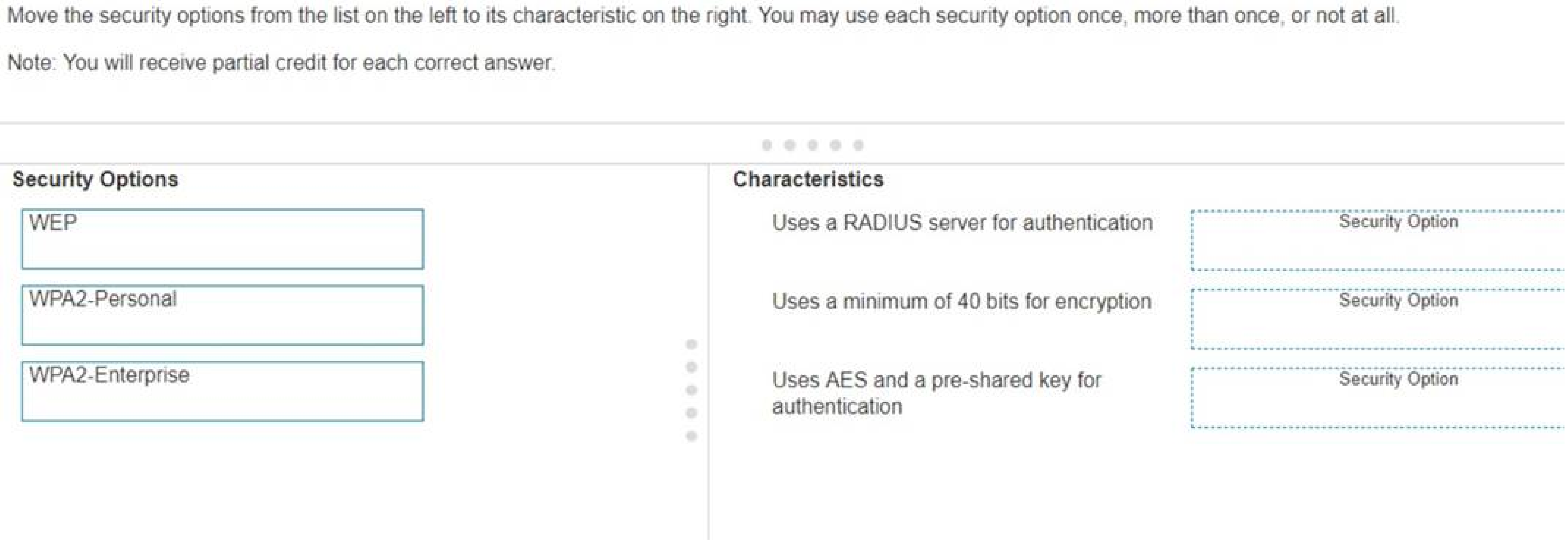
Cisco

Exam Questions 100-150

Cisco Certified Support Technician (CCST) Networking

NEW QUESTION 1
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.

Security Options

WEP

WPA2-Personal

WPA2-Enterprise

Characteristics

Uses a RADIUS server for authentication	Security Option
Uses a minimum of 40 bits for encryption	Security Option
Uses AES and a pre-shared key for authentication	Security Option

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-Enterprise uses 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 WEP (Wired Equivalent Privacy) is an outdated security protocol that uses a minimum of 40 bits for encryption (and up to 104 bits), which is relatively weak by today??s standards.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 2
An engineer configured a new VLAN named VLAN2 for the Data Center team. When the team tries 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 3
Which command will display all the current operational settings configured on a Cisco router?

A. show protocols

B. show startup-config
C. show version
D. show running-config

Answer: D

Explanation:

Router

The show running-config command is used on a Cisco router to display the current operational settings that are actively configured in the router??s RAM. This command outputs all the configurations that are currently being executed by the router, which includes interface configurations, routing protocols, access lists, and other settings. Unlike show startup-config, which shows the saved configuration that the router will use on the next reboot, show running-config reflects the live, current configuration in use.
References := The information is supported by multiple sources that detail the use of Cisco commands, particularly the show running-config command as the standard for viewing the active configuration on a Cisco device123.
? show running-config: This command displays the current configuration running on the router. It includes all the operational settings and configurations applied to the router.
? show protocols: This command shows the status of configured protocols on the
router but not the entire configuration.
? show startup-config: This command displays the configuration saved in NVRAM, which is used to initialize the router on startup, but not necessarily the current running configuration.
? show version: This command provides information about the router's software version, hardware components, and uptime but does not display the running configuration.
References:
? Cisco IOS Commands: Cisco IOS Commands

NEW QUESTION 4
A local company requires two networks in two new buildings. The addresses used in these networks must 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

Answer: AD

Explanation:
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 172.31.255.255 falls within the Class B private range.
* B. 192.16.0.0 to 192.16.255.255 is not a recognized private IP range. C. 11.0.0.0 to 11.255.255.255 is 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
A and D. References :=
? Reserved IP addresses on Wikipedia
? Private IP Addresses in Networking - GeeksforGeeks
? Understanding Private IP Ranges, Uses, Benefits, and Warnings

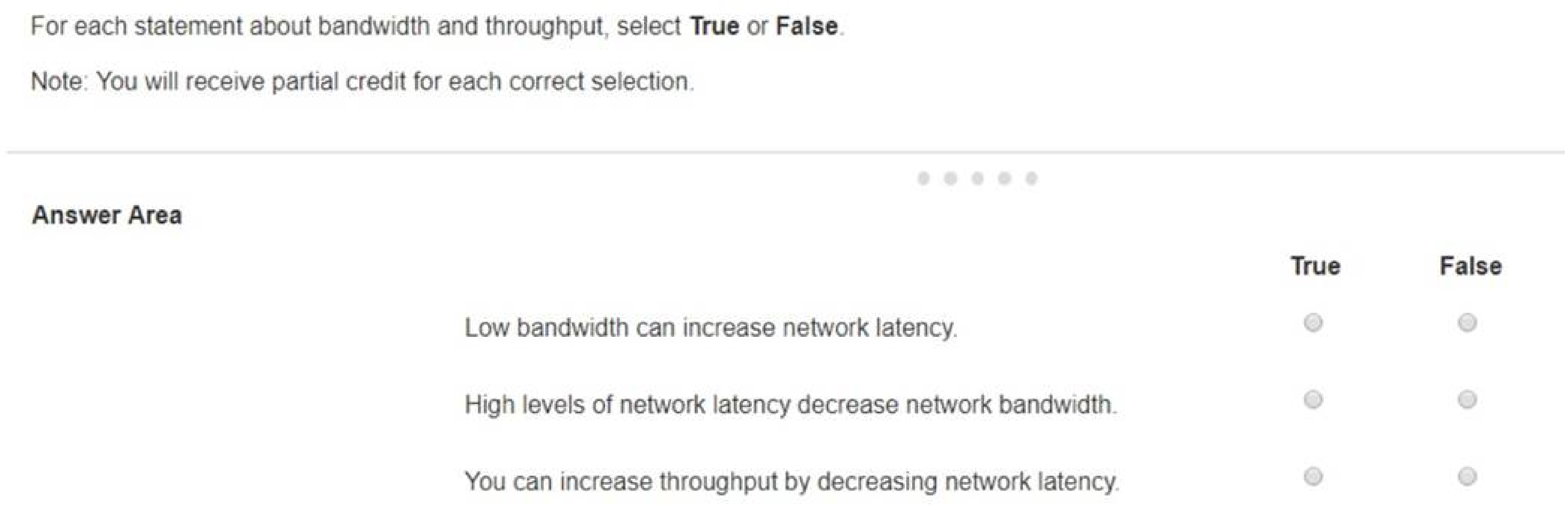
NEW QUESTION 5
A help desk technician receives the four trouble tickets listed below. Which ticket should receive the highest priority and be addressed first?

A. Ticket 1: A user requests relocation of a printer to a different network jack in the same offic
B. The jack must be patched and made active.
C. Ticket 2: An online webinar is taking place in the conference roo
D. The video conferencing equipment lost internet access.
E. Ticket 3: A user reports that response time for a cloud-based application is slower than usual.
F. Ticket 4: Two users report that wireless access in the cafeteria has been down for the last hour.

Answer: B

Explanation:
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

NEW QUESTION 6
For each statement about bandwidth and throughput, select True or False.
Note: You will receive partial credit for each correct selection.



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.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? 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

NEW QUESTION 7
A host is given the IP address 172.16.100.25 and the subnet mask 255.255.252.0.
What is the CIDR notation for this address?

A. 172.16.100.25 /23
B. 172.16.100.25 /20
C. 172.16.100.25 /21
D. 172.16.100.25 /22

Answer: D

Explanation:
The CIDR (Classless Inter-Domain Routing) notation for the subnet mask 255.255.252.0 is /22. This notation indicates that the first 22 bits of the IP address are used for network identification, and the remaining bits are used for host addresses within the network1. References :=

•Subnet Cheat Sheet – 24 Subnet Mask, 30, 26, 27, 29, and other IP Address CIDR Network References
==========================
•Subnet Mask to CIDR Notation: The given subnet mask is 255.255.252.0. To convert this to CIDR notation:
•Convert the subnet mask to binary: 11111111.11111111.11111100.00000000
•Count the number of consecutive 1s in the binary form: There are 22 ones.
•Therefore, the CIDR notation is /22. References:
•Understanding Subnetting and CIDR: Cisco CIDR Guide

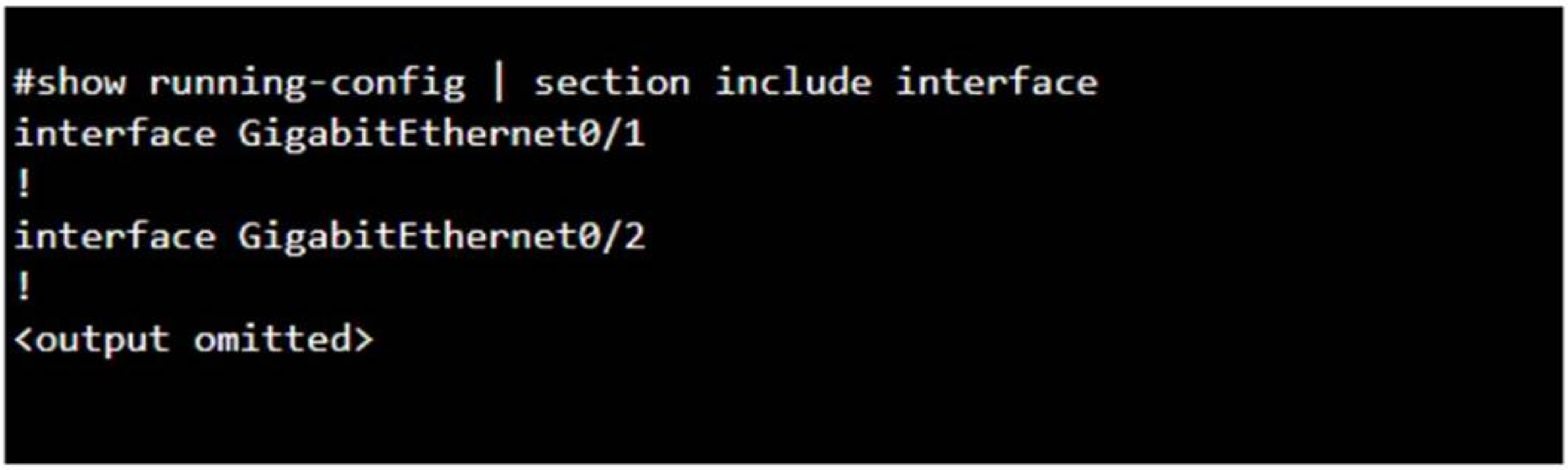
NEW QUESTION 8
What is the most compressed valid format of the IPv6 address 2001:0db8:0000:0016:0000:001b: 2000:0056?

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

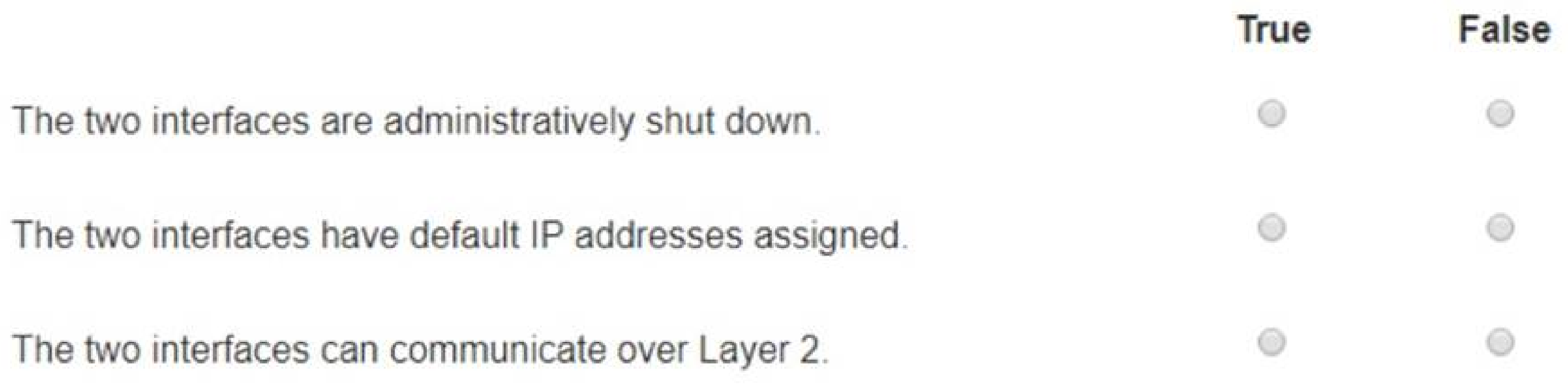
Explanation:
IPv6 addresses can be compressed by removing leading zeros and replacing consecutive groups of zeros with a double colon (::). Here??s how to compress the address 2001:0db8:0000:0016:0000:001b:2000:0056:
? Remove leading zeros from each segment:
? Replace the longest sequence of consecutive 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 9
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.



	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.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? 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

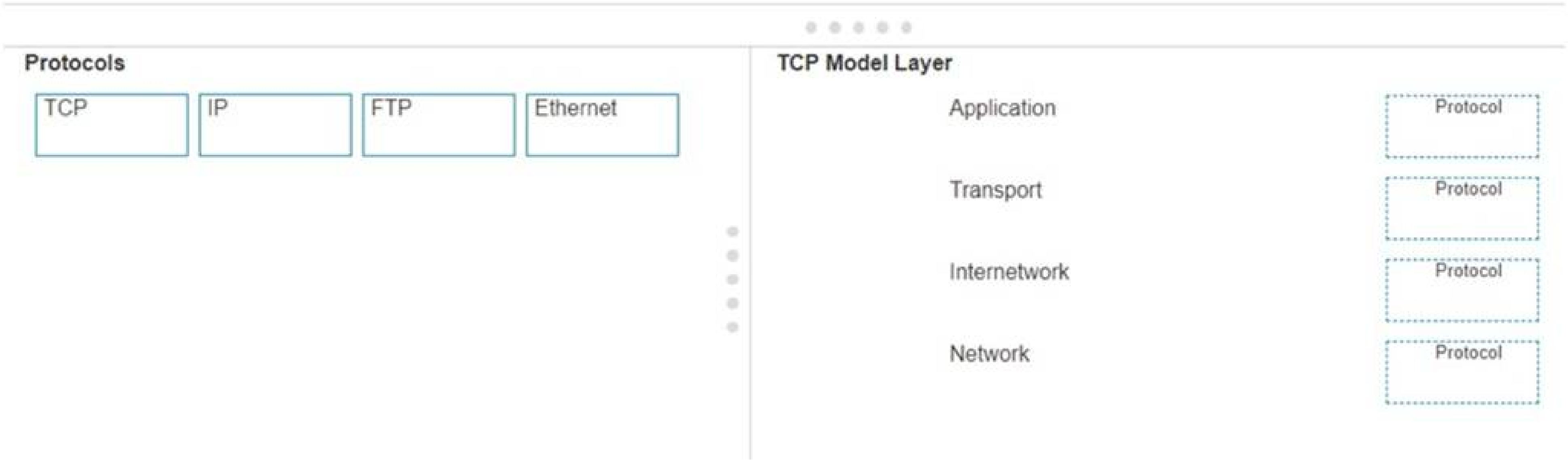
NEW QUESTION 10
Which wireless security option uses a pre-shared key to authenticate clients?

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 10
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 the Transport layer, which is responsible for providing communication between applications on different hosts1.
? IP (Internet Protocol): IP is part of the Internetwork layer, which is tasked with routing packets across network boundaries to their destination1.
? FTP (File Transfer Protocol): FTP operates at the Application layer, 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 the Network Interface layer, 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 15
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 19
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 23
......