Welcome to Cert007 - Your Ultimate IT Certification Partner

- Real Exam Questions
- Free Updates
- Expert Support
- Instant Access
- Money-Back Guarantee

Visit us at **https://www.cert007.com/** for more information

Exam : CCST Networking

Title : Cisco Certified Support Technician (CCST) NetworkingExam

Version : DEMO

1.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:
2001:db8:0000:0016:0000:001b:2000:0056 becomes 2001:db8:0:16:0:1b:2000:56
Replace the longest sequence of consecutive zeros with a double colon (::). In this case, the two consecutive zeros between the 16 and 1b:
2001:db8:0:16::1b:2000:56
Thus, the most compressed valid format of the IPv6 address is 2001:db8:0:16::1b:2000:56.
Reference: =
Cisco Learning Network
IPv6 Addressing (Cisco)

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

Answer Area

	True	False
Low bandwidth can increase network latency.	○	○
High levels of network latency decrease network bandwidth.	○	○
You can increase throughput by decreasing network latency.	○	○

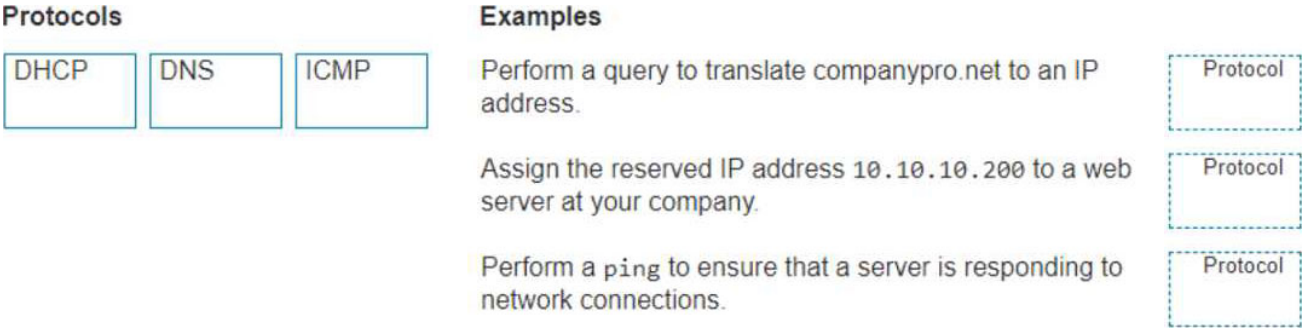
Answer:

Answer Area

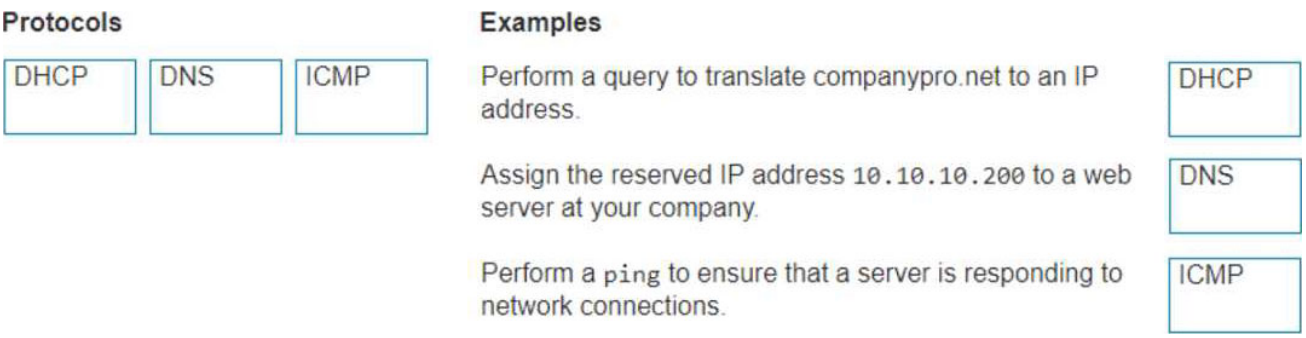
	True	False
Low bandwidth can increase network latency.	●	○
High levels of network latency decrease network bandwidth.	○	●
You can increase throughput by decreasing network latency.	●	○

Explanation:
Statement 1: Low bandwidth can increase network latency.
True: Low bandwidth can result in increased network latency because the network may become congested, leading to delays in data transmission.
Statement 2: High levels of network latency decrease network bandwidth.
False: High levels of network latency do not decrease the available network bandwidth, but they do affect the perceived performance and throughput of the network.
Statement 3: You can increase throughput by decreasing network latency.
True: Decreasing network latency can increase throughput because data can be transmitted more quickly and efficiently without delays.
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.
Low bandwidth can cause network congestion, which can increase latency as packets wait to be transmitted.
High latency does not reduce the actual bandwidth but can affect the overall performance and efficiency of data transmission.
Reducing latency can lead to higher throughput because the network can handle more data in a given period without delays.
Reference: Network Performance Metrics: Cisco Network Performance
Understanding Bandwidth and Latency: Bandwidth vs. Latency

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



Answer:



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.
DNS (Domain Name System): DNS is used to resolve domain names to IP addresses.
Assign the reserved IP address 10.10.10.200 to a web server at your company.
DHCP (Dynamic Host Configuration Protocol): DHCP is used to assign IP addresses to devices on a network.
Perform a ping to ensure that a server is responding to network connections.
ICMP (Internet Control Message Protocol): ICMP is used by network devices to send error messages and operational information, and it is the protocol used by the ping command.
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.
Reference: DNS Basics: What is DNS?
DHCP Overview: What is DHCP?
ICMP and Ping: Understanding ICMP

4.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.
Reference: =
• 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.
Reference: =
• Cisco Learning Network
• SFTP Overview (Cisco)

5.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? Note: You will receive partial credit for each correct selection. (Choose 2.)
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.
Reference: =
Reserved IP addresses on Wikipedia
Private IP Addresses in Networking - GeeksforGeeks
Understanding Private IP Ranges, Uses, Benefits, and Warnings