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
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

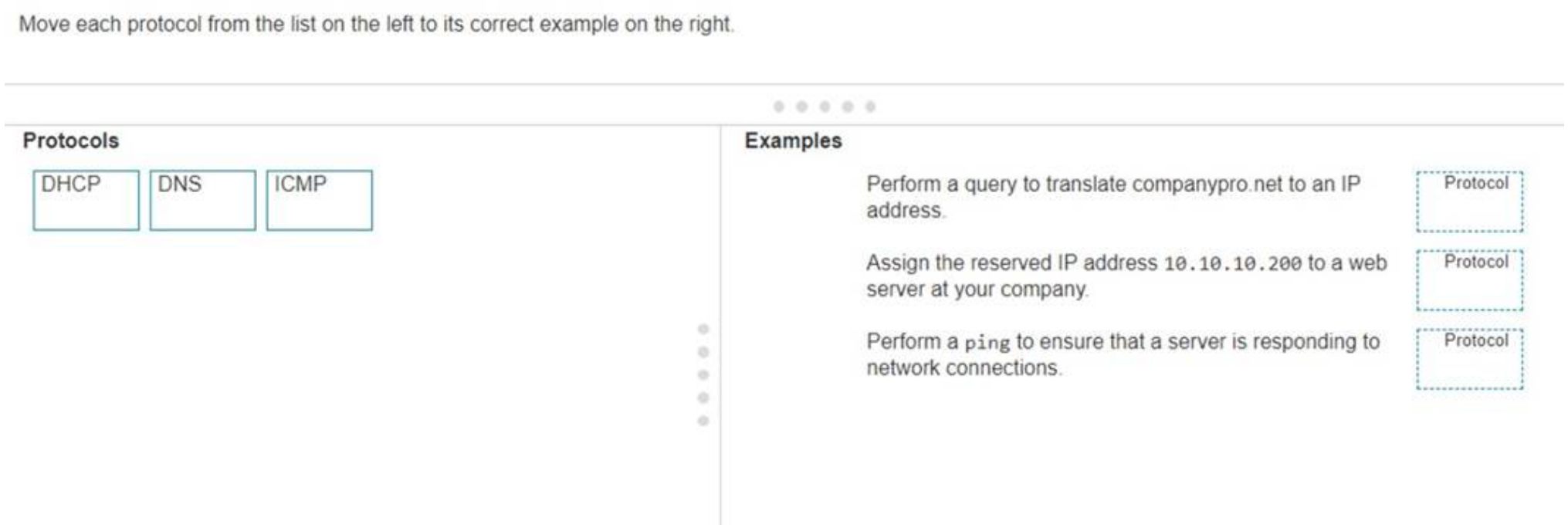
NEW QUESTION 4
An engineer configured a new VLAN named VLAN2 for the Data Center team. When the team tries to ping addresses outside VLAN2 from a computer in VLAN2, they are unable to reach them. What should the engineer configure?

A. Additional VLAN
B. Default route
C. Default gateway
D. Static route

Answer: C

Explanation:
When devices within a VLAN are unable to reach addresses outside their VLAN, it typically indicates that they do not have a configured path to external networks. The engineer should configure a default gateway for VLAN2. The default gateway is the IP address of the router??s interface that is connected to the VLAN, which will route traffic from the VLAN to other networks12.
References :=
•Understanding and Configuring VLAN Routing and Bridging on a Router Using the IRB Feature
•VLAN 2 not able to ping gateway - Cisco Community
==========
•VLANs: Virtual Local Area Networks (VLANs) logically segment network traffic to improve security and performance. Devices within the same VLAN can communicate directly.
•Default Gateway: For devices in VLAN2 to communicate with devices outside their VLAN, they need a default gateway configured. The default gateway is typically a router or Layer 3 switch that routes traffic between different VLANs and subnets.
•Additional VLAN: Not needed in this scenario as the issue is related to routing traffic outside VLAN2, not creating another VLAN.
•Default Route: While a default route on the router may be necessary, the primary issue for devices within VLAN2 is to have a configured default gateway.
•Static Route: This is used on routers to manually specify routes to specific networks but does not address the need for a default gateway on the client devices.
References:
•Cisco VLAN Configuration Guide: Cisco VLAN Configuration
•Understanding and Configuring VLANs: VLANs Guide

NEW QUESTION 5
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 6
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 7
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 8
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 without blinking.
Thus, the correct answer is C. Link is up and active. References :=
•Cisco Switch LED Indicators
•Cisco Ethernet Switch LED Patterns

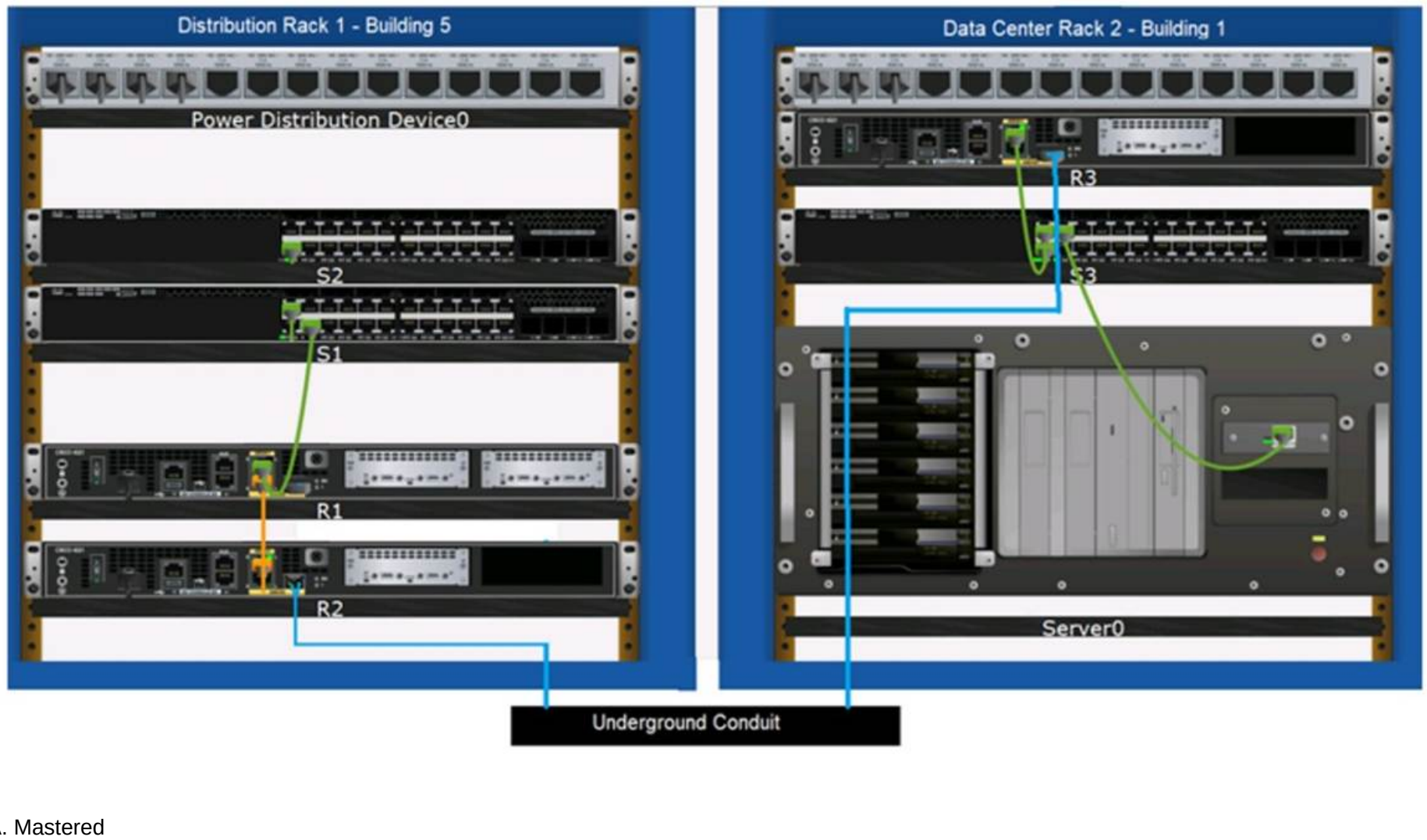
NEW QUESTION 9
A local company requires two networks in two new buildings. The addresses used in these networks must be in the private network range.
Which two address ranges should the company use? (Choose 2.) Note: You will receive partial credit for each correct selection.

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 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.

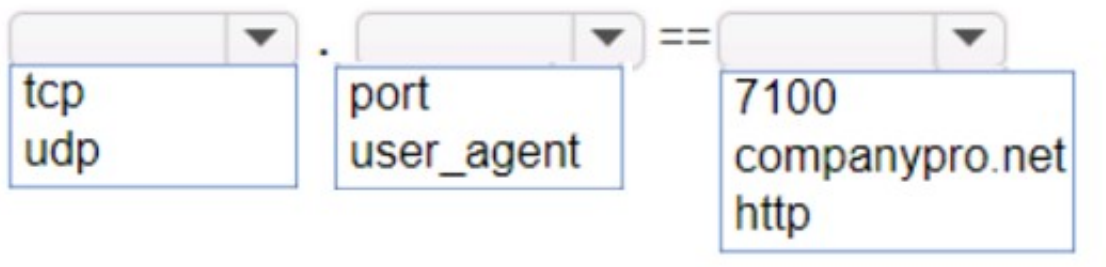


A. Mastered
B. Not Mastered

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 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 10
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.



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 12
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 15
HOTSPOT
You want to list the IPv4 addresses associated with the host name www.companypro.net.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To list the IPv4 addresses associated with the host name www.companypro.net, you should use the following command:
nslookup www.companypro.net
This command will query the DNS servers to find the IP address associated with the hostname provided. If you want to ensure that it returns the IPv4 address, you can specify the -type=A option, which stands for Address records that hold IPv4 addresses1. However, the nslookup command by default should return the IPv4 address if available.
To list the IPv4 addresses associated with the host name www.companypro.net, you should use the nslookup command.
? Command: nslookup
? Target: www.companypro.net So, the completed command is:
? nslookup www.companypro.net
? nslookup: This command is used to query the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.
? www.companypro.net: This is the domain name you want to query to obtain its
associated IP addresses. References:

? Using nslookup: nslookup Command Guide

NEW QUESTION 19
You plan to use a network firewall to protect computers at a small office.
For each statement about firewalls, select True or False. Note: You will receive partial credit for each correct selection.

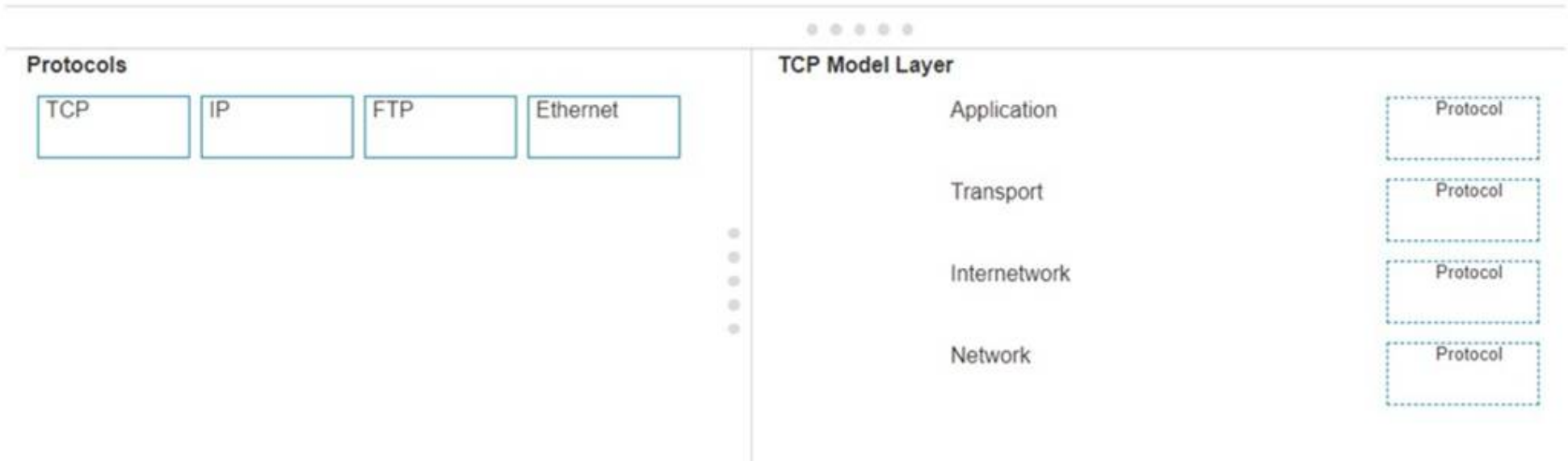
	True	False
A firewall can direct all web traffic to a specific IP address.	○	○
A firewall can block traffic to specific ports on internal computers.	○	○
A firewall can prevent specific apps from running on a computer.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? A firewall can direct all web traffic to a specific IP address.
? A firewall can block traffic to specific ports on internal computers.
? A firewall can prevent specific apps from running on a computer.
? Directing Web Traffic: Firewalls can manage traffic redirection using NAT and port forwarding rules to route web traffic to designated servers or devices within the network.
? Blocking Specific Ports: Firewalls can enforce security policies by blocking or
allowing traffic based on port numbers, ensuring that only permitted traffic reaches internal systems.
? Application Control: While firewalls manage network traffic, preventing applications
from running typically requires software specifically designed for endpoint protection and application management.
References:
? Understanding Firewalls: Firewall Capabilities

NEW QUESTION 20
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 21
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 23
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 28
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 29
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 30
.....

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/