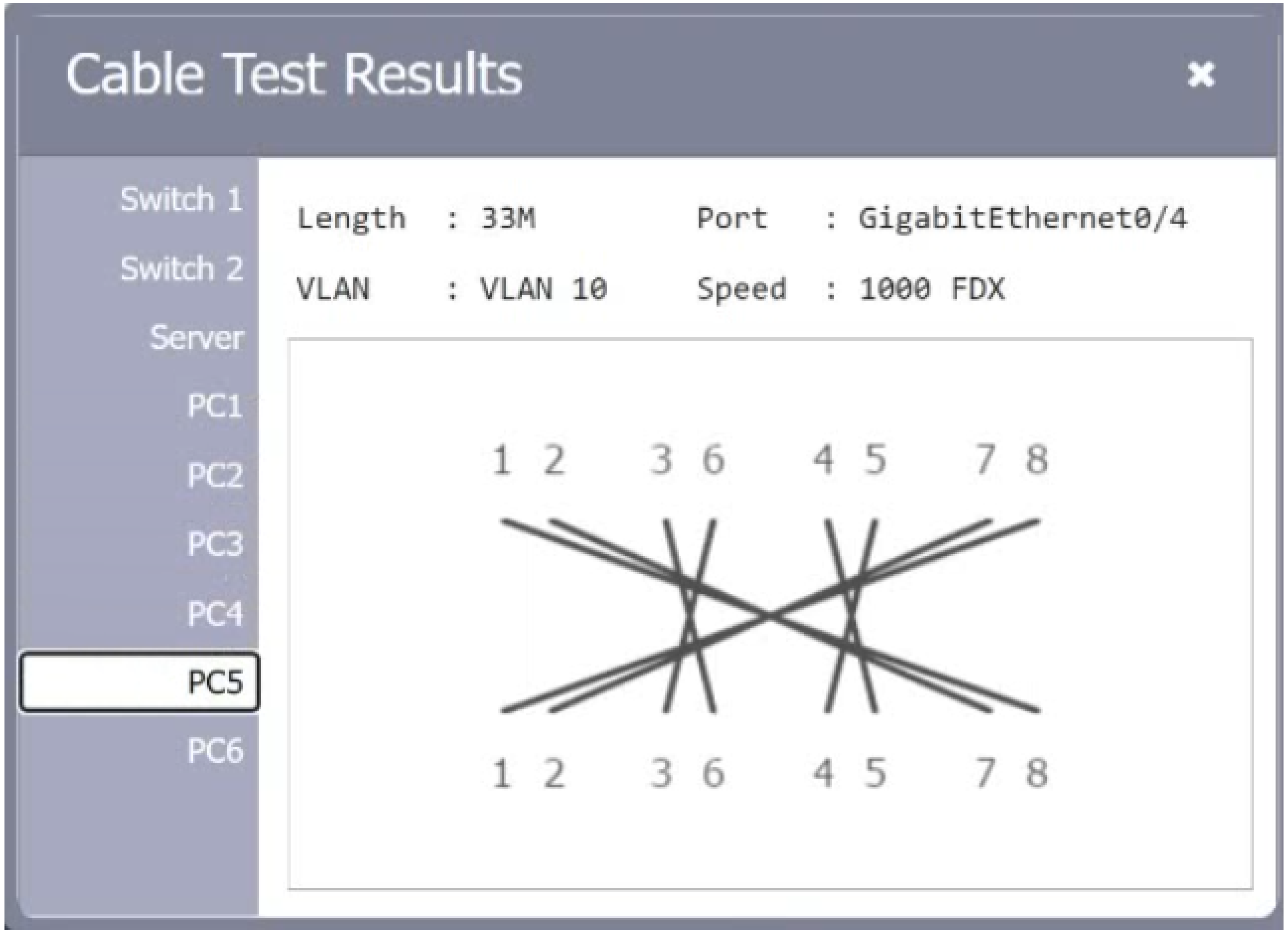
```
Length   : 12M          Port    : GigabitEthernet0/1
VLAN     : VLAN 10      Speed   : 1000 FDX
```



```
Length   : 20M        Port    : GigabitEthernet0/2
VLAN     : VLAN 10    Speed   : 1000 FDX
```

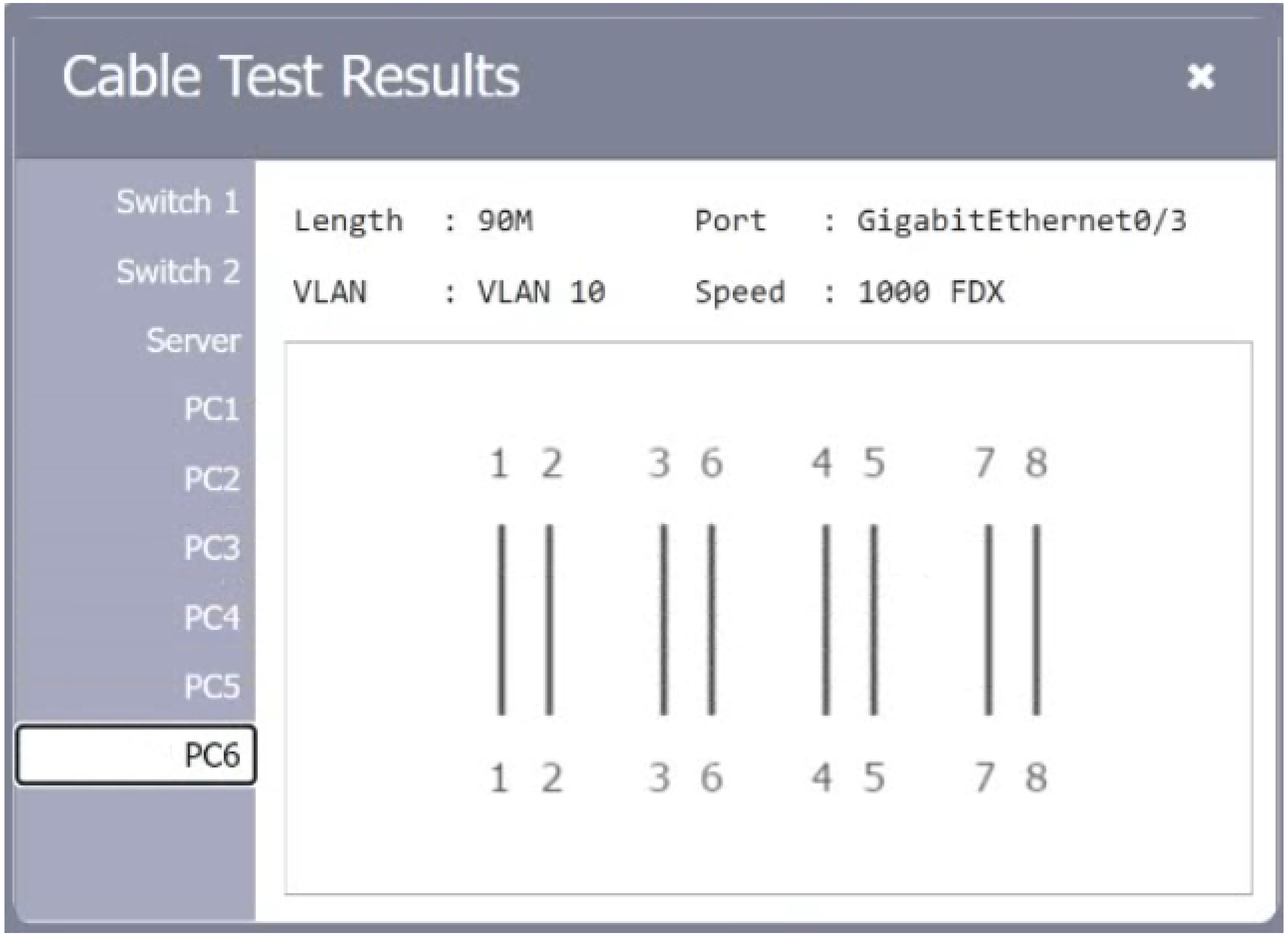


```
Length  : 18M        Port   : GigabitEthernet0/3
VLAN    : VLAN 11    Speed  : 1000 FDX
```



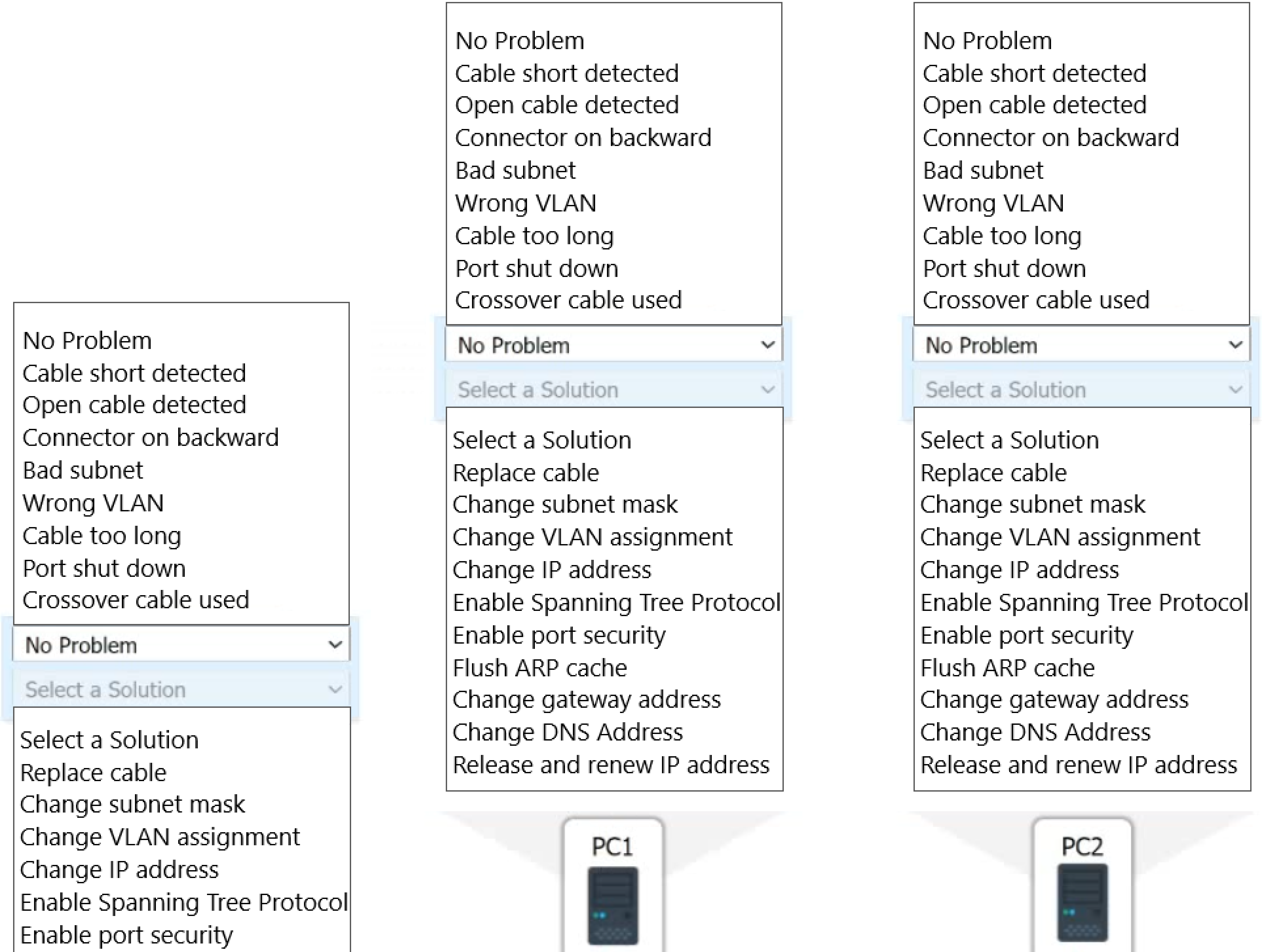
Cable Test Results

```
Length   : 33M          Port    : GigabitEthernet0/4
VLAN     : VLAN 10      Speed   : 1000 FDX
```



Cable Test Results

```
Length  : 90M        Port   : GigabitEthernet0/3
VLAN    : VLAN 10    Speed  : 1000 FDX
```


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

Options:

A- See the answer and solution below

Answer:

A

Question 10

Question Type: MultipleChoice

SIMULATION

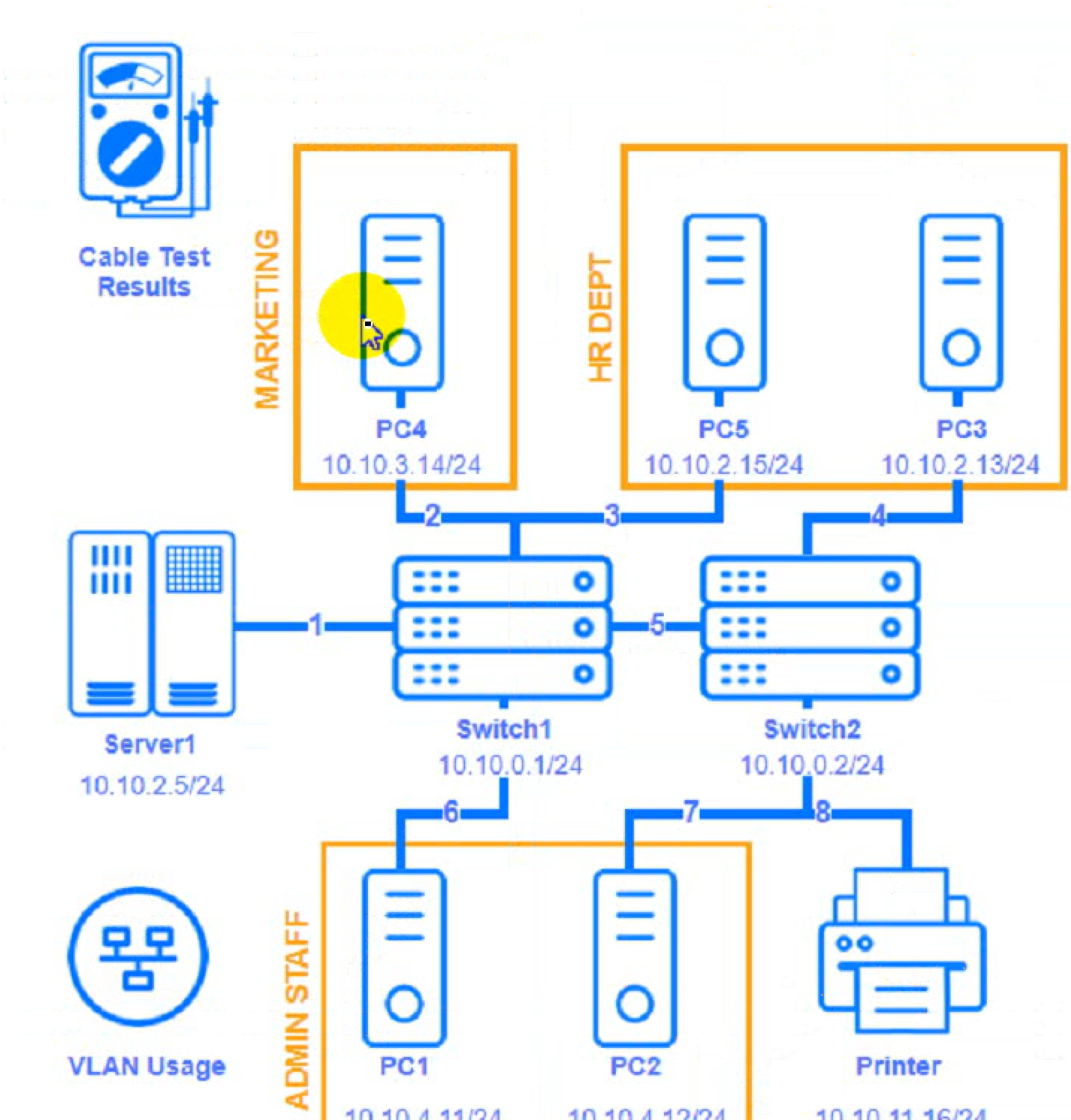
A network technician needs to resolve some issues with a customer's SOHO network.

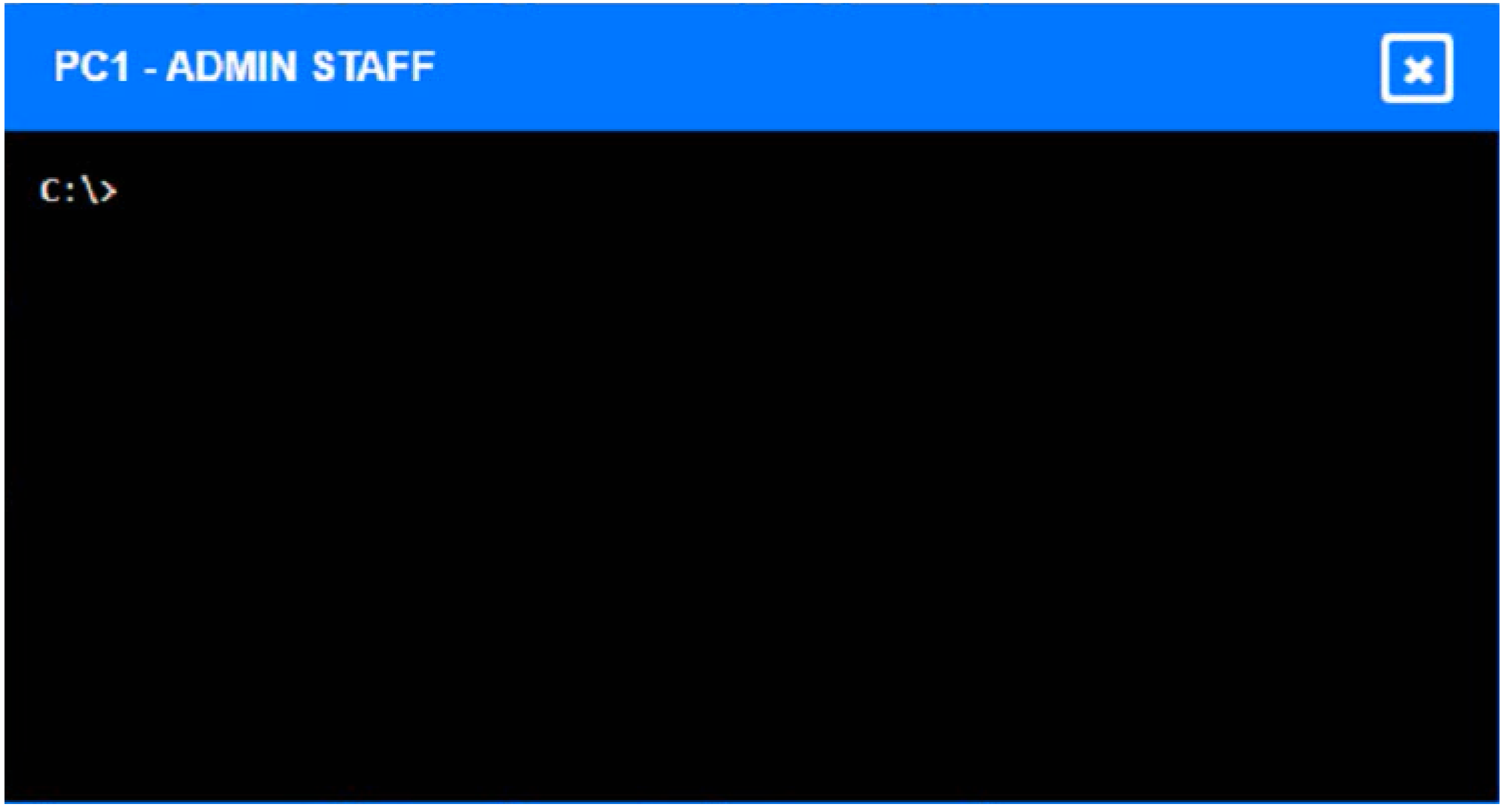
The customer reports that some of the devices are not connecting to the network, while others appear to work as intended.

INSTRUCTIONS

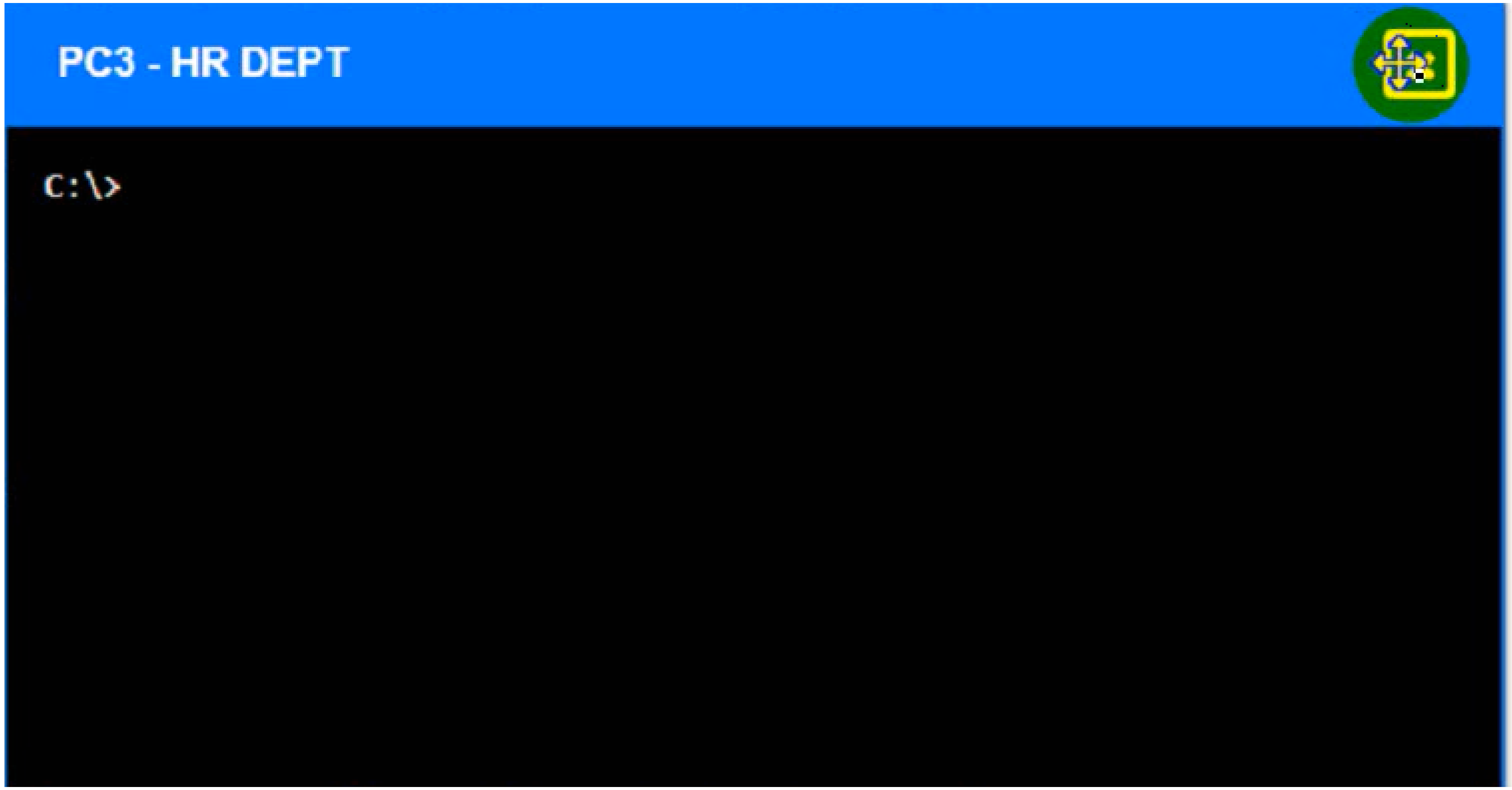
Troubleshoot all the network components and review the cable test results by Clicking on each device and cable.

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


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

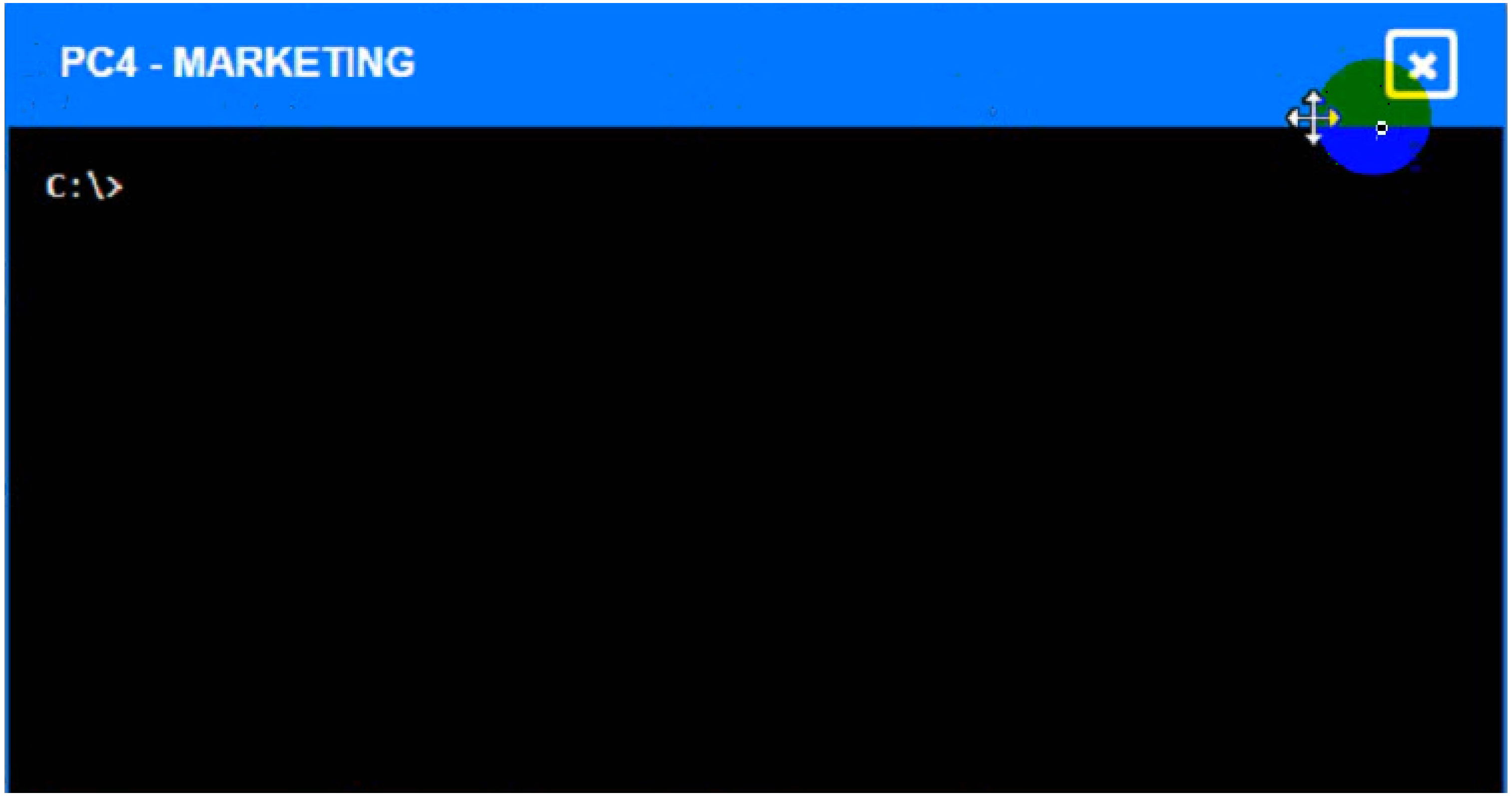


```
C:\>
```



PC3 - HR DEPT

```
C:\>
```



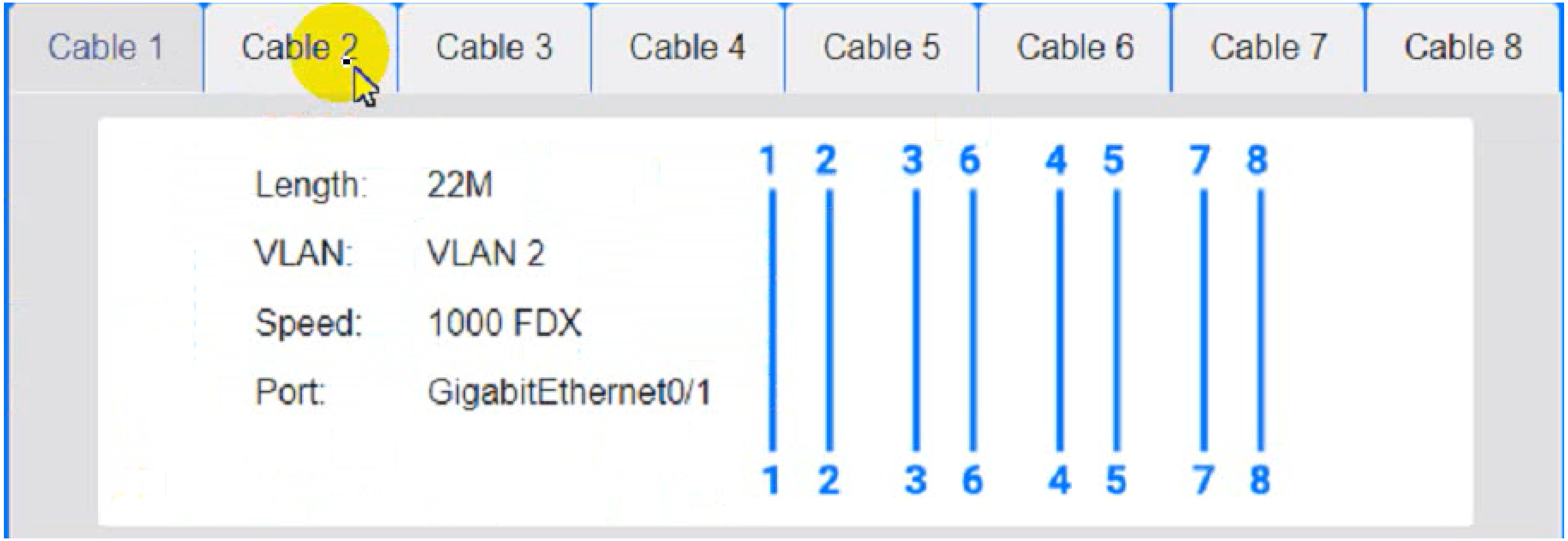
```
C:\>
```

```
C:\>
```

```
C:\>
```

Cable Test Results:

Cable 1:



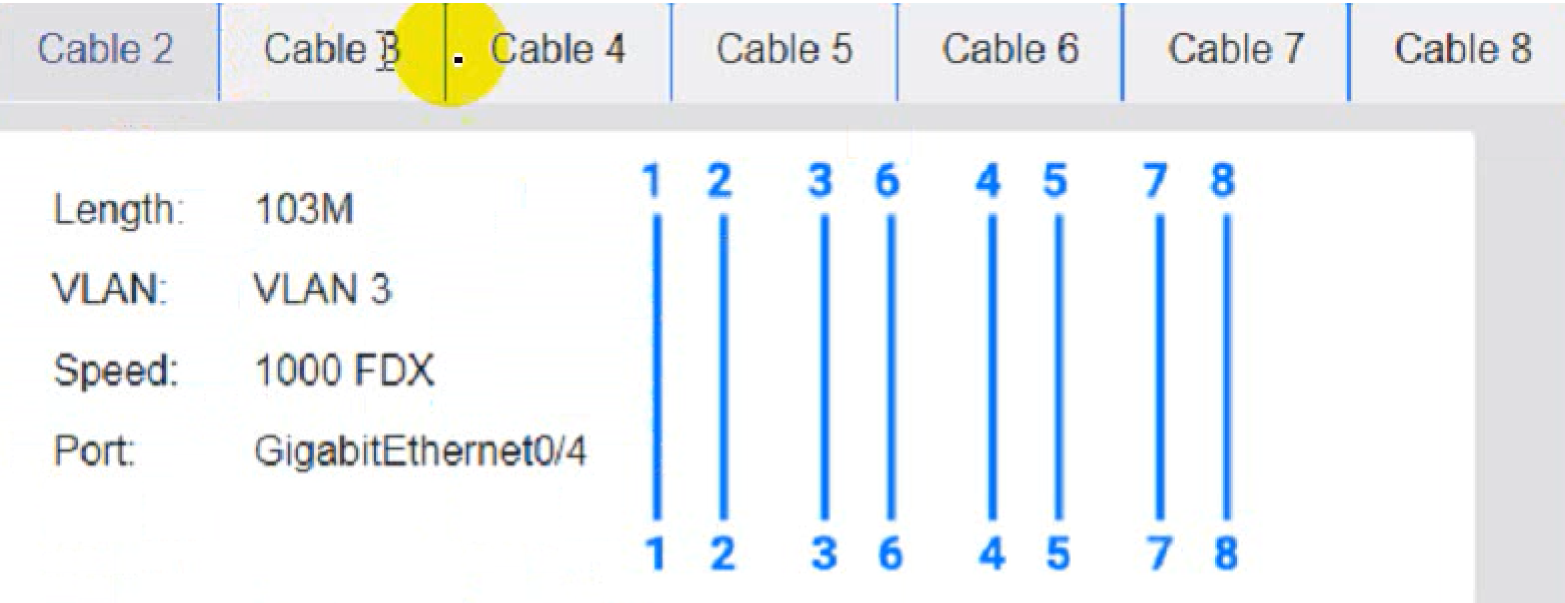
Length: 22M

VLAN: VLAN 2

Speed: 1000 FDX

Port: GigabitEthernet0/1

Cable 2:



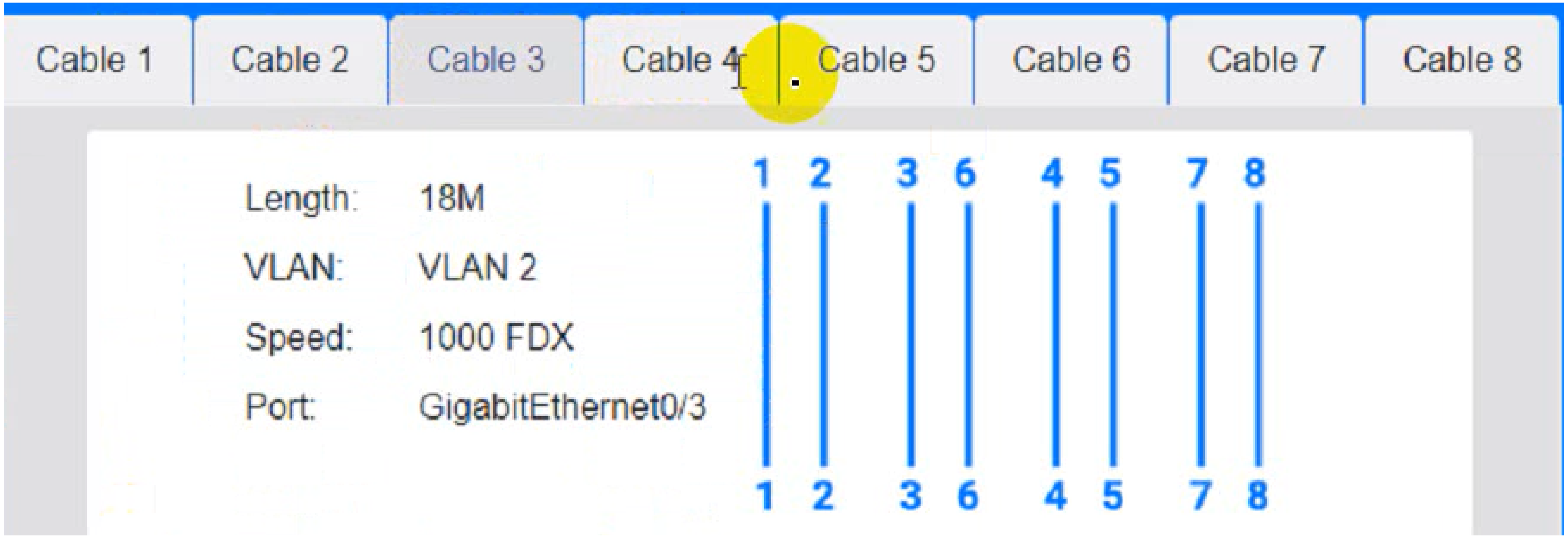
Length: 103M

VLAN: VLAN 3

Speed: 1000 FDX

Port: GigabitEthernet0/4

Cable 3:



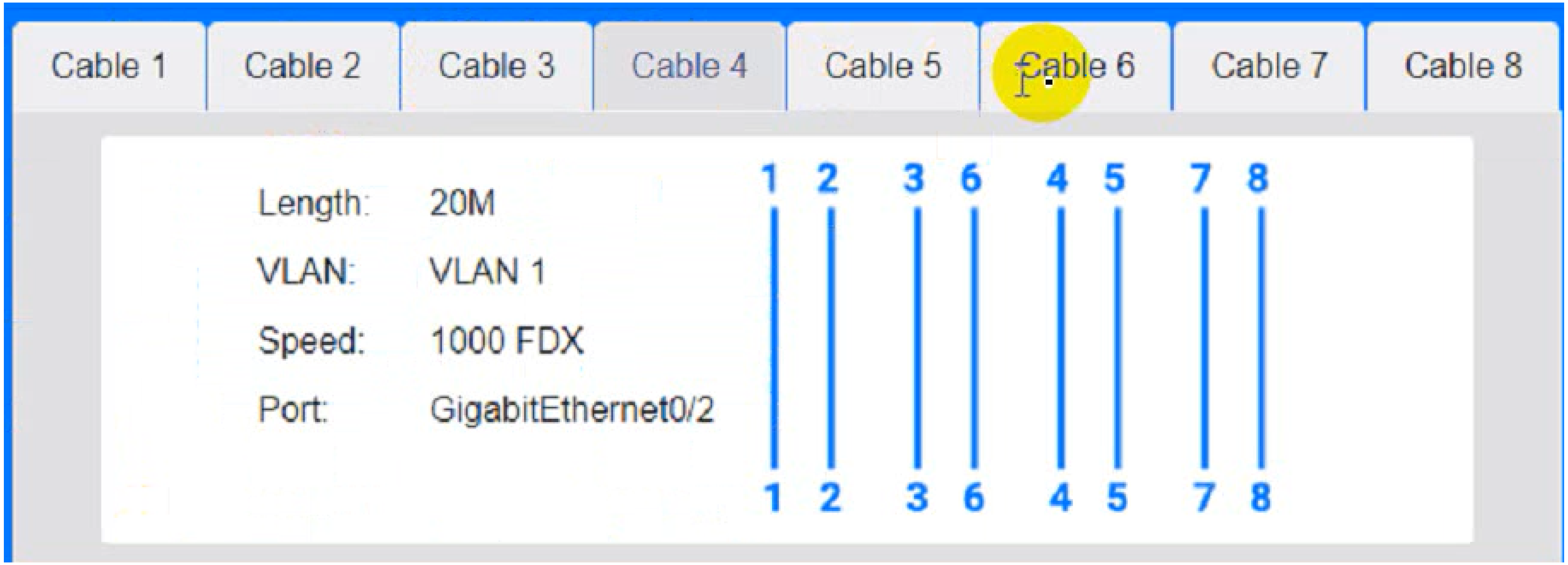
Length: 18M

VLAN: VLAN 2

Speed: 1000 FDX

Port: GigabitEthernet0/3

Cable 4:

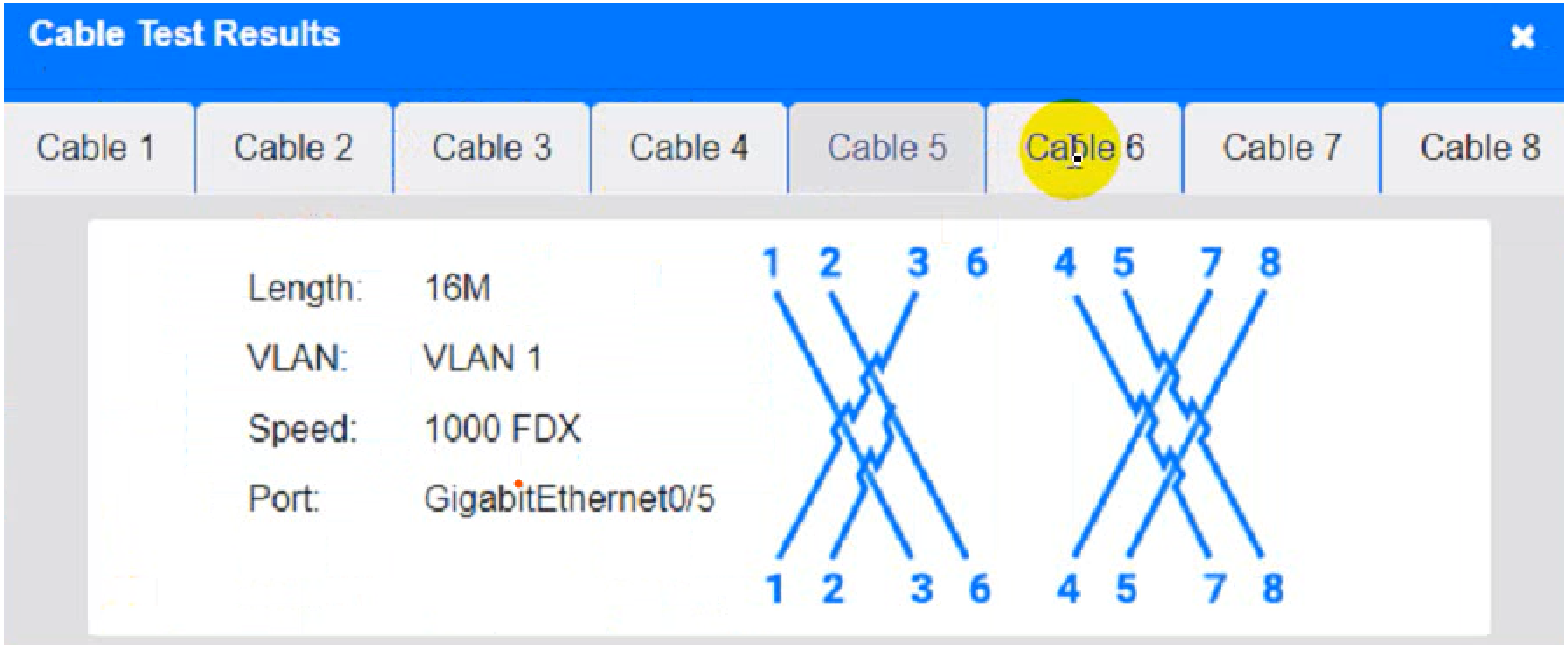


Length: 20M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/2

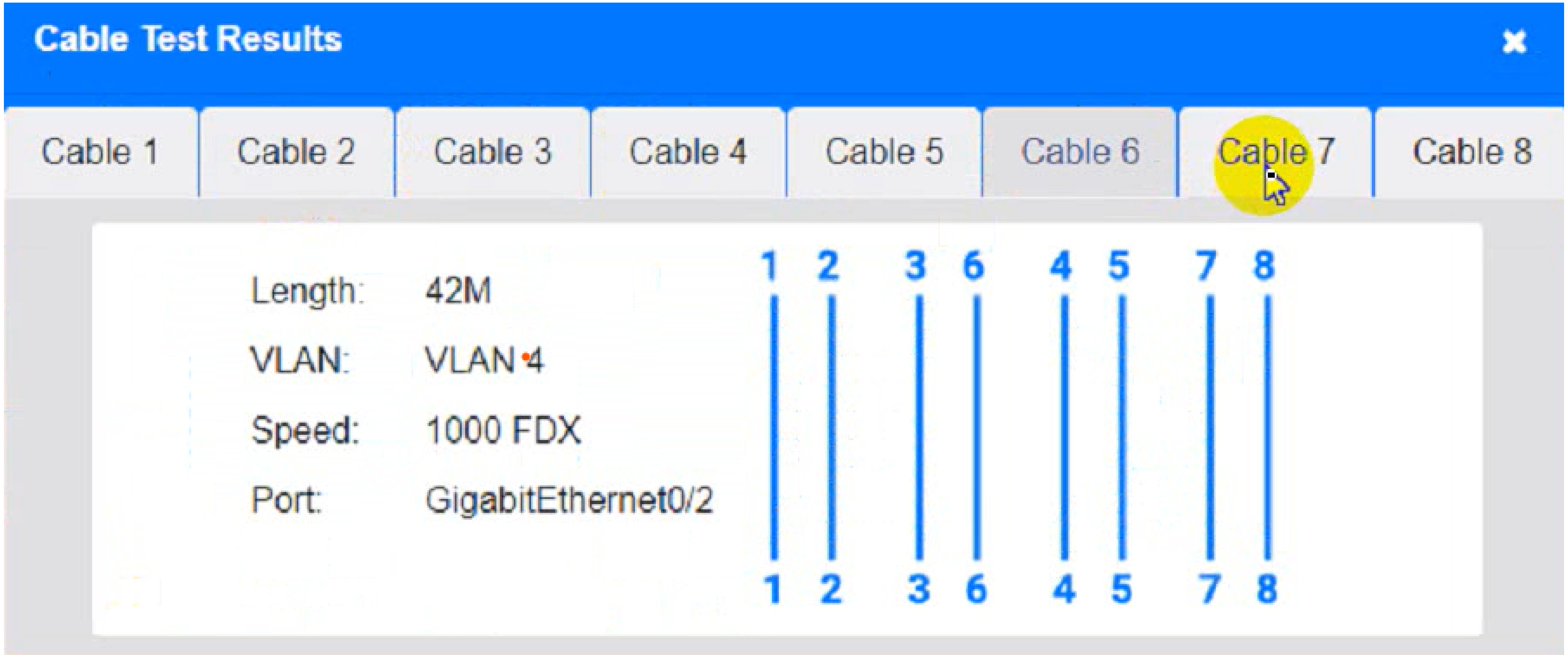


Length: 16M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/5

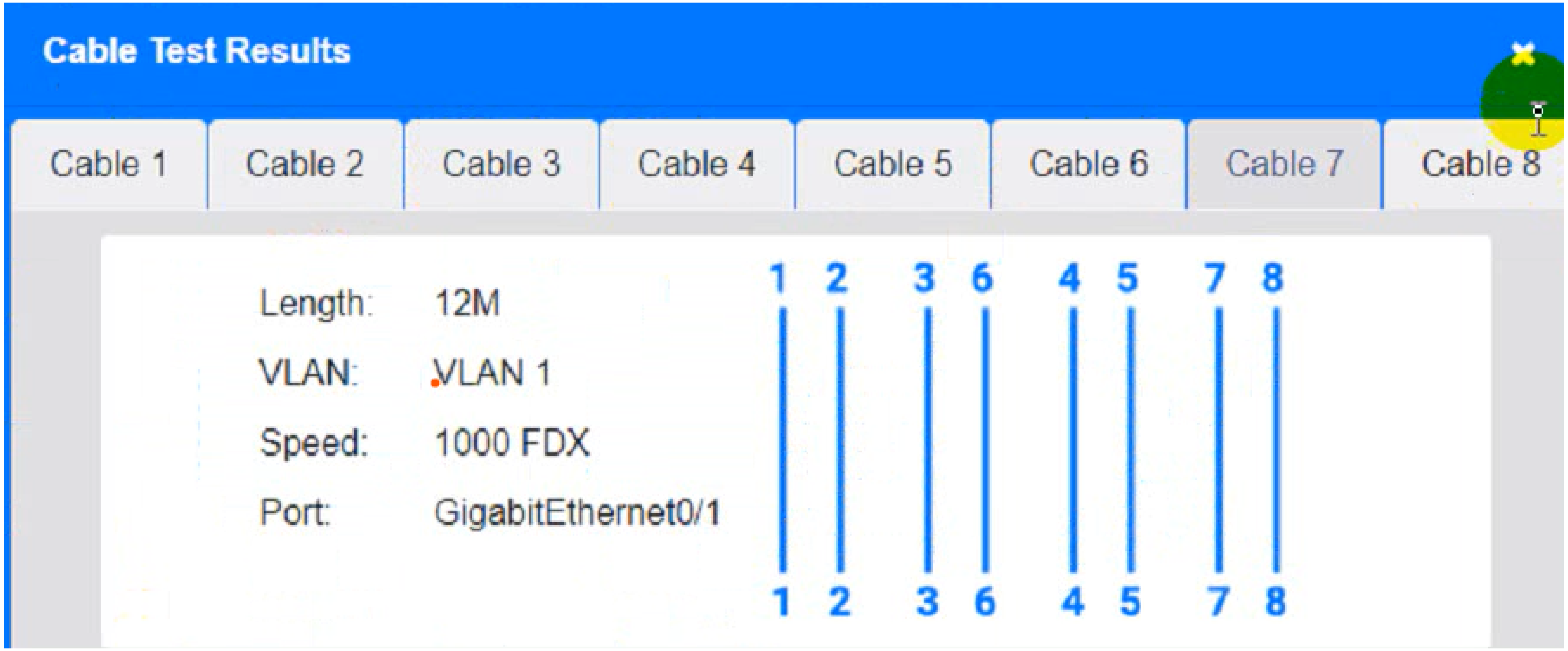


Length: 42M

VLAN: VLAN 4

Speed: 1000 FDX

Port: GigabitEthernet0/2

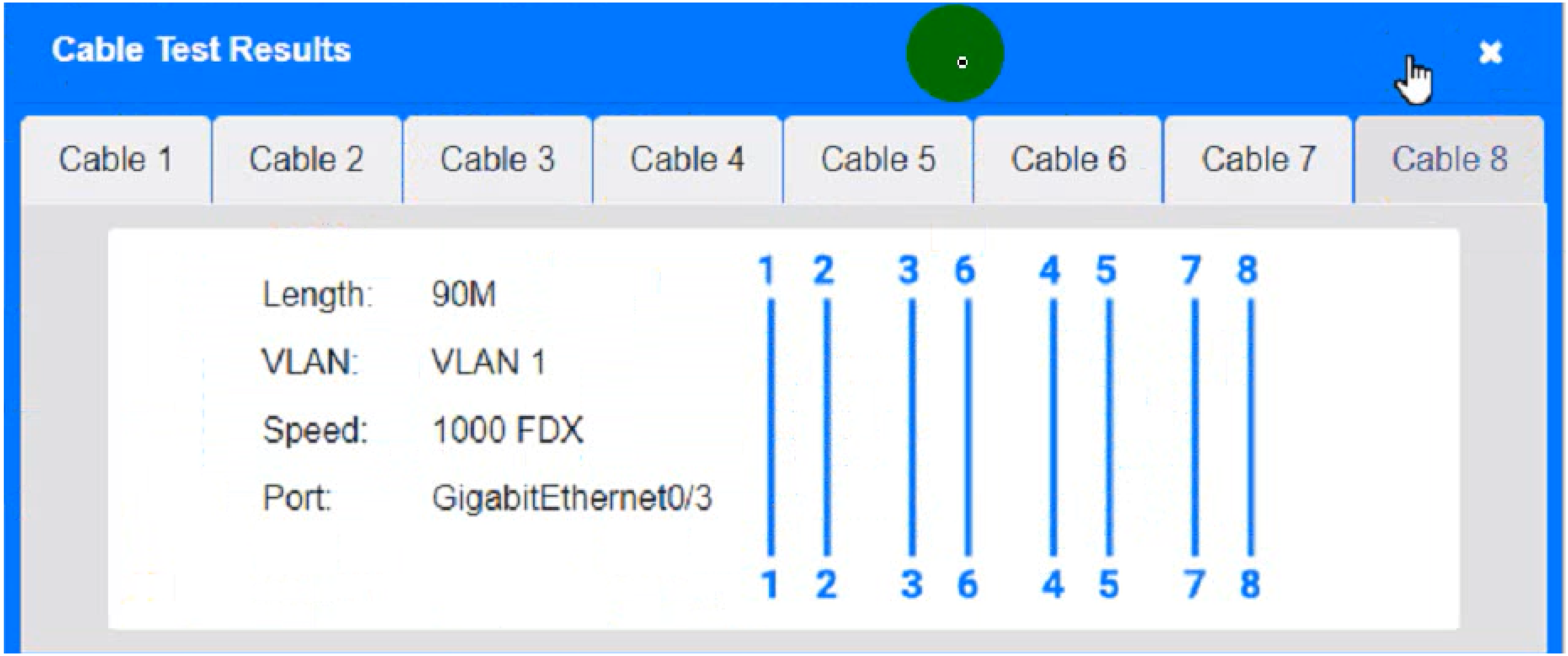


Length: 12M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/1

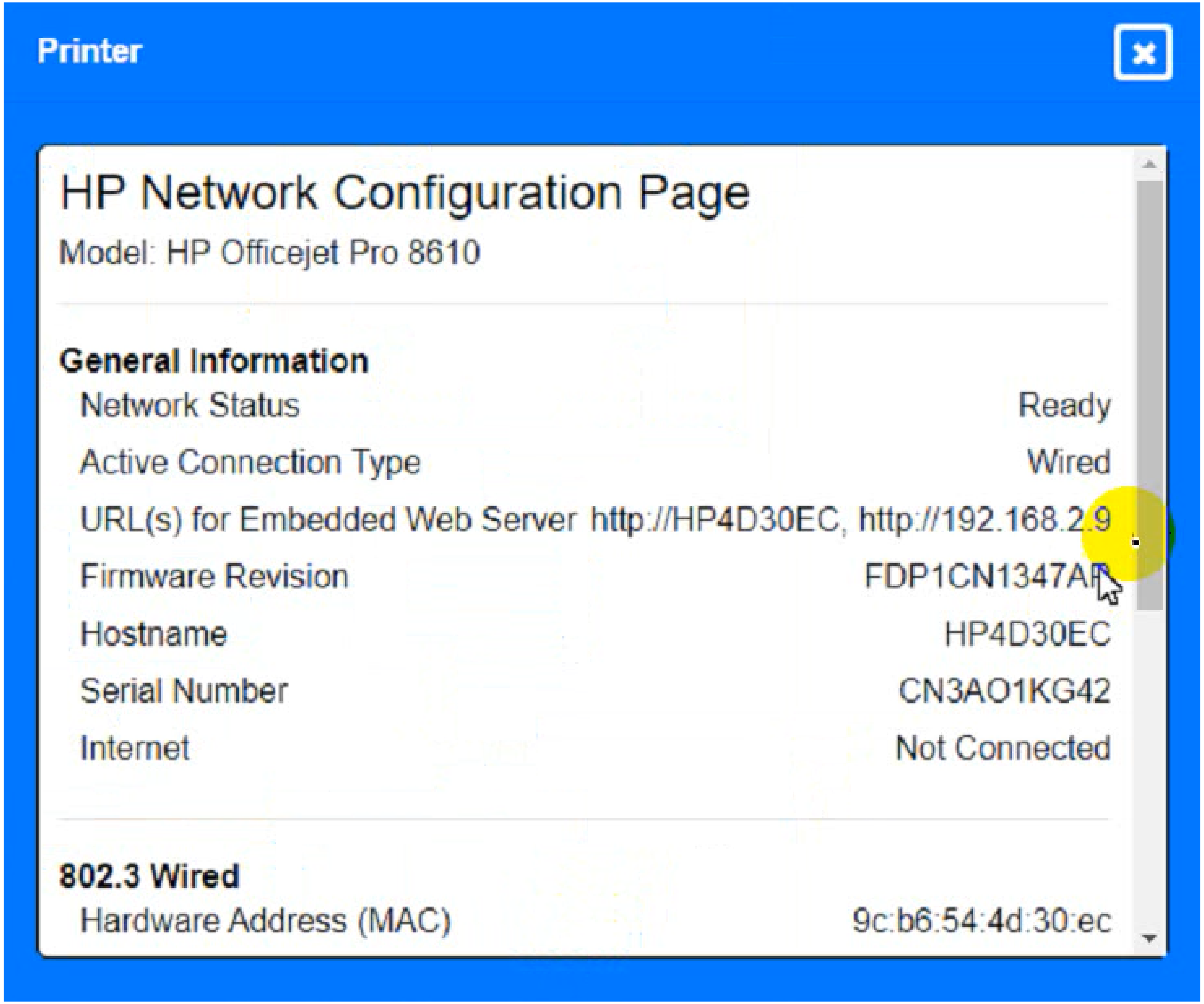


Length: 90M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/3



Printer

HP Network Configuration Page

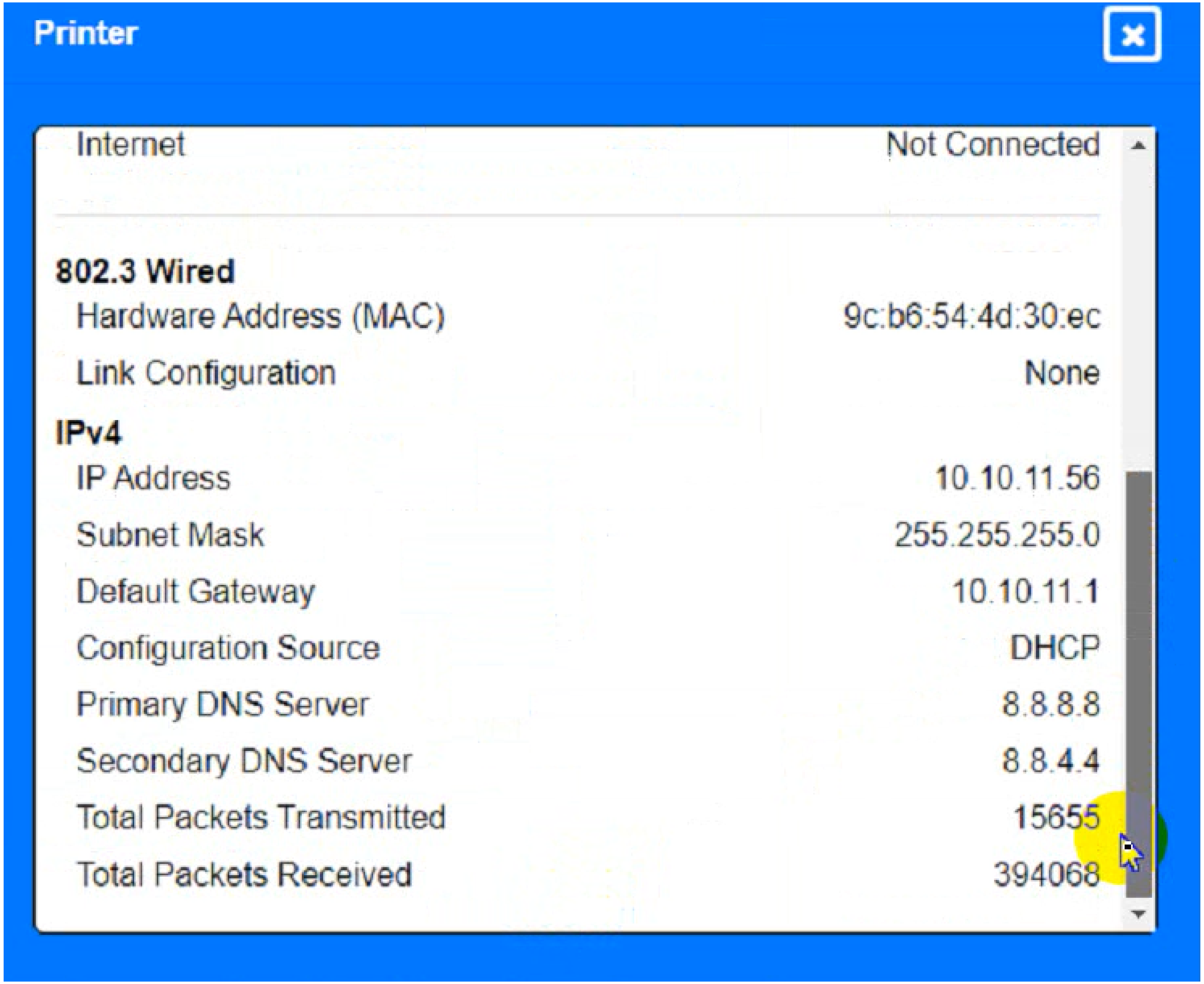
Model: HP Officejet Pro 8610

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



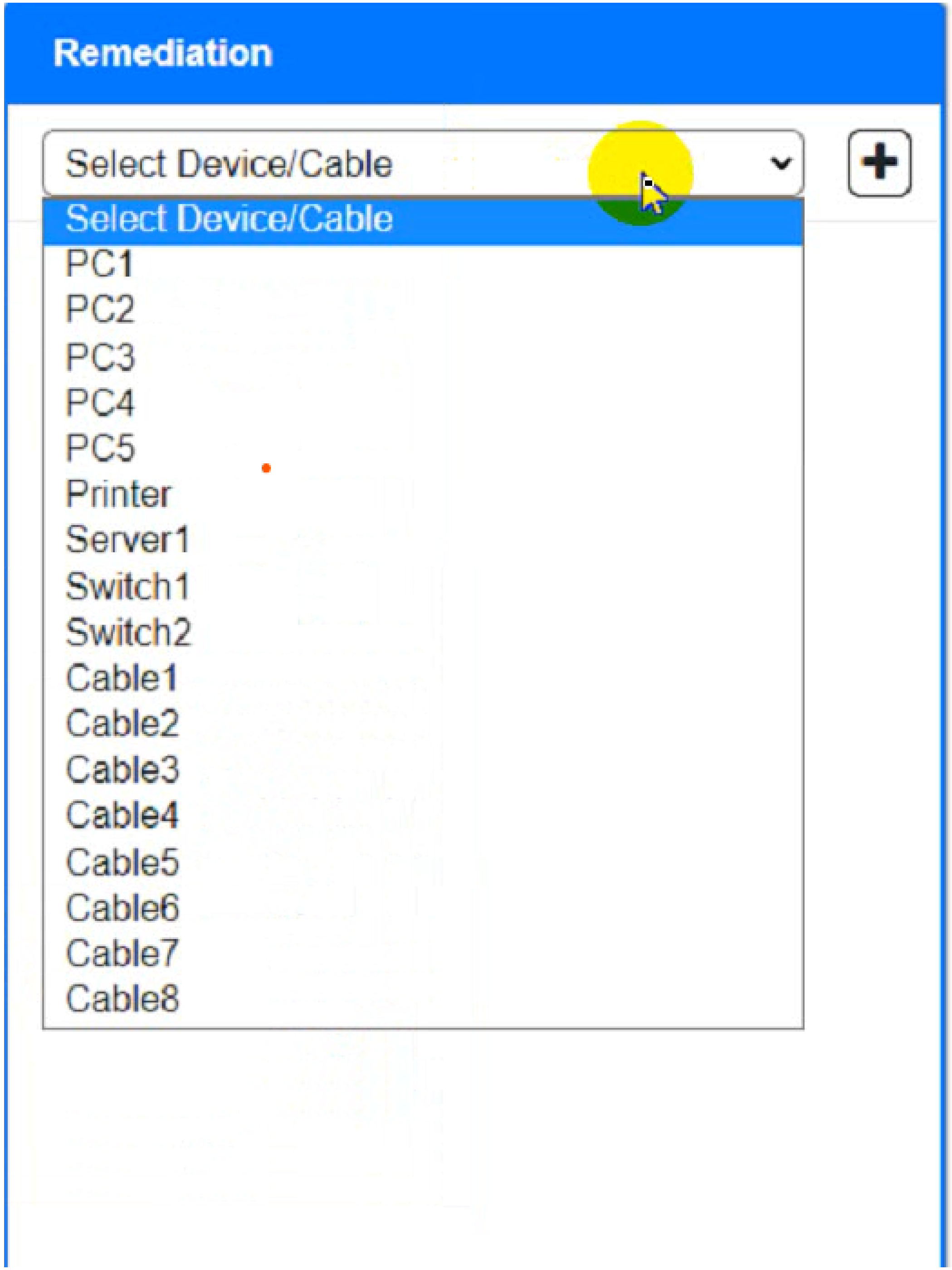
Internet	Not Connected

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

Remediation
Select Device/Cable
+
Select Device/Cable
PC1
PC2
PC3
PC4
PC5
Printer
Server1
Switch1
Switch2
Cable1
Cable2
Cable3
Cable4
Cable5
Cable6
Cable7
Cable8

Options:

A- See the Explanation for detailed information on this simulation

Answer:

A

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 11

Question Type: MultipleChoice

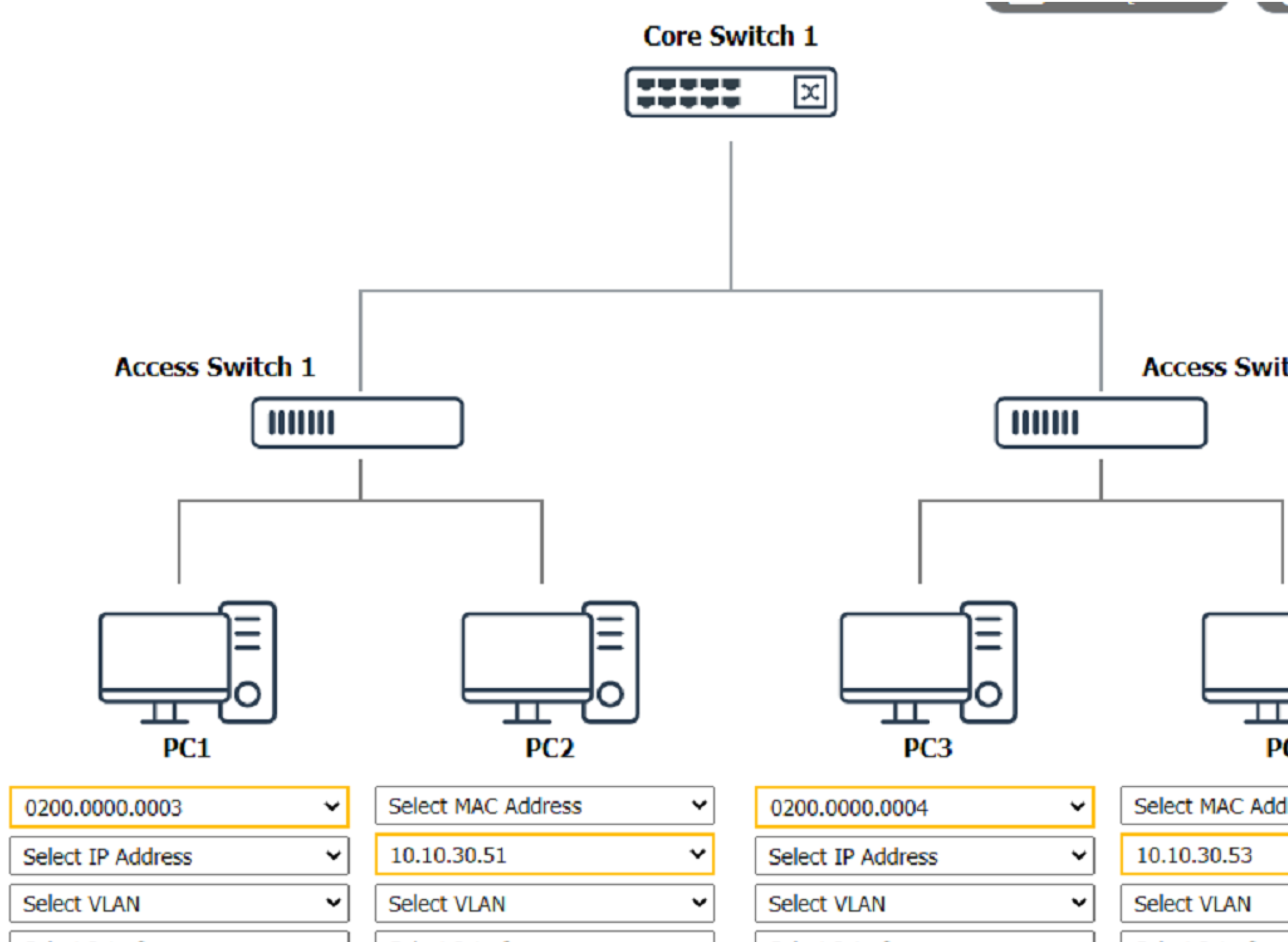
SIMULATION

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.

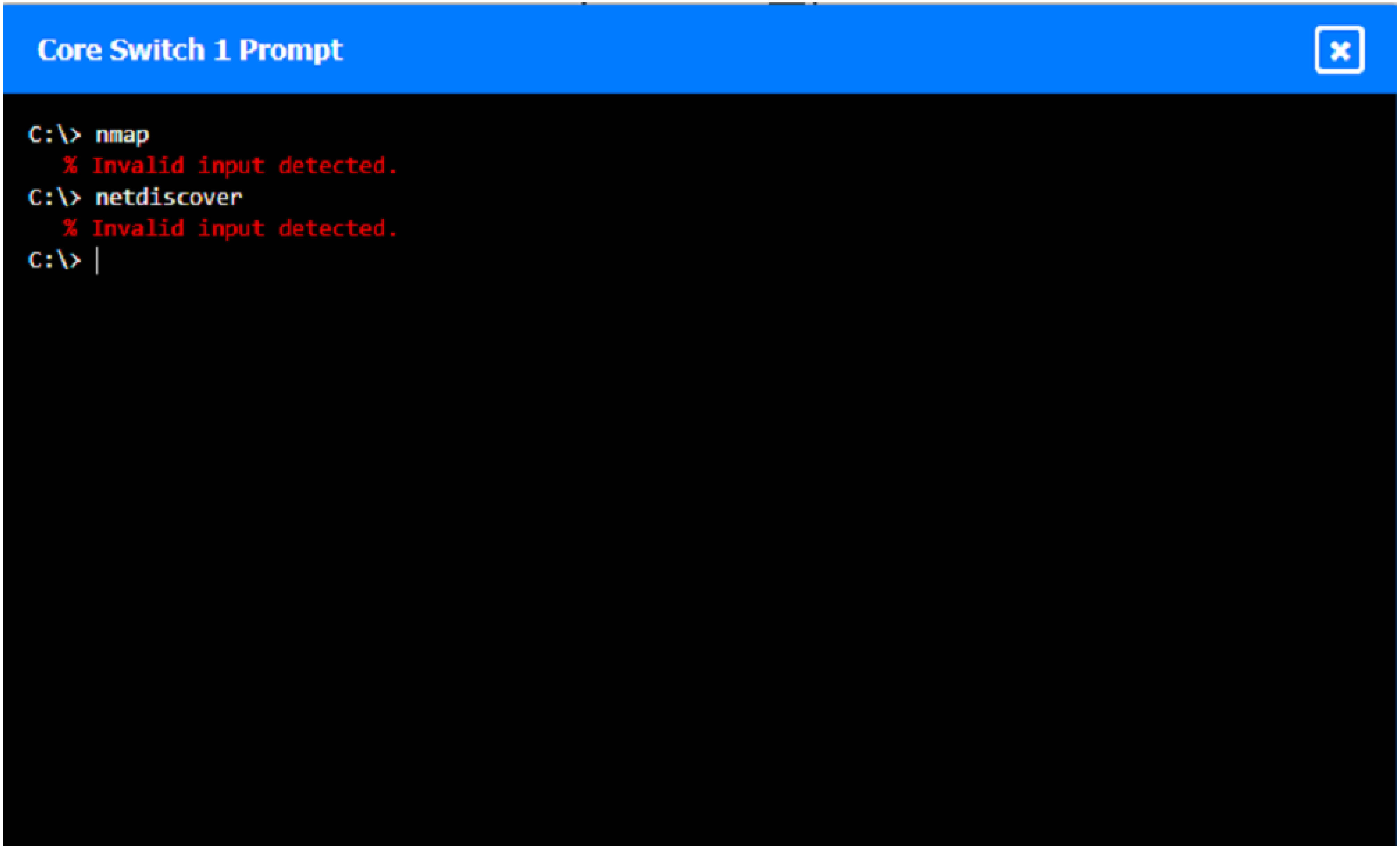


PC1
0200.0000.0003
Select IP Address
Select VLAN

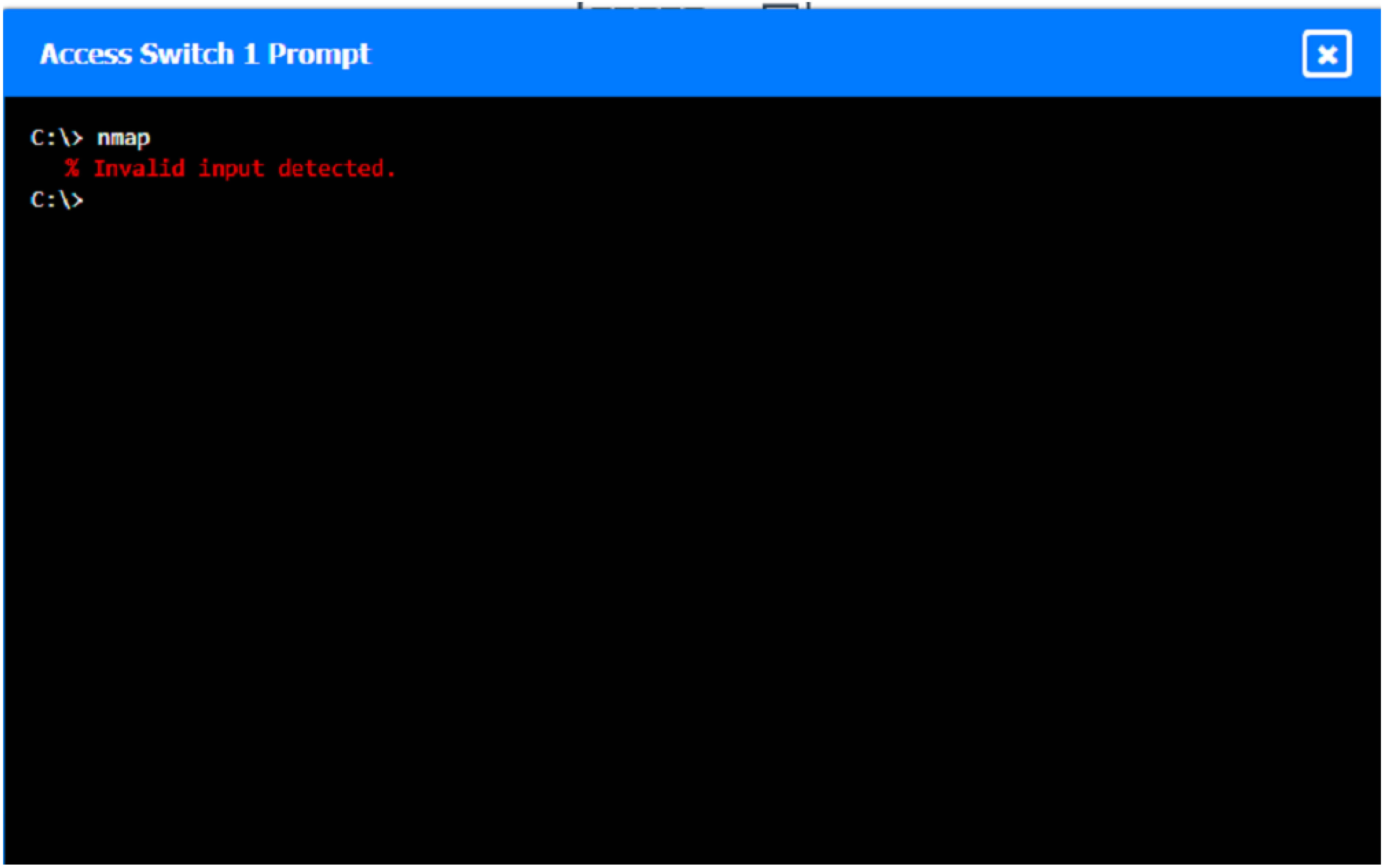
PC2
Select MAC Address
10.10.30.51
Select VLAN

PC3
0200.0000.0004
Select IP Address
Select VLAN

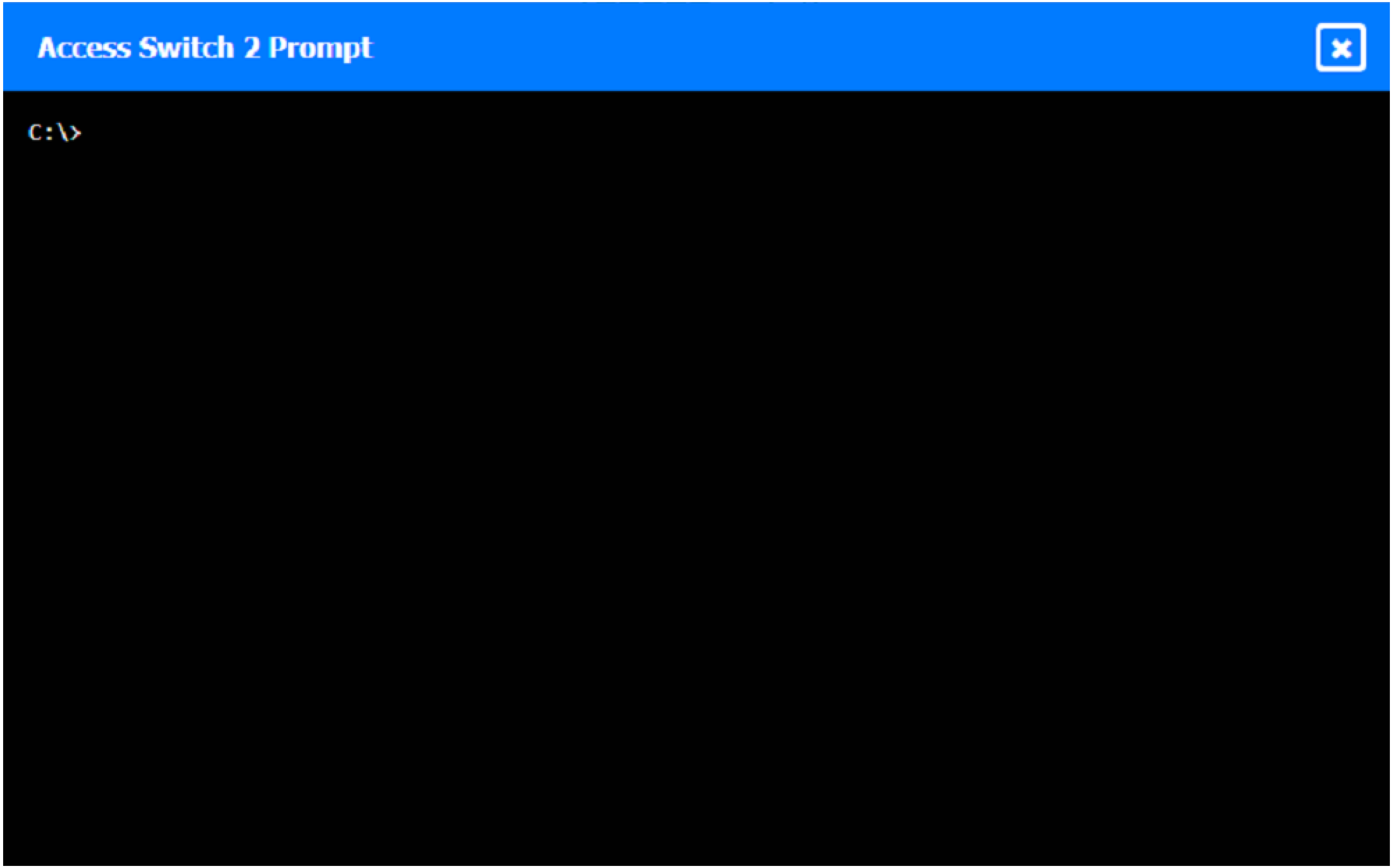
PC
Select MAC Add
10.10.30.53
Select VLAN



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



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



```
C:\>
```

Options:

A- See the Explanation for detailed information on this simulation

Answer:

A

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.