Cisco

Exam Questions CCST-Networking

Cisco Certified Support Technician (CCST) NetworkingExam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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
HOTSPOT
Computers in a small office are unable to access companypro.net. You run the ipconfig command on one of the computers. The results are shown in the exhibit.
You need to determine if you can reach the router.

```
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . . . . . . . : 192.168.0.14(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Sunday, January 8, 2023 11:00:02 AM
Lease Expires . . . . . . . . . . : Sunday, January 8, 2023 12:00:12 PM
Default Gateway . . . . . . . . . : 192.168.0.1
DHCP Server . . . . . . . . . . . : 192.168.0.1
DNS Servers . . . . . . . . . . . : 8.8.8.8
                                   8.8.4.4
NetBIOS over Tcpip. . . . . . . . : Enabled
```

Which command should you use? Complete the command by selecting the correct options from each drop-down lists.

A. Mastered
B. Not Mastered

Answer: A

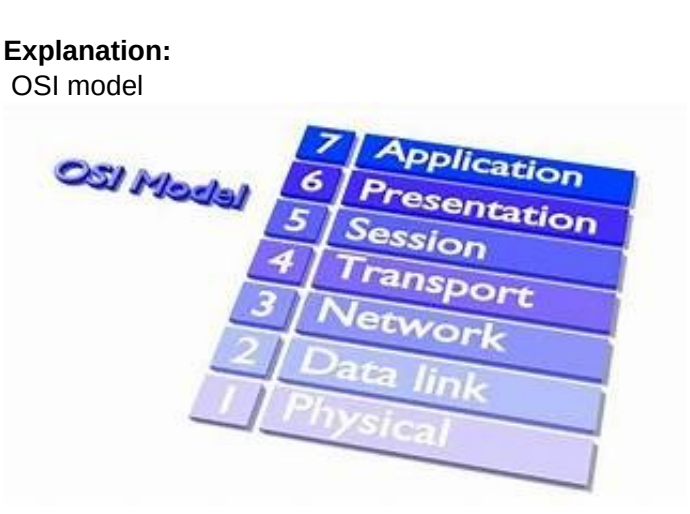
Explanation:
? ping: The ping command sends ICMP Echo Request messages to the target IP address and waits for an Echo Reply. It is commonly used to test the reachability of a network device.
? 192.168.0.1: This is the IP address of the default gateway (the router) as shown in theipconfigoutput. Pinging this address will help determine if the computer can communicate with the router.
References:
? Using the ping Command: ping Command Guide

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
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 6
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)

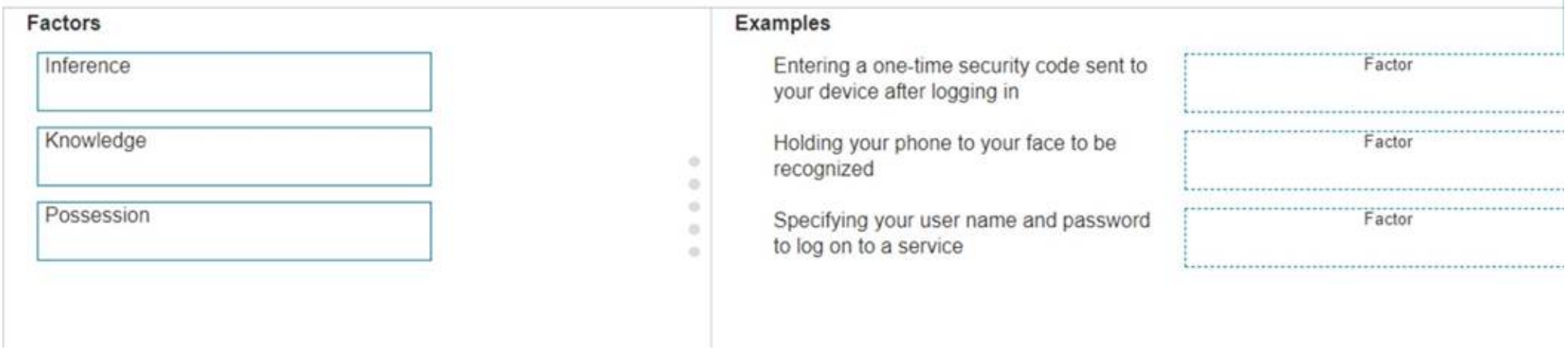
NEW QUESTION 7
A support technician examines the front panel of a Cisco switch and sees 4 Ethernet cables connected in the first four ports. Ports 1, 2, and 3 have a green LED. Port 4 has a blinking green light. What is the state of the Port 4?

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 8
DRAG DROP
Move the MFA factors from the list on the left to their correct examples on the right. You may use each factor once, more than once, or not at all.
Note: You will receive partial credit for each correct selection.



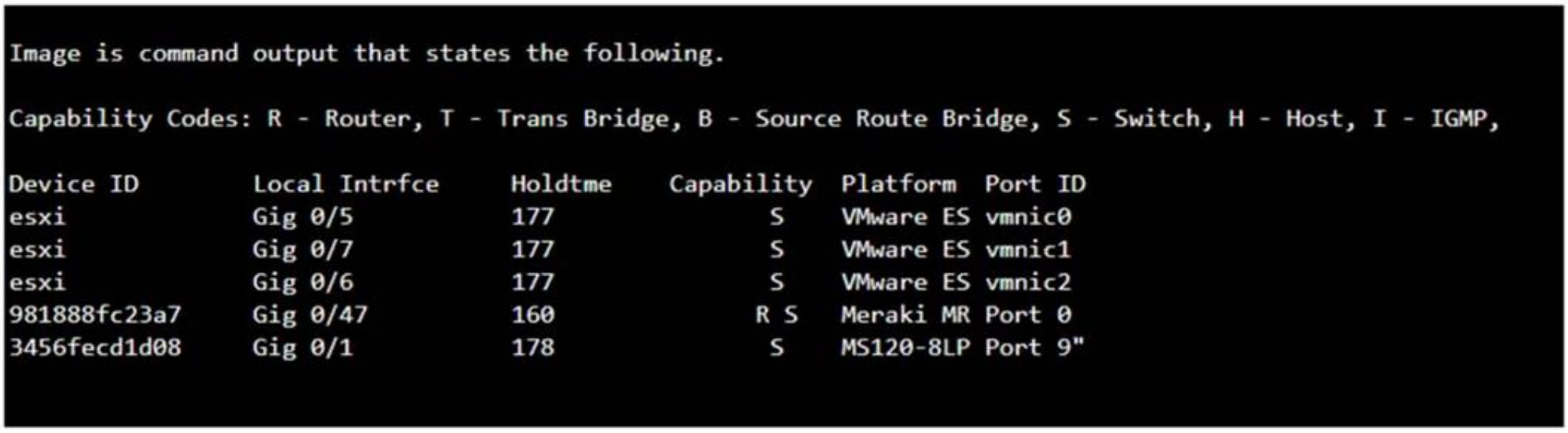
A. Mastered

B. Not Mastered

Answer: A

Explanation:
The correct matching of the MFA factors to their examples is as follows:
? Entering a one-time security code sent to your device after logging in: Possession
? Holding your phone to your face to be recognized: Inherence
? Specifying your user name and password to log on to a service: Knowledge Here??s why each factor matches the example:
? Possession: This factor is something the user has, like a mobile device. A one-
time security code sent to this device falls under this category.
? Inherence: This factor is something the user is, such as a biometric characteristic.
Facial recognition using a phone is an example of this factor.
? Knowledge: This factor is something the user knows, like a password or PIN. Multi-Factor Authentication (MFA) enhances security by requiring two or more of these factors to verify a user??s identity before granting access.
? Entering a one-time security code sent to your device after logging in.
? Holding your phone to your face to be recognized.
? Specifying your username and password to log on to a service.
? Possession Factor: This involves something the user has in their possession.
Receiving a one-time security code on a device (e.g., phone) is an example of this.
? Inference Factor (Inherence/Biometric): This involves something inherent to the user, such as biometric verification (e.g., facial recognition or fingerprint scanning).
? Knowledge Factor: This involves something the user knows, such as login credentials (username and password).
References:
? Multi-Factor Authentication (MFA) Explained: MFA Guide
? Understanding Authentication Factors: Authentication Factors

NEW QUESTION 9
Which command will display the following output?

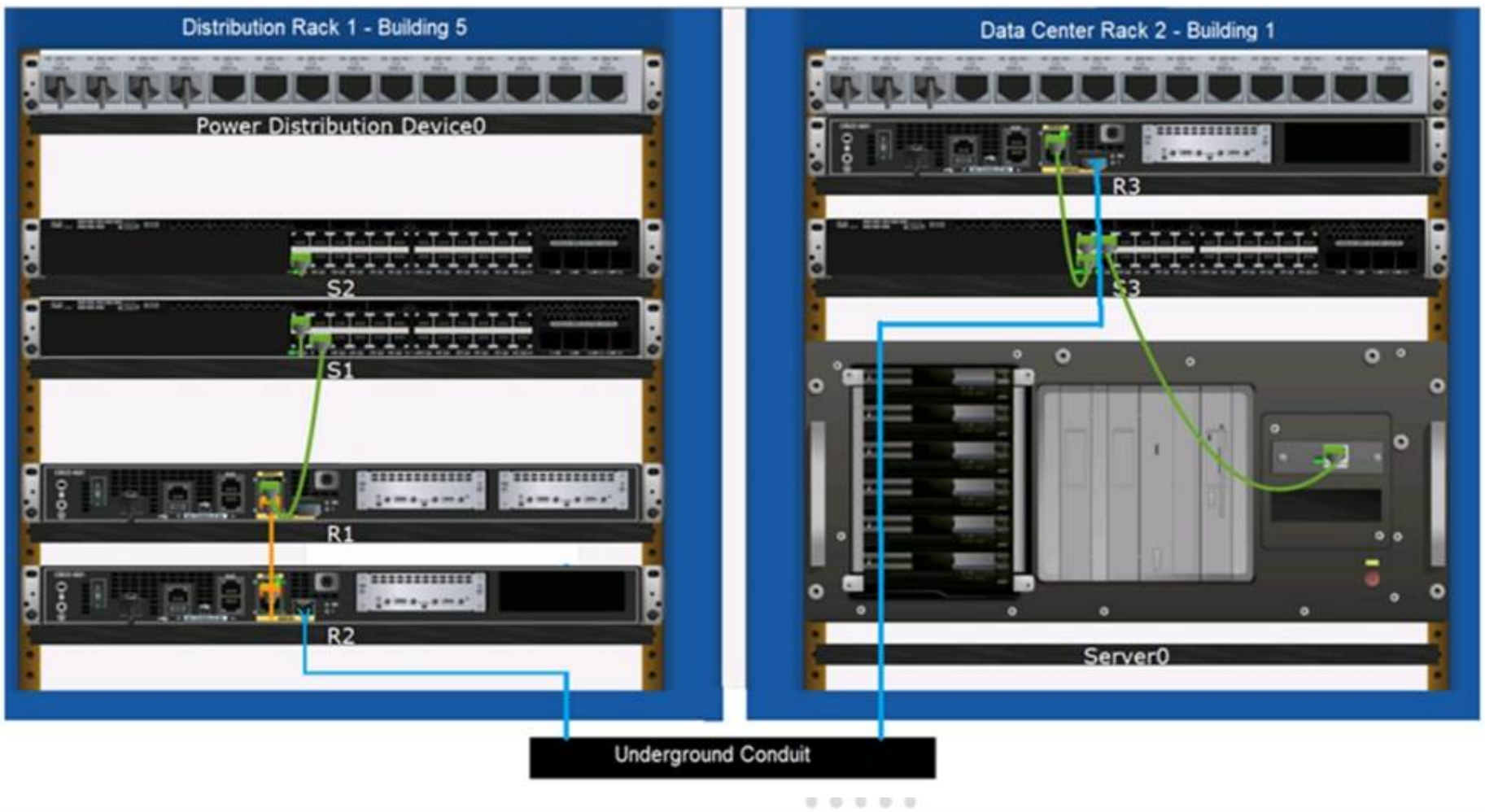


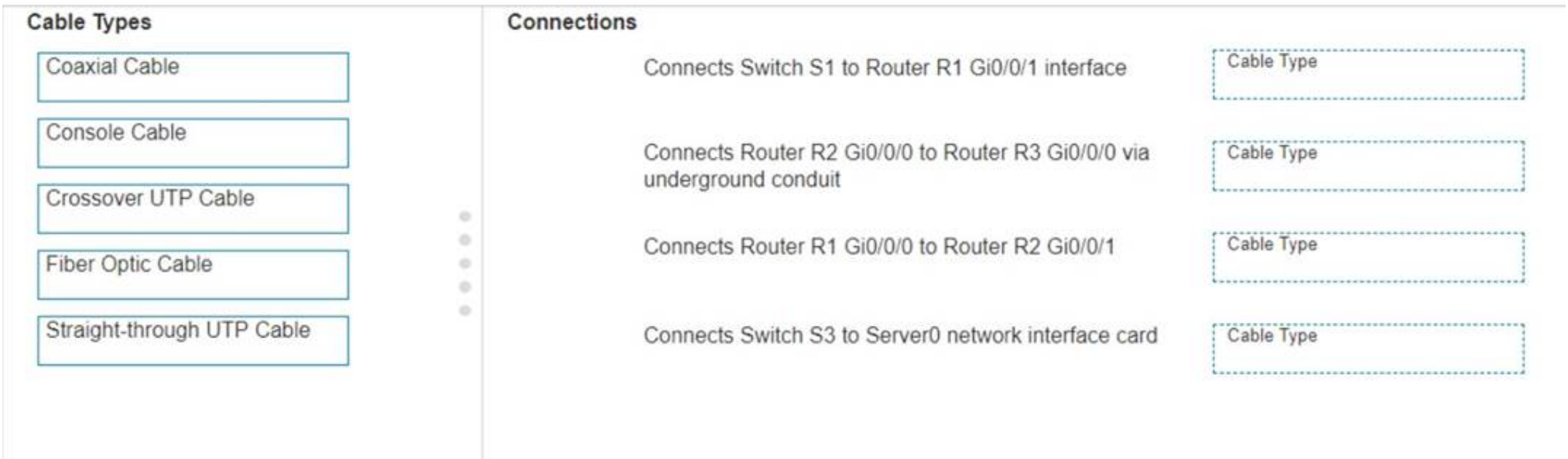
A. show mac-address-table
B. show cdp neighbor
C. show inventory
D. show ip interface

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
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.





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 interfaceCable Type: = Straight-through UTP Cable
Connects Router R2 Gi0/0/0 to Router R3 Gi0/0/0 via underground conduitCable Type
: = Fiber Optic Cable
Connects Router R1 Gi0/0/0 to Router R2 Gi0/0/1Cable Type: = Crossover UTP Cable
Connects Switch S3 to Server0 network interface cardCable Type: = Straight-through UTP Cable
The choices are based on standard networking practices where:
? Straight-through UTP cablesare typically used to connect a switch to a router or a network interface card.
? Fiber optic cablesare ideal for long-distance, high-speed data transmission, such as connections through an underground conduit.
? Crossover UTP cablesare 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

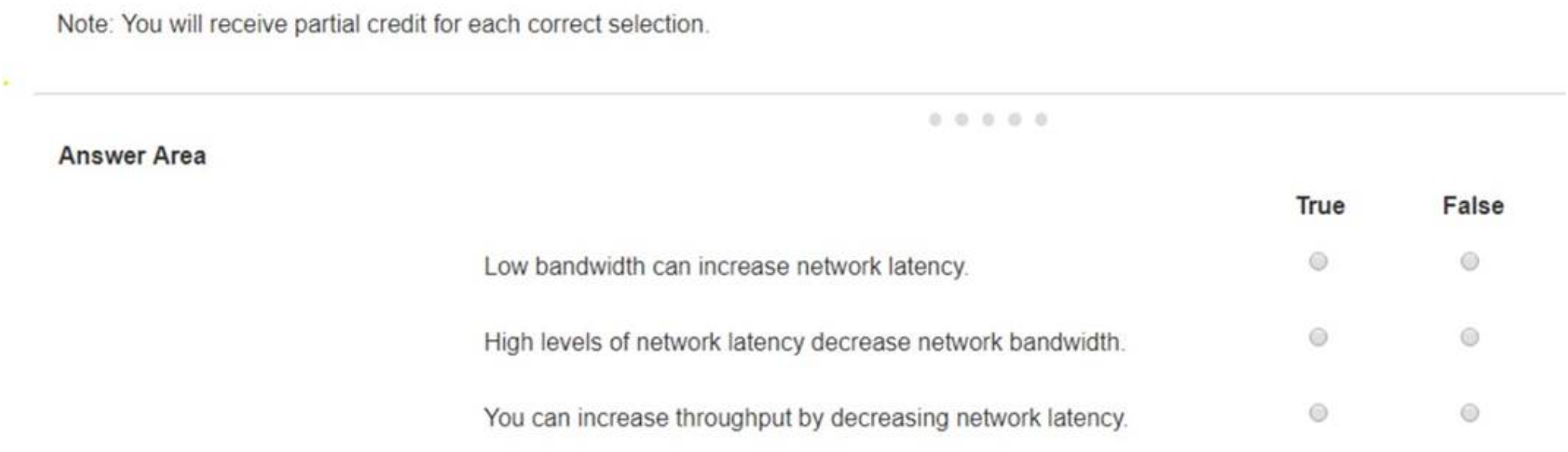
NEW QUESTION 10
Which standard contains the specifications for Wi-Fi networks?

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 12
HOTSPOT
For each statement about bandwidth and throughput, select True or False. Note: You will receive partial credit for each correct selection.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Statement 1: Low bandwidth can increase network latency.
? Statement 2: High levels of network latency decrease network bandwidth.
? Statement 3: You can increase throughput by decreasing network latency.
? Bandwidth vs. Latency: Bandwidth refers to the maximum rate at which data can be transferred over a network path. Latency is the time it takes for a data packet to travel from the source to the destination.
References:
? Network Performance Metrics: Cisco Network Performance
? Understanding Bandwidth and Latency: Bandwidth vs. Latency

NEW QUESTION 14
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?

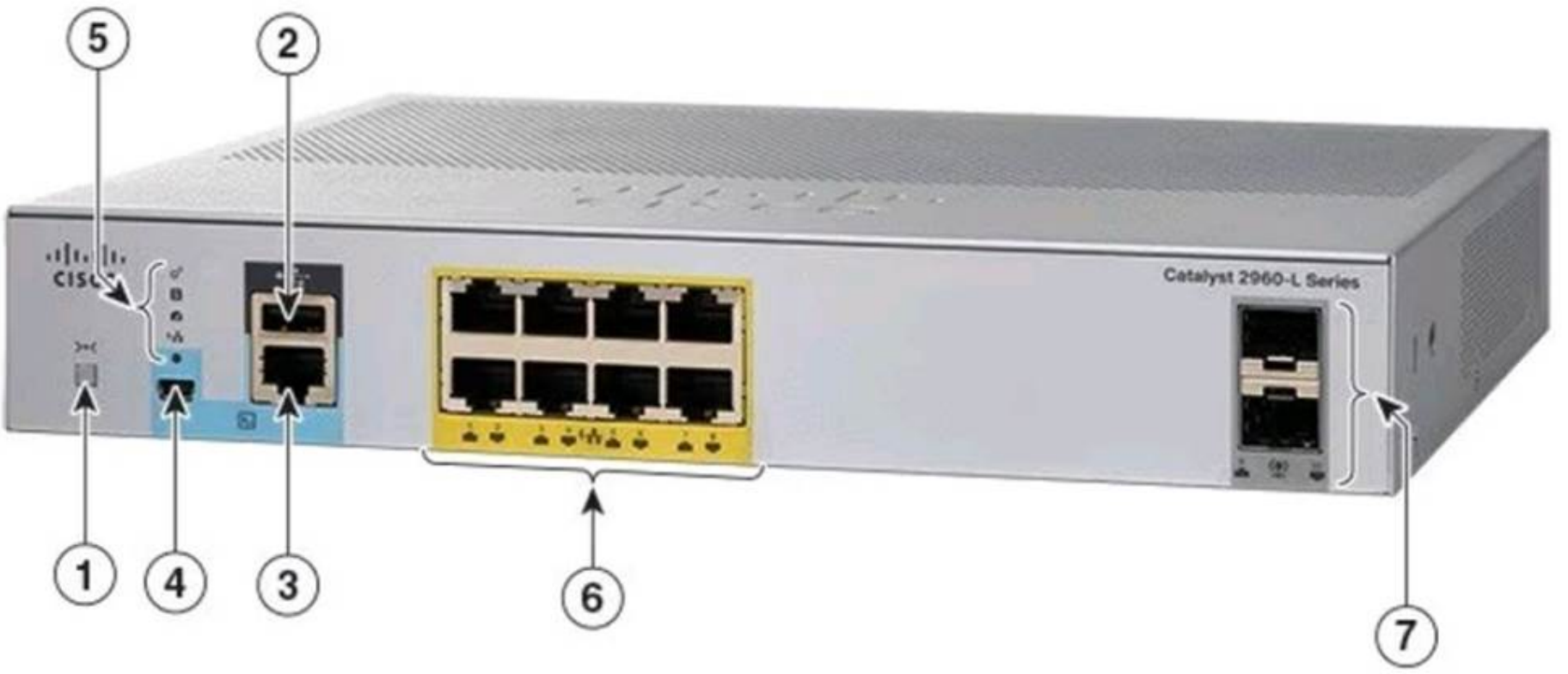
A. ping -t
B. tracert
C. ipconfig/all
D. nslookup

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 16
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 17
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 offic
B. The jack must be patched and made active.
C. Ticket 2: An online webinar is taking place in the conference roo
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 18
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 23
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 24
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 27
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 32

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 35
.....

Relate Links

100% Pass Your CCST-Networking Exam with Exambible Prep Materials

https://www.exambible.com/CCST-Networking-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/