Cisco

Exam Questions 100-150

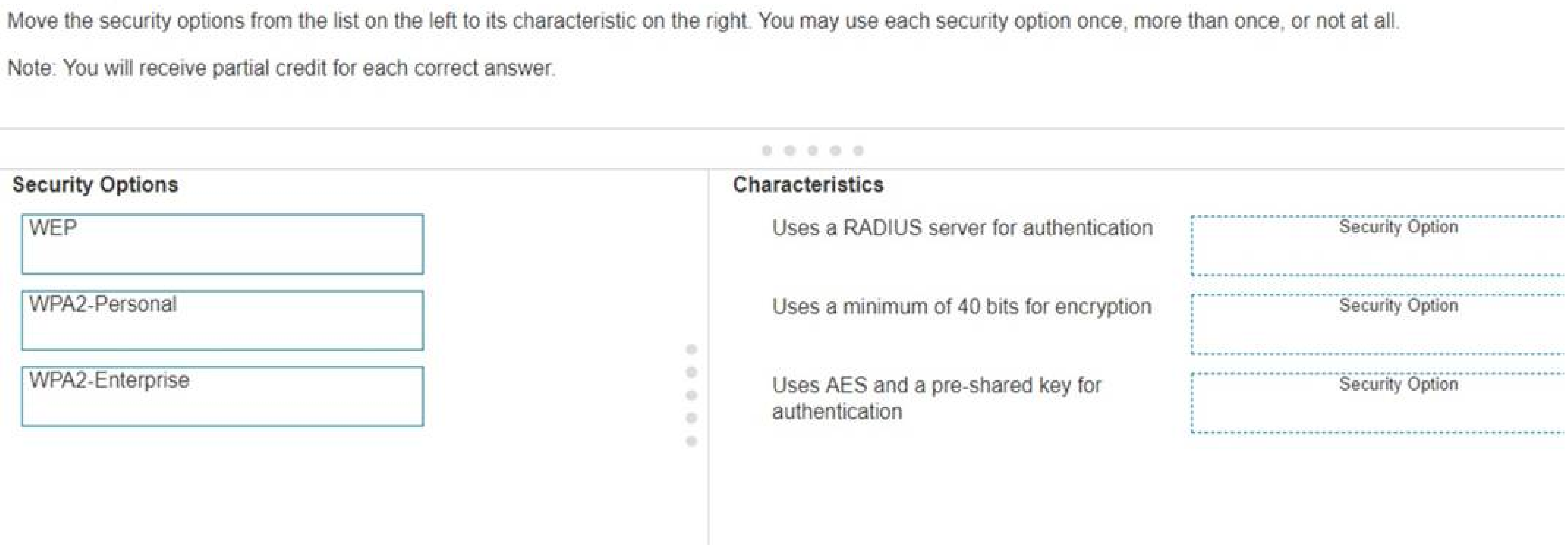
Cisco Certified Support Technician (CCST) Networking

NEW QUESTION 1

DRAG DROP

Move the security options from the list on the left to its characteristic on the right. You may use each security option once, more than once, or not at all.

Note: You will receive partial credit for each correct answer.



Move the security options from the list on the left to its characteristic on the right. You may use each security option once, more than once, or not at all.

Note: You will receive partial credit for each correct answer.

Security Options

- WEP
- WPA2-Personal
- WPA2-Enterprise

Characteristics

Uses a RADIUS server for authentication	Security Option
Uses a minimum of 40 bits for encryption	Security Option
Uses AES and a pre-shared key for authentication	Security Option

A. Mastered

B. Not Mastered

Answer: A

Explanation:

The correct matching of the security options to their characteristics is as follows:

? WPA2-Enterprise: Uses a RADIUS server for authentication

? WEP: Uses a minimum of 40 bits for encryption

? WPA2-Personal: Uses AES and a pre-shared key for authentication Here??s why each security option matches the characteristic:

? WPA2-Enterprise uses a RADIUS server for authentication, which provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.

? WEP (Wired Equivalent Privacy) is an outdated security protocol that uses a minimum of 40 bits for encryption (and up to 104 bits), which is relatively weak by today??s standards.

? WPA2-Personal (Wi-Fi Protected Access 2 - Personal) uses the Advanced Encryption Standard (AES) for encryption and a pre-shared key (PSK) for authentication, which is shared among users to access the network.

These security options are essential for protecting wireless networks from unauthorized access and ensuring data privacy.

NEW QUESTION 2

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 3

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 4
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 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
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.

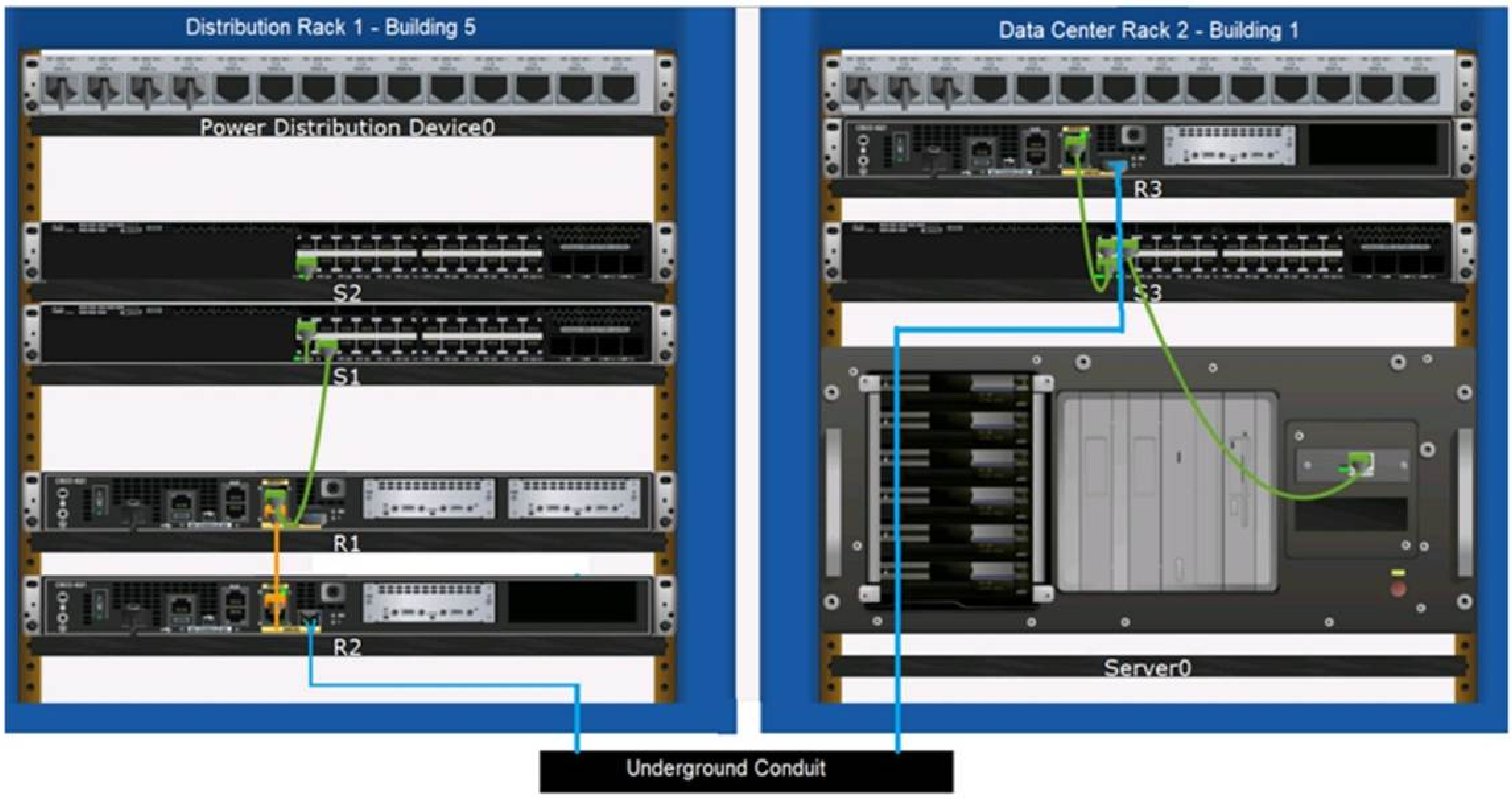
A. 172.16.0.0 to 172.31.255.255
B. 192.16.0.0 to 192.16.255.255
C. 11.0.0.0 to 11.255.255.255
D. 192.168.0.0 to 192.168.255.255

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 7
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.

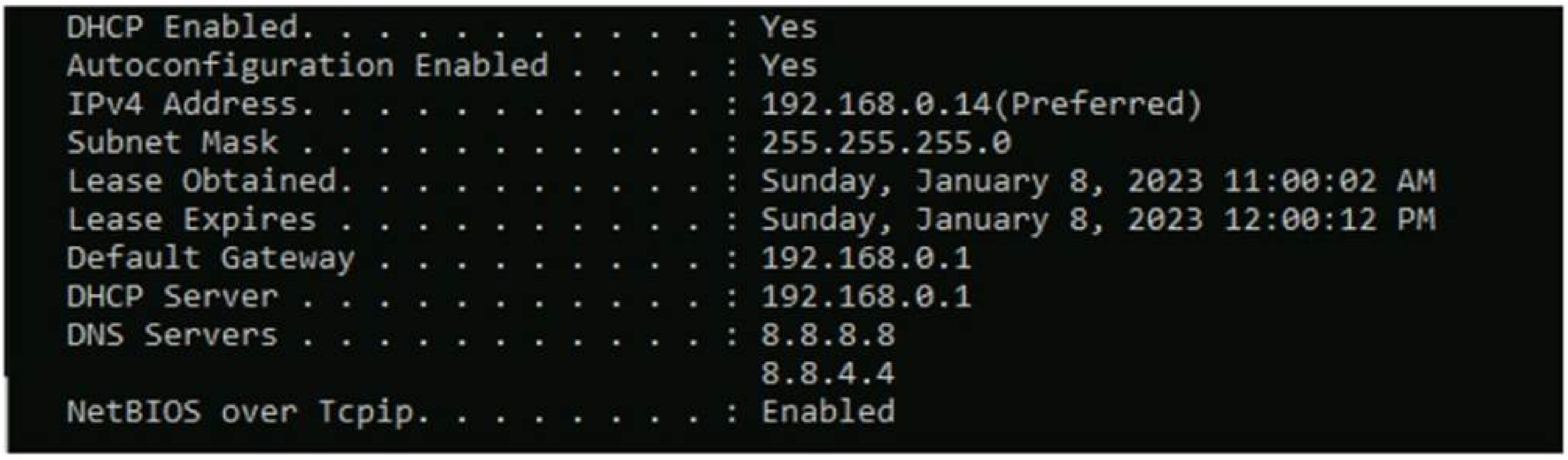

Distribution Rack 1 - Building 5
Power Distribution Device0
S2
S1
R1
R2
Data Center Rack 2 - Building 1
R3
S3
Server0
Underground Conduit

A. Mastered
B. Not Mastered

Answer: A

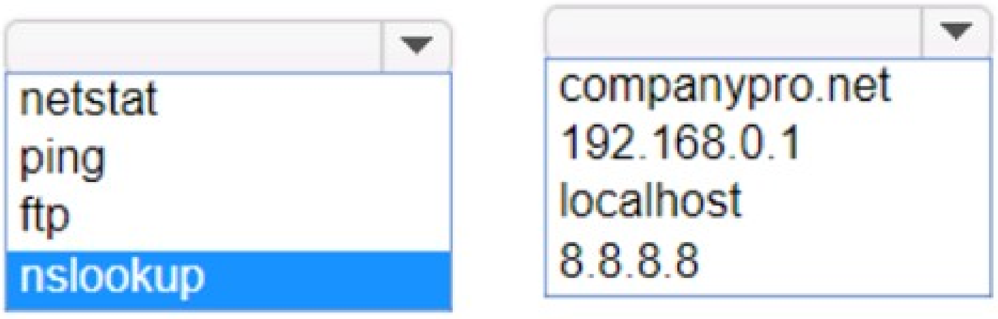
Explanation:
Based on the image description provided, here are the cable types matched with the appropriate connection descriptions:
Connects Switch S1 to Router R1 Gi0/0/1 interface Cable Type: = Straight-through UTP Cable
Connects Router R2 Gi0/0/0 to Router R3 Gi0/0/0 via underground conduit Cable 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 8
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.

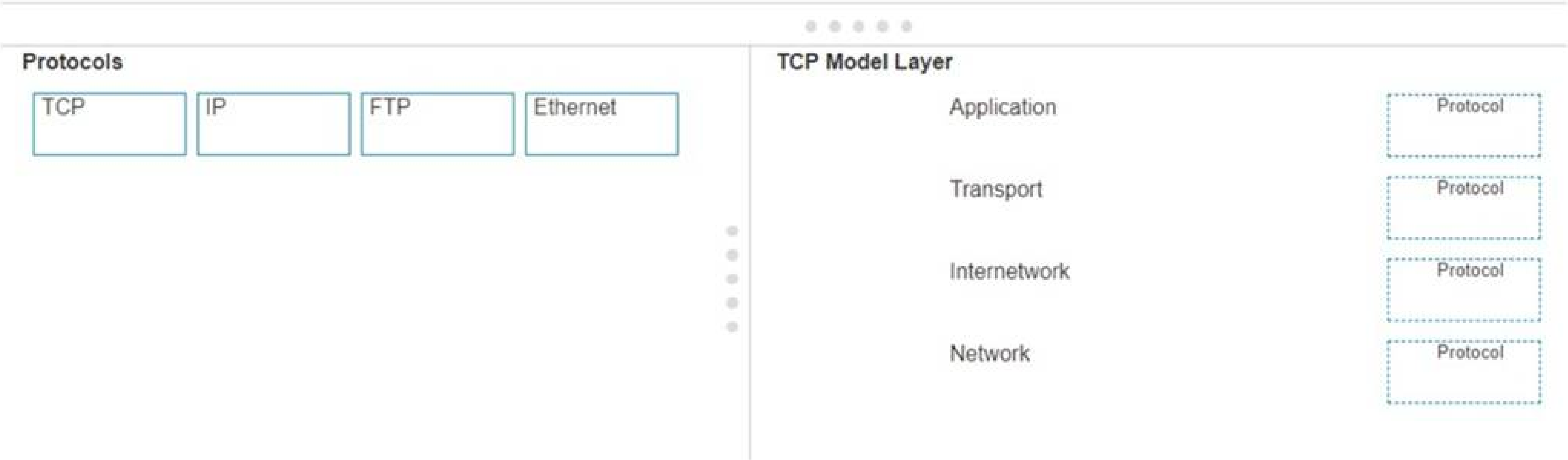


A. Mastered
B. Not Mastered

Answer: A

Explanation:
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 9
DRAG DROP
Move each protocol from the list on the left to the correct TCP/IP model layer on the right. Note: You will receive partial credit for each correct match.



A. Mastered
B. Not Mastered

Answer: A

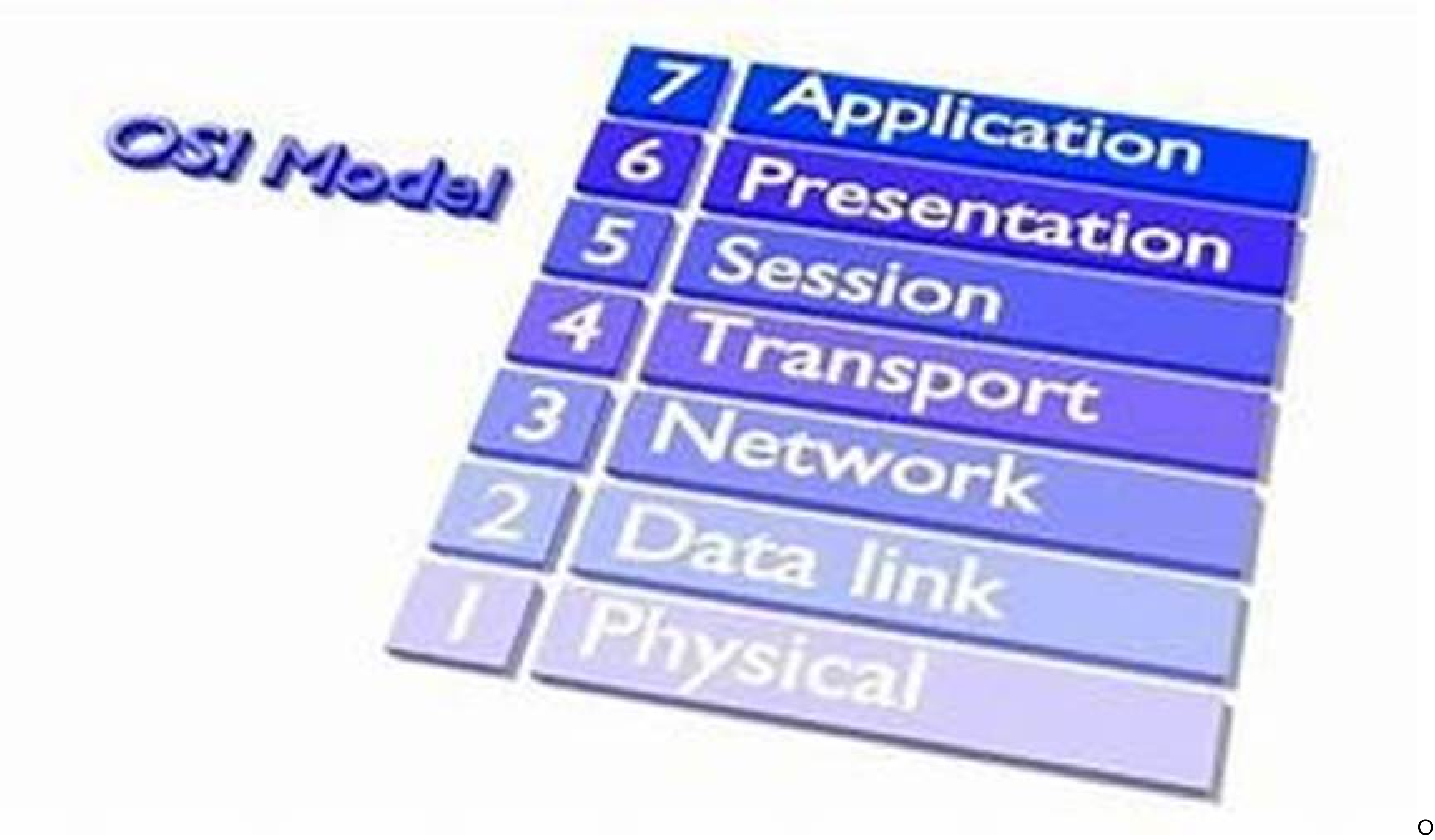
Explanation:
Here??s how each protocol aligns with the correct TCP/IP model layer:
? TCP (Transmission Control Protocol): This protocol belongs to the Transport layer, which is responsible for providing communication between applications on different hosts1.
? IP (Internet Protocol): IP is part of the Internetwork layer, which is tasked with routing packets across network boundaries to their destination1.
? FTP (File Transfer Protocol): FTP operates at the Application layer, which supports application and end-user processes. It is used for transferring files over the network1.
? Ethernet: While not a protocol within the TCP/IP stack, Ethernet is associated with the Network Interface layer, which corresponds to the link layer of the TCP/IP model and is responsible for the physical transmission of data1.
The TCP/IP model layers are designed to work collaboratively to transmit data from one layer to another, with each layer having specific protocols that perform functions necessary for the data transmission process1.
? TCP:
? IP:
? FTP:
? Ethernet:
? Transport Layer: This layer is responsible for providing communication services directly to the application processes running on different hosts. TCP is a core protocol in this layer.
? Internetwork Layer: This layer is responsible for logical addressing, routing, and
packet forwarding. IP is the primary protocol for this layer.
? Application Layer: This layer interfaces directly with application processes and provides common network services. FTP is an example of a protocol operating in this layer.
? Network Layer: In the TCP/IP model, this layer includes both the data link and physical layers of the OSI model. Ethernet is a protocol used in this layer to define network standards and communication protocols at the data link and physical levels.
References:
? TCP/IP Model Overview: Cisco TCP/IP Model
? Understanding the TCP/IP Model: TCP/IP Layers

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 13
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 17
......

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

100-150 Practice Exam Features:

* 100-150 Questions and Answers Updated Frequently

* 100-150 Practice Questions Verified by Expert Senior Certified Staff

* 100-150 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 100-150 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 100-150 Practice Test Here