Cisco

Exam Questions 100-150

Cisco Certified Support Technician (CCST) Networking

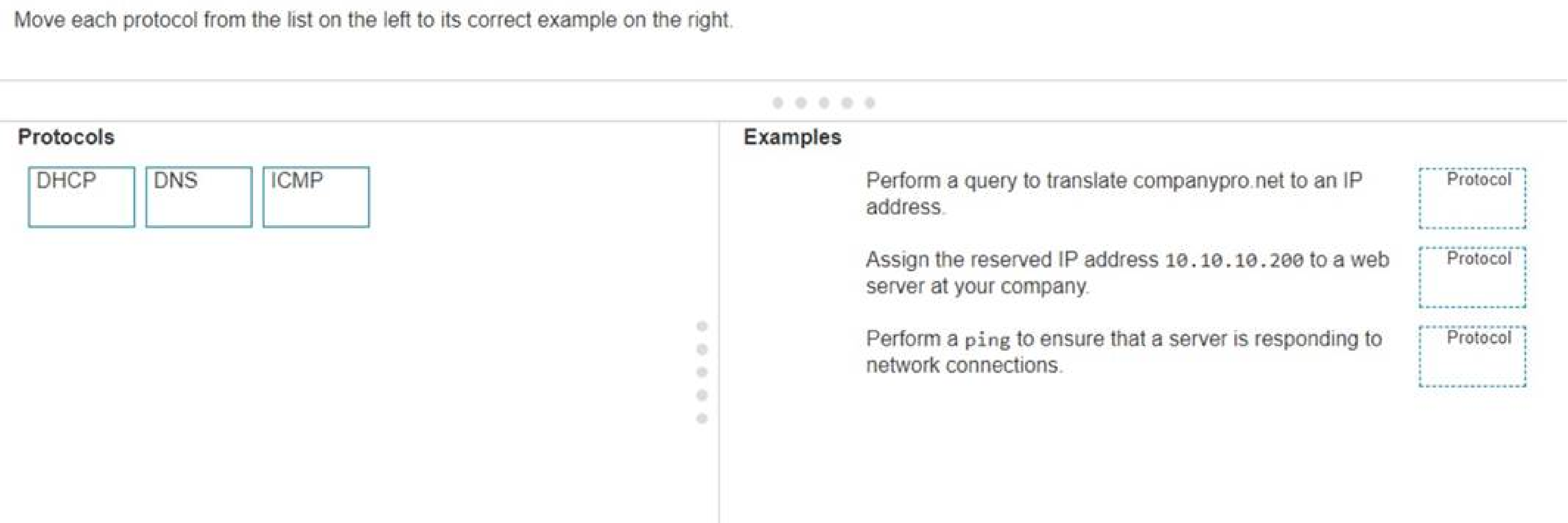
NEW QUESTION 1
A user initiates a trouble ticket stating that an external web page is not loading. You determine that other resources both internal and external are still reachable. Which command can you use to help locate where the issue is in the network path to the external web page?

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
DRAG DROP
Move each protocol from the list on the left to its correct example on the right.


Move each protocol from the list on the left to its correct example on the right.

Perform a query to translate companypro.net to an IP address.

Assign the reserved IP address 10.10.10.200 to a web server at your company.

Perform a ping to ensure that a server is responding to network connections.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The correct matching of the protocols to their examples is as follows:
? DHCP: Assign the reserved IP address 10.10.10.200 to a web server at your company.
? DNS: Perform a query to translate companypro.net to an IP address.
? ICMP: Perform a ping to ensure that a server is responding to network connections.
Here??s how each protocol corresponds to its example:
? DHCP (Dynamic Host Configuration Protocol) is used to assign IP addresses to
devices on a network. In this case, DHCP would be used to assign the reserved IP address 10.10.10.200 to a web server.
? DNS (Domain Name System) is used to translate domain names into IP
addresses. Therefore, to translate companypro.net to an IP address, DNS would be utilized.
? ICMP (Internet Control Message Protocol) is used for sending error messages and
operational information indicating success or failure when communicating with another IP address. An example of this is using the ping command to check if a server is responding to network connections.
These protocols are essential for the smooth operation of networks and the internet.
? Perform a query to translate companypro.net to an IP address.
? Assign the reserved IP address 10.10.10.200 to a web server at your company.
? Perform a ping to ensure that a server is responding to network connections.
? DNS (Domain Name System): DNS translates human-friendly domain names like "companypro.net" into IP addresses that computers use to identify each other on the network.
? DHCP (Dynamic Host Configuration Protocol): DHCP automatically assigns IP addresses to devices on a network, ensuring that no two devices have the same IP address.
? ICMP (Internet Control Message Protocol): ICMP is used for diagnostic or control

purposes, and the ping command uses ICMP to test the reachability of a host on an IP network.
References:
? DNS Basics: What is DNS?
? DHCP Overview: What is DHCP?
? ICMP and Ping: Understanding ICMP

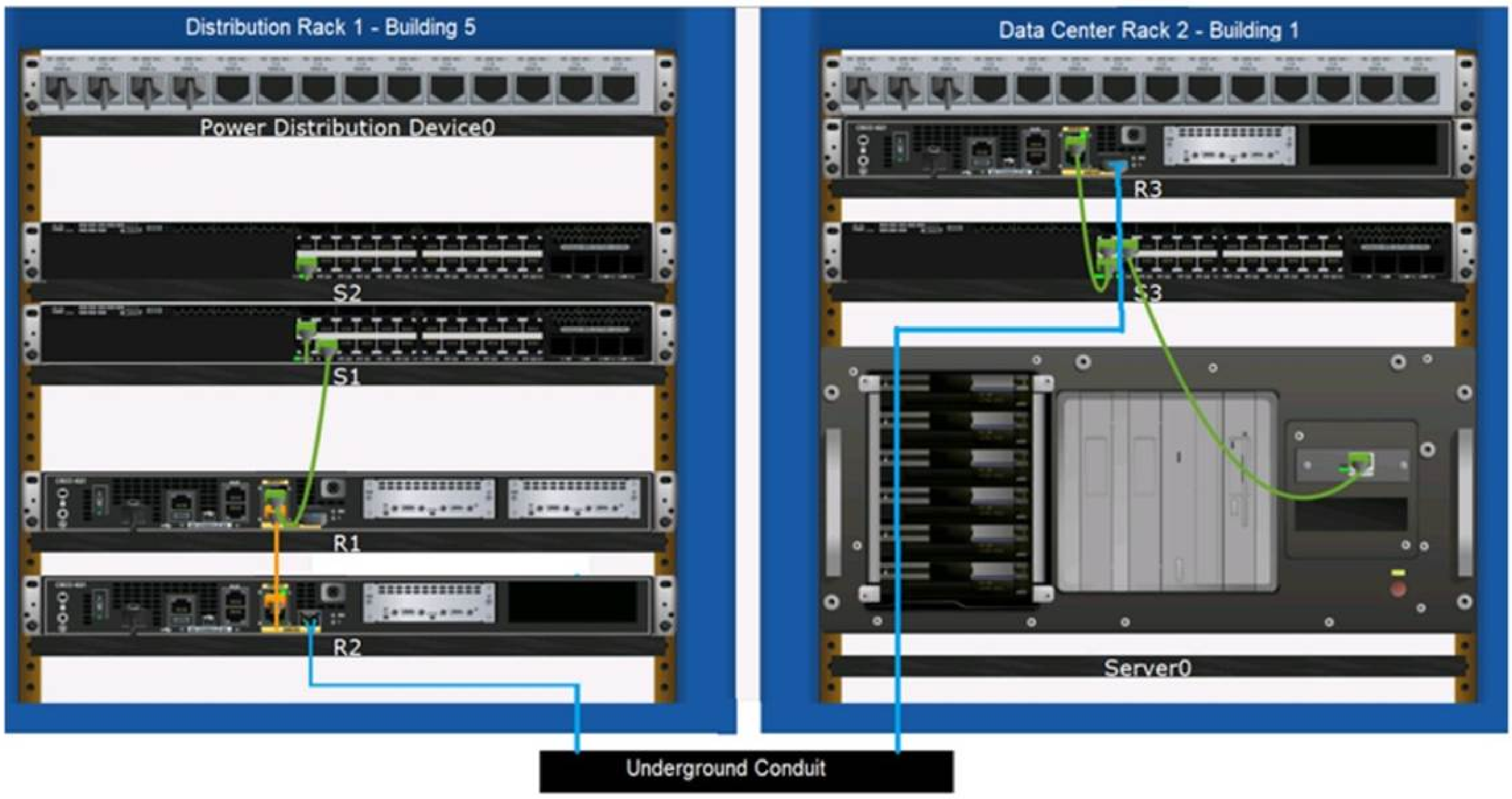
NEW QUESTION 3
A local company requires two networks in two new buildings. The addresses used in these networks must be in the private network range.
Which two address ranges should the company use? (Choose 2.) Note: You will receive partial credit for each correct selection.

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 4
DRAG DROP
Examine the connections shown in the following image. Move the cable types on the right to the appropriate connection description on the left. You may use each cable type more than once or not at all.


Distribution Rack 1 - Building 5
Power Distribution Device0
S2
S1
R1
R2
Data Center Rack 2 - Building 1
R3
S3
Server0
Underground Conduit

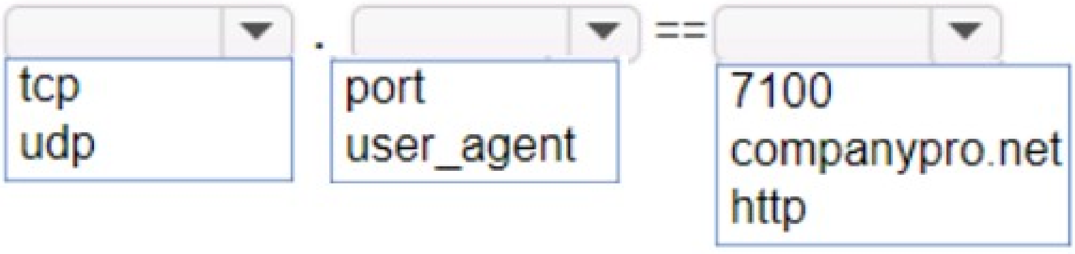
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Based on the image description provided, here are the cable types matched with the appropriate connection descriptions:
Connects Switch S1 to Router R1 Gi0/0/1 interface Cable Type: = Straight-through UTP Cable
Connects Router R2 Gi0/0/0 to Router R3 Gi0/0/0 via underground conduit Cable Type: = Fiber Optic Cable
Connects Router R1 Gi0/0/0 to Router R2 Gi0/0/1 Cable Type: = Crossover UTP Cable Connects Switch S3 to Server0 network interface card Cable Type: = Straight-through UTP Cable
The choices are based on standard networking practices where:
? Straight-through UTP cables are typically used to connect a switch to a router or a network interface card.
? Fiber optic cables are ideal for long-distance, high-speed data transmission, such as connections through an underground conduit.

? Crossover UTP cables are used to connect similar devices, such as router-to- router connections.
These matches are consistent with the color-coded cables in the image: green for switch connections, yellow for router-to-router connections within the same rack, and blue for inter-rack connections. The use of these cables follows the Ethernet cabling standards.
? Connects Switch S1 to Router R1 Gi0/0/1 interface:
? Connects Router R2 Gi0/0/0 to Router R3 Gi0/0/0 via underground conduit:
? Connects Router R1 Gi0/0/0 to Router R2 Gi0/0/1:
? Connects Switch S3 to Server0 network interface card:
? Straight-through UTP Cable: Used to connect different devices (e.g., switch to router, switch to server).
? Crossover UTP Cable: Used to connect similar devices directly (e.g., router to
router, switch to switch).
? Fiber Optic Cable: Used for long-distance and high-speed connections, often between buildings or data centers.
References:
? Network Cable Types and Uses: Cisco Network Cables
? Understanding Ethernet Cabling: Ethernet Cable Guide

NEW QUESTION 5
HOTSPOT
An app on a user's computer is having problems downloading data. The app uses the following URL to download data:
https://www.companypro.net:7100/api
You need to use Wireshark to capture packets sent to and received from that URL. Which Wireshark filter options would you use to filter the results? Complete the command by selecting the correct option from each drop-down list. Note: You will receive partial credit for each correct selection.



tcp
udp

.

port
user_agent

==

7100
companypro.net
http

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To capture packets sent to and received from the URL https://www.companypro.net:7100/api using Wireshark, you would use the following filter options:
? Protocol: tcp
? Filter Type: port
? Port Number: 7100
This filter setup in Wireshark will display all TCP packets that are sent to or received from port 7100, which is the port specified in the URL for the API service. Since HTTPS typically uses TCP as the transport layer protocol, filtering by TCP and the specific port number will help isolate the relevant packets for troubleshooting the app??s data download issues.
? cp: The app is using HTTPS, which relies on the TCP protocol for communication.
? port: The specific port number used by the application, which in this case is 7100.
? 7100: This is the port specified in the URL (https://www.companypro.net:7100/api). This filter will capture all TCP traffic on port 7100, allowing you to analyze the packets related to the application's data download.
References:
? Wireshark Filters: Wireshark Display Filters

NEW QUESTION 6
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 7
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?

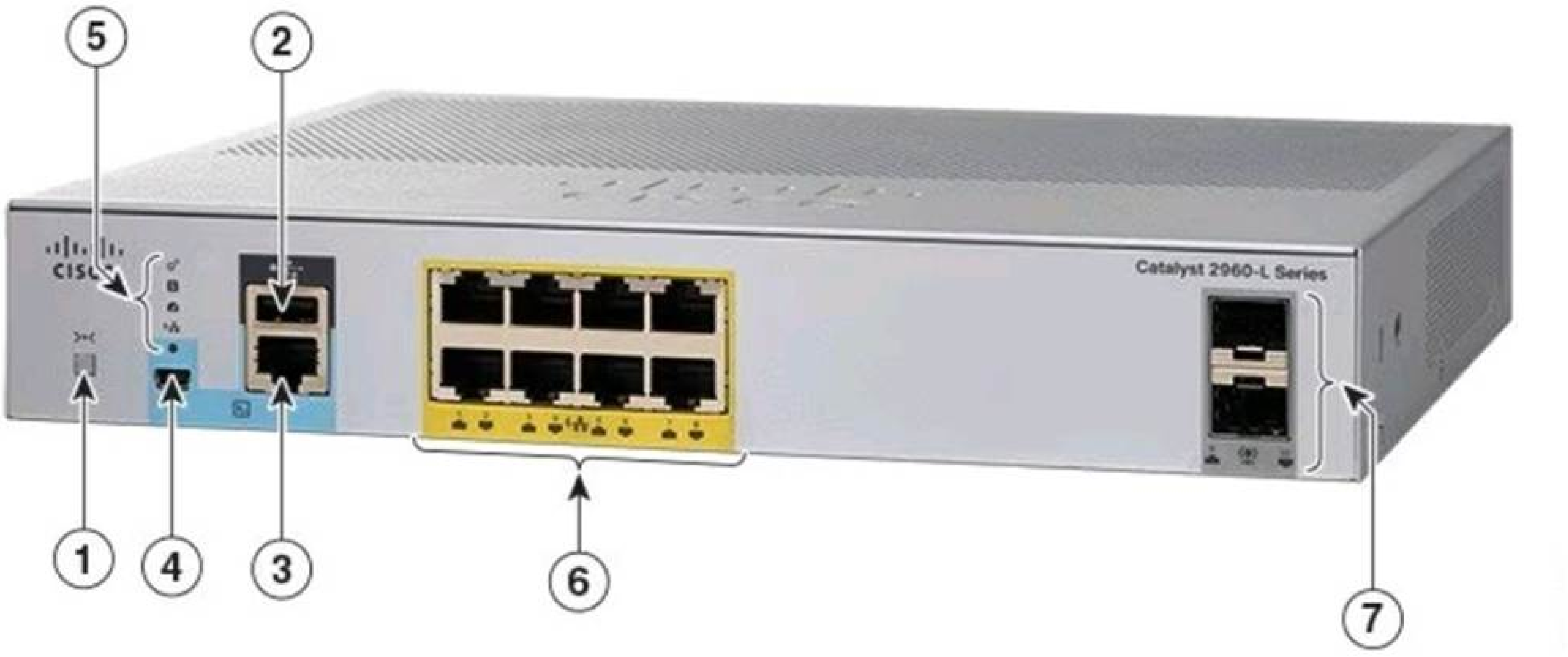
A. SNMP
B. Console
C. SSH
D. Telnet

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 the console 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
========================

NEW QUESTION 8
A Cisco PoE switch is shown in the following image. Which type of port will provide both data connectivity and power to an IP phone?



A. Port identified with number 2
B. Ports identified with numbers 3 and 4
C. Ports identified with number 6
D. Ports identified with number 7

Answer: C

Explanation:
In the provided image of the Cisco PoE switch, the ports identified with number 6 are the standard RJ-45 Ethernet ports typically found on switches that provide both data connectivity and Power over Ethernet (PoE). PoE ports are designed to supply power to devices such as IP phones, wireless access points, and other PoE-enabled devices directly through the Ethernet cable.
Ports:
•2: Console port (for management and configuration)
•3 and 4: Specific function ports (often for management)
•6: RJ-45 Ethernet ports (capable of providing PoE)
•7: SFP ports (for fiber connections, typically do not provide PoE) Thus, the correct answer is C. Ports identified with number 6. References :=
•Cisco Catalyst 2960-L Series Switches Data Sheet
•Cisco PoE Overview

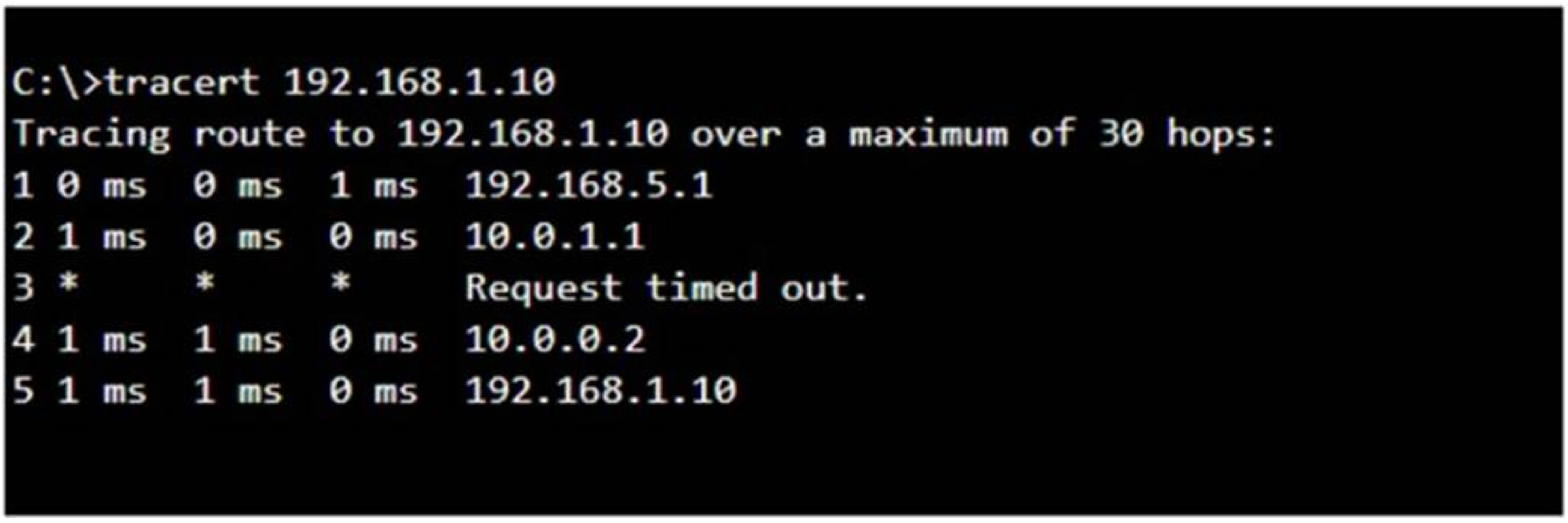
NEW QUESTION 9
Which protocol allows you to securely upload files to another computer on the internet?

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 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 is reachable 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
......

Relate Links

100% Pass Your 100-150 Exam with Exambible Prep Materials

https://www.exambible.com/100-150-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/