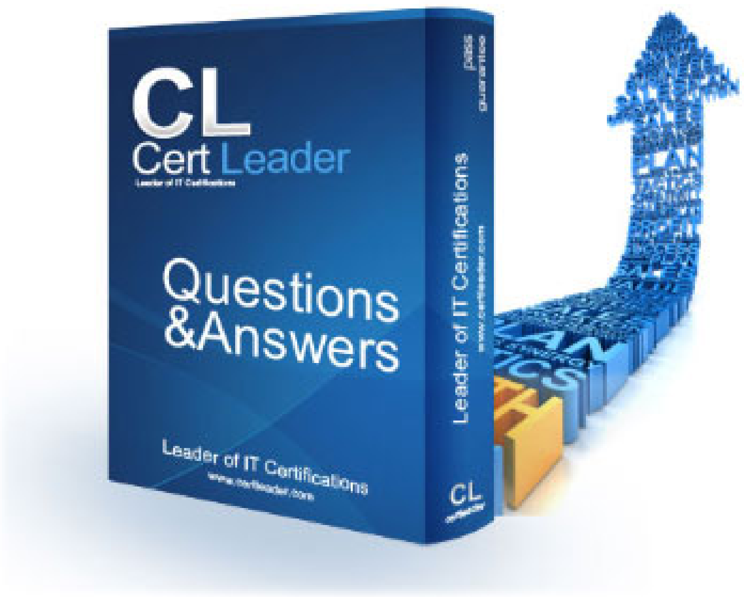
CCST-Networking Dumps

Cisco Certified Support Technician (CCST) NetworkingExam

https://www.certleader.com/CCST-Networking-dumps.html



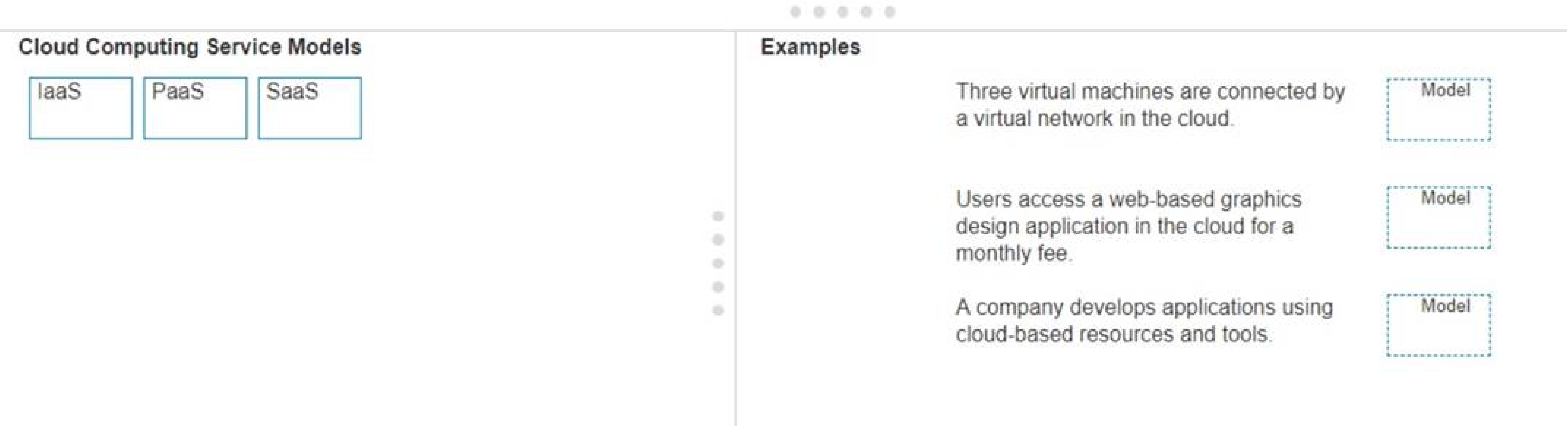
NEW QUESTION 1
A host is given the IP address 172.16.100.25 and the subnet mask 255.255.252.0. What is the CIDR notation for this address?

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 2
DRAG DROP
Move each cloud computing service model from the list on the left to the correct example on the right
Note: You will receive partial credit for each correct answer.



Cloud Computing Service Models

IaaS PaaS SaaS

Examples

Three virtual machines are connected by a virtual network in the cloud. Model

Users access a web-based graphics design application in the cloud for a monthly fee. Model

A company develops applications using cloud-based resources and tools. Model

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Three virtual machines are connected by a virtual network in the cloud.
? Users access a web-based graphics design application in the cloud for a monthly fee.
? A company develops applications using cloud-based resources and tools.
? IaaS (Infrastructure as a Service): Provides virtualized hardware resources that customers can use to build their own computing environments.
? PaaS (Platform as a Service): Offers a platform with tools and services to develop,
test, and deploy applications.
? SaaS (Software as a Service): Delivers fully functional applications over the internet that users can access and use without managing the underlying infrastructure.
References:
? Cloud Service Models: Understanding IaaS, PaaS, SaaS
? NIST Definition of Cloud Computing:NIST Cloud Computing

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:

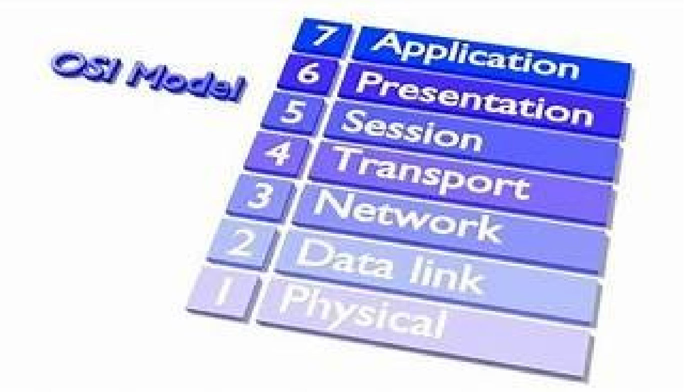
Router
Theshow running-configcommand is used on a Cisco router to display the current operational settings that are actively configured in the router??s RAM. This command outputs all the configurations that are currently being executed by the router, which includes interface configurations, routing protocols, access lists, and other settings. Unlikeshow startup-config, which shows the saved configuration that the router will use on the next reboot,show running-configreflects the live, current configuration in use.
References:= The information is supported by multiple sources that detail the use of Cisco commands, particularly theshow running-configcommand 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
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

Answer: C

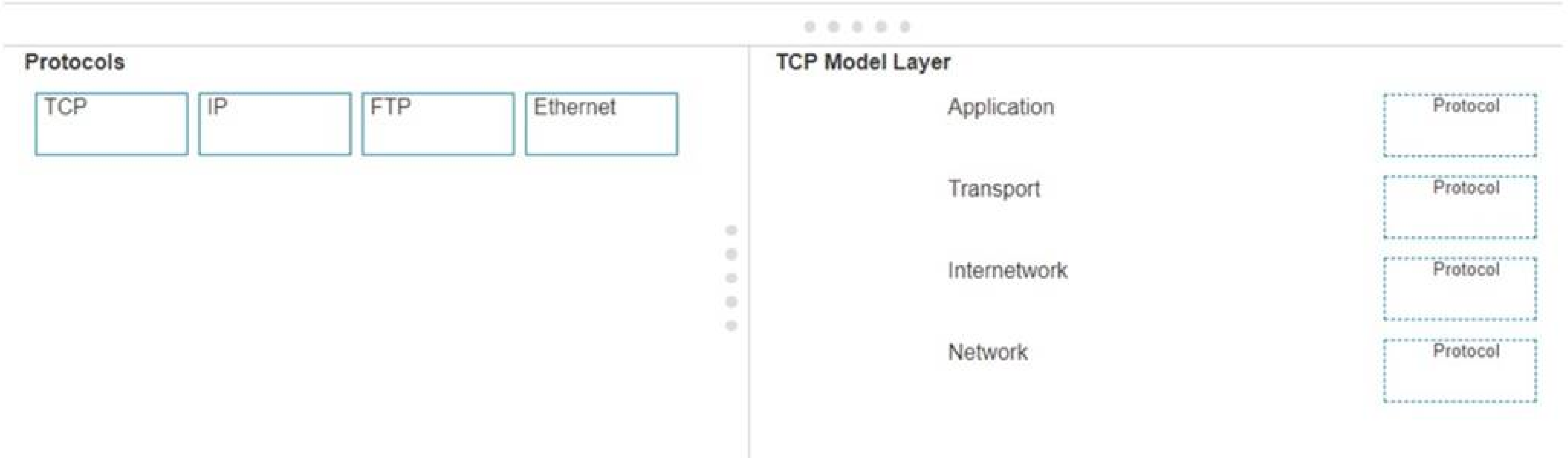
Explanation:
OSI model



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

NEW QUESTION 5
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.



Protocols

TCP | IP | FTP | Ethernet

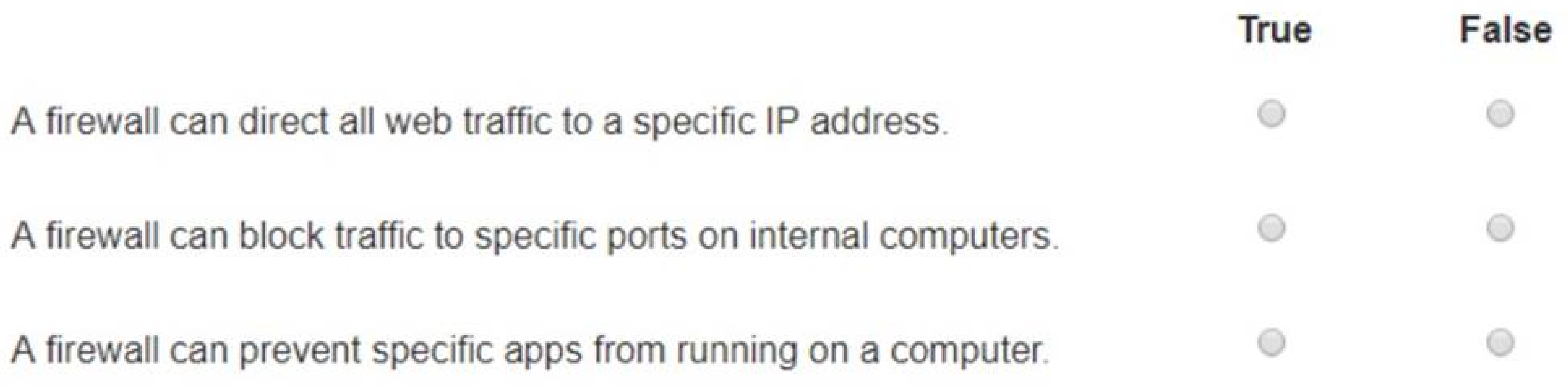
TCP Model Layer	
Application	Protocol
Transport	Protocol
Internetwork	Protocol
Network	Protocol

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 6
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.



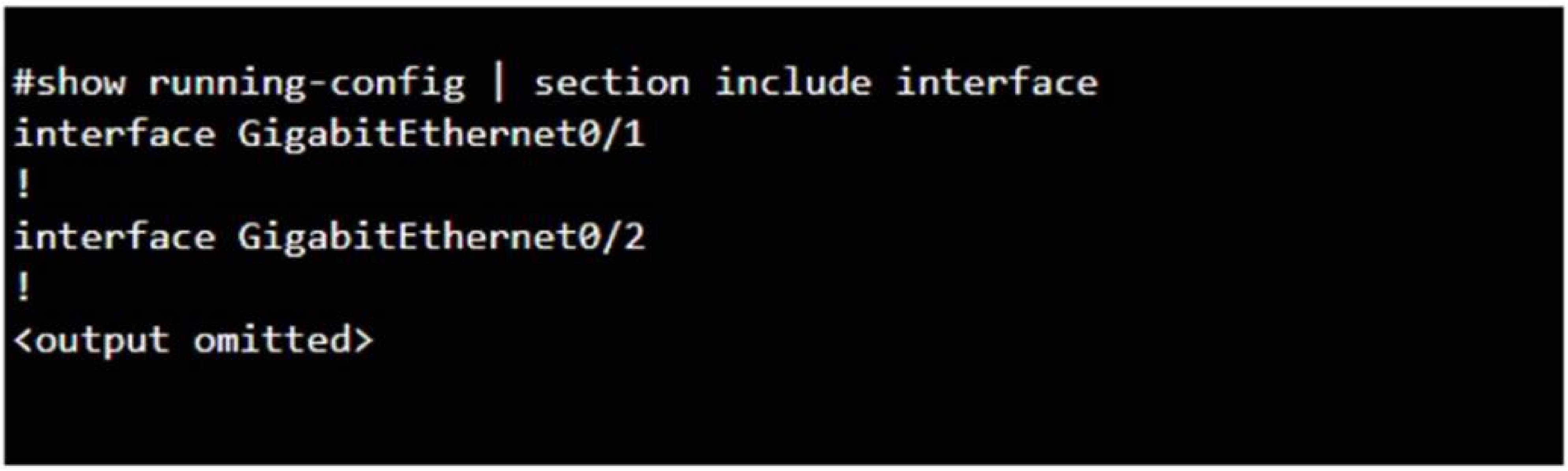
	True	False
A firewall can direct all web traffic to a specific IP address.	○	○
A firewall can block traffic to specific ports on internal computers.	○	○
A firewall can prevent specific apps from running on a computer.	○	○

A. Mastered
B. Not Mastered

Answer: A

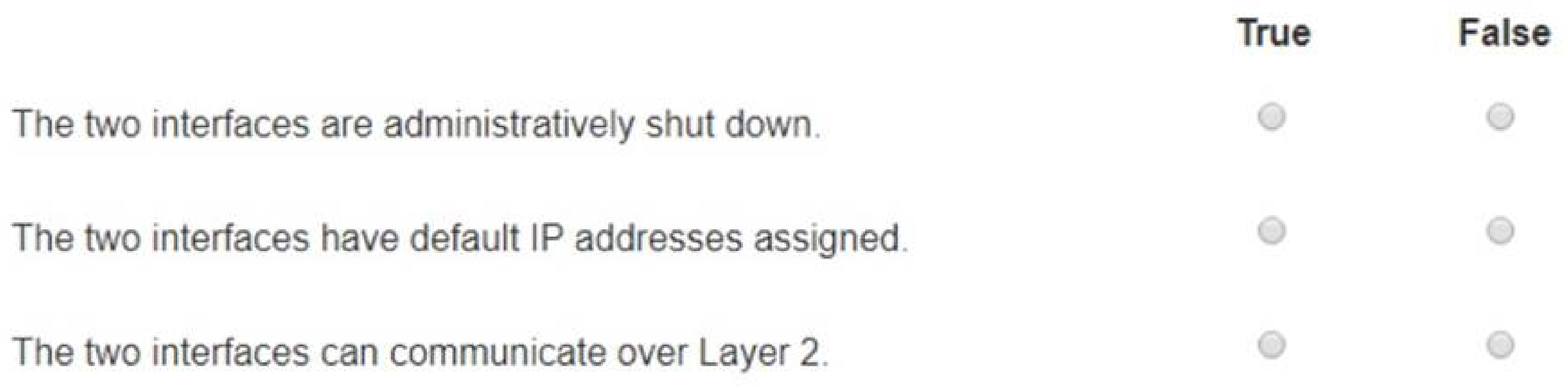
Explanation:
? A firewall can direct all web traffic to a specific IP address.
? A firewall can block traffic to specific ports on internal computers.
? A firewall can prevent specific apps from running on a computer.
? Directing Web Traffic: Firewalls can manage traffic redirection using NAT and port 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 7
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.



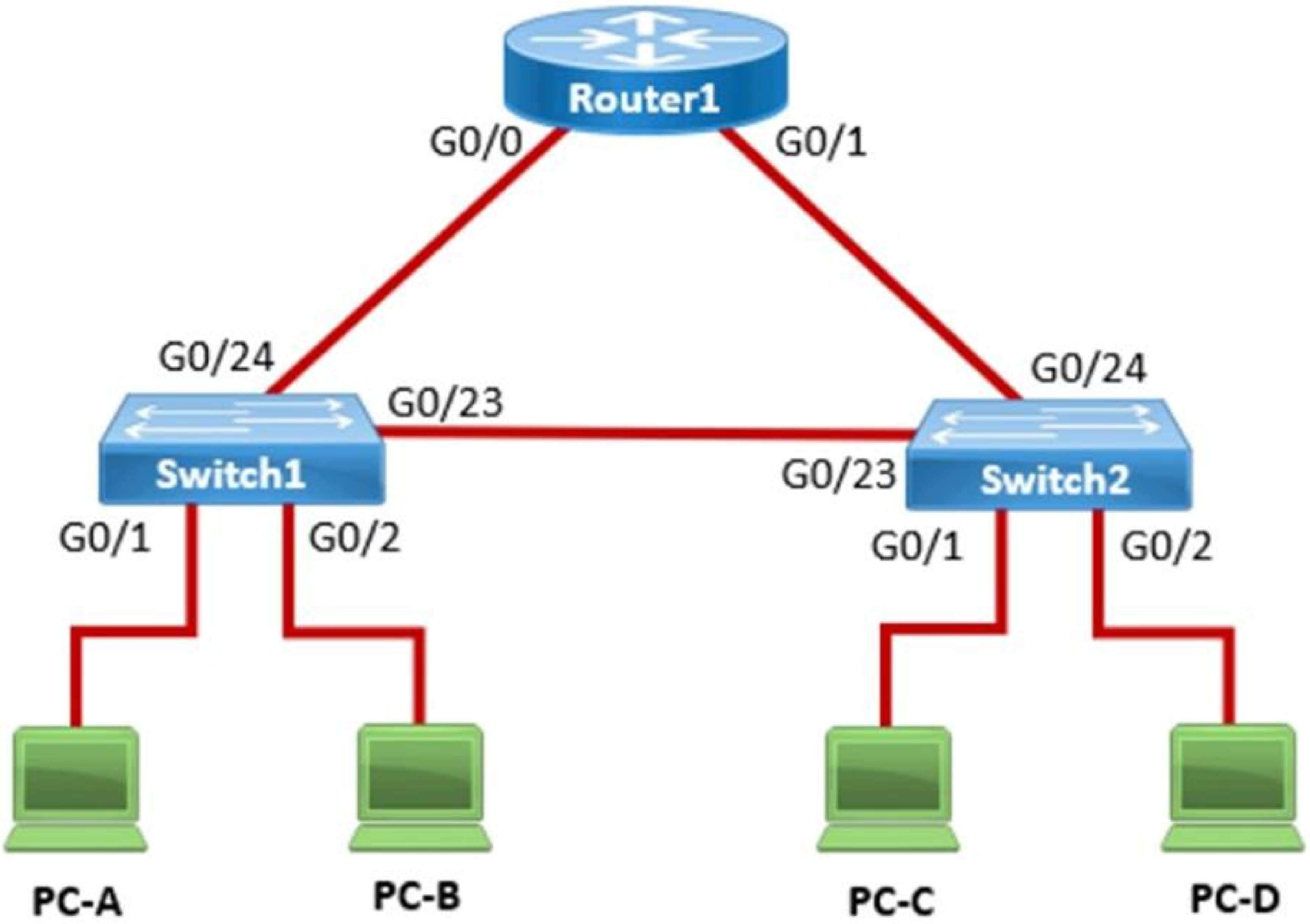
	True	False
The two interfaces are administratively shut down.	○	○
The two interfaces have default IP addresses assigned.	○	○
The two interfaces can communicate over Layer 2.	○	○

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 8
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 9
A user initiates a trouble ticket stating that an external web page is not loading. You determine that other resources both internal and external are still reachable. Which command can you use to help locate where the issue is in the network path to the external web page?

A. ping -t
B. tracert
C. ipconfig/all
D. nslookup

Answer: B

Explanation:
The tracert command is used to determine the route taken by packets across an IP network. When a user reports that an external web page is not loading, while other resources are accessible, it suggests there might be an issue at a certain point in the network path to the specific web page. The tracert command helps to diagnose where the breakdown occurs by displaying a list of routers that the packets pass through on their way to the destination. It can identify the network segment where the packets stop progressing, which is valuable for pinpointing where the connectivity issue lies. References := Cisco CCST Networking Certification FAQs – CISCONET Training Solutions, Command Prompt (CMD): 10 network-related commands you should know, Network Troubleshooting Commands Guide: Windows, Mac & Linux - Comparitech, How to Use the Traceroute and Ping Commands to Troubleshoot Network, Network Troubleshooting Techniques: Ping,
Traceroute, PathPing.
•tracert Command: This command is used to determine the path packets take to reach a destination. It lists all the hops (routers) along the way and can help identify where the delay or failure occurs.

•ping -t: This command sends continuous ping requests and is useful for determining if a host is reachable but does not provide path information.
•ipconfig /all: This command displays all current TCP/IP network configuration values and can be used to verify network settings but not to trace a network path.
•nslookup: This command queries the DNS to obtain domain name or IP address mapping, useful for DNS issues but not for tracing network paths.
References:
•Microsoft tracert Command: tracert Command Guide
•Troubleshooting Network Issues with tracert: Network Troubleshooting Guide

NEW QUESTION 10
A Cisco switch is not accessible from the network. You need to view its running configuration.
Which out-of-band method can you use to access it?

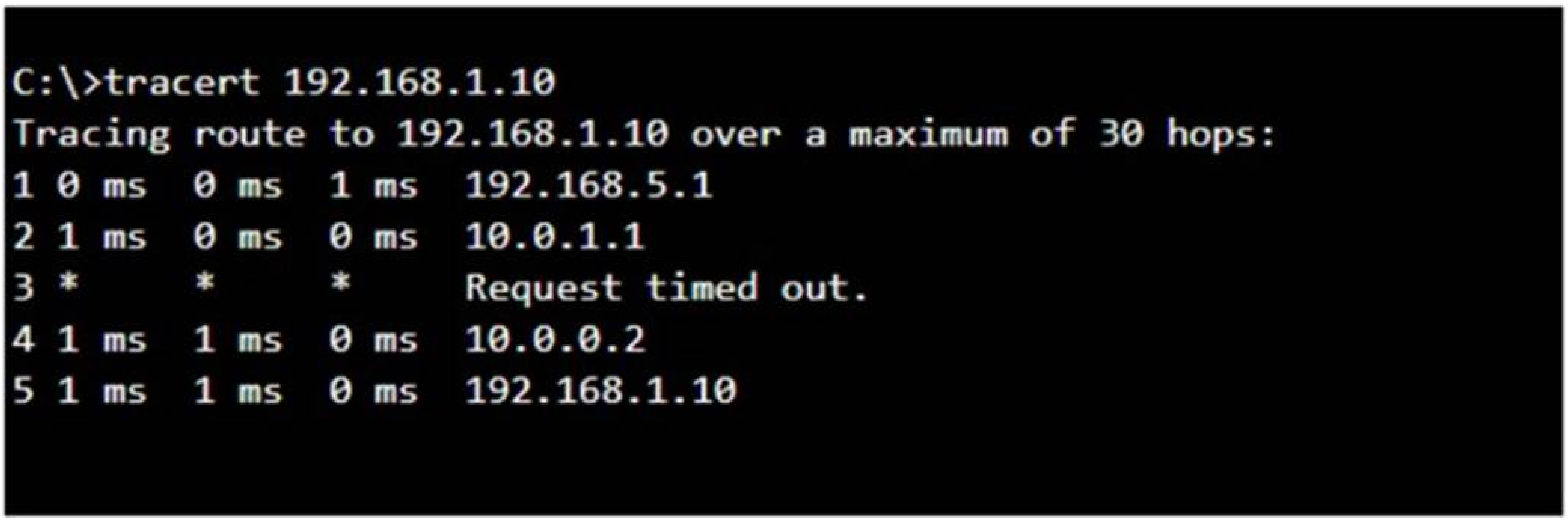
A. SNMP
B. Console
C. SSH
D. Telnet

Answer: B

Explanation:

Out-of-band management
When a Cisco switch is not accessible from the network, the recommended out-of-band method to access its running configuration is through theconsole port. Out-of-band management involves accessing the network device through a dedicated management channel that is not part of the data network.The console port provides direct access to the switch??s Command Line Interface (CLI) without using the network, which is essential when the switch cannot be accessed remotely via the network12.
References:=
? Out-of-band (OOB) network interface configuration guidelines
? Out of band management configuration
========================
If you have any more questions or need further assistance, feel free to ask!

NEW QUESTION 10
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:



```
C:\>tracert 192.168.1.10
Tracing route to 192.168.1.10 over a maximum of 30 hops:
1 0 ms  0 ms  1 ms  192.168.5.1
2 1 ms  0 ms  0 ms  10.0.1.1
3 *     *     *     Request timed out.
4 1 ms  1 ms  0 ms  10.0.0.2
5 1 ms  1 ms  0 ms  192.168.1.10
```

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.

Answer: C

Explanation:
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 reachable12. References :=
•How to Use Traceroute Command to Read Its Results
•How to Use the Tracert Command in Windows

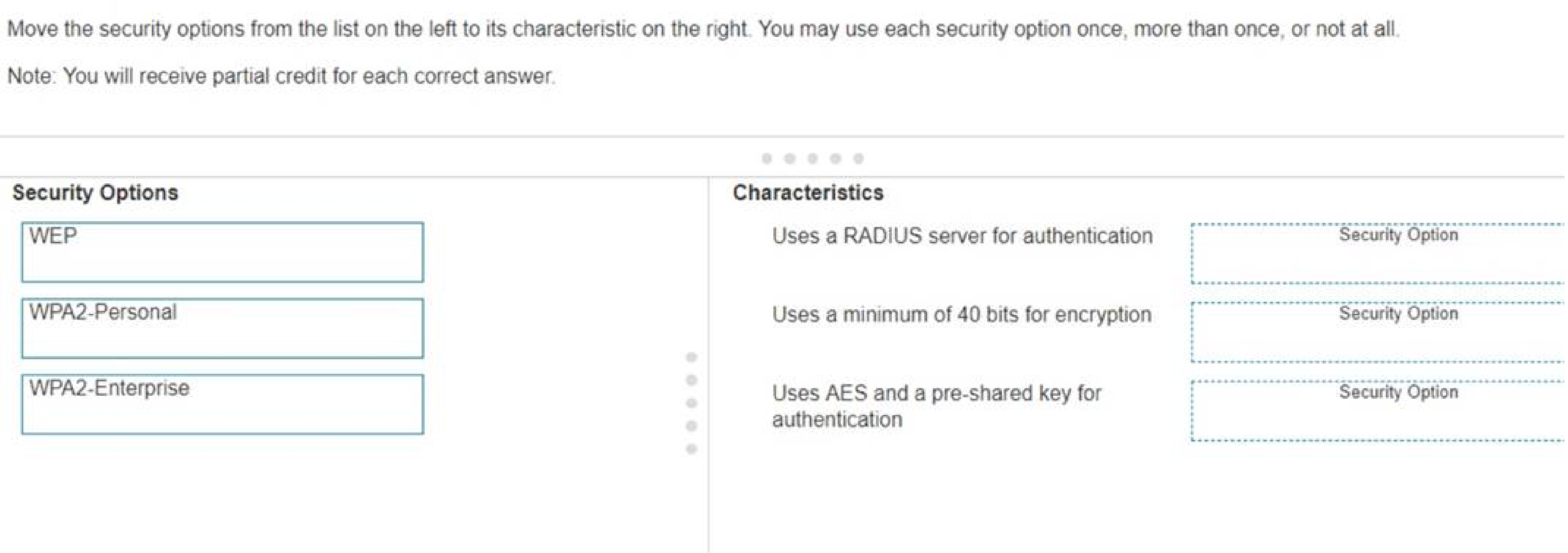
NEW QUESTION 13
Which device protects the network by permitting or denying traffic based on IP address, port number, or application?

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 18
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-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 23
......