Free Questions for N10-009

Shared by Lyons on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- Port
B- DNS
C- MAC
D- Content

Answer:

D

Explanation:

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

Question 2

Question Type: MultipleChoice

Which of the following ports is used for secure email?

Options:

A- 25

B- 110
C- 143
D- 587

Answer:

D

Explanation:

Port 587 is used for secure email submission. This port is designated for message submission by mail clients to mail servers using the SMTP protocol, typically with STARTTLS for encryption.

Port 25: Traditionally used for SMTP relay, but not secure and often blocked by ISPs for outgoing mail due to spam concerns.

Port 110: Used for POP3 (Post Office Protocol version 3), not typically secured.

Port 143: Used for IMAP (Internet Message Access Protocol), which can be secured with STARTTLS or SSL/TLS.

Port 587: Specifically used for authenticated email submission (SMTP) with encryption, ensuring secure transmission of email from clients to servers.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses email protocols and ports, including secure email transmission.

Cisco Networking Academy: Provides training on securing email communications and the use of appropriate ports.

Network+ Certification All-in-One Exam Guide: Explains email protocols, ports, and security considerations for email transmission.

Question 3

Question Type: MultipleChoice

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

Options:

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

Answer:

B

Explanation:

Jumbo frames are Ethernet frames with a payload greater than the standard maximum transmission unit (MTU) of 1500 bytes. Configuring jumbo frames can reduce overhead and increase efficiency in storage networks by allowing more data to be sent in each frame, thus reducing the number of frames needed to transmit the same amount of data.

Reduced Overhead: By sending larger frames, the relative overhead for headers and acknowledgments is reduced.

Increased Efficiency: Larger frames mean fewer packets to process, leading to better utilization of network bandwidth and improved performance in high-throughput environments like storage networks.

Configuration: Requires support from all devices in the network path, including switches and network interface cards (NICs).

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Explains jumbo frames and their benefits in reducing network overhead.

Cisco Networking Academy: Provides training on network optimization techniques, including the use of jumbo frames.

Network+ Certification All-in-One Exam Guide: Covers advanced Ethernet features, including jumbo frames and their configuration for improved network performance.

Question 4

Question Type: MultipleChoice

Which of the following facilities is the best example of a warm site in the event of information

system disruption?

Options:

A- A combination of public and private cloud services to restore data
B- A partial infrastructure, software, and data on site
C- A full electrical infrastructure in place, but no customer devices on site
D- A full infrastructure in place, but no current data on site

Answer:

D

Explanation:

A warm site typically has a full infrastructure ready, but it lacks the most up-to-date data or is not immediately operational. It requires some configuration or data restoration to become fully functional.

Question 5

Question Type: MultipleChoice

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?

Options:

A- Update the network ACLs.
B- Place the device in a screened subnet.
C- Enable content filtering.
D- Change the default admin passwords.

Answer:

D

Explanation:

Changing default admin passwords is a fundamental first step in device hardening to prevent unauthorized access.

Question 6

Question Type: MultipleChoice

Following a fire in a data center, the cabling was replaced. Soon after, an administrator notices network issues. Which of the following are the most likely causes of the network issues? (Select two).

Options:

A- The switches are not the correct voltage.
B- The HVAC system was not verified as fully functional after the fire.
C- The VLAN database was not deleted before the equipment was brought back online.
D- The RJ45 cables were replaced with unshielded cables.
E- The wrong transceiver type was used for the new termination.
F- The new RJ45 cables are a higher category than the old ones.

Answer:

D, E

Explanation:

Unshielded cables (D) are more prone to interference and may not be suitable for certain environments, especially after a fire where interference could be heightened.

Using the wrong transceiver (E) for new terminations can lead to compatibility issues, causing network failures.

Question 7

Question Type: MultipleChoice

SIMULATION

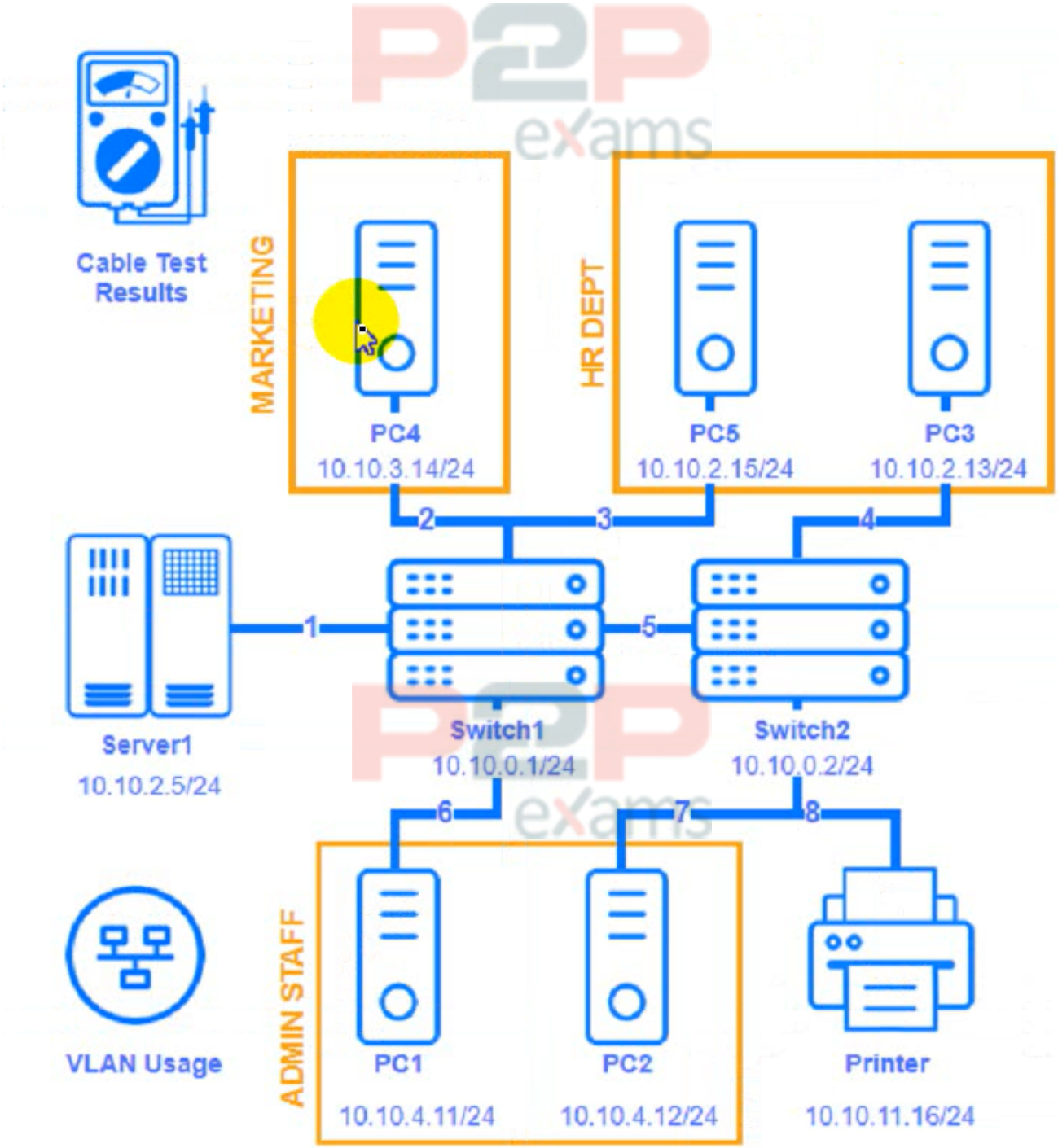
A network technician needs to resolve some issues with a customer's SOHO network.

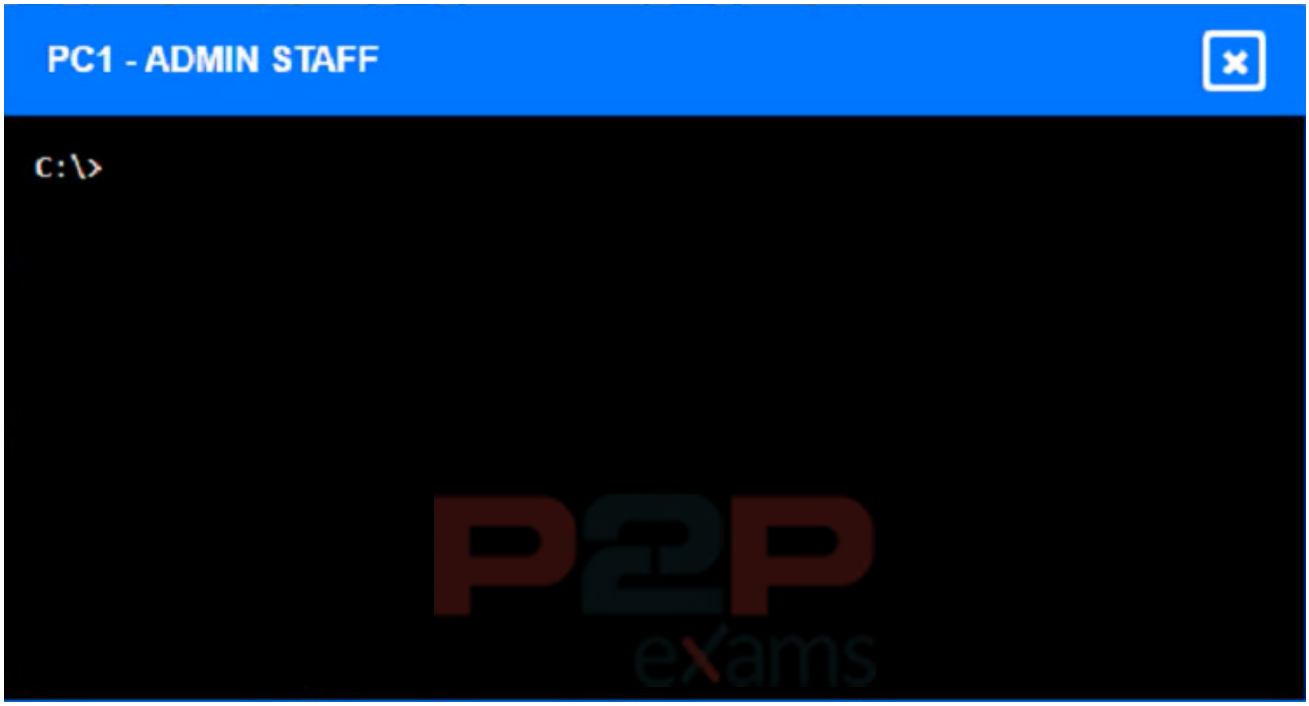
The customer reports that some of the devices are not connecting to the network, while others appear to work as intended.

INSTRUCTIONS

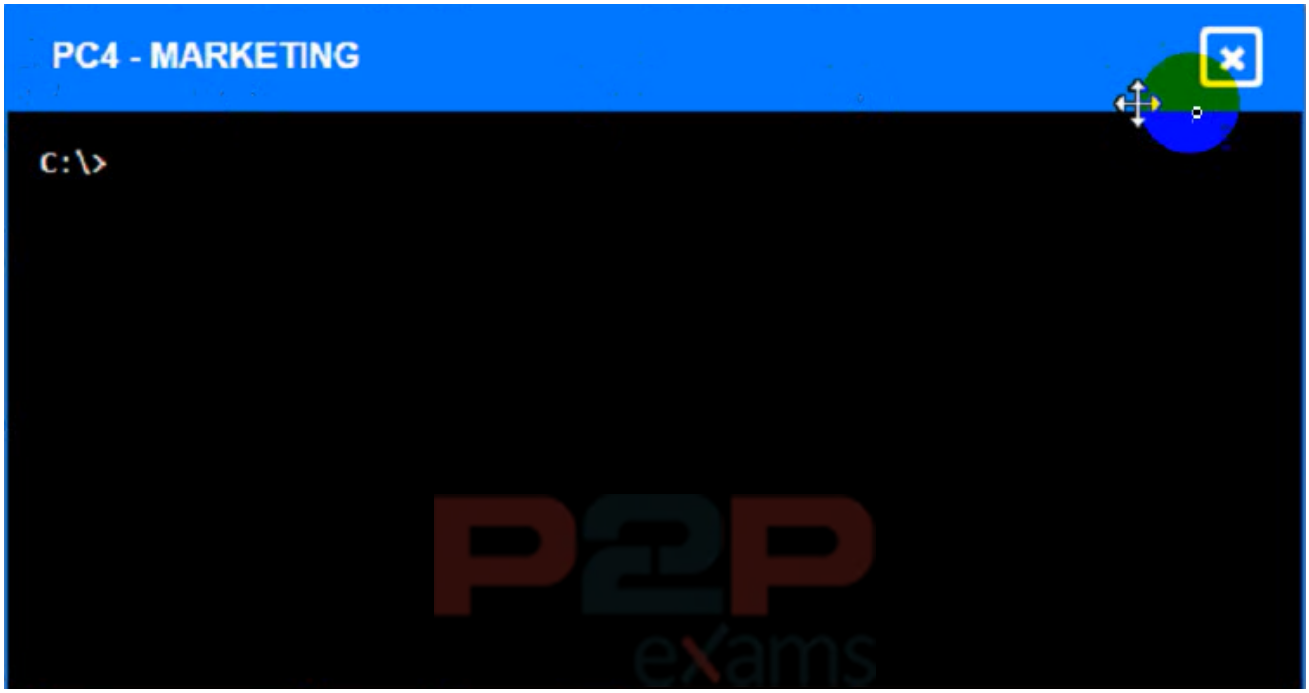
Troubleshoot all the network components and review the cable test results by Clicking on each device and cable.

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




PC1 - ADMIN STAFF
C:\>

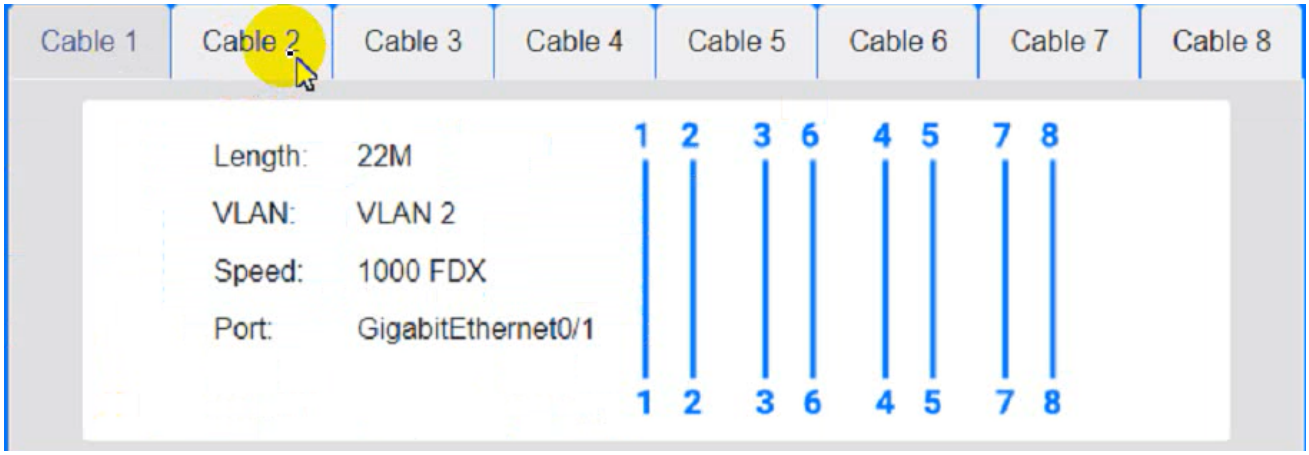

PC3 - HR DEPT
C:\>


PC4 - MARKETING
C:\>

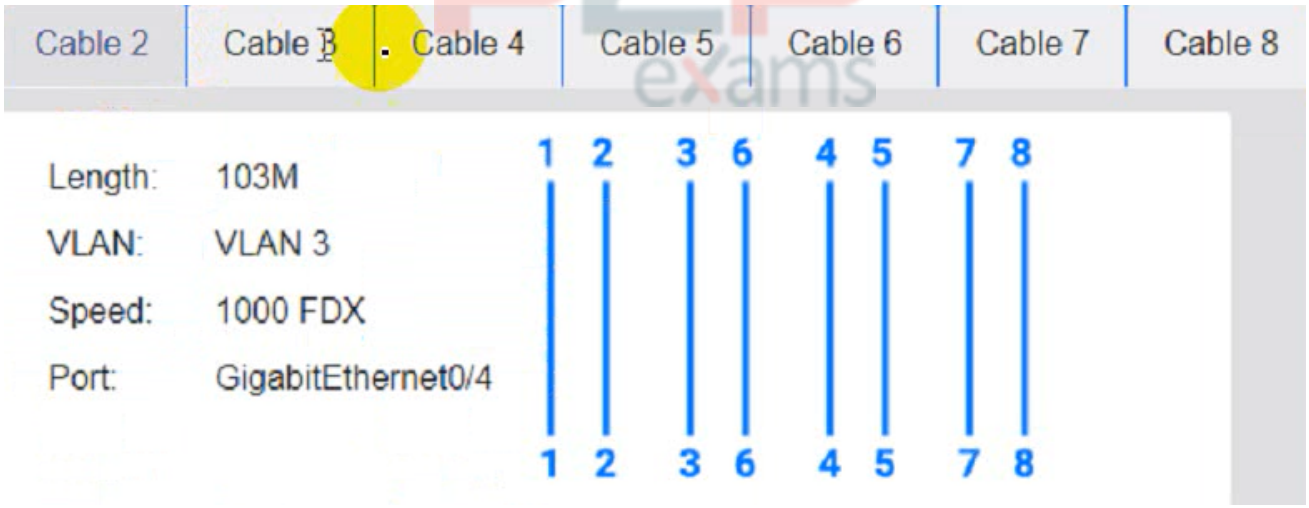

PC5 - HR DEPT
C:\>

Cable Test Results:

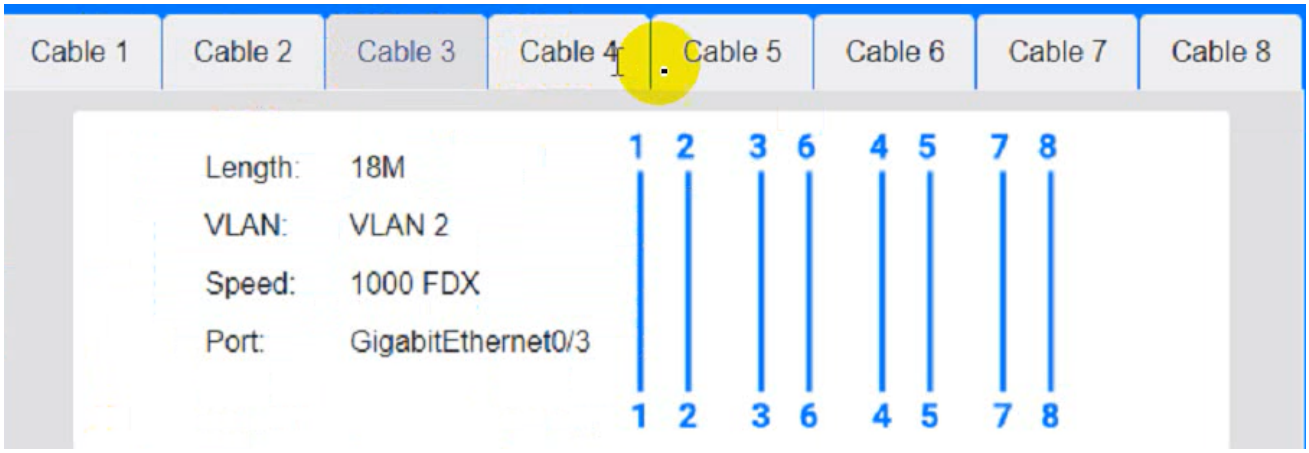
Cable 1:



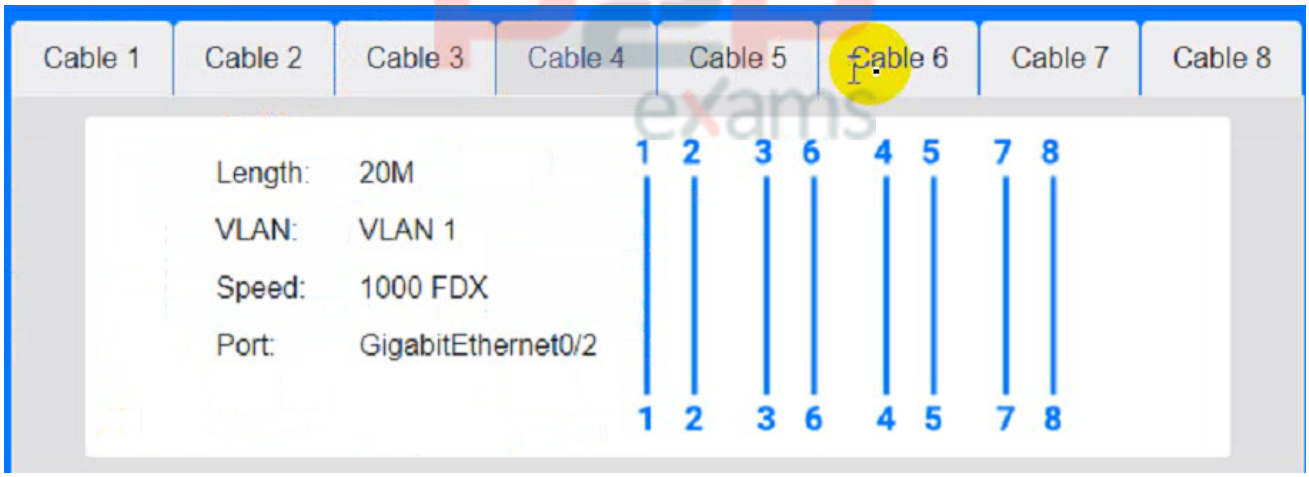
Cable 2:

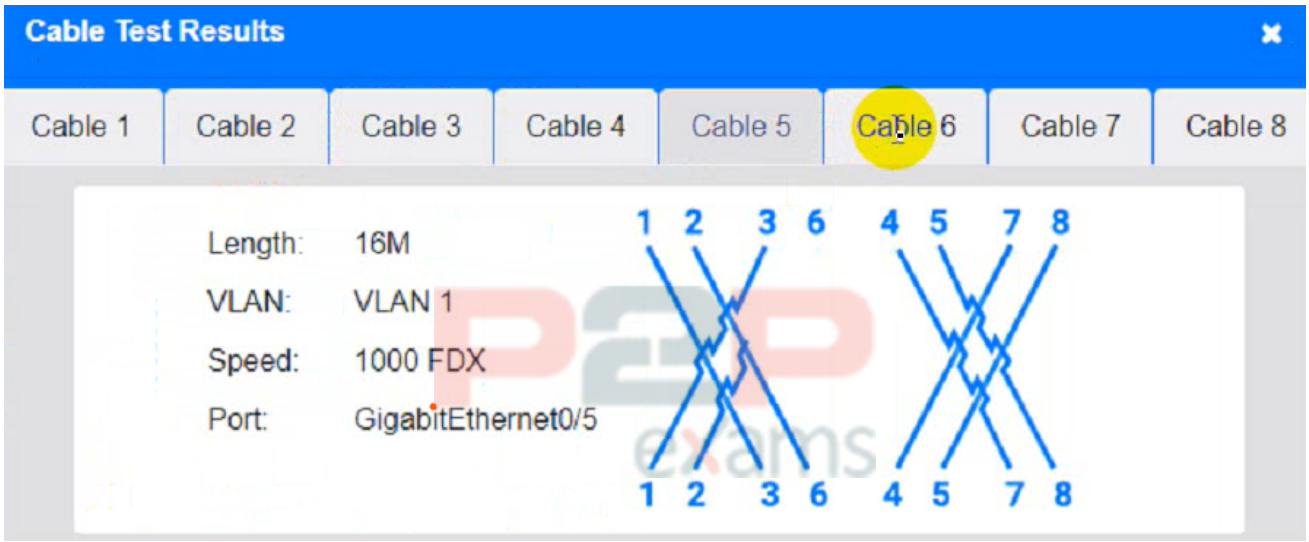


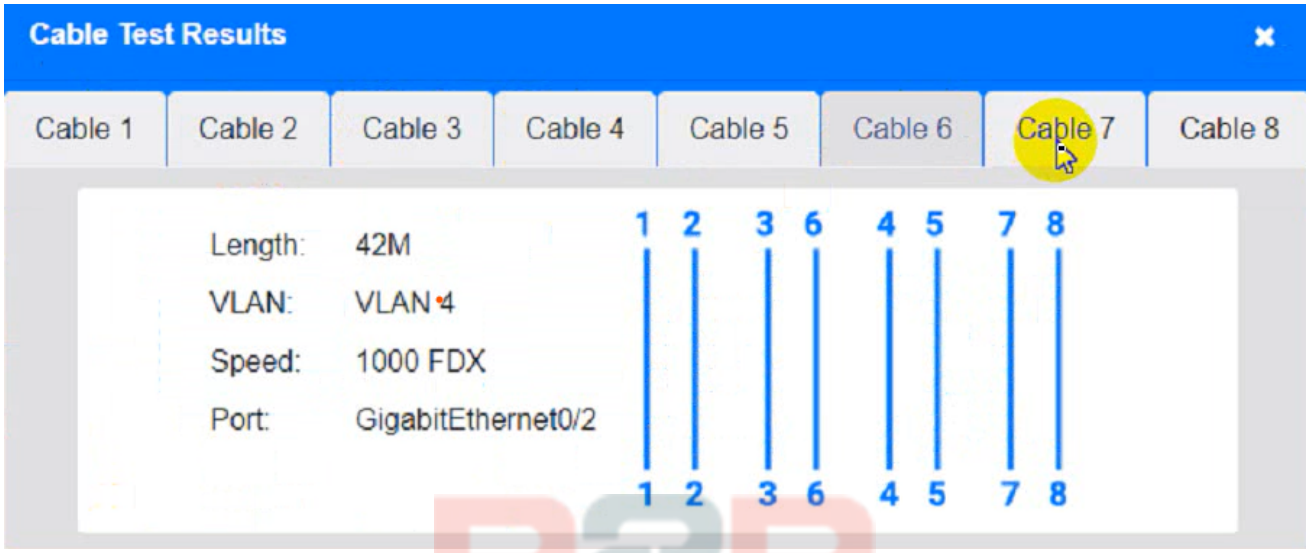
Cable 3:

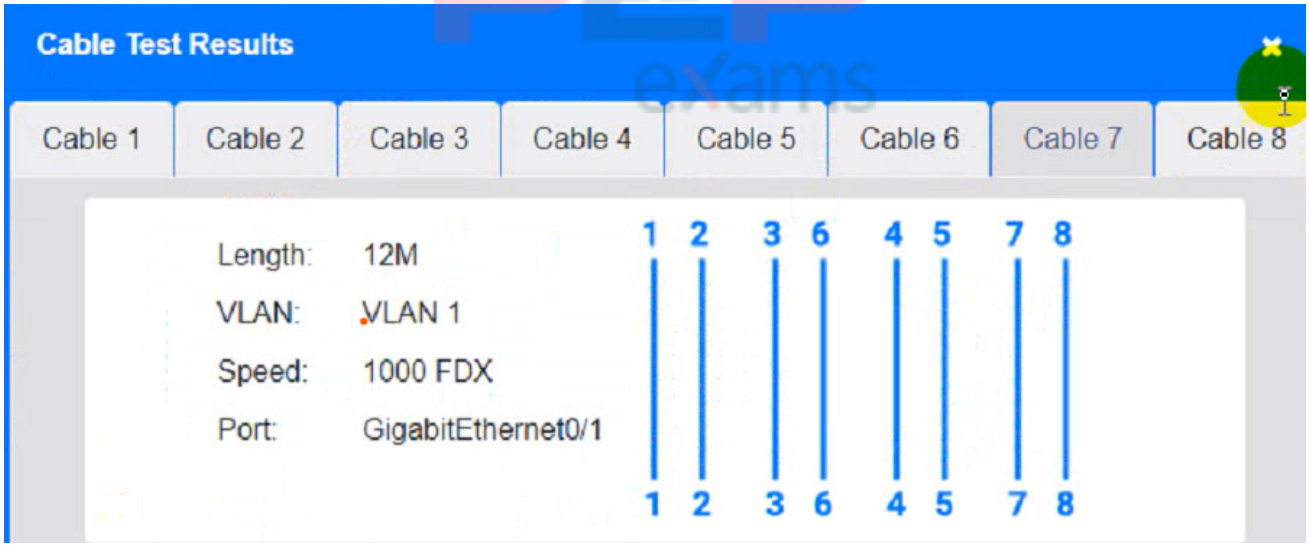

Cable 1
Cable 2
Cable 3
Cable 4
Cable 5
Cable 6
Cable 7
Cable 8
Length: 18M
VLAN: VLAN 2
Speed: 1000 FDX
Port: GigabitEthernet0/3
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

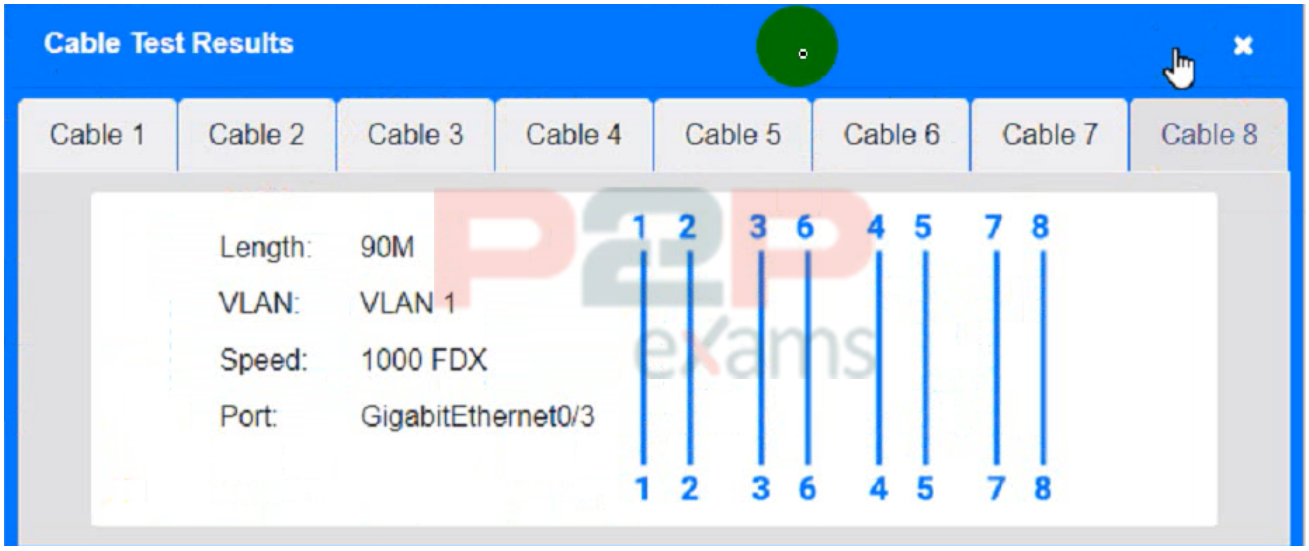
Cable 4:

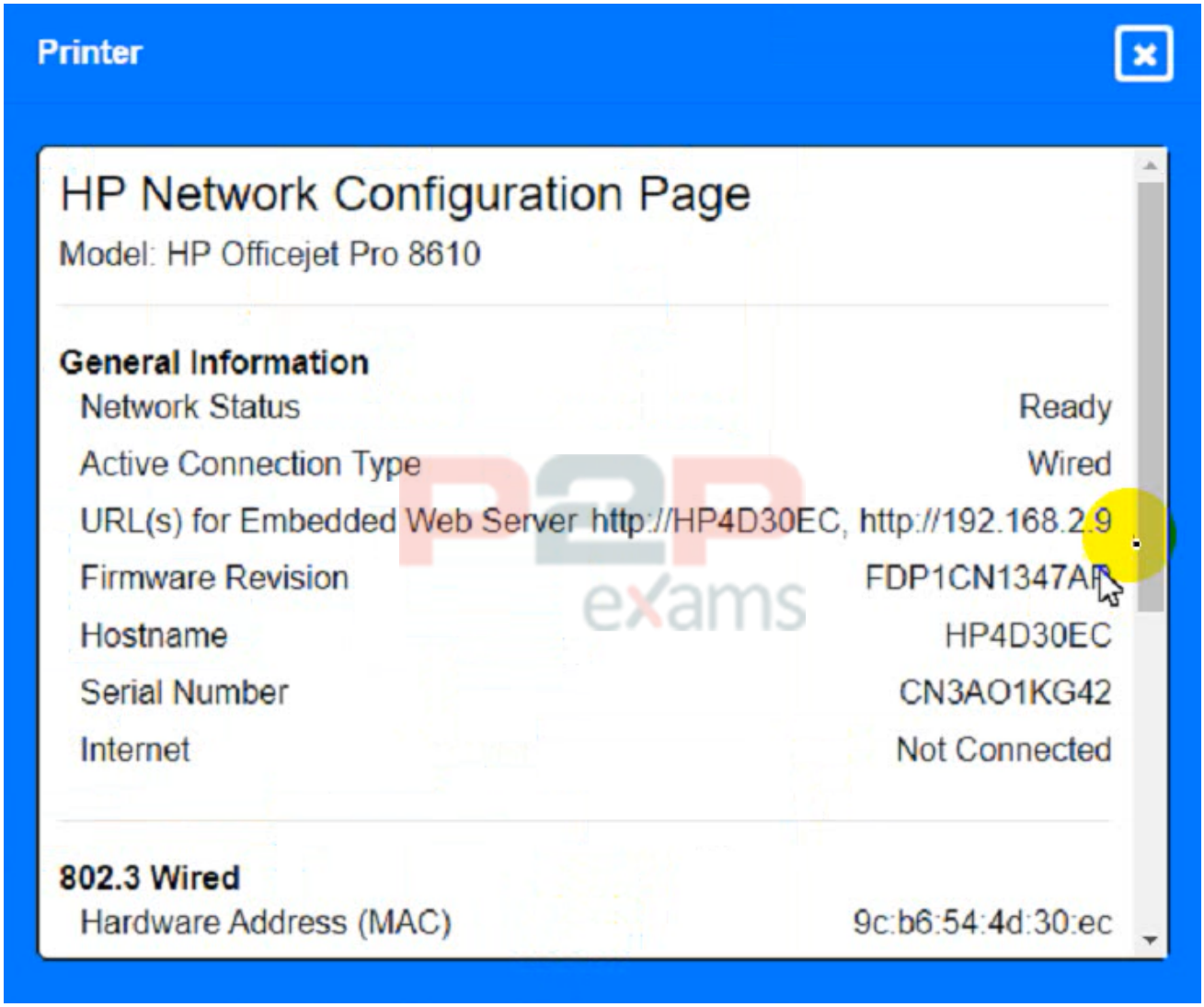

Cable 1
Cable 2
Cable 3
Cable 4
Cable 5
Cable 6
Cable 7
Cable 8
Length: 20M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/2
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

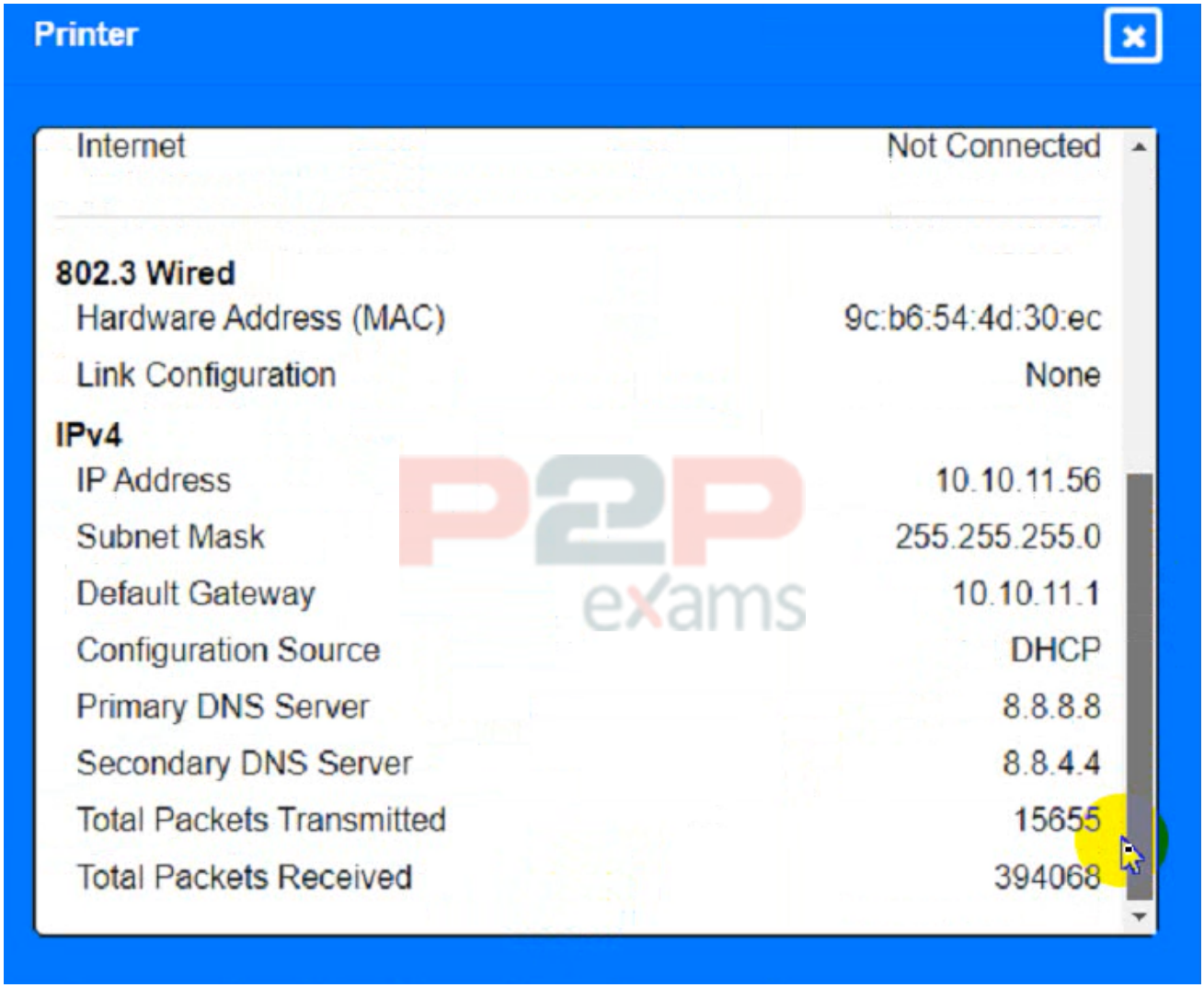

Cable Test Results
Cable 1
Cable 2
Cable 3
Cable 4
Cable 5
Cable 6
Cable 7
Cable 8
Length: 16M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/5
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8

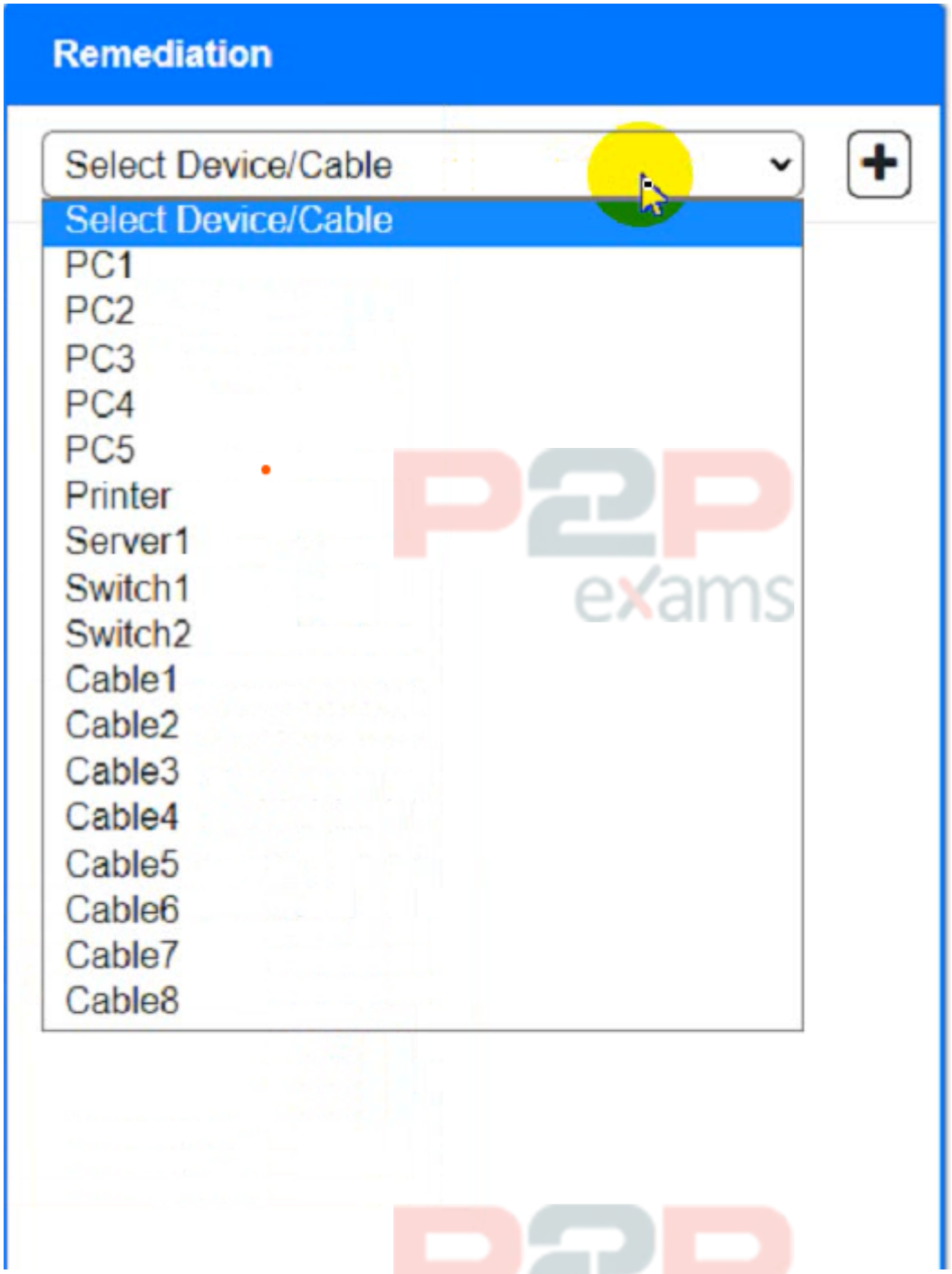

Cable Test Results
Cable 1
Cable 2
Cable 3
Cable 4
Cable 5
Cable 6
Cable 7
Cable 8
Length: 42M
VLAN: VLAN 4
Speed: 1000 FDX
Port: GigabitEthernet0/2
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8


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


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


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


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



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 8

Question Type: MultipleChoice

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

Options:

A- Too much wireless reflection
B- Too much wireless absorption
C- Too many wireless repeaters
D- Too many client connections

Answer:

A

Explanation:

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

Question 9

Question Type: MultipleChoice

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

Options:

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

Answer:

C

Explanation:

An access point (AP) provides users with an extended footprint that allows connections from multiple devices within a designated Wireless Local Area Network (WLAN).

Router: Typically used to connect different networks, not specifically for extending wireless coverage.

Switch: Used to connect devices within a wired network, not for providing wireless access.

Access Point (AP): Extends wireless network coverage, allowing multiple wireless devices to connect to the network.

Firewall: Primarily used for network security, controlling incoming and outgoing traffic based on security rules, not for providing wireless connectivity.

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Explains the roles and functions of network appliances, including access points.

Cisco Networking Academy: Provides training on deploying and managing wireless networks with access points.

Network+ Certification All-in-One Exam Guide: Covers network devices and their roles in creating and managing networks.

Question 10

Question Type: MultipleChoice

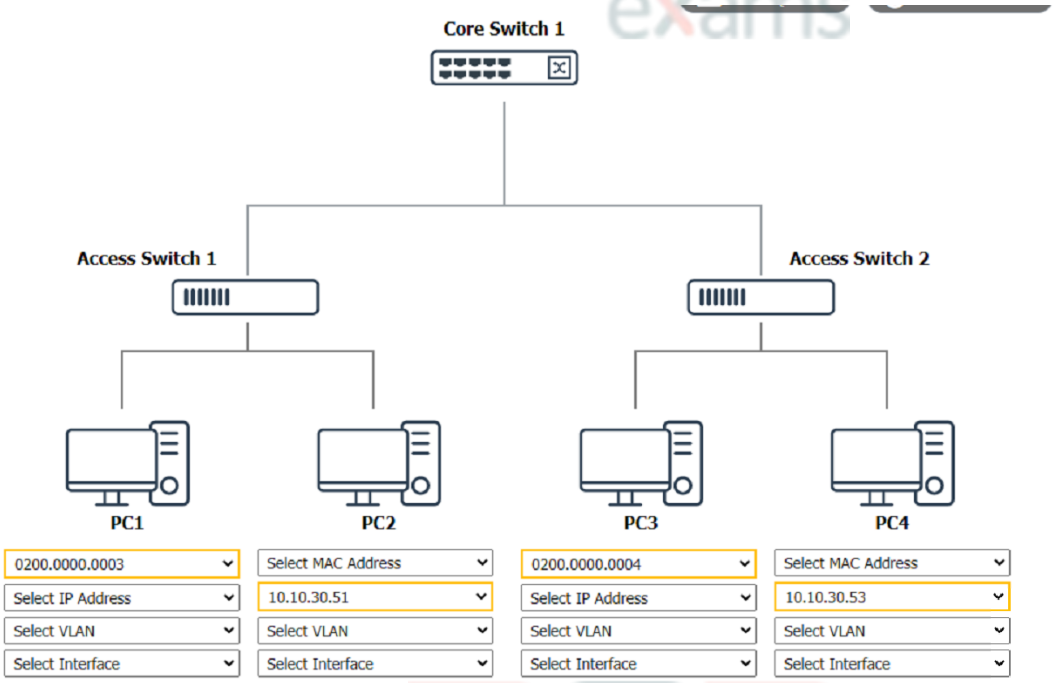
SIMULATION

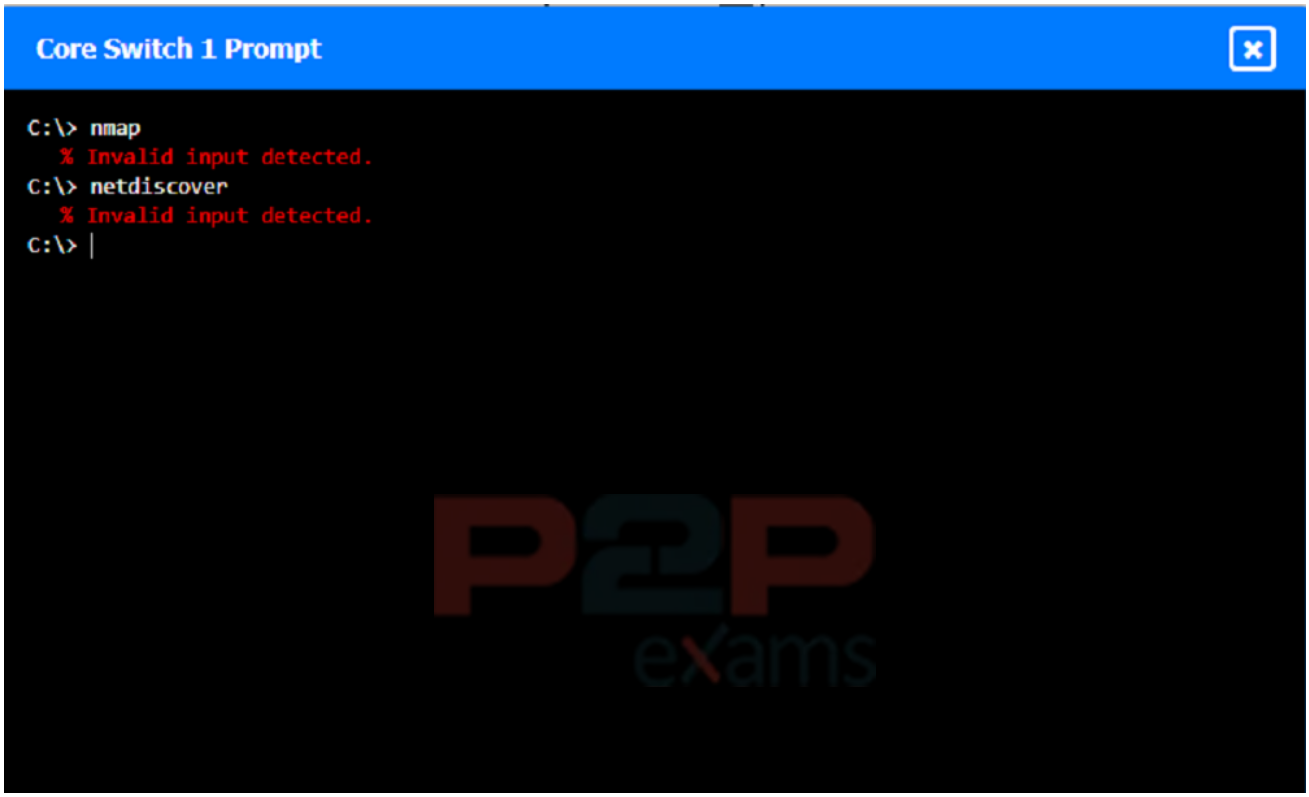
A network technician was recently onboarded to a company. A manager has

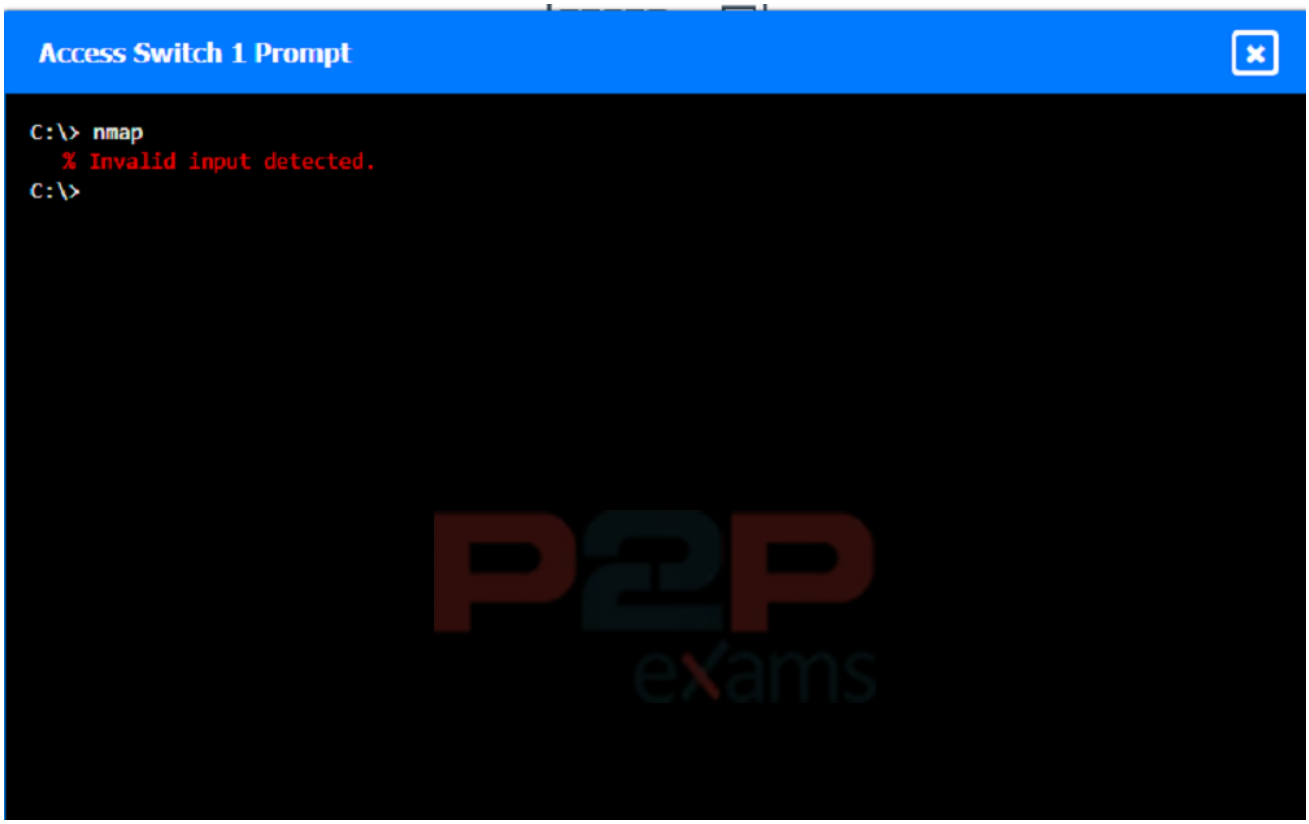
tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.

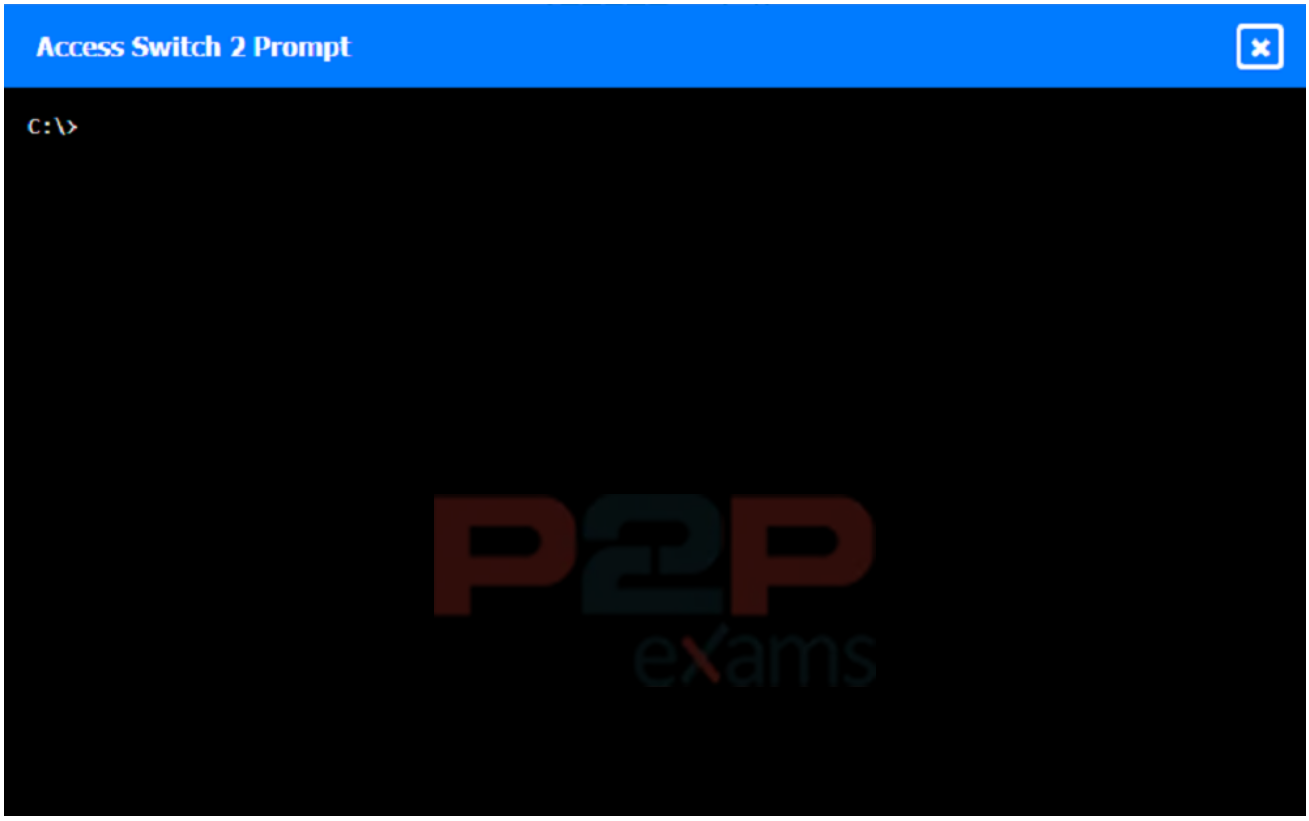
Instructions:

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.




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


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



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.

Question 11

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.

P2P exams