Cisco

Exam Questions 100-150

Cisco Certified Support Technician (CCST) Networking

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
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 a server. 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)

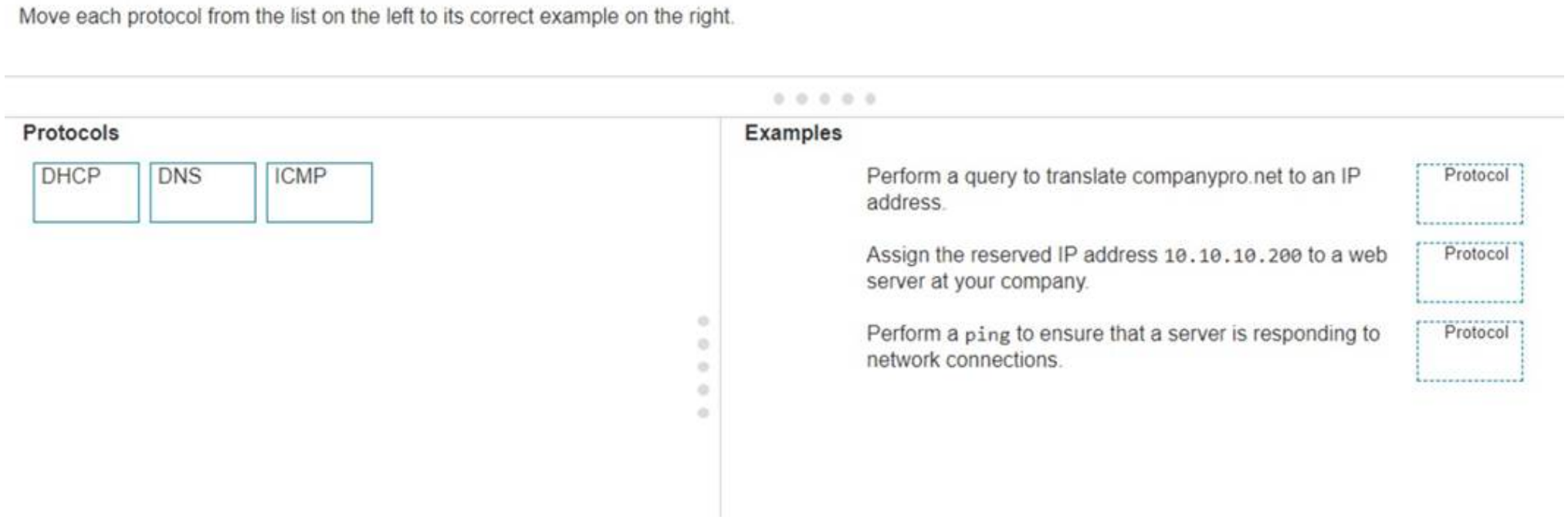
NEW QUESTION 2
A user initiates a trouble ticket stating that an external web page is not loading. You determine that other resources both internal and external are still reachable. Which command can you use to help locate where the issue is in the network path to the external web page?

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 3
DRAG DROP
Move each protocol from the list on the left to its correct example on the right.



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 4
Which command will display all the current operational settings configured on a Cisco router?

A. show protocols
B. show startup-config
C. show version
D. show running-config

Answer: D

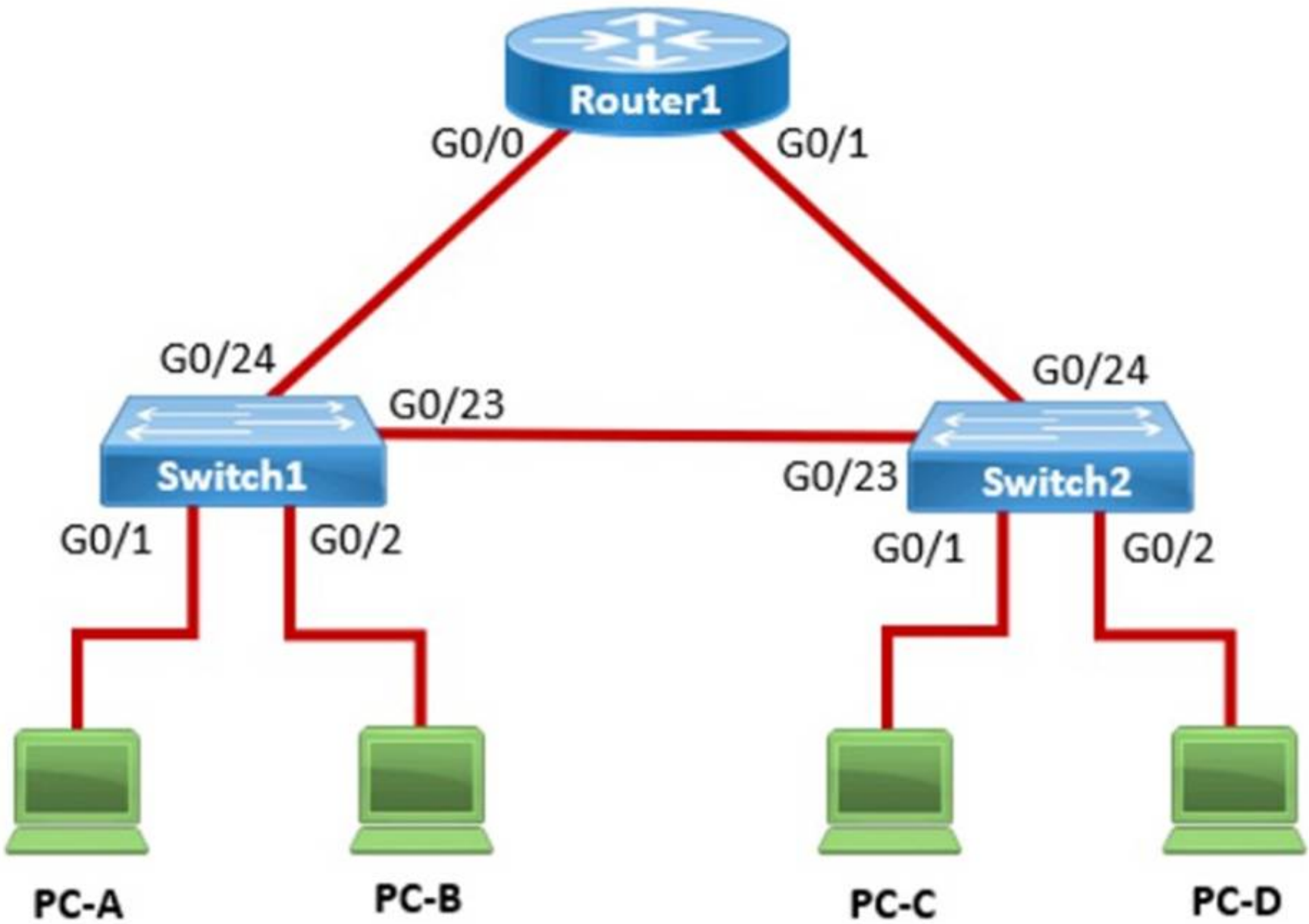
Explanation:


Router

The show running-config command is used on a Cisco router to display the current operational settings that are actively configured in the router??s RAM. This command outputs all the configurations that are currently being executed by the router, which includes interface configurations, routing protocols, access lists, and other settings. Unlike show startup-config, which shows the saved configuration that the router will use on the next reboot, show running-config reflects the live, current configuration in use.
References := The information is supported by multiple sources that detail the use of Cisco commands, particularly the show running-config command as the standard for viewing the active configuration on a Cisco device123.

? show running-config: This command displays the current configuration running on the router. It includes all the operational settings and configurations applied to the router.
? show protocols: This command shows the status of configured protocols on the
router but not the entire configuration.
? show startup-config: This command displays the configuration saved in NVRAM, which is used to initialize the router on startup, but not necessarily the current running configuration.
? show version: This command provides information about the router's software version, hardware components, and uptime but does not display the running configuration.
References:
? Cisco IOS Commands: Cisco IOS Commands

NEW QUESTION 5
In the network shown in the following graphic, Switch1 is a Layer 2 switch.



PC-A sends a frame to PC-C. Switch1 does not have a mapping entry for the MAC address of PC-C. Which action does Switch1 take?

A. Switch1 queries Switch2 for the MAC address of PC-C.
B. Switch1 drops the frame and sends an error message back to PC-A.
C. Switch1 floods the frame out all active ports except port G0/1.
D. Switch1 sends an ARP request to obtain the MAC address of PC-C.

Answer: 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 6
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 7
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

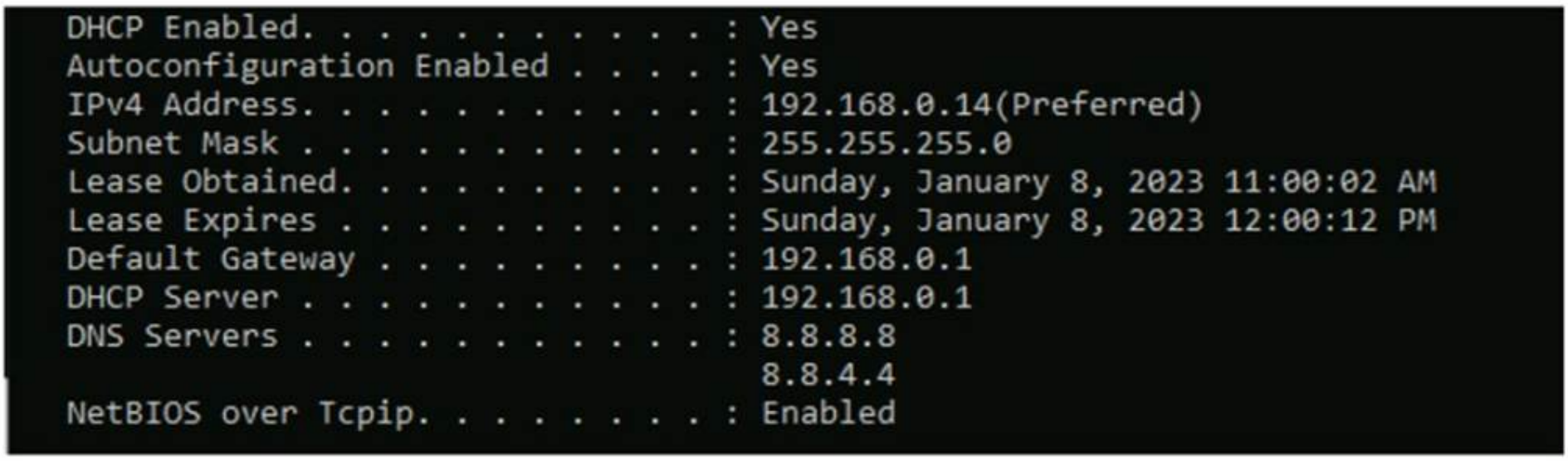
NEW QUESTION 8
What is the most compressed valid format of the IPv6 address 2001:0db8:0000:0016:0000:001b: 2000:0056?

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

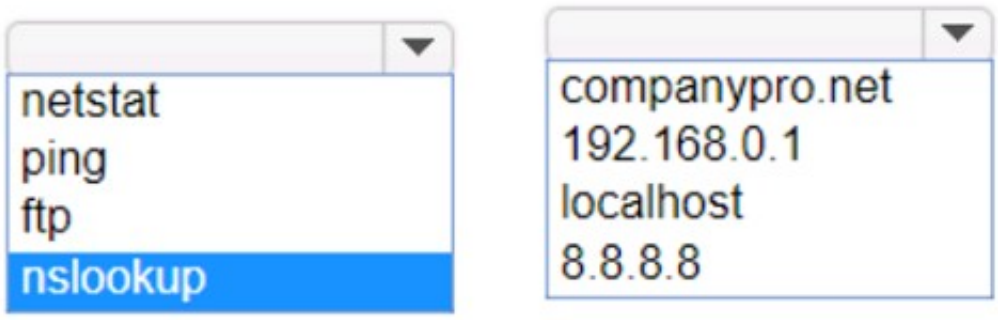
Answer: D

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 9
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.



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:
To determine if you can reach the router, you should use the ping command followed by the IP address of the router. The ping command is a network utility used to test the
reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.
The Default Gateway in the ipconfig results is typically the router??s IP address in a home or small office network. In this case, the Default Gateway is 192.168.0.1, which is the address you would ping to check connectivity to the router.
References :=
? How to Use the Ping Command
? Testing Network Connectivity with the Ping Command
==========
To determine if you can reach the router, you should use the ping command with the IP address of the router.
? Command: ping
? Target: 192.168.0.1 So, the completed command is:
? ping 192.168.0.1
Step by Step Comprehensive and Detailed 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 the ipconfig output. Pinging this address will help determine if the computer can communicate with the router.
References:
? Using the ping Command: ping Command Guide

NEW QUESTION 10
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 10
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 14
You need to connect a computer's network adapter to a switch using a 1000BASE-T cable. Which connector should you use?

A. Coax
B. RJ-11
C. OS2 LC
D. RJ-45

Answer: D

Explanation:

•1000BASE-T Cable: This refers to Gigabit Ethernet over twisted-pair cables (Cat 5e or higher).
•Connector: RJ-45 connectors are used for Ethernet cables, including those used for 1000BASE-T.
•Coax: Used for cable TV and older Ethernet standards like 10BASE2.
•RJ-11: Used for telephone connections.
•OS2 LC: Used for fiber optic connections. References:
•Ethernet Standards and Cables: Ethernet Cable Guide

NEW QUESTION 16
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 19
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 21
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 22
.....

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/