Vendor: Cisco

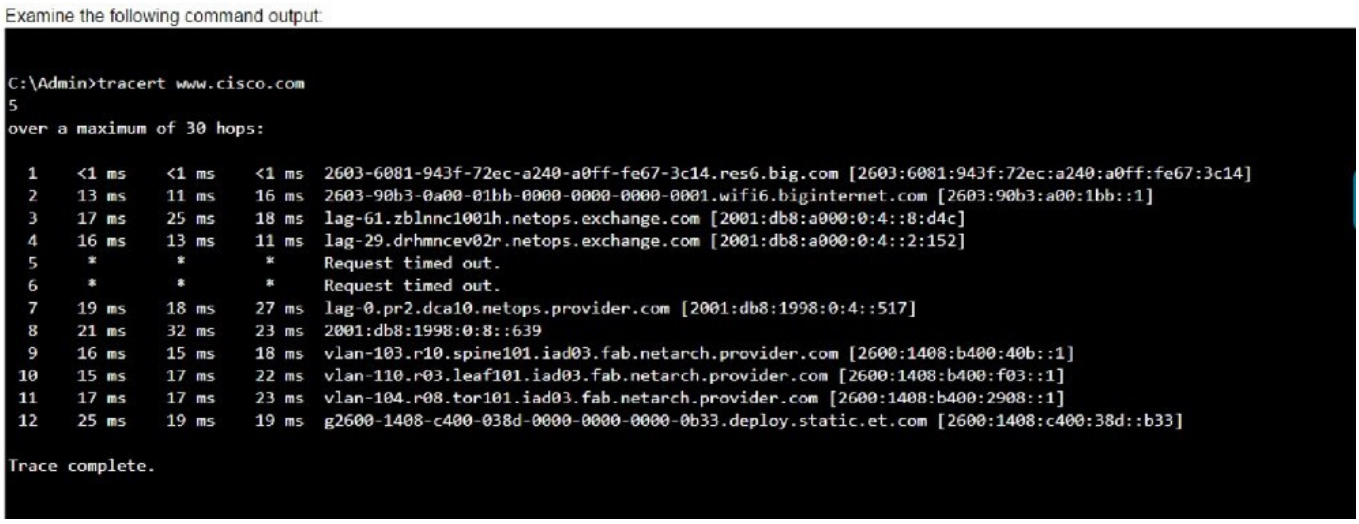
Exam Code:CCST-NETWORKING

Exam Name: Cisco Certified Support Technician (CCST) NetworkingExam

Version: Demo

QUESTION 1

Examine the following output:



Which two conclusions can you make from the output of the tracert command? (Choose 2.)

Note: You will receive partial credit for each correct answer.

A. The trace successfully reached the www.cisco.com server.

B. The trace failed after the fourth hop.

C. The IPv6 address associated with the www.cisco.com server is 2600:1408: c400: 38d: : b33.

D. The routers at hops 5 and 6 are offline.

E. The device sending the trace has IPv6 address 2600:1408:c400:38d :: b33.

Correct Answer: AC

-Statement A: "The trace successfully reached the www.cisco.com server." This is true as indicated by the "Trace complete" message at the end, showing that the trace has reached its destination. -Statement C: "The IPv6 address associated

with the www.cisco.com server is 2600:1408:c400:38d::b33." This is true because the final hop in the trace, which is the destination, has this IPv6 address.

-Statement B: "The trace failed after the fourth hop." This is incorrect as the trace continues beyond the fourth hop, despite some intermediate timeouts. -Statement D: "The routers at hops 5 and 6 are offline." This is not necessarily true. The

routers might be configured to not respond to traceroute requests.

-Statement E: "The device sending the trace has IPv6 address 2600:1408:c400:38d::b33."

This is incorrect; this address belongs to the destination server, not the sender.

References:

-Understanding Traceroute: Traceroute Guide

QUESTION 2

A local company requires two networks in two new buildings. The addresses used in these networksmust be in the private network range.

Which two address ranges should the company use? (Choose 2.)

Note: You will receive partial credit for each correct selection.

A. 172.16.0.0 to 172.31.255.255

B. 192.16.0.0 to 192.16.255.255

C. 11.0.0.0 to 11.255.255.255

D. 192.168.0.0 to 192.168.255.255

Correct Answer: AD

The private IP address ranges that are set aside specifically for use within private networks and not routable on the internet are as follows: Class A: 10.0.0.0 to 10.255.255.255 Class B: 172.16.0.0 to 172.31.255.255 Class C: 192.168.0.0 to 192.168.255.255 These ranges are defined by the Internet Assigned Numbers Authority (IANA) and are used for local communications within a private network123. Given the options: A.172.16.0.0 to 172.31.255.255falls within the Class B private range. B.

192.16.0.0 to 192.16.255.255is not a recognized private IP range. C.11.0.0.0 to 11.255.255.255is not a recognized private IP range. D.192.168.0.0 to 192.168.255.255 falls within the Class C private range.

Therefore, the correct selections that the company should use for their private networks are AandD.

References:

Reserved IP addresses on Wikipedia

Private IP Addresses in Networking - GeeksforGeeks Understanding Private IP Ranges, Uses, Benefits, and Warnings

---

QUESTION 3

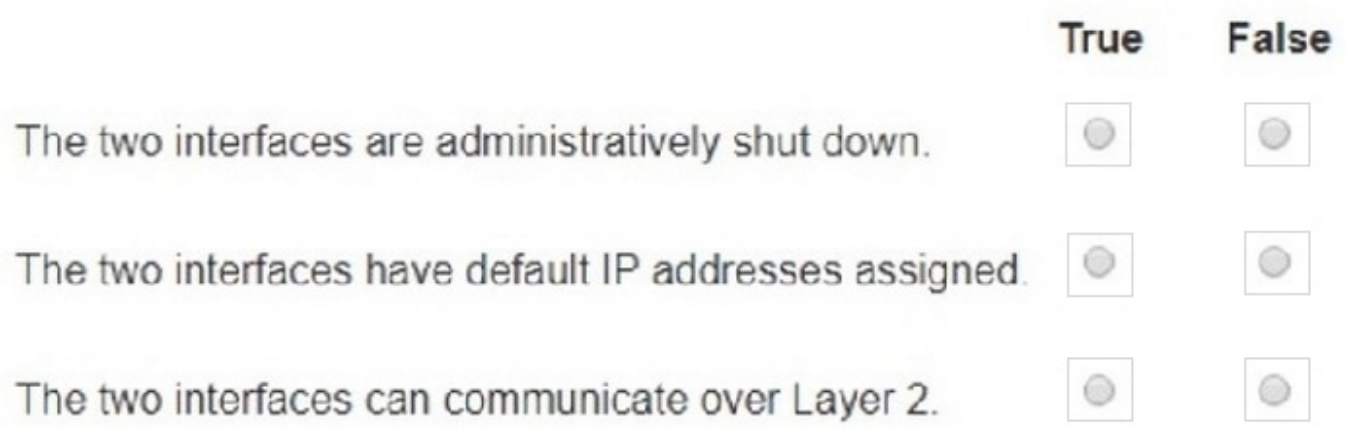
HOTSPOT

You purchase a new Cisco switch, turn it on, and connect to its console port. You then run the following command:

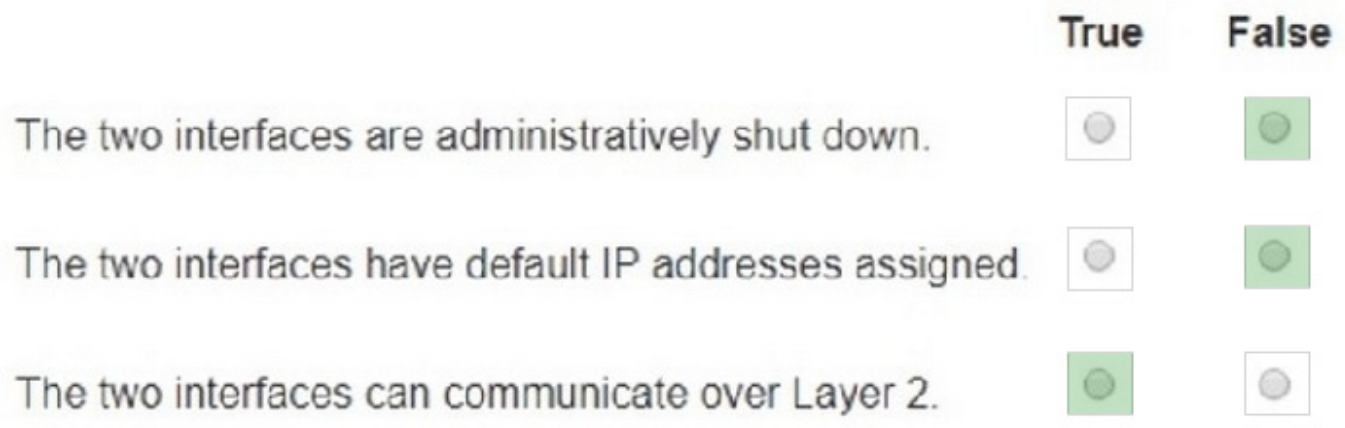
```
#show running-config | section include interface
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
<output omitted>
```

For each statement about the output, select True or False. Note: You will receive partial credit for each correct selection.

Hot Area:



Correct Answer:



The two interfaces are administratively shut down:

The two interfaces have default IP addresses assigned:

The two interfaces can communicate over Layer 2:

Interface Status: The absence of the "shutdown" command means the interfaces are not administratively shut down.

IP Address Assignment: There is no evidence in the output that IP addresses have been assigned to the interfaces, which would typically be shown as "ip address" entries.

Layer 2 Communication: Switch interfaces in their default state operate at Layer 2, enabling them to forward Ethernet frames and participate in Layer 2 communication.

References:

Cisco IOS Interface Configuration: Cisco Interface Configuration Understanding Cisco Switch Interfaces: Cisco Switch Interfaces

---

QUESTION 4

HOTSPOT

You want to list the IPv4 addresses associated with the host name www.companypro.net.

Complete the command by selecting the correct option from each drop-down list.

Hot Area:

Correct Answer:

To list the IPv4 addresses associated with the host name www.companypro.net, you should use the following command:

nslookup www.companypro.net

This command will query the DNS servers to find the IP address associated with the hostname provided.If you want to ensure that it returns the IPv4 address, you can specify the-type=Aoption, which stands for Address records that hold IPv4

addresses1. However, thenslookupcommand by default should return the IPv4 address if available. To list the IPv4 addresses associated with the host namewww.companypro.net, you should use thenslookupcommand.

Command: nslookup

Target:www.companypro.net

So, the completed command is:

nslookupwww.companypro.net

nslookup: This command is used to query the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record. www.companypro.net: This is the domain name you want to query to obtain its

associated IP addresses.

References:

Using nslookup: nslookup Command Guide

QUESTION 5

Which device protects the network by permitting or denying traffic based on IP address, port number, or application?

A. Firewall

B. Access point

C. VPN gateway

D. Intrusion detection system

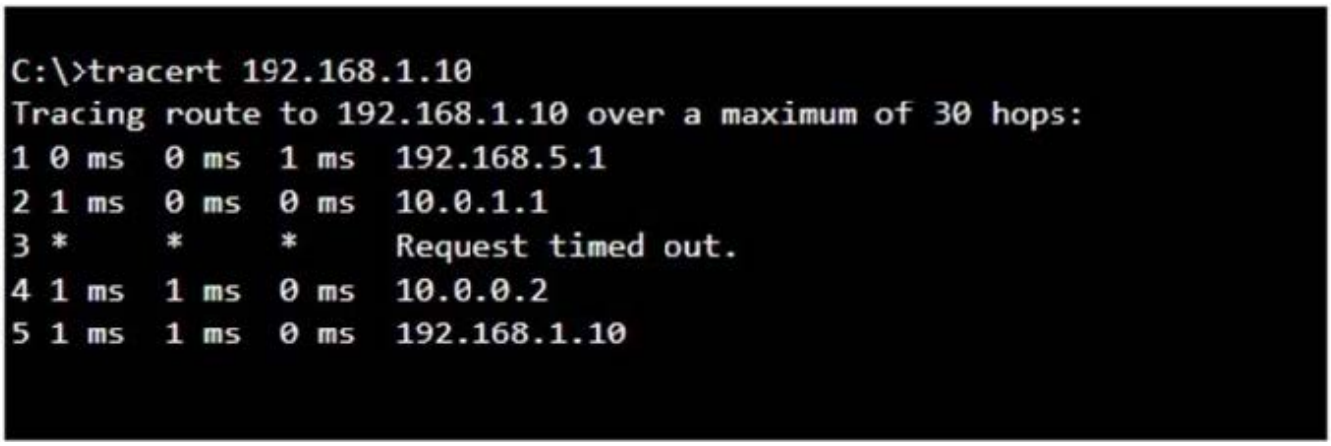
Correct Answer: A

Firewall: A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It permits or denies traffic based on IP addresses, port numbers, or applications. Access Point: This is a device that allows wireless devices to connect to a wired network using Wi-Fi. It does not perform traffic filtering based on IP, port, or application. VPN Gateway: This device allows for secure connections between networks over the internet, but it is not primarily used for traffic filtering based on IP, port, or application. Intrusion Detection System (IDS): This device monitors network traffic for suspicious activity and policy violations, but it does not actively permit or deny traffic. References: Understanding Firewalls: Firewall Basics

---

QUESTION 6

A user reports that a company website is not available. The help desk technician issues a tracert command to determine if the server hosting the website isreachable over the network. The output of the command is shown as follows:



What can you tell from the command output?

A. The router at hop 3 is not forwarding packets to the IP address 192.168.1.10.

B. The server address 192.168.1.10 is being blocked by a firewall on the router at hop 3.

C. The server with the address 192.168.1.10 is reachable over the network.

D. Requests to the web server at 192.168.1.10 are being delayed and time out.

Correct Answer: C

The tracert command output shows the path taken to reach the destination IP address, 192.168.1.10. The command output indicates:

-Hops 1 and 2 are successfully reached.

-Hop 3 times out, meaning the router at hop 3 did not respond to the tracert request.

However, this does not necessarily indicate a problem with forwarding packets, as some routers may be configured to block or not respond to ICMP requests. -Hops 4 and 5 are successfully reached, with hop 5 being the destination IP

192.168.1.10, indicating that the server is reachable.

Thus, the correct answer is C. The server with the address 192.168.1.10 is reachable over the network.

References:

-Cisco Traceroute Command

-Understanding Traceroute

The tracert command output indicates that the server with the address 192.168.1.10 is reachable over the network. The asterisk (*) at hop 3 suggests that the probe sent to that hop did not return a response, which could be due to a variety of

reasons such as a firewall blocking ICMP packets or the router at that hop being configured not to respond to ICMP requests. However, since the subsequent hops (4 and 5) are showing response times, it means that the packets are indeed

getting through and the server is reachable.

References:

-How to Use Traceroute Command to Read Its Results

-How to Use the Tracert Command in Windows

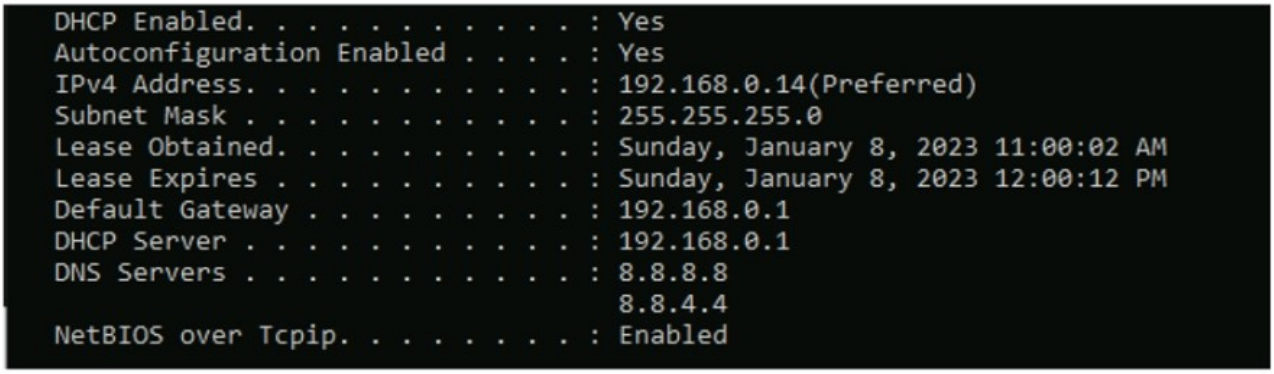
QUESTION 7

HOTSPOT

Computers in a small office are unable to access companypro.net. You run the ipconfig command on one of the computers. The results are shown in the

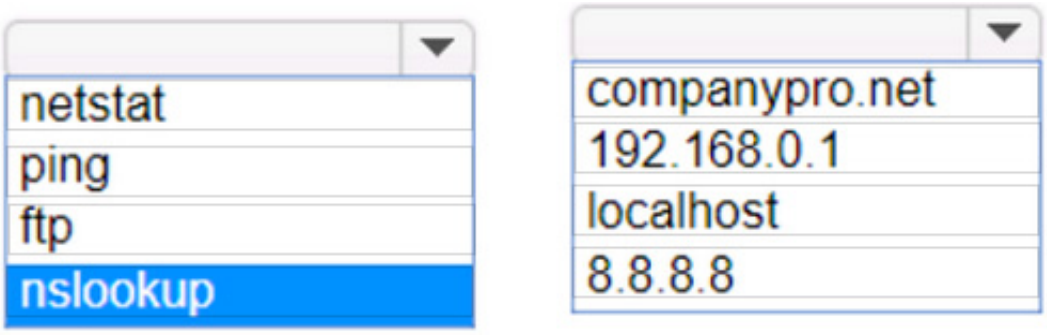
exhibit.

You need to determine if you can reach the router.

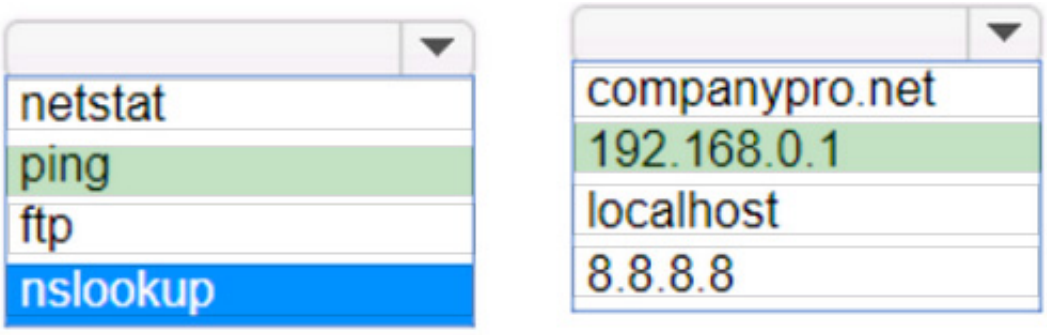


Which command should you use? Complete the command by selecting the correct options from each drop-down lists.

Hot Area:



Correct Answer:



To determine if you can reach the router, you should use thepingcommand followed by the IP address of the router. Thepingcommand is a network utility used to test the reachability of a host on an Internet Protocol (IP) network and to

measure the round-trip time for messages sent from the originating host to a destination computer. The Default Gateway in theipconfigresults is typically the router\\'s IP address in a home or small office network. In this case, the Default

Gateway is192.168.0.1, which is the address you would ping to check connectivity to the router.

References:

How to Use the Ping Command

Testing Network Connectivity with the Ping Command ==========

To determine if you can reach the router, you should use thepingcommand with the IP address of the router.

Command:ping

Target:192.168.0.1

So, the completed command is:

ping 192.168.0.1

Step by Step Comprehensive and Detailed Explanation:

ping: The ping command sends ICMP Echo Request messages to the target IP address and waits for an Echo Reply. It is commonly used to test the reachability of a network device.

192.168.0.1: This is the IP address of the default gateway (the router) as shown in theipconfigoutput. Pinging this

address will help determine if the computer can communicate with the router.

References:

Using the ping Command: ping Command Guide

QUESTION 8

Which wireless security option uses a pre-shared key to authenticate clients?

A. WPA2-Personal

B. 802.1x

C. 802.1q

D. WPA2-Enterprise

Correct Answer: A

WPA2-Personal, also known as WPA2-PSK (Pre-Shared Key), is the wireless security option that uses a pre-shared key to authenticate clients. This method is designed for home and small office networks and doesn\\'t require an

authentication server. Instead, every user on the network uses the same key or passphrase to connect.

References:

-What is a Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)?

-Exploring WPA-PSK and WiFi Security

==========

-WPA2-Personal: This wireless security option uses a pre-shared key (PSK) for authentication. Each client that connects to the network must use this key to gain access. It is designed for home and small office networks where simplicity and

ease of use are important.

-WPA2-Enterprise: Unlike WPA2-Personal, WPA2-Enterprise uses 802.1x authentication with an authentication server (such as RADIUS) and does not rely on a pre-shared key. -802.1x: This is a network access control protocol for LANs,

particularly wireless LANs. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. -802.1q: This is a networking standard that supports VLAN tagging on Ethernet networks and is not related to wireless

security.

References:

Cisco Documentation on WPA2 Security: Cisco WPA2 Understanding Wireless Security: Wireless Security Guide

---

QUESTION 9

During the data encapsulation process, which OSI layer adds a header that contains MAC addressing information and a trailer used for error checking?

A. Network

B. Transport

C. Data Link

D. Session

Correct Answer: C

OSI model During the data encapsulation process, theData Link layerof the OSI model is responsible for adding a header that contains MAC addressing information and a trailer used for error checking.The header typically includes the source and destination MAC addresses, while the trailer contains a Frame Check Sequence (FCS) which is used for error detection1. The Data Link layer ensures that messages are delivered to the proper device on a LAN using hardware addresses and translates messages from the Network layer into bits for the Physical layer to transmit. It also controls how data is placed onto the medium and is received from the medium through the physical hardware. References: The OSI Model The 7 Layers of Networking Explained in Plain English OSI Model - Network Direction Which layer adds both header and trailer to the data? What is OSI Model | 7 Layers Explained - GeeksforGeeks

---

QUESTION 10

Which command will display the following output?

Image is command output that states the following.

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,

Device ID       Local Intrfce     Holdtme    Capability  Platform  Port ID
esxi            Gig 0/5           177              S    VMware ES vmnic0
esxi            Gig 0/7           177              S    VMware ES vmnic1
esxi            Gig 0/6           177              S    VMware ES vmnic2
981888fc23a7    Gig 0/47          160            R S    Meraki MR Port 0
3456fecd1d08    Gig 0/1           178              S    MS120-8LP Port 9"
```

A. show mac-address-table

B. show cdp neighbor

C. show inventory

D. show ip interface

Correct Answer: B

The command that will display the output provided, which includes capability codes, local interface details, device IDs, hold times, and platform port ID capabilities, is the show cdp neighbor command. This command is used in Cisco devices

to display current information about neighboring devices detected by Cisco Discovery Protocol (CDP), which includes details such as the interface through which the neighbor is connected, the type of device, and the port ID of the device1.

References:

-Cisco - show cdp neighbors

The provided output is from the Cisco Discovery Protocol (CDP) neighbor table. The show cdp neighbor command displays information about directly connected Cisco devices, including Device ID, Local Interface, Holdtime, Capability,

Platform, and Port ID.

-A. show mac-address-table: Displays the MAC address table on the switch.

-C. show inventory: Displays information about the hardware inventory of the device.

-D. show ip interface: Displays IP interface status and configuration.

Thus, the correct answer is B. show cdp neighbor.

References:

-Cisco CDP Neighbor Command

-Understanding CDP

QUESTION 11

HOTSPOT

For each statement about bandwidth and throughput, select True or False.

Note: You will receive partial credit for each correct selection.

Hot Area:

For each statement about bandwidth and throughput, select **True** or **False**.

Note: You will receive partial credit for each correct selection.

Answer Area

	True	False
Low bandwidth can increase network latency.	○	○
High levels of network latency decrease network bandwidth.	○	○
You can increase throughput by decreasing network latency.	○	○

Correct Answer:

For each statement about bandwidth and throughput, select **True** or **False**.

Note: You will receive partial credit for each correct selection.

Answer Area

	True	False
Low bandwidth can increase network latency.	●	○
High levels of network latency decrease network bandwidth.	○	●
You can increase throughput by decreasing network latency.	●	○

Statement 1: Low bandwidth can increase network latency. Statement 2: High levels of network latency decrease

network bandwidth. Statement 3: You can increase throughput by decreasing network latency.

Bandwidth vs. Latency: Bandwidth refers to the maximum rate at which data can be transferred over a network path. Latency is the time it takes for a data packet to travel from the source to the destination.

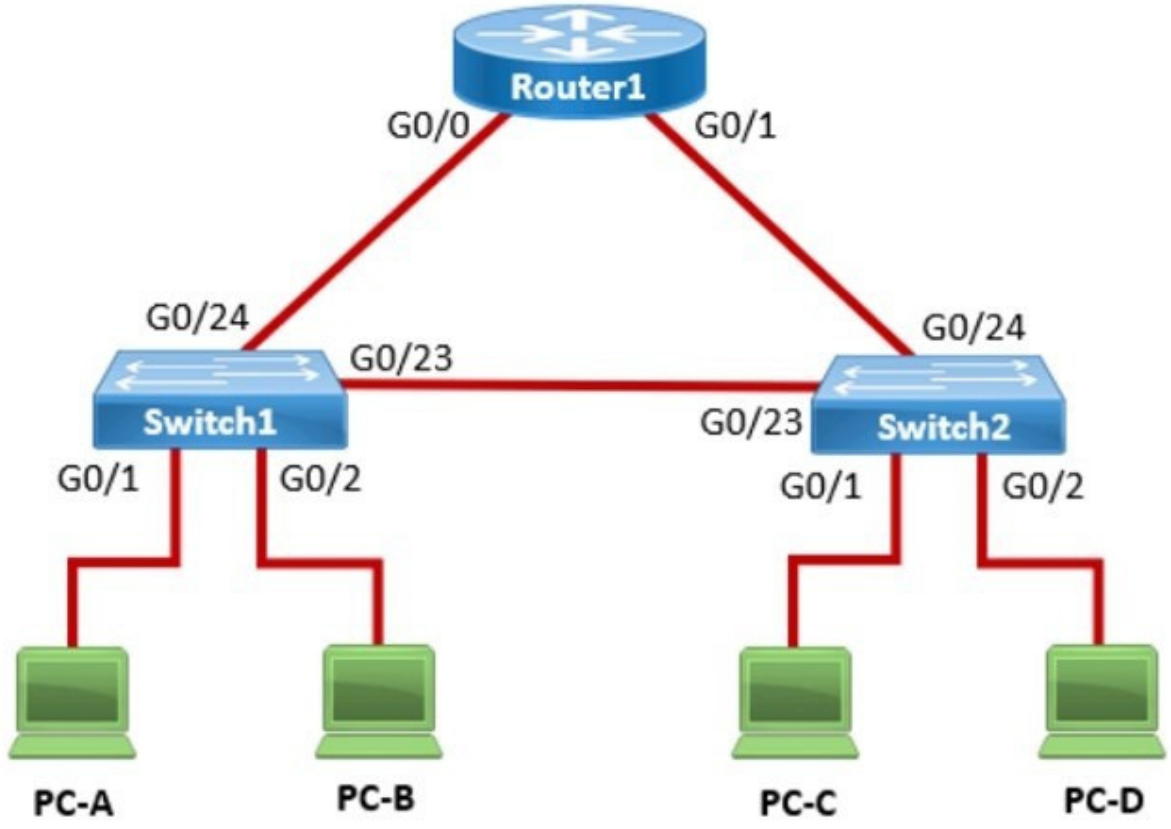
References:

Network Performance Metrics: Cisco Network Performance Understanding Bandwidth and Latency: Bandwidth vs. Latency

---

QUESTION 12

In the network shown in the following graphic, Switch1 is a Layer 2 switch.



PC-A sends a frame to PC-C. Switch1 does not have a mapping entry for the MAC address of PC-C. Which action does Switch1 take?

A. Switch1 queries Switch2 for the MAC address of PC-C.

B. Switch1 drops the frame and sends an error message back to PC-A.

C. Switch1 floods the frame out all active ports except port G0/1.

D. Switch1 sends an ARP request to obtain the MAC address of PC-C.

Correct Answer: B

In a network, when a Layer 2 switch (like Switch1) receives a frame destined for a MAC address that is not in its MAC address table, it performs a flooding operation. This means the switch will send the frame out of all ports except the port on

which the frame was received. This flooding ensures that if the destination device is connected to one of the other ports, it will receive the frame and respond, allowing the switch to learn its MAC address. A. Switch1 queries Switch2 for the

MAC address of PC-C: This does not happen in Layer 2 switches; they do not query other switches for MAC addresses. A. Switch1 drops the frame and sends an error message back to PC-A: This is not the default behavior for unknown

unicast frames. D. Switch1 sends an ARP request to obtain the MAC address of PC-C: ARP is used by devices to map IP addresses to MAC addresses, not by switches to find unknown MAC addresses.

Thus, the correct answer is B. Switch1 floods the frame out all active ports except port G0/1.

References:

Cisco Layer 2 Switching Overview

Switching Mechanisms (Cisco)