Cisco

Exam Questions CCST-Networking

Cisco Certified Support Technician (CCST) NetworkingExam

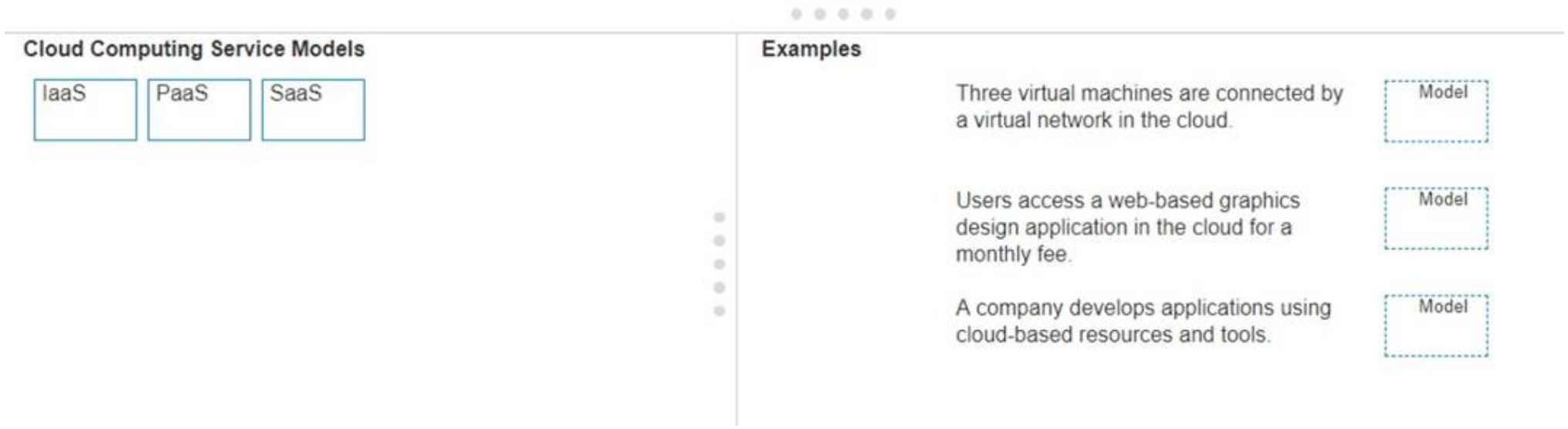
NEW QUESTION 1
A host is given the IP address 172.16.100.25 and the subnet mask 255.255.252.0. What is the CIDR notation for this address?

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.



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
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

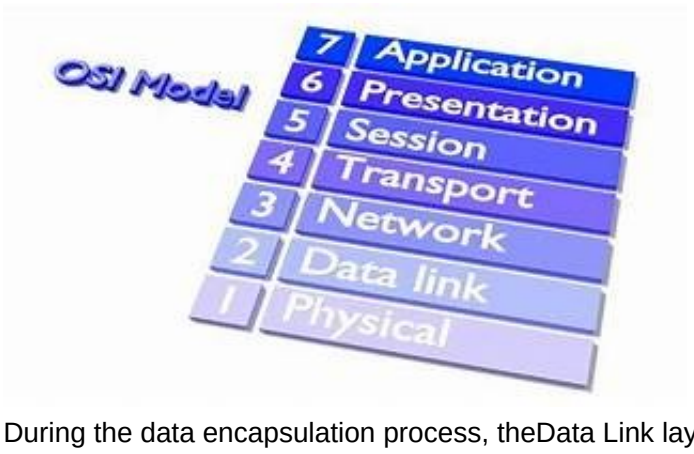
? IPv6 Addressing (Cisco)

NEW QUESTION 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
A local company requires two networks in two new buildings. The addresses used in these networksmust 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 172.31.255.255falls within the Class B private range. B. 192.16.0.0 to 192.16.255.255is not a recognized private IP range.
C.11.0.0.0 to 11.255.255.255is 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
AandD. References:=
? Reserved IP addresses on Wikipedia
? Private IP Addresses in Networking - GeeksforGeeks
? Understanding Private IP Ranges, Uses, Benefits, and Warnings

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
Which component of the AAA service security model provides identity verification?

A. Authorization
B. Auditing
C. Authentication
D. Accounting

Answer: C

Explanation:
The AAA service security model consists of three components: Authentication, Authorization, and Accounting.
•Authentication: This is the process of verifying the identity of a user or device. It ensures that only legitimate users can access the network or service.
•Authorization: This determines what an authenticated user is allowed to do or access within the network.
•Auditing/Accounting: This component tracks the actions of the user, including what resources they access and what changes they make.
Thus, the correct answer is C. Authentication. References :=
•Cisco AAA Overview
•Understanding AAA (Authentication, Authorization, and Accounting)

NEW QUESTION 8
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 9
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,

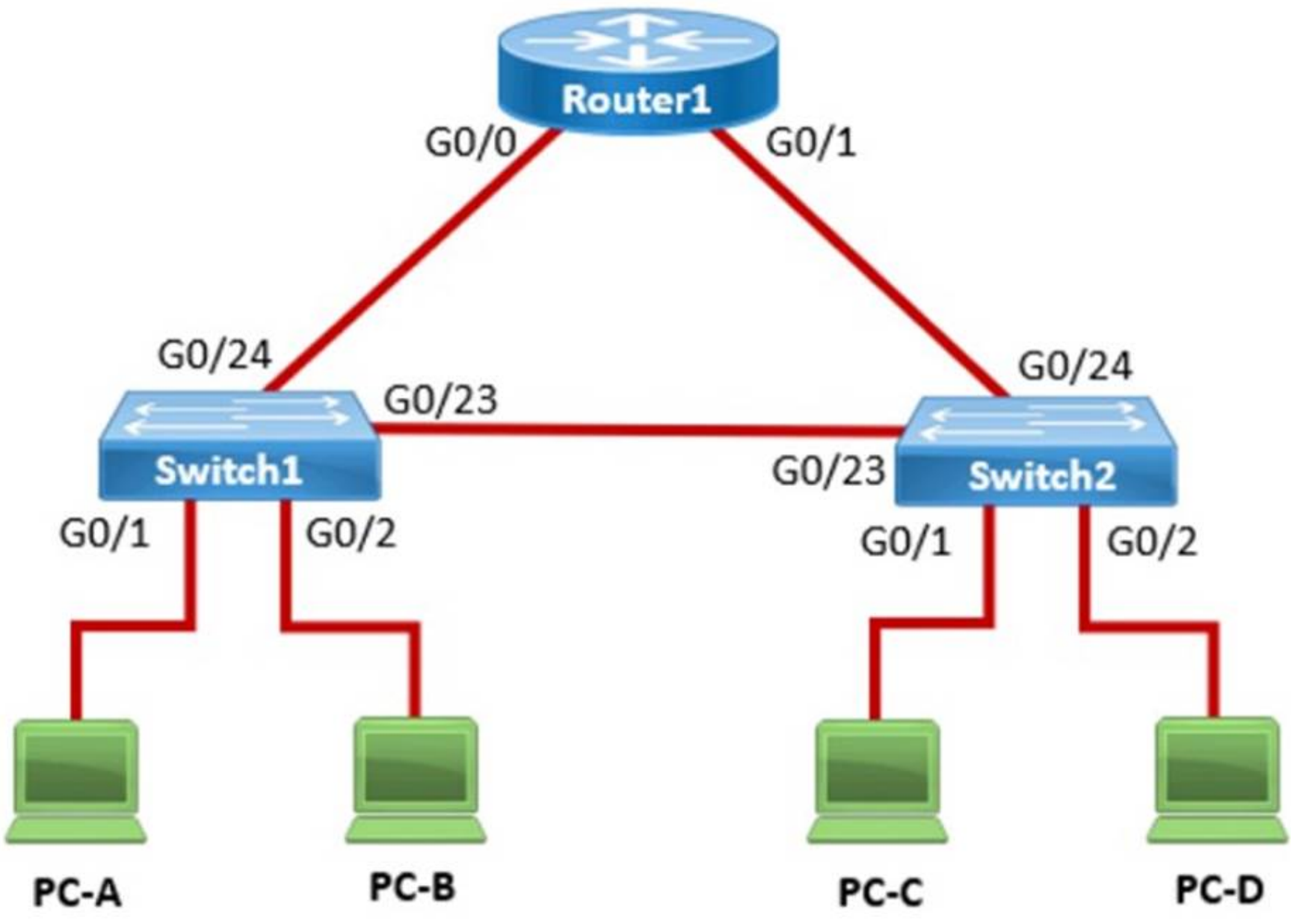
Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
esxi	Gig 0/5	177	S	VMware ES	vmnic0
esxi	Gig 0/7	177	S	VMware ES	vmnic1
esxi	Gig 0/6	177	S	VMware ES	vmnic2
981888fc23a7	Gig 0/47	160	R S	Meraki MR	Port 0
3456fecd1d08	Gig 0/1	178	S	MS120-8LP	Port 9"

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 10
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 15
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 18
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 22
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 24
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!

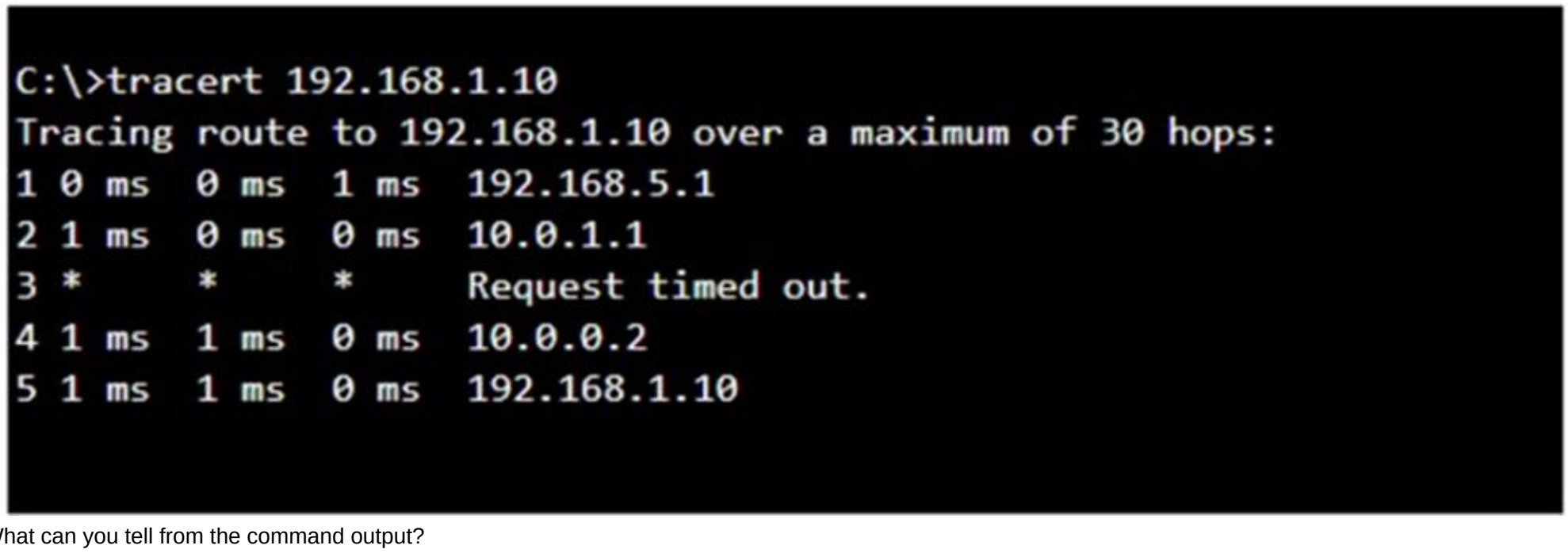
NEW QUESTION 28
Which protocol allows you to securely upload files to another computer on the internet?

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 33
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:



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 35
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 36
.....

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