CCST-Networking Q&As

Cisco Certified Support Technician (CCST) Networking

Pass Cisco CCST-Networking Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/ccst-networking.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

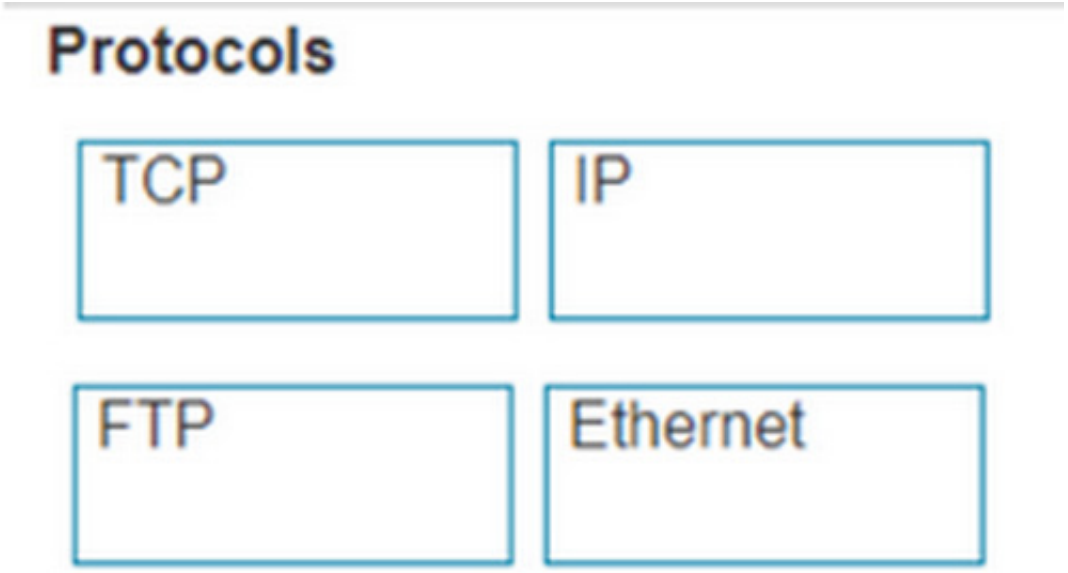
QUESTION 1

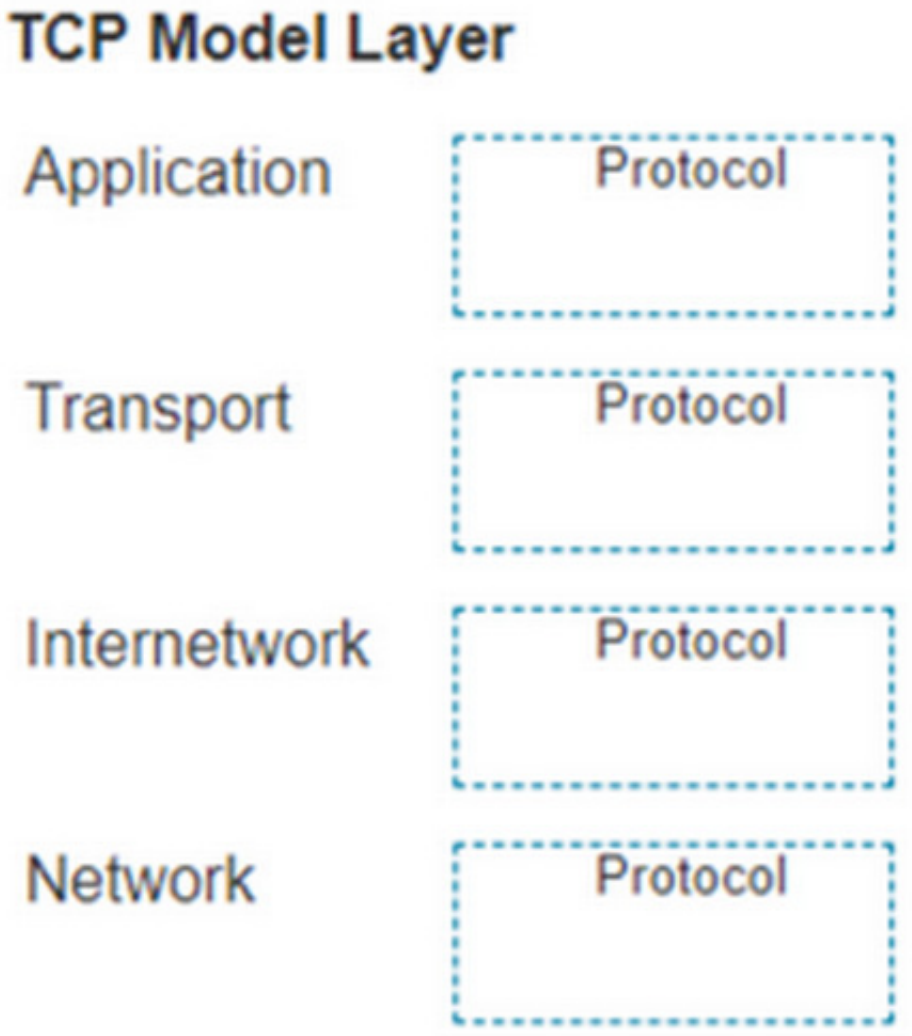
DRAG DROP

Move each protocol from the list on the left to the correct TCP/IP model layer on the right.

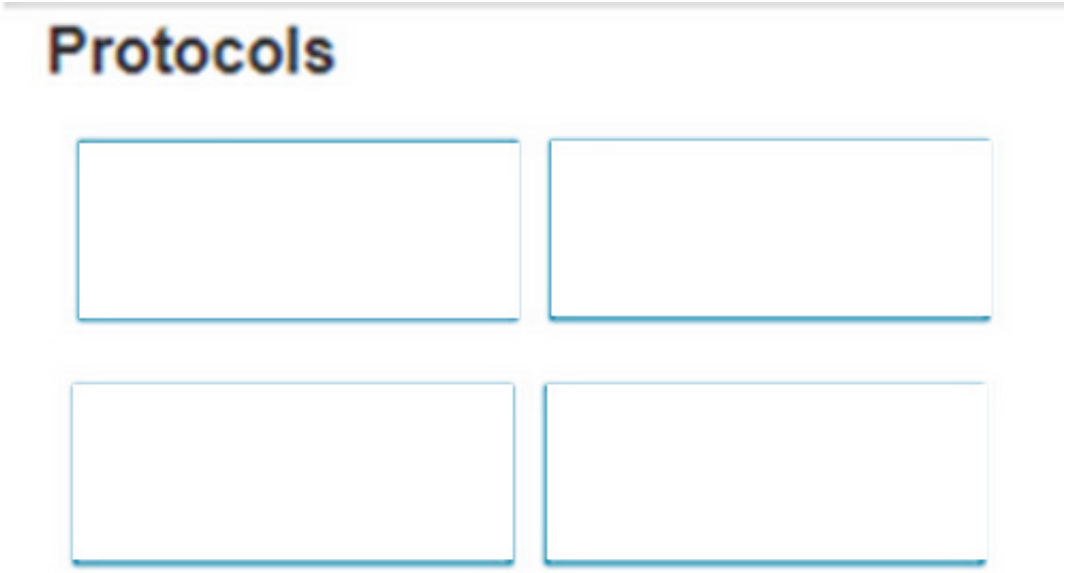
Note: You will receive partial credit for each correct match.

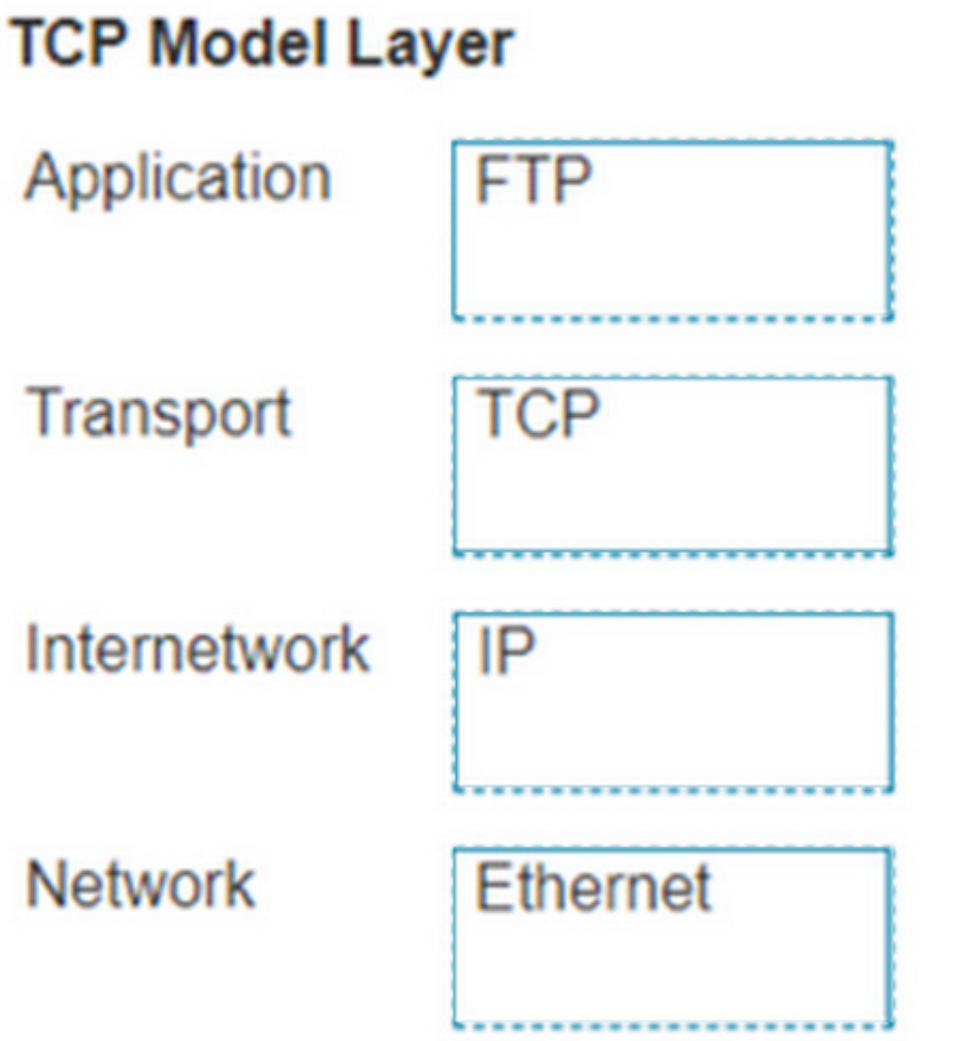
Select and Place:


Protocols
TCP
IP
FTP
Ethernet


TCP Model Layer
Application
Protocol
Transport
Protocol
Internetwork
Protocol
Network
Protocol

Correct Answer:


Protocols


TCP Model Layer
Application
FTP
Transport
TCP
Internetwork
IP
Network
Ethernet

Here\\'s how each protocol aligns with the correct TCP/IP model layer:

TCP (Transmission Control Protocol): This protocol belongs to theTransportlayer, which is responsible for providing communication between applications on different hosts1.

IP (Internet Protocol): IP is part of theInternetworklayer, which is tasked with routing packets across network boundaries to their destination. FTP (File Transfer Protocol): FTP operates at theApplicationlayer, which supports application and

end-user processes.It is used for transferring files over the network.

Ethernet: While not a protocol within the TCP/IP stack, Ethernet is associated with theNetwork Interfacelayer, which corresponds to the link layer of the TCP/IP model and is responsible for the physical transmission of data1. The TCP/IP

model layers are designed to work collaboratively to transmit data from one layer to another, with each layer having specific protocols that perform functions necessary for the data transmission process.

TCP:

IP:

FTP:

Ethernet:

Transport Layer: This layer is responsible for providing communication services directly to the application processes running on different hosts. TCP is a core protocol in this layer.

Internetwork Layer: This layer is responsible for logical addressing, routing, and packet forwarding. IP is the primary protocol for this layer. Application Layer: This layer interfaces directly with application processes and provides common

network services. FTP is an example of a protocol operating in this layer.

Network Layer: In the TCP/IP model, this layer includes both the data link and physical layers of the OSI model. Ethernet is a protocol used in this layer to define network standards and communication protocols at the data link and physical

levels.

References:

TCP/IP Model Overview: Cisco TCP/IP Model

Understanding the TCP/IP Model: TCP/IP Layers

QUESTION 2

A support technician examines the front panel of a Cisco switch and sees 4 Ethernet cables connected in the first four ports. Ports 1, 2, and 3 have a green

LED. Port 4 has a blinking green light.

What is the state of the Port 4?

A. Link is up with cable malfunctions.

B. Link is up and not stable.

C. Link is up and active.

D. Link is up and there is no activity.

Correct Answer: C

On a Cisco switch, a port with a blinking green LED typically indicates that the port is up (active) and is currently transmitting or receiving data. This is a normal state indicating active traffic on the port.

-A. Link is up with cable malfunctions: Usually indicated by an amber or blinking amber light.

-B. Link is up and not stable: Not typically indicated by a green blinking light.

-D. Link is up and there is no activity: Would be indicated by a solid green light withoutblinking.

Thus, the correct answer is C. Link is up and active.

References:

-Cisco Switch LED Indicators

-Cisco Ethernet Switch LED Patterns

QUESTION 3

A help desk technician receives the four trouble tickets listed below. Which ticket should receive the highest priority and be addressed first?

A. Ticket 1: A user requests relocation of a printer to a different network jack in the same office. The jack must be patched and made active.

B. Ticket 2: An online webinar is taking place in the conference room. The video conferencing equipment lost internet access.

C. Ticket 3: A user reports that response time for a cloud-based application is slower than usual.

D. Ticket 4: Two users report that wireless access in the cafeteria has been down for the last hour.

Correct Answer: B

When prioritizing trouble tickets, the most critical issues affecting business operations or high-impact activities should be addressed first. Here\\'s a breakdown of the tickets:

Ticket 1: Relocation of a printer, while necessary, is not urgent and does not impact critical operations.

Ticket 2: An ongoing webinar losing internet access is critical, especially if the webinar is time-sensitive and involves multiple participants. Ticket 3: Slower response time for a cloud-based application is important but typically not as urgent as

a complete loss of internet access for a live event. Ticket 4: Wireless access down in the cafeteria affects users but does not have the same immediate impact as a live webinar losing connectivity. Thus, the correct answer is B. Ticket 2: An

online webinar is taking place in the conference room. The video conferencing equipment lost internet access.

References:

IT Help Desk Best Practices

Prioritizing IT Support Tickets

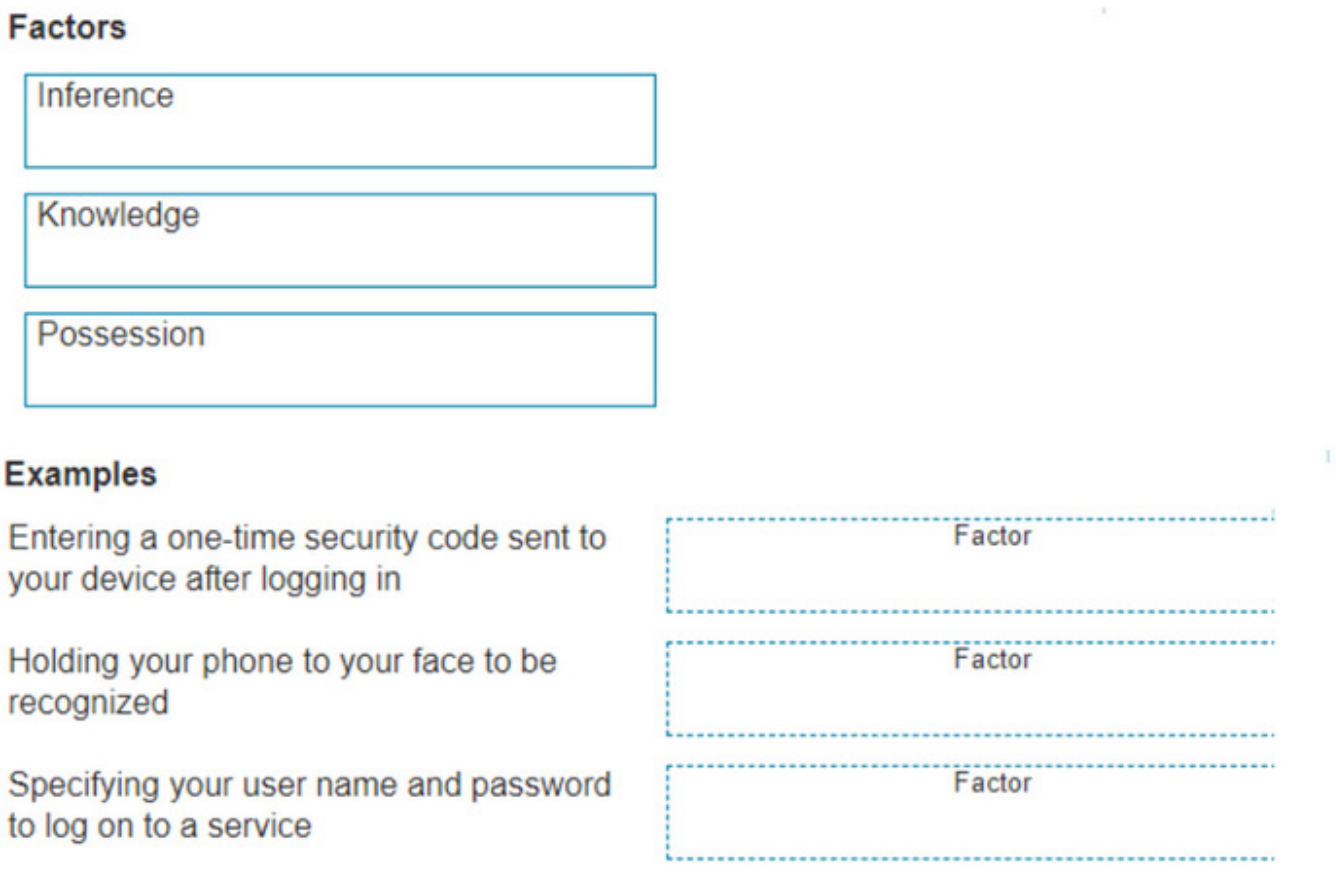
QUESTION 4

DRAG DROP

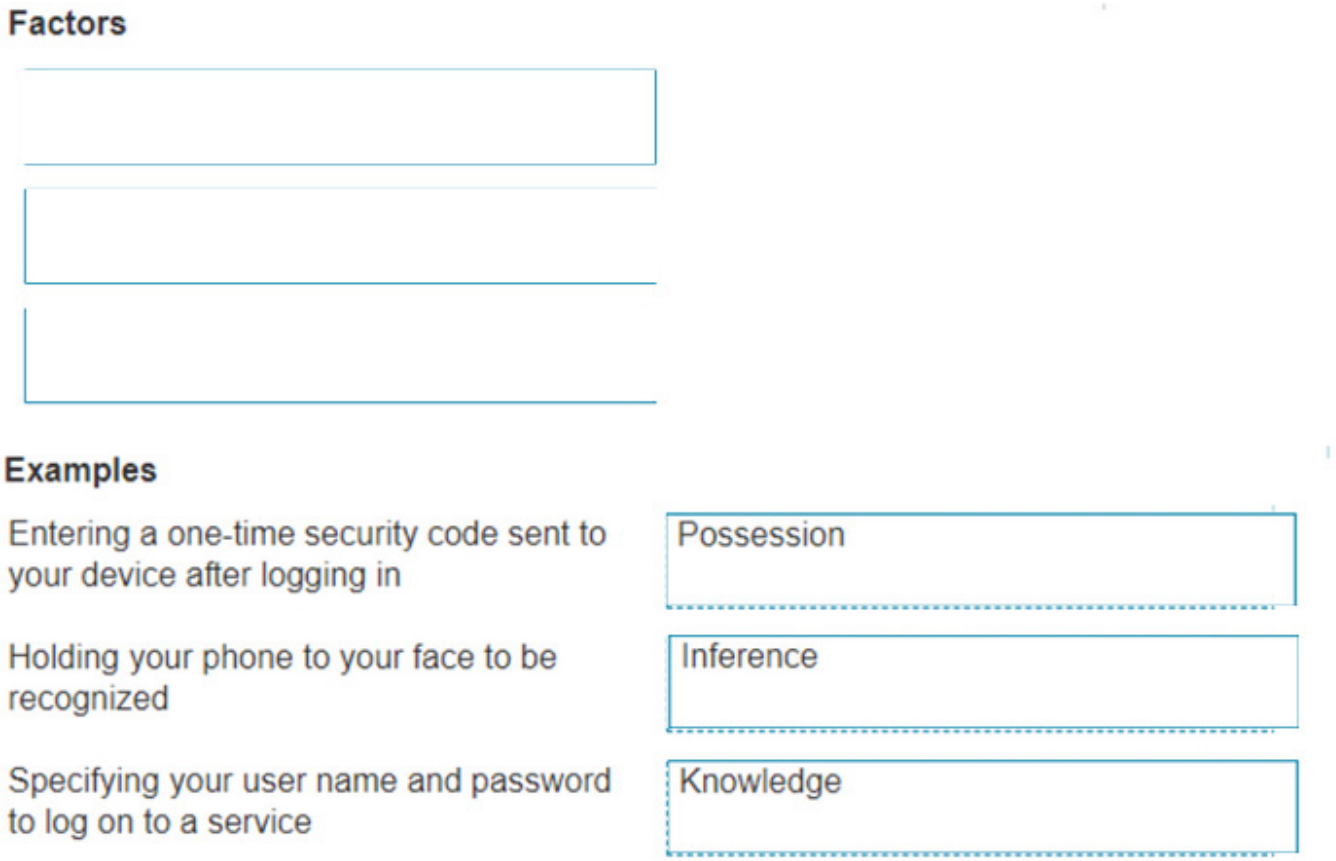
Move the MFA factors from the list on the left to their correct examples on the right. You may use each factor once, more than once, or not at all.

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

Select and Place:



Correct Answer:



The correct matching of the MFA factors to their examples is as follows:

Entering a one-time security code sent to your device after logging in: Possession Holding your phone to your face to be recognized: Inherence Specifying your user name and password to log on to a service: Knowledge Here\\'s why each

factor matches the example:

Possession: This factor is something the user has, like a mobile device. A one- time security code sent to this device falls under this category. Inherence: This factor is something the user is, such as a biometric characteristic. Facial

recognition using a phone is an example of this factor. Knowledge: This factor is something the user knows, like a password or PIN. Multi-Factor Authentication (MFA) enhances security by requiring two or more of these factors to verify a

user\\'s identity before granting access.

Entering a one-time security code sent to your device after logging in. Holding your phone to your face to be recognized. Specifying your username and password to log on to a service.

Possession Factor: This involves something the user has in their possession. Receiving a one-time security code on a device (e.g., phone) is an example of this. Inference Factor (Inherence/Biometric): This involves something inherent to the

user, such as biometric verification (e.g., facial recognition or fingerprint scanning). Knowledge Factor: This involves something the user knows, such as login credentials (username and password).

References:

Multi-Factor Authentication (MFA) Explained: MFA Guide Understanding Authentication Factors: Authentication Factors

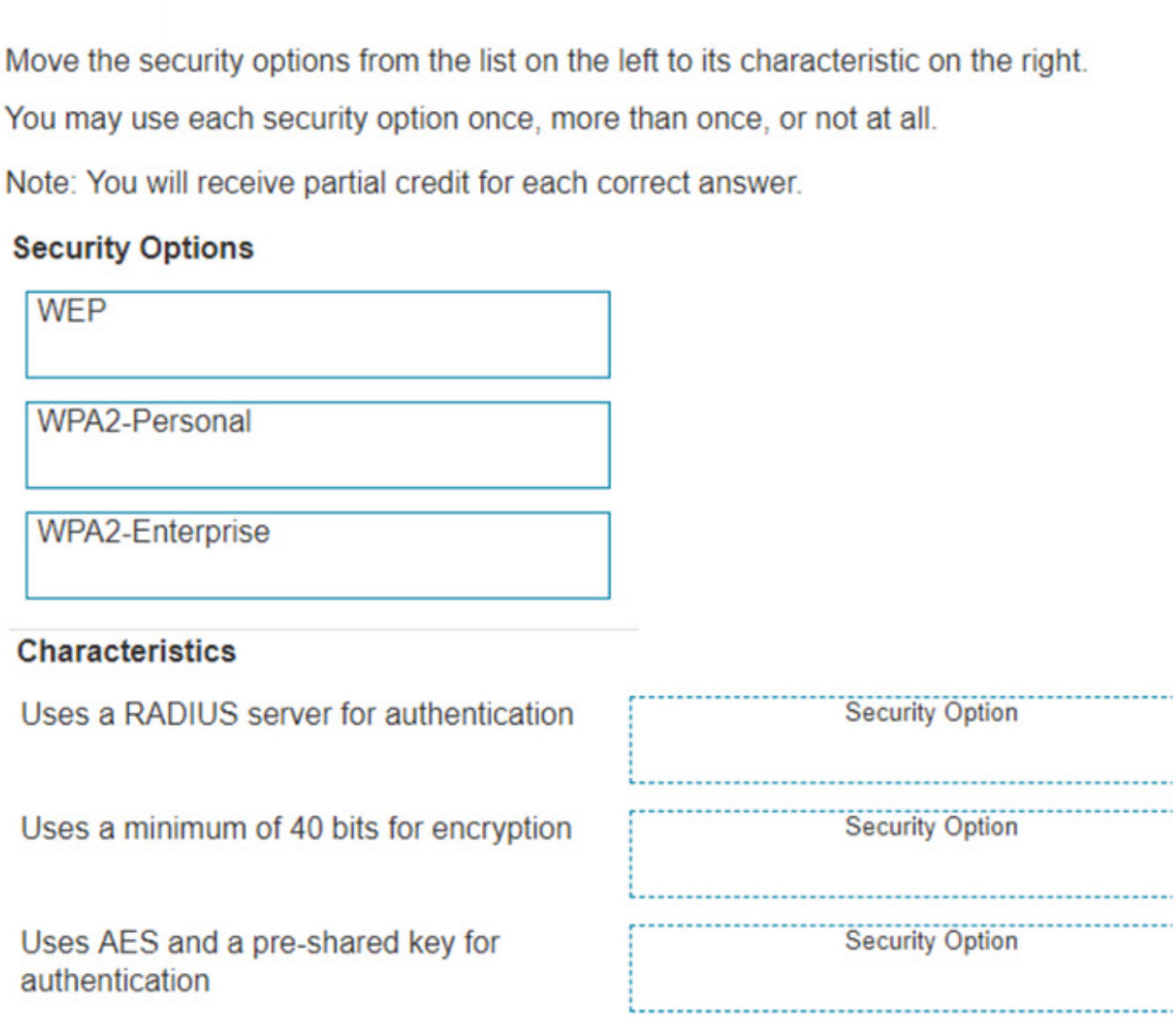
QUESTION 5

DRAG DROP

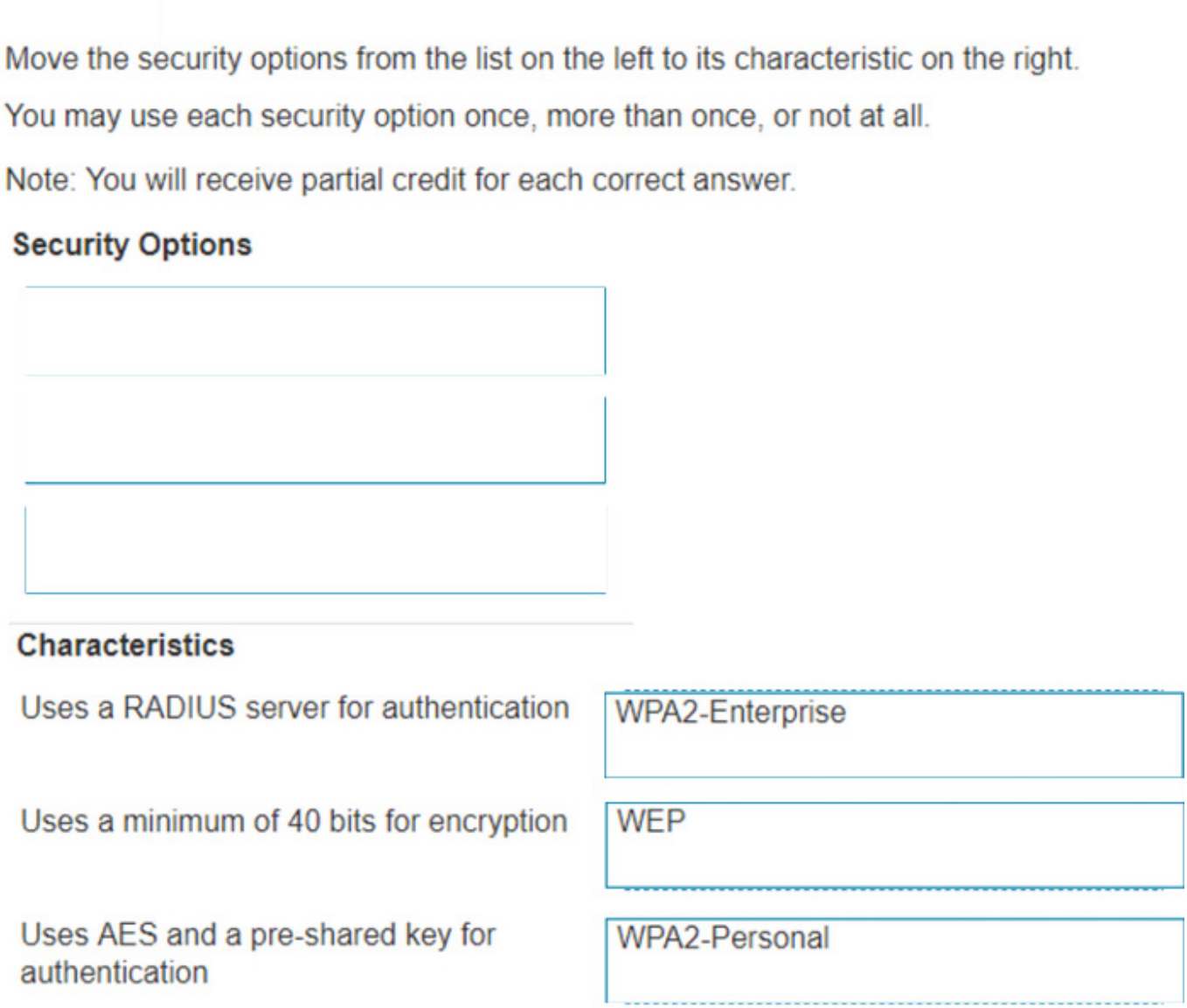
Move the security options from the list on the left to its characteristic on the right. You may use each security option once, more than once, or not at all.

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

Select and Place:



Correct Answer:



The correct matching of the security options to their characteristics is as follows:

WPA2-Enterprise: Uses a RADIUS server for authentication WEP: Uses a minimum of 40 bits for encryption

WPA2-Personal: Uses AES and a pre-shared key for authentication Here\\'s why each security option matches the characteristic:

WPA2-Enterpriseuses a RADIUS server for authentication, which provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.

WEP (Wired Equivalent Privacy)is an outdated security protocol that uses a minimum of 40 bits for encryption (and up to 104 bits), which is relatively weak by today\\'s standards.

WPA2-Personal(Wi-Fi Protected Access 2 - Personal) uses the Advanced Encryption Standard (AES) for encryption and a pre-shared key (PSK) for authentication, which is shared among users to access the network. These security options

are essential for protecting wireless networks from unauthorized access and ensuring data privacy.

QUESTION 6

HOTSPOT

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

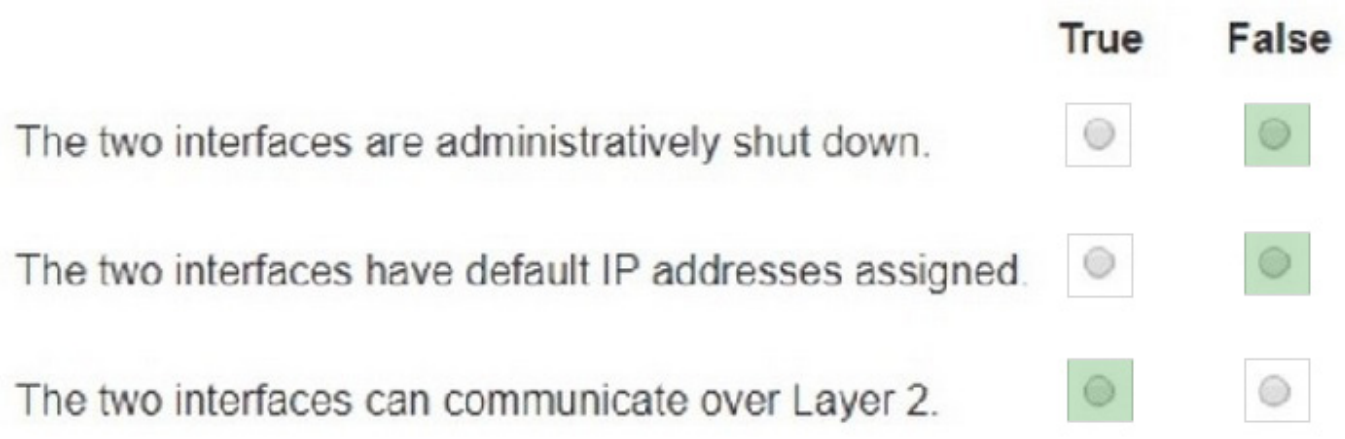
```
#show running-config | section include interface
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
<output omitted>
```

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

Hot Area:

	True	False
The two interfaces are administratively shut down.	○	○
The two interfaces have default IP addresses assigned.	○	○
The two interfaces can communicate over Layer 2.	○	○

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 7

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 8

What is the purpose of assigning an IP address to the management VLAN interface on a Layer 2 switch?

A. To enable the switch to act as a default gateway for the attached devices

B. To enable the switch to resolve URLs for the attached the devices

C. To enable the switch to provide DHCP services to other switches in the network

D. To enable access to the CLI on the switch through Telnet or SSH

Correct Answer: D

The primary purpose of assigning an IP address to the management VLAN interface on a Layer 2 switch is to facilitate remote management of the switch. By configuring an IP address on the management VLAN, network administrators can

access the switch\\'s Command Line Interface (CLI) remotely using protocols such as Telnet or Secure Shell (SSH). This allows for convenient configuration changes, monitoring, and troubleshooting without needing physical access to the

switch1.

References:

-Understanding the Management VLAN

-Cisco - VLAN Configuration Guide

-Remote Management of Switches

Assigning an IP address to the management VLAN interface (often the VLAN 1 interface by default) on a Layer 2 switch allows network administrators to remotely manage the switch using protocols such as Telnet or SSH. This IP address

does not affect the switch\\'s ability to route traffic between VLANs but provides a means to access and configure the switch through its Command Line Interface (CLI).

-A: The switch does not act as a default gateway; this is typically a function of a Layer 3 device like a router.

-B: The switch does not resolve URLs; this is typically a function of DNS servers.

-C: The switch can relay DHCP requests but does not typically provide DHCP services

itself; this is usually done by a dedicated DHCP server or router.

Thus, the correct answer is D. To enable access to the CLI on the switch through Telnet or SSH.

References :

-Cisco VLAN Management Overview

-Cisco Catalyst Switch Management

QUESTION 9

Which address is included in the 192.168.200.0/24 network?

A. 192.168.199.13

B. 192.168.200.13

C. 192.168.201.13

D. 192.168.1.13

Correct Answer: B

192.168.200.0/24 Network: This subnet includes all addresses from 192.168.200.0 to 192.168.200.255. The /24 indicates a subnet mask of 255.255.255.0, which allows for 256 addresses.

192.168.199.13: This address is in the 192.168.199.0/24 subnet, not the 192.168.200.0/24 subnet.

192.168.200.13: This address is within the 192.168.200.0/24 subnet. ?92.168.201.13: This address is in the 192.168.201.0/24 subnet, not the 192.168.200.0/24 subnet.

192.168.1.13: This address is in the 192.168.1.0/24 subnet, not the 192.168.200.0/24 subnet.

References:

Subnetting Guide: Subnetting Basics

QUESTION 10

HOTSPOT

An app on a user\\'s computer is having problems downloading data. The app uses the following URL to download data:

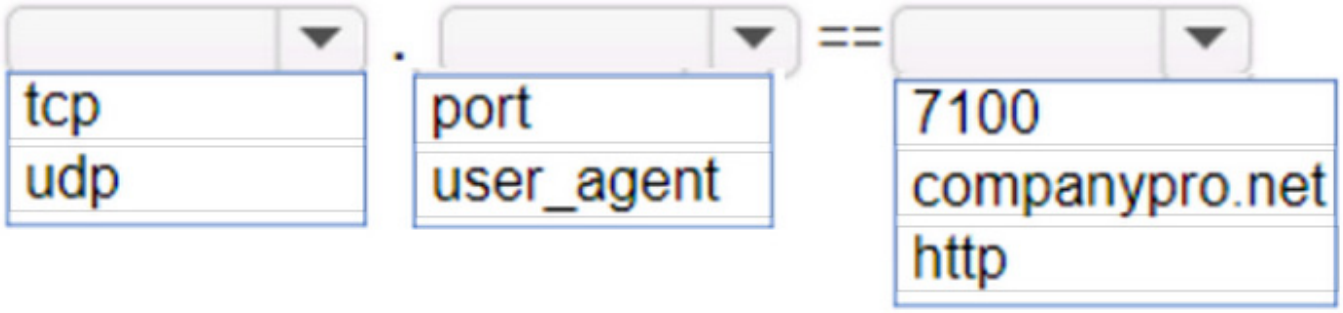
https://www.companypro.net:7100/api

You need to use Wireshark to capture packets sent to and received from that URL.

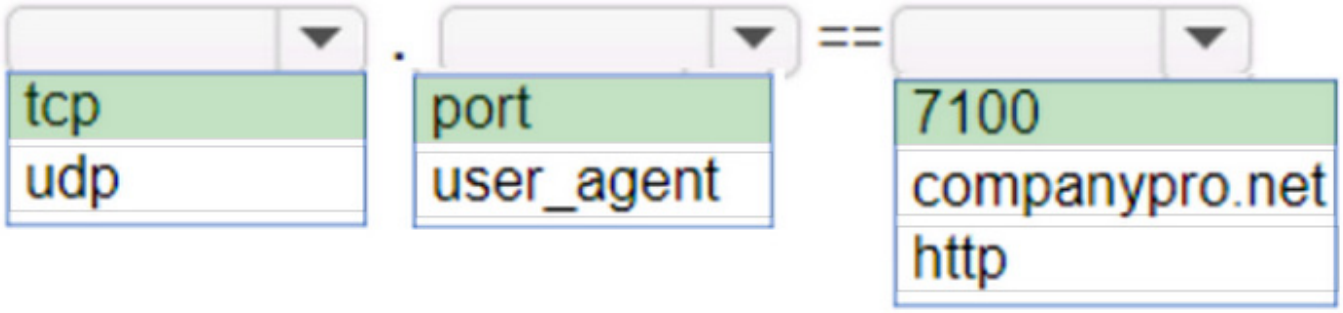
Which Wireshark filter options would you use to filter the results? Complete the command by selecting the correct option from each drop-down list.

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

Hot Area:



Correct Answer:



To capture packets sent to and received from the URLhttps://www.companypro.net:7100/apiusing Wireshark, you would use the following filter options:

Protocol:tcp

Filter Type:port

Port Number:7100

This filter setup in Wireshark will display all TCP packets that are sent to or received from port 7100, which is the port specified in the URL for the API service. Since HTTPS typically uses TCP as the transport layer protocol, filtering by TCP

and the specific port number will help isolate the relevant packets for troubleshooting the app\\'s data download issues.

cp: The app is using HTTPS, which relies on the TCP protocol for communication. port: The specific port number used by the application, which in this case is 7100. 7100: This is the port specified in the URL (https://

www.companypro.net:7100/api). This filter will capture all TCP traffic on port 7100, allowing you to analyze the packets related to the application\\'s data download.

References:

Wireshark Filters: Wireshark Display Filters

QUESTION 11

You want to store files that will be accessible by every user on your network.

Which endpoint device do you need?

A. Access point

B. Server

C. Hub

D. Switch

Correct Answer: B

To store files that will be accessible by every user on a network, you would need aserver. A server is a computer system that provides data to other computers. It can serve data to systems on a local network (LAN) or a wide network (WAN)

over the internet.In this context, a file server would be set up to store and manage files, allowing users on the network to access them from their own devices1.

References:

What is a Server?

Understanding Servers and Their Functions

A server is a computer designed to process requests and deliver data to other computers over a local network or the internet. In this case, to store files that will be accessible by every user on the network, a file server is the appropriate

endpoint device. It provides a centralized location for storing and managing files, allowing users to access and share files easily. A. Access point: Provides wireless connectivity to a network. C. Hub: A basic networking device that connects

multiple Ethernet devices together, making them act as a single network segment. D. Switch: A networking device that connects devices on a computer network by using packet switching to forward data to the destination device.

Thus, the correct answer is B. Server.

References:

File Server Overview (Cisco)

Server Roles in Networking (Cisco)

QUESTION 12

Which information is included in the header of a UDP segment?

A. IP addresses

B. Sequence numbers

C. Port numbers

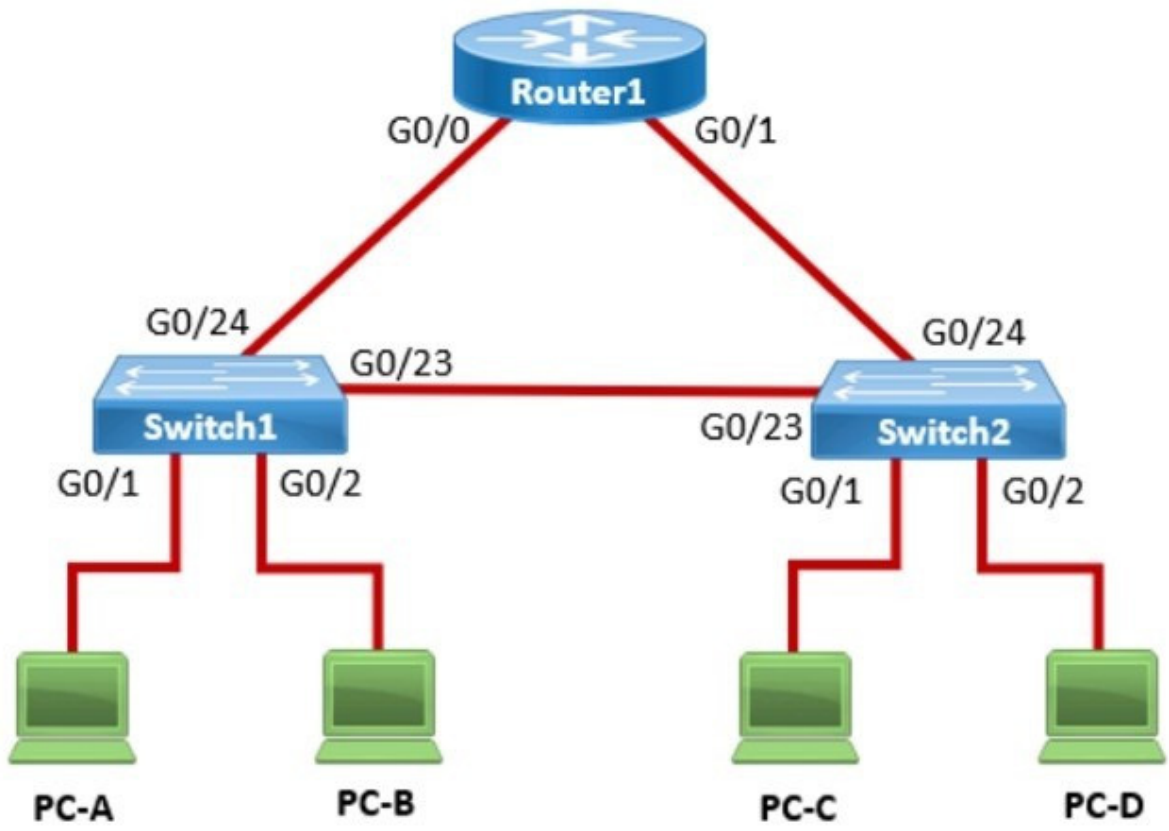
D. MAC addresses

Correct Answer: C

The header of a UDP (User Datagram Protocol) segment includesport numbers. Specifically, it contains the source port number and the destination port number, which are used to identify the sending and receiving applications. UDP headers do not include IP addresses or MAC addresses, as those are part of the IP and Ethernet frame headers, respectively.Additionally, UDP does not use sequence numbers, which are a feature of TCP (Transmission Control Protocol) for ensuring reliable delivery of data segments1. References: Segmentation Explained with TCP and UDP Header User Datagram Protocol (UDP) - GeeksforGeeks Which three fields are used in a UDP segment header ========== UDP Header: The header of a UDP segment includes the following key fields: IP Addresses: These are included in the IP header, not the UDP header. Sequence Numbers: These are part of the TCP header, not UDP. MAC Addresses: These are part of the Ethernet frame header and are not included in the UDP header. References: RFC 768 - User Datagram Protocol: RFC 768 Cisco Guide on UDP: Cisco UDP Guide

QUESTION 13

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.

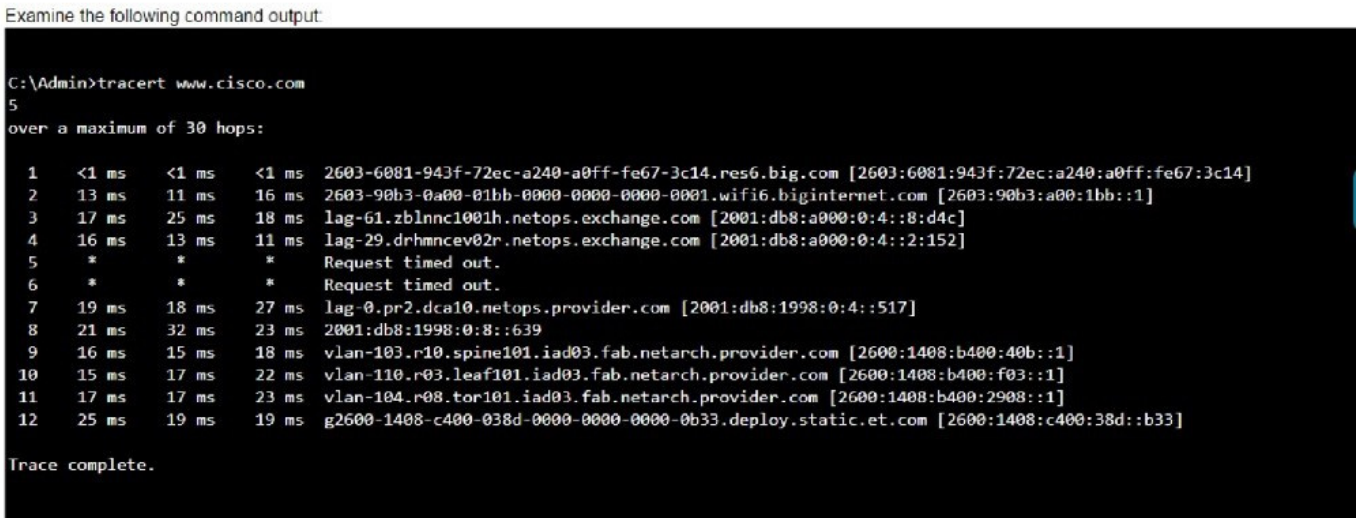
References:

Cisco Layer 2 Switching Overview

Switching Mechanisms (Cisco)

QUESTION 14

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:

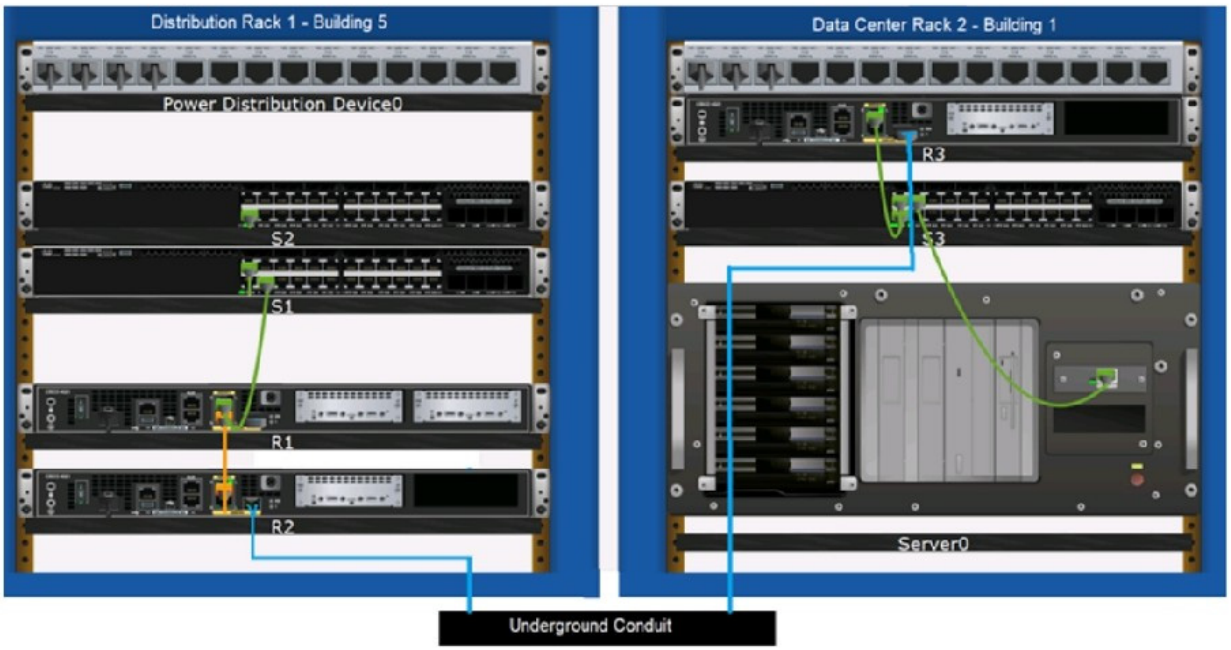
-Understanding Traceroute: Traceroute Guide

QUESTION 15

DRAG DROP

Examine the connections shown in the following image. Move the cable types on the right to the appropriate connection description on the left. You may

use each cable type more than once or not at all.



Select and Place:

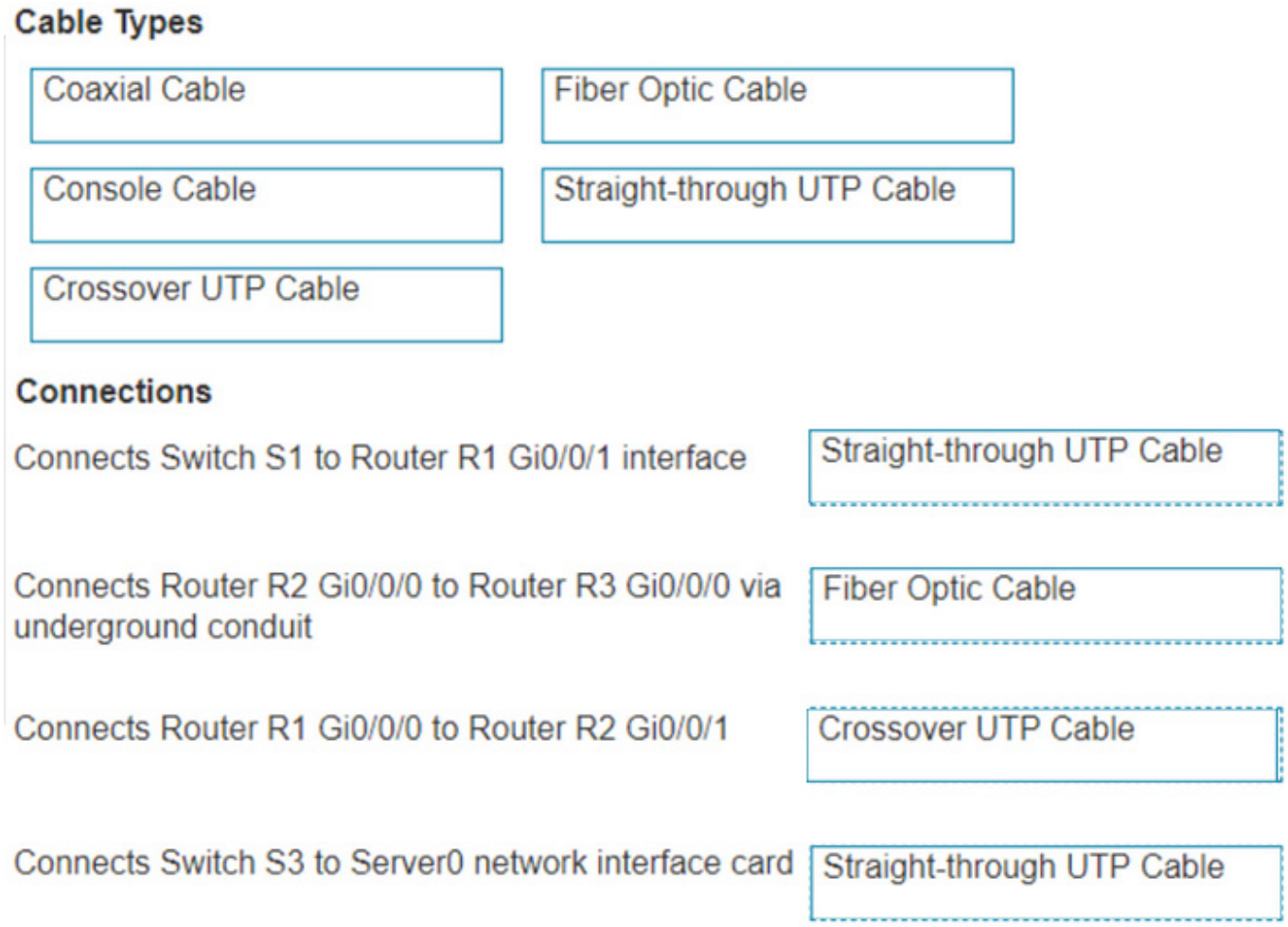
Cable Types

Coaxial Cable	Fiber Optic Cable
Console Cable	Straight-through UTP Cable
Crossover UTP Cable	

Connections

Connects Switch S1 to Router R1 Gi0/0/1 interface	Cable Type
Connects Router R2 Gi0/0/0 to Router R3 Gi0/0/0 via underground conduit	Cable Type
Connects Router R1 Gi0/0/0 to Router R2 Gi0/0/1	Cable Type
Connects Switch S3 to Server0 network interface card	Cable Type

Correct Answer:



Based on the image description provided, here are the cable types matched with the appropriate connection descriptions:

Connects Switch S1 to Router R1 Gi0/0/1 interfaceCable Type: = Straight-through UTP Cable

Connects Router R2 Gi0/0/0 to Router R3 Gi0/0/0 via underground conduitCable Type : = Fiber Optic Cable

Connects Router R1 Gi0/0/0 to Router R2 Gi0/0/1Cable Type: = Crossover UTP Cable Connects Switch S3 to Server0 network interface cardCable Type: = Straight-through UTP Cable

The choices are based on standard networking practices where:

Straight-through UTP cablesare typically used to connect a switch to a router or a network interface card.

Fiber optic cablesare ideal for long-distance, high-speed data transmission, such as connections through an underground conduit.

Crossover UTP cablesare used to connect similar devices, such as router-to-router connections.

These matches are consistent with the color-coded cables in the image: green for switch connections, yellow for router-to-router connections within the same rack, and blue for inter-rack connections. The use of these cables follows the

Ethernet cabling standards.

Connects Switch S1 to Router R1 Gi0/0/1 interface:

Connects Router R2 Gi0/0/0 to Router R3 Gi0/0/0 via underground conduit:

Connects Router R1 Gi0/0/0 to Router R2 Gi0/0/1:

Connects Switch S3 to Server0 network interface card:

Straight-through UTP Cable: Used to connect different devices (e.g., switch to router, switch to server).

Crossover UTP Cable: Used to connect similar devices directly (e.g., router to router, switch to switch).

Fiber Optic Cable: Used for long-distance and high-speed connections, often between buildings or data centers.

References:

Network Cable Types and Uses: Cisco Network Cables Understanding Ethernet Cabling: Ethernet Cable Guide