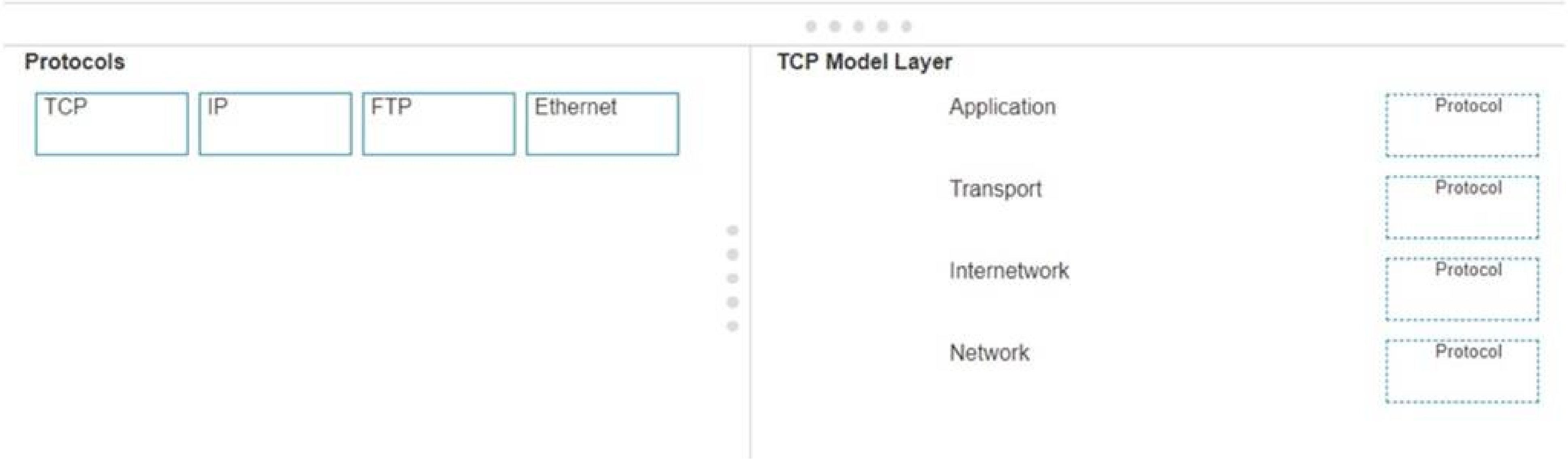
Cisco

Exam Questions CCST-Networking

Cisco Certified Support Technician (CCST) NetworkingExam

NEW 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.



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 2
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 3
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

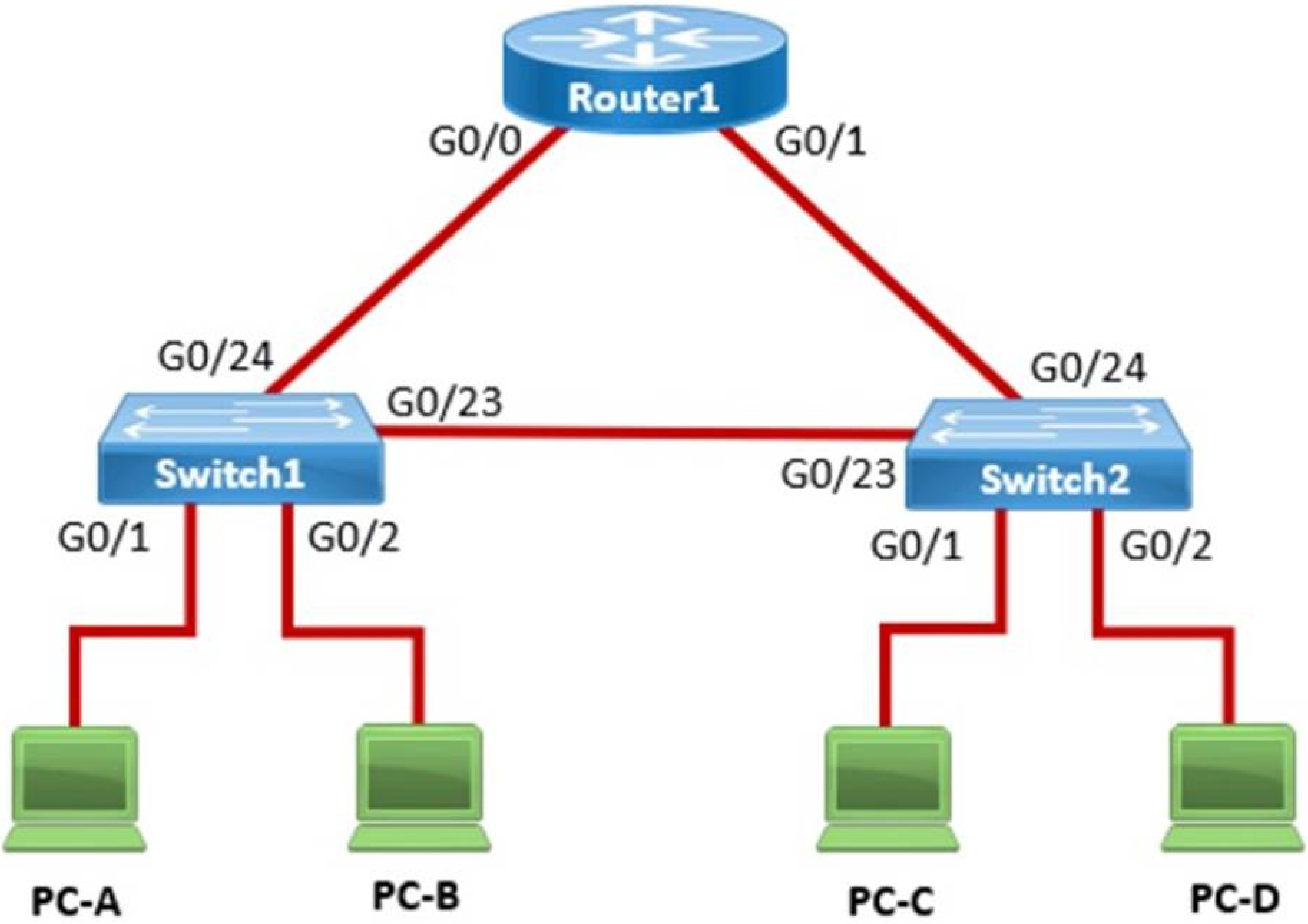
NEW QUESTION 4
Which standard contains the specifications for Wi-Fi networks?

A. GSM
B. LTE
C. IEEE 802.11
D. IEEE 802.3
E. EIA/TIA 568A

Answer: C

Explanation:
The IEEE 802.11 standard contains the specifications for Wi-Fi networks. It is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in various frequencies, including but not limited to 2.4 GHz, 5 GHz, and 6 GHz1. This standard is maintained by the Institute of Electrical and Electronics Engineers (IEEE) and is commonly referred to as Wi-Fi. The standard has evolved over time to include several amendments that improve speed, range, and reliability of wireless networks.
References :=
•The Most Common Wi-Fi Standards and Types, Explained
•802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a
•Wi-Fi Standards Explained - GeeksforGeeks
========================

NEW QUESTION 5
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 6
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 7
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 8
You want to store files that will be accessible by every user on your network. Which endpoint device do you need?

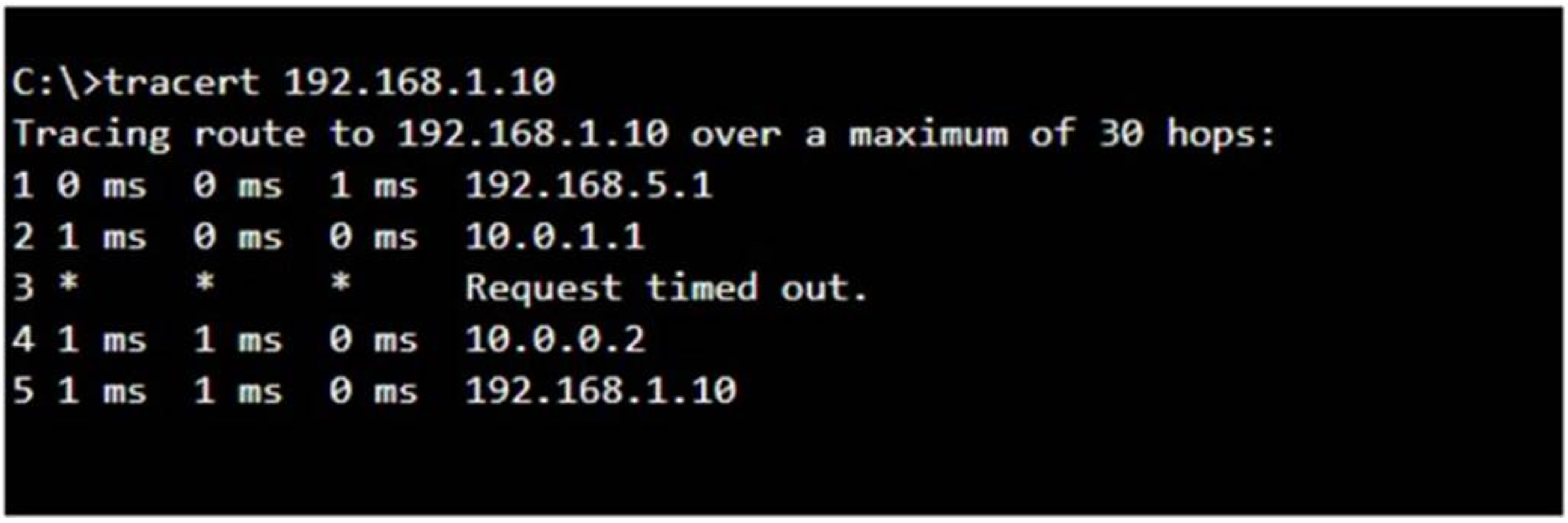
A. Access point
B. Server
C. Hub

D. Switch

Answer: B

Explanation:
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)

NEW QUESTION 9
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 10
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 10
......