Cisco

Exam Questions CCST-Networking

Cisco Certified Support Technician (CCST) NetworkingExam

NEW QUESTION 1
What is the most compressed valid format of the IPv6 address 2001:0db8:0000:0016:0000:001b: 2000:0056?

A. 2001:db8: : 16: : 1b:2:56
B. 2001:db8: : 16: : 1b: 2000: 56
C. 2001:db8: 16: :1b:2:56
D. 2001:db8: 0:16: :1b: 2000:56

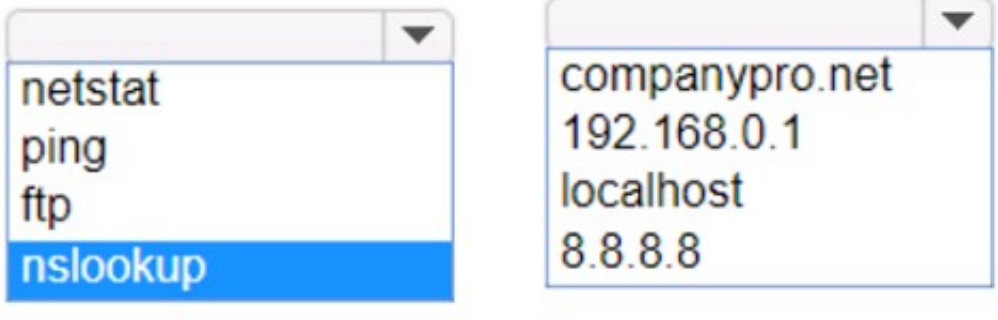
Answer: D

Explanation:
IPv6 addresses can be compressed by removing leading zeros and replacing consecutive groups of zeros with a double colon (::). Here??s how to compress the address 2001:0db8:0000:0016:0000:001b:2000:0056:
? Remove leading zeros from each segment:
? Replace the longest sequence of consecutive zeros with a double colon (::). In this case, the two consecutive zeros between the 16 and 1b:
Thus, the most compressed valid format of the IPv6 address is 2001:db8:0:16::1b:2000:56.
References:=
? Cisco Learning Network
? IPv6 Addressing (Cisco)

NEW QUESTION 2
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.

```
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . . . . . . . : 192.168.0.14(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Sunday, January 8, 2023 11:00:02 AM
Lease Expires . . . . . . . . . . : Sunday, January 8, 2023 12:00:12 PM
Default Gateway . . . . . . . . . : 192.168.0.1
DHCP Server . . . . . . . . . . . : 192.168.0.1
DNS Servers . . . . . . . . . . . : 8.8.8.8
                                   8.8.4.4
NetBIOS over Tcpip. . . . . . . . : Enabled
```

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

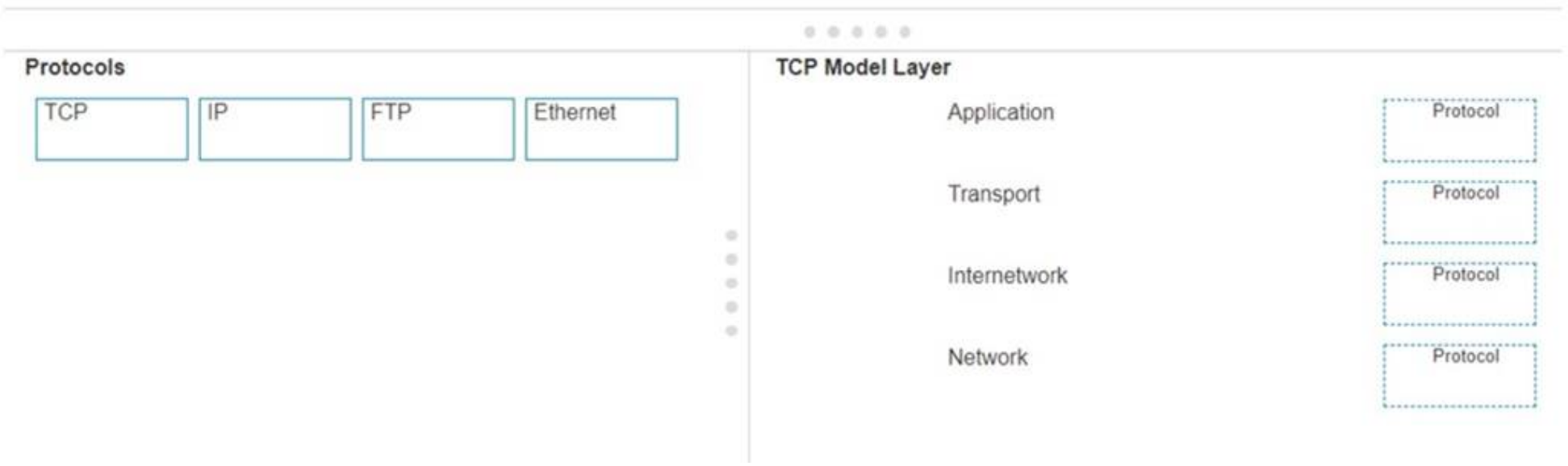


A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 3
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
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 destination1.
? FTP (File Transfer Protocol): FTP operates at theApplicationlayer, which supports application and end-user processes.It is used for transferring files over the network1.
? 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 process1.
? 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

NEW QUESTION 4
You need to connect a computer's network adapter to a switch using a 1000BASE-T cable. Which connector should you use?

A. Coax
B. RJ-11
C. OS2 LC
D. RJ-45

Answer: D

Explanation:
•1000BASE-T Cable: This refers to Gigabit Ethernet over twisted-pair cables (Cat 5e or higher).
•Connector: RJ-45 connectors are used for Ethernet cables, including those used for 1000BASE-T.
•Coax: Used for cable TV and older Ethernet standards like 10BASE2.
•RJ-11: Used for telephone connections.
•OS2 LC: Used for fiber optic connections. References:
•Ethernet Standards and Cables: Ethernet Cable Guide

NEW QUESTION 5
HOTSPOT
You plan to use a network firewall to protect computers at a small office. For each statement about firewalls, select True or False.
Note: You will receive partial credit for each correct selection.

	True	False
A firewall can direct all web traffic to a specific IP address.	○	○
A firewall can block traffic to specific ports on internal computers.	○	○
A firewall can prevent specific apps from running on a computer.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? A firewall can direct all web traffic to a specific IP address.
? A firewall can block traffic to specific ports on internal computers.
? A firewall can prevent specific apps from running on a computer.
? Directing Web Traffic: Firewalls can manage traffic redirection using NAT and port forwarding rules to route web traffic to designated servers or devices within the network.
? Blocking Specific Ports: Firewalls can enforce security policies by blocking or
allowing traffic based on port numbers, ensuring that only permitted traffic reaches internal systems.
? Application Control: While firewalls manage network traffic, preventing applications
from running typically requires software specifically designed for endpoint protection and application management.
References:
? Understanding Firewalls: Firewall Capabilities
? Network Security Best Practices: Network Security Guide

NEW QUESTION 6
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.

Answer: C

Explanation:
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

NEW QUESTION 7
What is the purpose of assigning an IP address to the management VLAN interface on a Layer 2 switch?

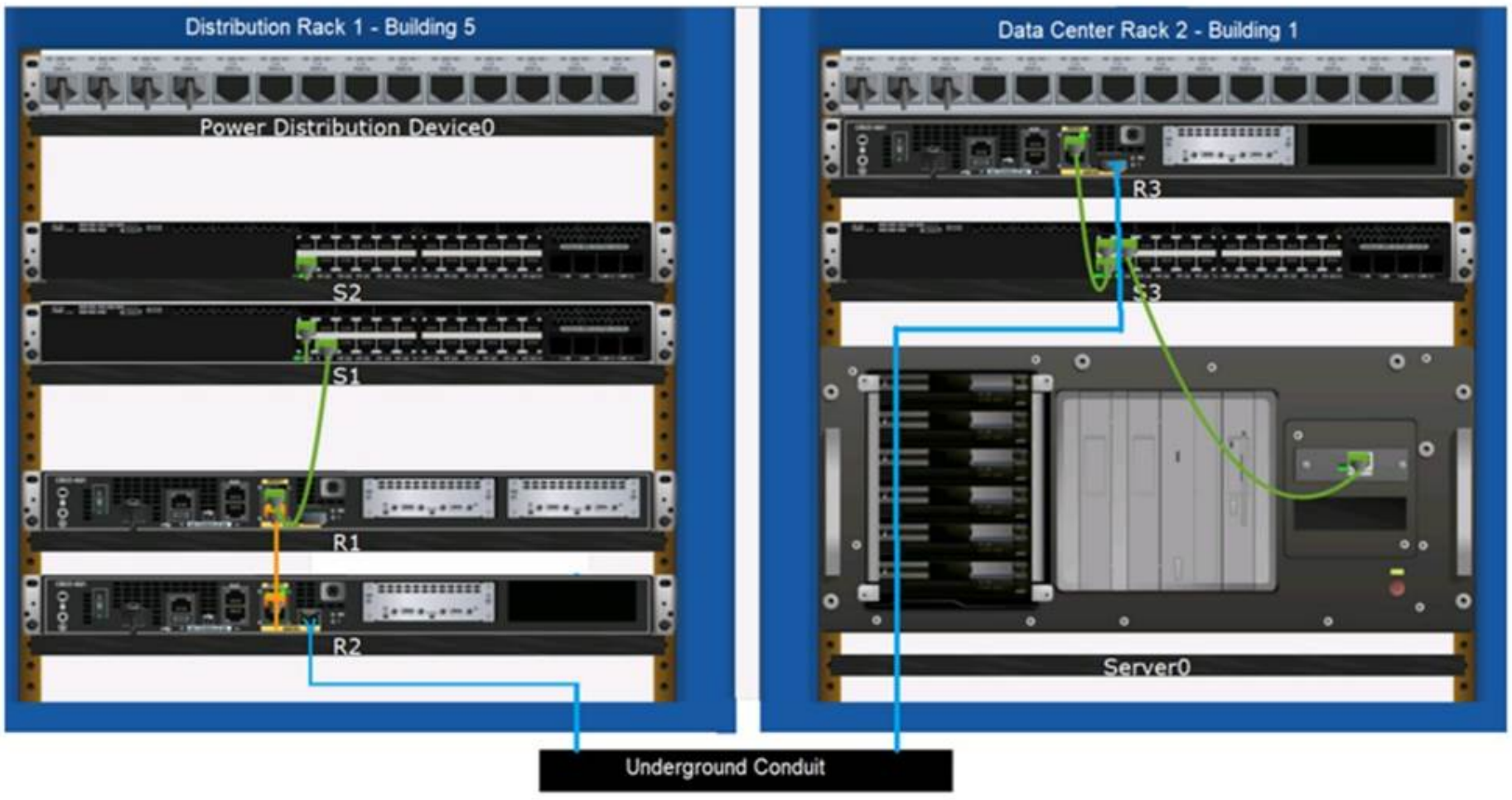
A. To enable the switch to act as a default gateway for the attached devices
B. To enable the switch to resolve URLs for the attached the devices
C. To enable the switch to provide DHCP services to other switches in the network
D. To enable access to the CLI on the switch through Telnet or SSH

Answer: D

Explanation:
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

NEW QUESTION 8
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.



Cable Types

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

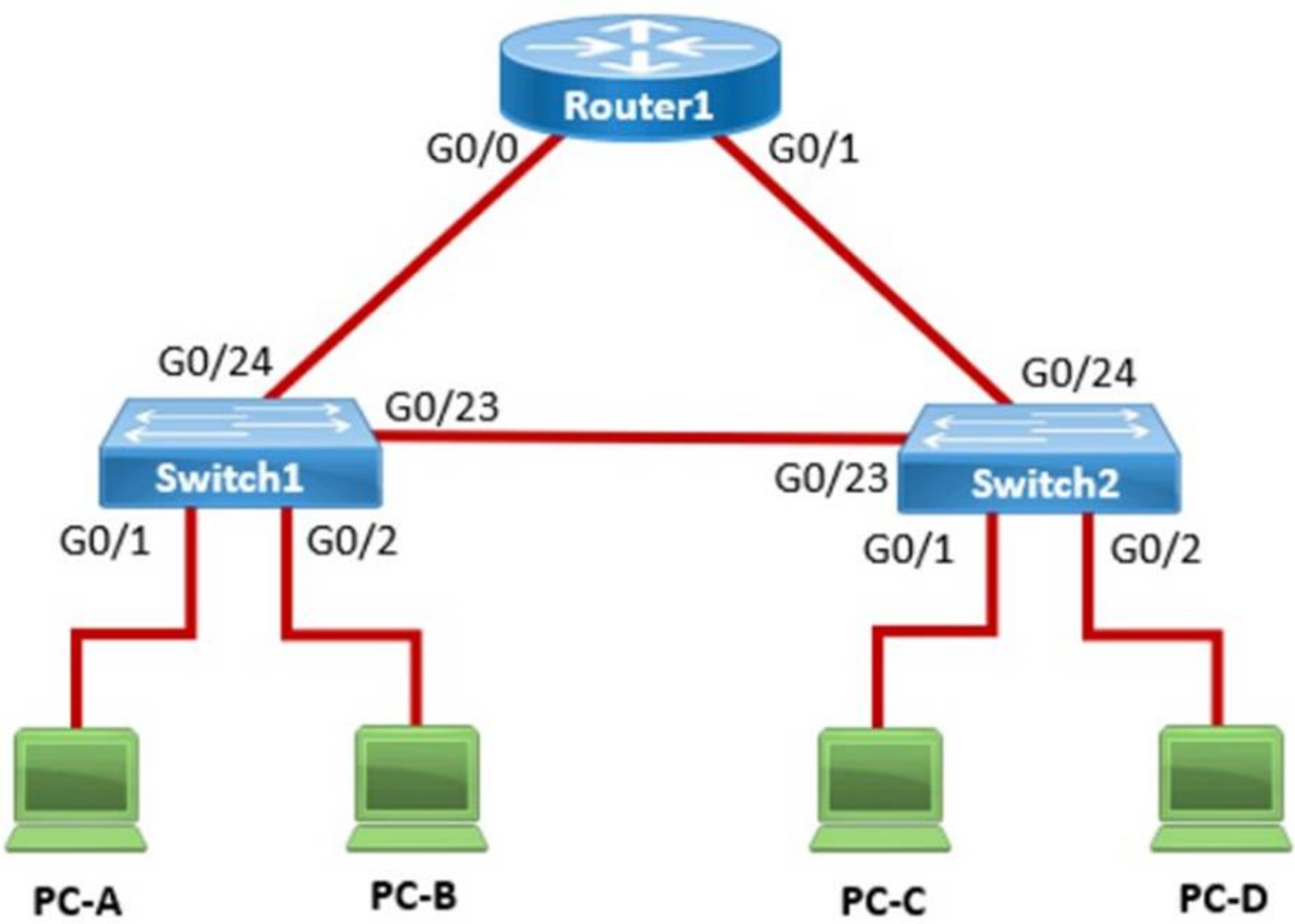
A. Mastered
B. Not Mastered

Answer: A

Explanation:
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

NEW QUESTION 9
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.

Answer: B

Explanation:
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)

NEW QUESTION 10
Which two statements are true about the IPv4 address of the default gateway configured on a host? (Choose 2.)
Note: You will receive partial credit for each correct selection.

A. The IPv4 address of the default gateway must be the first host address in the subnet.
B. The same default gateway IPv4 address is configured on each host on the local network.
C. The default gateway is the Loopback0 interface IPv4 address of the router connected to the same local network as the host.

D. The default gateway is the IPv4 address of the router interface connected to the same local network as the host.
E. Hosts learn the default gateway IPv4 address through router advertisement messages.

Answer: BD

Explanation:
•Statement B: "The same default gateway IPv4 address is configured on each host on the local network." This is true because all hosts on the same local network (subnet) use the same default gateway IP address to send packets destined for other networks.
•Statement D: "The default gateway is the IPv4 address of the router interface connected to the same local network as the host." This is true because the default gateway is the IP address of the router's interface that is directly connected to the local network.
•Statement A: "The IPv4 address of the default gateway must be the first host address in the subnet." This is not necessarily true. The default gateway can be any address within the subnet range.
•Statement C: "The default gateway is the Loopback0 interface IPv4 address of the router connected to the same local network as the host." This is not true; the default gateway is the IP address of the router's physical or logical interface connected to the local network.
•Statement E: "Hosts learn the default gateway IPv4 address through router advertisement messages." This is generally true for IPv6 with Router Advertisement (RA) messages, but not typically how IPv4 hosts learn the default gateway address.
References:
•Cisco Default Gateway Configuration: Cisco Default Gateway

NEW QUESTION 10
An engineer configured a new VLAN named VLAN2 for the Data Center team. When the teamtries to ping addresses outside VLAN2 from a computer in VLAN2, they are unable to reach them. What should the engineer configure?

A. Additional VLAN
B. Default route
C. Default gateway
D. Static route

Answer: C

Explanation:
When devices within a VLAN are unable to reach addresses outside their VLAN, it typically indicates that they do not have a configured path to external networks. The engineer should configure a default gateway for VLAN2. The default gateway is the IP address of the router??s interface that is connected to the VLAN, which will route traffic from the VLAN to other networks12.
References :=
•Understanding and Configuring VLAN Routing and Bridging on a Router Using the IRB Feature
•VLAN 2 not able to ping gateway - Cisco Community
==========
•VLANs: Virtual Local Area Networks (VLANs) logically segment network traffic to improve security and performance. Devices within the same VLAN can communicate directly.
•Default Gateway: For devices in VLAN2 to communicate with devices outside their VLAN, they need a default gateway configured. The default gateway is typically a router or Layer 3 switch that routes traffic between different VLANs and subnets.
•Additional VLAN: Not needed in this scenario as the issue is related to routing traffic outside VLAN2, not creating another VLAN.
•Default Route: While a default route on the router may be necessary, the primary issue for devices within VLAN2 is to have a configured default gateway.
•Static Route: This is used on routers to manually specify routes to specific networks but does not address the need for a default gateway on the client devices.
References:
•Cisco VLAN Configuration Guide: Cisco VLAN Configuration
•Understanding and Configuring VLANs: VLANs Guide

NEW QUESTION 13
Which information is included in the header of a UDP segment?

A. IP addresses
B. Sequence numbers
C. Port numbers
D. MAC addresses

Answer: C

Explanation:
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

NEW QUESTION 14
A Cisco PoE switch is shown in the following image. Which type of port will provide both data connectivity and power to an IP phone?

A. Port identified with number 2
B. Ports identified with numbers 3 and 4
C. Ports identified with number 6
D. Ports identified with number 7

Answer: C

Explanation:
In the provided image of the Cisco PoE switch, the ports identified with number 6 are the standard RJ-45 Ethernet ports typically found on switches that provide both data connectivity and Power over Ethernet (PoE). PoE ports are designed to supply power to devices such as IP phones, wireless access points, and other PoE-enabled devices directly through the Ethernet cable.
Ports:
•2: Console port (for management and configuration)
•3 and 4: Specific function ports (often for management)
•6: RJ-45 Ethernet ports (capable of providing PoE)
•7: SFP ports (for fiber connections, typically do not provide PoE) Thus, the correct answer is C. Ports identified with number 6. References :=
•Cisco Catalyst 2960-L Series Switches Data Sheet
•Cisco PoE Overview

NEW QUESTION 16
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
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

NEW QUESTION 18
Which protocol allows you to securely upload files to another computer on the internet?

A. SFTP
B. ICMP
C. NTP
D. HTTP

Answer: A

Explanation:
SFTP, or Secure File Transfer Protocol, is a protocol that allows for secure file transfer capabilities between networked hosts. It is a secure extension of the File Transfer Protocol (FTP). SFTP encrypts both commands and data, preventing passwords and sensitive information from being transmitted openly over the network. It is typically used for secure file transfers over the internet and is built on the Secure Shell (SSH) protocol1. References :=
•What Is SFTP? (Secure File Transfer Protocol)
•How to Use SFTP to Safely Transfer Files: A Step-by-Step Guide
•Secure File Transfers: Best Practices, Protocols And Tools
The Secure File Transfer Protocol (SFTP) is a secure version of the File Transfer Protocol (FTP) that uses SSH (Secure Shell) to encrypt all commands and data. This ensures that sensitive information, such as usernames, passwords, and files being transferred, are securely transmitted over the network.
•ICMP (Internet Control Message Protocol) is used for network diagnostics and is not designed for file transfer.
•NTP (Network Time Protocol) is used to synchronize clocks between computer systems and is not related to file transfer.
•HTTP (HyperText Transfer Protocol) is used for transmitting web pages over the internet and does not inherently provide secure file transfer capabilities.
Thus, the correct protocol that allows secure uploading of files to another computer on the internet is SFTP.
References :=
•Cisco Learning Network
•SFTP Overview (Cisco)

NEW QUESTION 19
Which two pieces of information should you include when you initially create a support ticket? (Choose 2.)

A. A detailed description of the fault
B. Details about the computers connected to the network
C. A description of the conditions when the fault occurs
D. The actions taken to resolve the fault
E. The description of the top-down fault-finding procedure

Answer: AC

Explanation:
? Statement A: "A detailed description of the fault." This is essential for support staff to understand the nature of the problem and begin troubleshooting effectively.
? Statement C: "A description of the conditions when the fault occurs." This helps in reproducing the issue and identifying patterns that might indicate the cause of the fault.
? Statement B: "Details about the computers connected to the network." While useful, this is not as immediately critical as understanding the fault itself and the conditions under which it occurs.
? Statement D: "The actions taken to resolve the fault." This is important but typically follows the initial report.
? Statement E: "The description of the top-down fault-finding procedure." This is more of a troubleshooting methodology than information typically included in an initial support ticket.
References:
? Best Practices for Submitting Support Tickets: Support Ticket Guidelines

NEW QUESTION 23
Which wireless security option uses a pre-shared key to authenticate clients?

A. WPA2-Personal
B. 802.1x
C. 802.1q
D. WPA2-Enterprise

Answer: A

Explanation:
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 connect1.
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

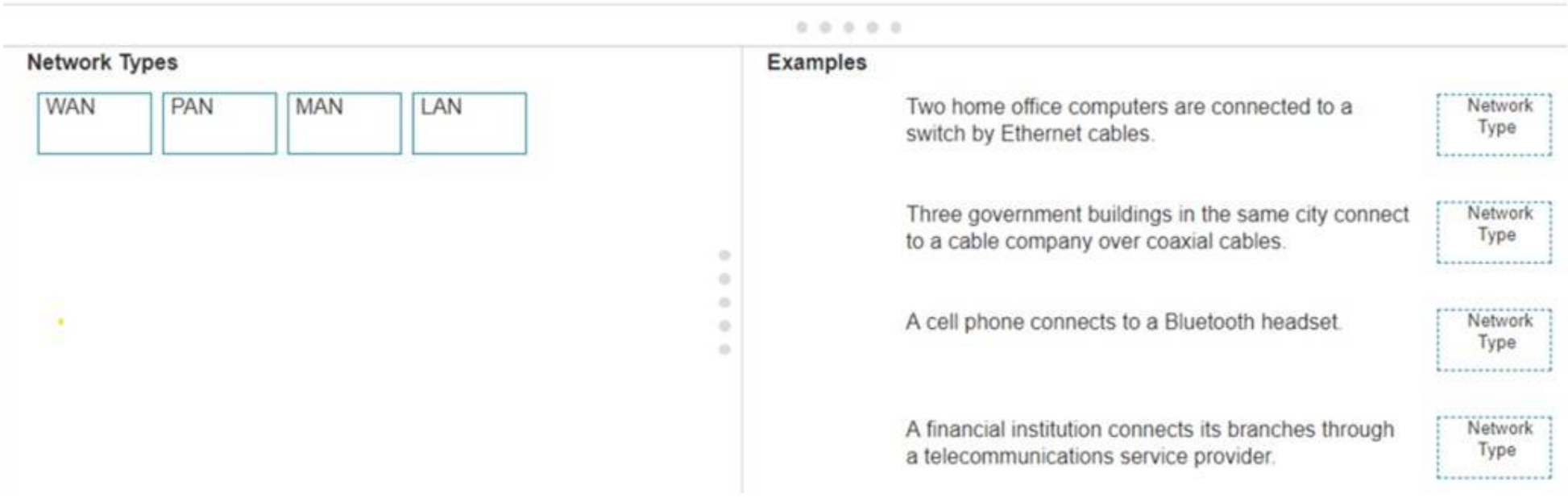
NEW QUESTION 24
Which device protects the network by permitting or denying traffic based on IP address, port number, or application?

A. Firewall
B. Access point
C. VPN gateway
D. Intrusion detection system

Answer: A

Explanation:
? 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

NEW QUESTION 26
DRAG DROP
Move each network type from the list on the left to the correct example on the right.



A. Mastered
B. Not Mastered

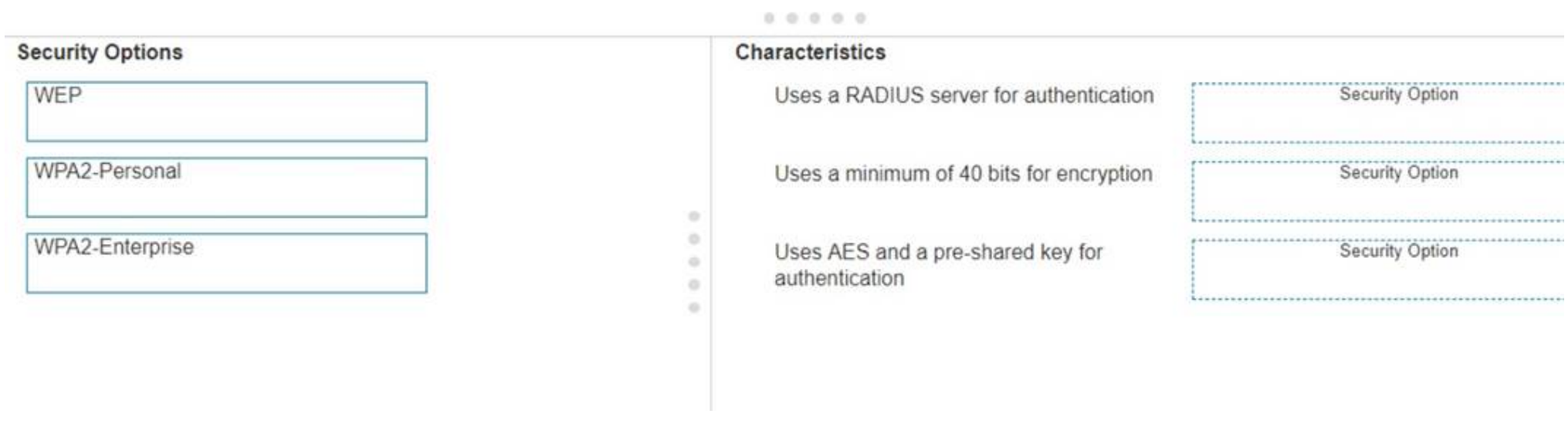
Answer: A

Explanation:
? Two home office computers are connected to a switch by Ethernet cables.
? Three government buildings in the same city connect to a cable company over coaxial cables.
? A cell phone connects to a Bluetooth headset.
? A financial institution connects its branches through a telecommunications service provider.
? LAN (Local Area Network): Used for connecting devices within a small geographical area such as a single building or home.
? MAN (Metropolitan Area Network): Covers a larger geographical area than a LAN, typically a city or campus.
? PAN (Personal Area Network): Connects devices within the range of an individual person, such as connecting a phone to a Bluetooth headset.
? WAN (Wide Area Network): Spans large geographical areas, connecting multiple LANs across cities, countries, or continents.
References:
? Network Types Overview: Cisco Networking Basics
? Understanding Different Network Types: Network Types Guide

NEW QUESTION 30
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.

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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
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.

NEW QUESTION 33
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CCST-Networking Practice Exam Features:

* CCST-Networking Questions and Answers Updated Frequently

* CCST-Networking Practice Questions Verified by Expert Senior Certified Staff

* CCST-Networking Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CCST-Networking Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year