

Cisco

Exam Questions 100-150

Cisco Certified Support Technician (CCST) Networking



NEW QUESTION 1

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 2

Which command will display the following output?

Image is command output that states the following.

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
esxi	Gig 0/5	177	S	VMware ES	vmnic0
esxi	Gig 0/7	177	S	VMware ES	vmnic1
esxi	Gig 0/6	177	S	VMware ES	vmnic2
981888fc23a7	Gig 0/47	160	R S	Meraki MR	Port 0
3456fec1d08	Gig 0/1	178	S	MS120-8LP	Port 9"

- A. show mac-address-table
- B. show cdp neighbor
- C. show inventory
- D. show ip interface

Answer: B

Explanation:

The command that will display the output provided, which includes capability codes, local interface details, device IDs, hold times, and platform port ID capabilities, is the show cdp neighbor command. This command is used in Cisco devices to display current information about neighboring devices detected by Cisco Discovery Protocol (CDP), which includes details such as the interface through which the neighbor is connected, the type of device, and the port ID of the device1.

References :=

- Cisco - show cdp neighbors

The provided output is from the Cisco Discovery Protocol (CDP) neighbor table. The show cdp neighbor command displays information about directly connected Cisco devices, including Device ID, Local Interface, Holdtime, Capability, Platform, and Port ID.

- A. show mac-address-table: Displays the MAC address table on the switch.
- C. show inventory: Displays information about the hardware inventory of the device.
- D. show ip interface: Displays IP interface status and configuration. Thus, the correct answer is B. show cdp neighbor.

References :=

- Cisco CDP Neighbor Command
- Understanding CDP

NEW QUESTION 3

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

Answer: B

Explanation:

- 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.
- 192.168.201.13: 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

NEW QUESTION 4

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 without blinking.

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

- Cisco Switch LED Indicators
- Cisco Ethernet Switch LED Patterns

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 office.
- B. The jack must be patched and made active.
- C. Ticket 2: An online webinar is taking place in the conference room.
- 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.

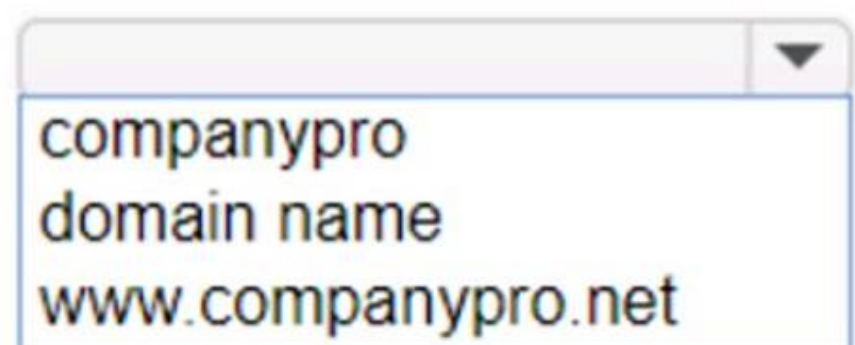
References :=

- ? IT Help Desk Best Practices
- ? Prioritizing IT Support Tickets

NEW QUESTION 6

HOTSPOT

You want to list the IPv4 addresses associated with the host name www.companypro.net.



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=A option, which stands for Address records that hold IPv4 addresses1. However, the nslookup command by default should return the IPv4 address if available.
To list the IPv4 addresses associated with the host name www.companypro.net, you should use the nslookup command.
? Command: nslookup
? Target: www.companypro.net So, the completed command is:
? nslookup www.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 7

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.	<input type="radio"/>	<input type="radio"/>
A firewall can block traffic to specific ports on internal computers.	<input type="radio"/>	<input type="radio"/>
A firewall can prevent specific apps from running on a computer.	<input type="radio"/>	<input type="radio"/>

A. Mastered
B. Not Mastered

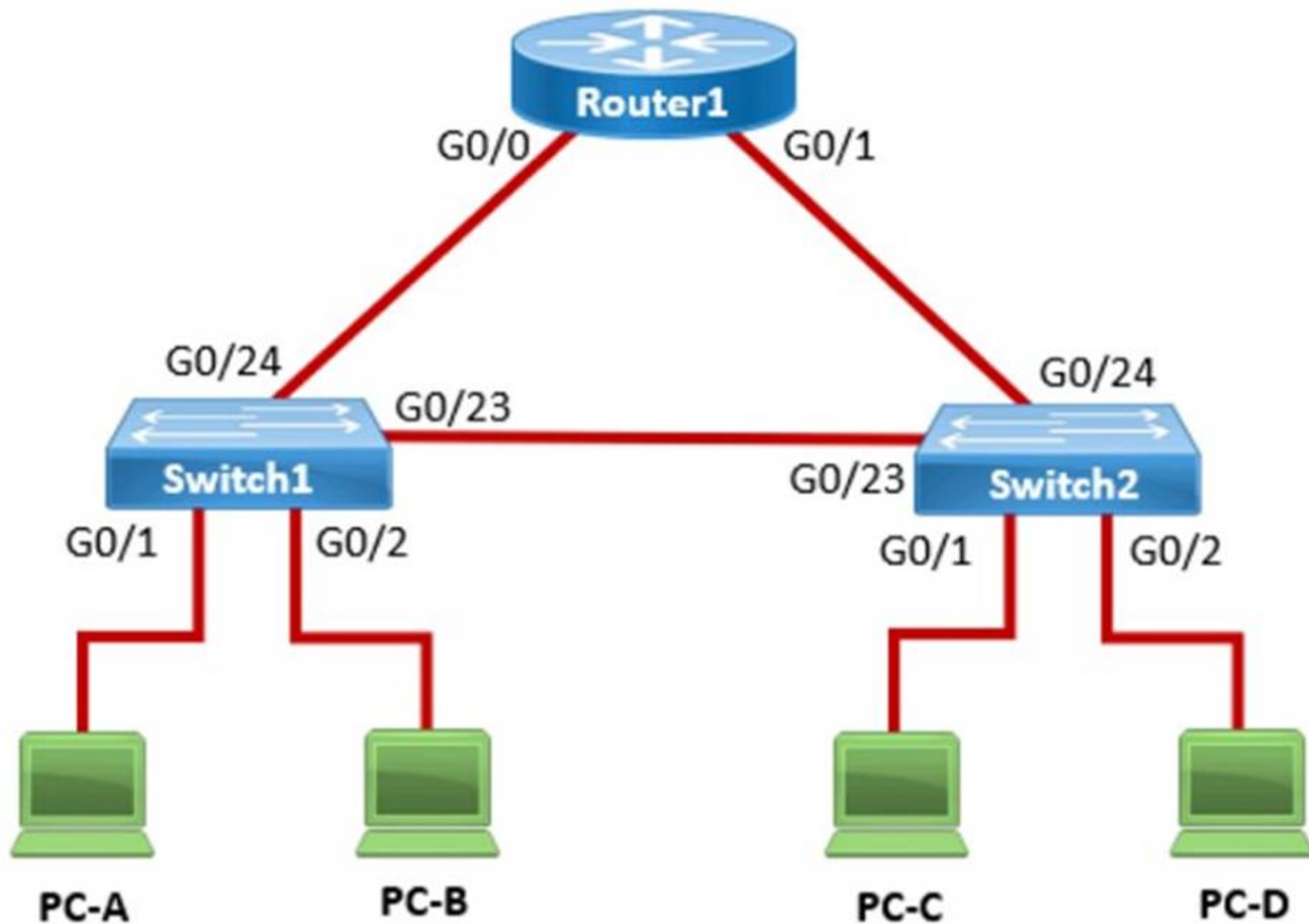
Answer: A

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

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: C

Explanation:

Understanding How Layer 2 Switches Handle Unknown MAC Addresses Switches operate at Layer 2 (Data Link Layer) of the OSI model and maintain a MAC address table (CAM table) to forward frames efficiently.

? When a switch receives a frame, it checks its MAC address table to see if it knows the destination MAC address.

? If the destination MAC address is not in the table (meaning the switch does not know which port leads to PC-C), the switch follows the flooding behavior.

What Happens When Switch1 Receives a Frame from PC-A to PC-C?

? Switch1 checks its MAC table:

? Switch1 does not know where PC-C is:

? Switch2 receives the frame and follows the same process:

? Once PC-C responds, Switch1 and Switch2 learn its MAC address and update their tables.

Why Other Options Are Incorrect:

* A. Switch1 queries Switch2 for the MAC address of PC-C.

? Incorrect: Switches do not query other switches directly for MAC addresses.

Instead, they rely on learning MAC addresses dynamically through frame forwarding.

* B. Switch1 drops the frame and sends an error message back to PC-A.

? Incorrect: Switches do not drop frames for unknown MAC addresses. Instead, they flood the frames out all ports except the incoming port.

* D. Switch1 sends an ARP request to obtain the MAC address of PC-C.

? Incorrect:

Conclusion

Since Switch1 does not know the destination MAC address, it floods the frame out all active ports except the port it was received on. This is the default behavior of Layer 2 switches when they encounter an unknown MAC address.

Thus, the correct answer is: C. Switch1 floods the frame out all active ports except port G0/1.

References

? Cisco CCNA 200-301 Official Guide – MAC Address Table & Frame Forwarding

? RFC 894 – Standard for Ethernet Frame Forwarding

? Cisco Networking Essentials – Switch Flooding Behavior

NEW QUESTION 9

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 10

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 switch.

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 10

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 11

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, the Data Link layer of 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 16

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 19

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 includes port 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 23

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

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

100-150 Practice Exam Features:

- * 100-150 Questions and Answers Updated Frequently
- * 100-150 Practice Questions Verified by Expert Senior Certified Staff
- * 100-150 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 100-150 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 100-150 Practice Test Here](#)