

Cisco

Exam Questions CCST-Networking

Cisco Certified Support Technician (CCST) NetworkingExam



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: 11111111.11111111.1111100.00000000

•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.

Cloud Computing Service Models	Examples
IaaS	Three virtual machines are connected by a virtual network in the cloud. Model
PaaS	Users access a web-based graphics design application in the cloud for a monthly fee. Model
SaaS	A company develops applications using cloud-based resources and tools. Model

- 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

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 4

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.

netstat
ping
ftp
nslookup

companypro.net
192.168.0.1
localhost
8.8.8.8

- 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 5

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 6

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.

Protocols

TCP

IP

FTP

Ethernet

TCP Model Layer

Application

Transport

Internetwork

Network

Protocol

Protocol

Protocol

Protocol

- 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 theTransportlayer, which is responsible for providing communication between applications on different hosts1.

? IP (Internet Protocol): IP is part of theInternetworklayer, which is tasked with routing packets across network boundaries to their destination1.

? FTP (File Transfer Protocol): FTP operates at theApplicationlayer, 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 theNetwork Interfacelayer, 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 7

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.

tcp
udp

.

port
user_agent

==

7100
companypro.net
http

- 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 8

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 9

HOTSPOT

You purchase a new Cisco switch, turn it on, and connect to its console port. You then run the following command:

```
#show running-config | section include interface
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
<output omitted>
```

For each statement about the output, select True or False. Note: You will receive partial credit for each correct selection.

	True	False
The two interfaces are administratively shut down.	<input type="radio"/>	<input type="radio"/>
The two interfaces have default IP addresses assigned.	<input type="radio"/>	<input type="radio"/>
The two interfaces can communicate over Layer 2.	<input type="radio"/>	<input type="radio"/>

A. Mastered

B. Not Mastered

Answer: A

Explanation:

? The two interfaces are administratively shut down:

? The two interfaces have default IP addresses assigned:

? The two interfaces can communicate over Layer 2:

? Interface Status: The absence of the "shutdown" command means the interfaces are not administratively shut down.

? IP Address Assignment: There is no evidence in the output that IP addresses have been assigned to the interfaces, which would typically be shown as "ip address" entries.

? Layer 2 Communication: Switch interfaces in their default state operate at Layer 2, enabling them to forward Ethernet frames and participate in Layer 2 communication.

References:

? Cisco IOS Interface Configuration: Cisco Interface Configuration

? Understanding Cisco Switch Interfaces: Cisco Switch Interfaces

NEW QUESTION 10

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 10

What is the purpose of assigning an IP address to the management VLAN interface on a Layer 2 switch?

A. To enable the switch to act as a default gateway for the attached devices

B. To enable the switch to resolve URLs for the attached the devices

C. To enable the switch to provide DHCP services to other switches in the network

D. To enable access to the CLI on the switch through Telnet or SSH

Answer: D

Explanation:

The primary purpose of assigning an IP address to the management VLAN interface on a Layer 2 switch is to facilitate remote management of the switch. By configuring an IP address on the management VLAN, network administrators can access the switch's Command Line Interface (CLI) remotely using protocols such as Telnet or Secure Shell (SSH). This allows for convenient configuration changes, monitoring, and troubleshooting without needing physical access to the switch.

References :=

•Understanding the Management VLAN

•Cisco - VLAN Configuration Guide

•Remote Management of Switches

Assigning an IP address to the management VLAN interface (often the VLAN 1 interface by default) on a Layer 2 switch allows network administrators to remotely manage the switch using protocols such as Telnet or SSH. This IP address does not affect the switch's ability to route traffic between VLANs but provides a means to access and configure the switch through its Command Line Interface (CLI).

•A: The switch does not act as a default gateway; this is typically a function of a Layer 3 device like a router.

•B: The switch does not resolve URLs; this is typically a function of DNS servers.

•C: The switch can relay DHCP requests but does not typically provide DHCP services itself; this is usually done by a dedicated DHCP server or router.

Thus, the correct answer is D. To enable access to the CLI on the switch through Telnet or SSH.

References :=

•Cisco VLAN Management Overview

•Cisco Catalyst Switch Management

NEW QUESTION 13

Examine the following output:

Examine the following command output:

```
C:\Admin>tracert www.cisco.com
5
over a maximum of 30 hops:

 1  <1 ms  <1 ms  <1 ms  2603-6081-943f-72ec-a240-a0ff-fe67-3c14.res6.big.com [2603:6081:943f:72ec:a240:a0ff:fe67:3c14]
 2  13 ms  11 ms  16 ms  2603-90b3-0a00-01bb-0000-0000-0000-0001.wifi6.biginternet.com [2603:90b3:a00:1bb::1]
 3  17 ms  25 ms  18 ms  lag-61.zblnnc1001h.netops.exchange.com [2001:db8:a000:0:4::8:d4c]
 4  16 ms  13 ms  11 ms  lag-29.drhmncev02r.netops.exchange.com [2001:db8:a000:0:4::2:152]
 5  *      *      *      Request timed out.
 6  *      *      *      Request timed out.
 7  19 ms  18 ms  27 ms  lag-0.pr2.dca10.netops.provider.com [2001:db8:1998:0:4::517]
 8  21 ms  32 ms  23 ms  2001:db8:1998:0:8::639
 9  16 ms  15 ms  18 ms  vlan-103.r10.spine101.iad03.fab.netarch.provider.com [2600:1408:b400:40b::1]
10  15 ms  17 ms  22 ms  vlan-110.r03.leaf101.iad03.fab.netarch.provider.com [2600:1408:b400:f03::1]
11  17 ms  17 ms  23 ms  vlan-104.r08.tor101.iad03.fab.netarch.provider.com [2600:1408:b400:2908::1]
12  25 ms  19 ms  19 ms  g2600-1408-c400-038d-0000-0000-0000-0b33.deploy.static.et.com [2600:1408:c400:38d::b33]

Trace complete.
```

Which two conclusions can you make from the output of the tracert command? (Choose 2.) Note: You will receive partial credit for each correct answer.

- A. The trace successfully reached the www.cisco.com server.
- B. The trace failed after the fourth hop.
- C. The IPv6 address associated with the www.cisco.com server is 2600:1408: c400: 38d: : b33.
- D. The routers at hops 5 and 6 are offline.
- E. The device sending the trace has IPv6 address 2600:1408:c400:38d :: b33.

Answer: AC

Explanation:

- Statement A: "The trace successfully reached the www.cisco.com server." This is true as indicated by the "Trace complete" message at the end, showing that the trace has reached its destination.
- Statement C: "The IPv6 address associated with the www.cisco.com server is 2600:1408:c400:38d::b33." This is true because the final hop in the trace, which is the destination, has this IPv6 address.
- Statement B: "The trace failed after the fourth hop." This is incorrect as the trace continues beyond the fourth hop, despite some intermediate timeouts.
- Statement D: "The routers at hops 5 and 6 are offline." This is not necessarily true. The routers might be configured to not respond to traceroute requests.
- Statement E: "The device sending the trace has IPv6 address 2600:1408:c400:38d::b33." This is incorrect; this address belongs to the destination server, not the sender. References:
- Understanding Traceroute: Traceroute Guide

NEW QUESTION 15

HOTSPOT

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

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.	<input type="radio"/>	<input type="radio"/>
High levels of network latency decrease network bandwidth.	<input type="radio"/>	<input type="radio"/>
You can increase throughput by decreasing network latency.	<input type="radio"/>	<input type="radio"/>

- 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 20

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. tracer
- C. ipconfig/all
- D. nslookup

Answer: B

Explanation:

The tracer 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 tracer 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.

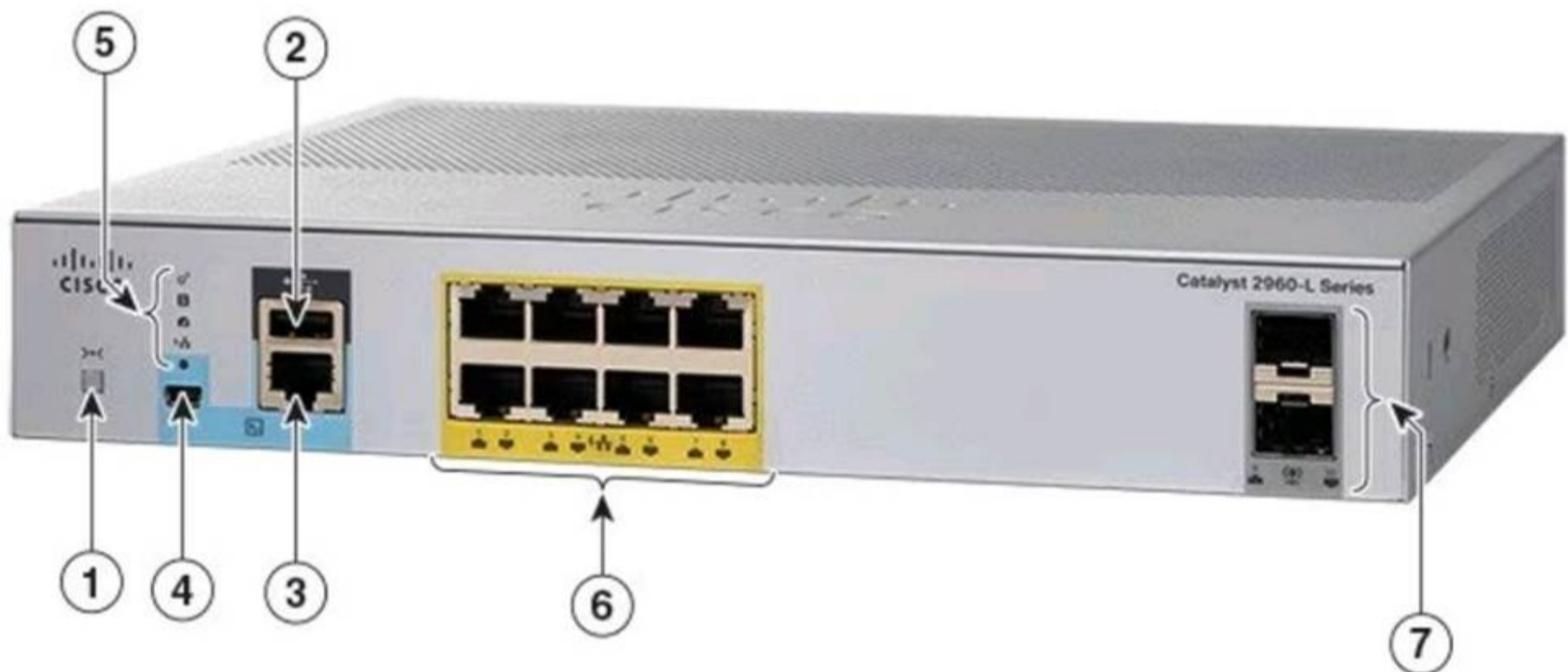
- tracer Command: This command is used to determine the path packets take to reach a destination. It lists all the hops (routers) along the way and can help identify where the delay or failure occurs.
- ping -t: This command sends continuous ping requests and is useful for determining if a host is reachable 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 tracer Command: tracer Command Guide
- Troubleshooting Network Issues with tracer: Network Troubleshooting Guide

NEW QUESTION 21

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 25

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 28

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 30

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:
 0 0 ms  0 ms  1 ms  192.168.5.1
 1 1 ms  0 ms  0 ms  10.0.1.1
 2 *      *      *      Request timed out.
 3 1 ms  1 ms  0 ms  10.0.0.2
 4 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 33

DRAG DROP

Move each network type from the list on the left to the correct example on the right.

Network Types

WAN

PAN

MAN

LAN

Examples

Two home office computers are connected to a switch by Ethernet cables.

Network Type

Three government buildings in the same city connect to a cable company over coaxial cables.

Network Type

A cell phone connects to a Bluetooth headset.

Network Type

A financial institution connects its branches through a telecommunications service provider.

Network Type

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- ? Two home office computers are connected to a switch by Ethernet cables.
- ? Three government buildings in the same city connect to a cable company over coaxial cables.
- ? A cell phone connects to a Bluetooth headset.
- ? A financial institution connects its branches through a telecommunications service provider.
- ? LAN (Local Area Network): Used for connecting devices within a small geographical area such as a single building or home.
- ? MAN (Metropolitan Area Network): Covers a larger geographical area than a LAN, typically a city or campus.
- ? PAN (Personal Area Network): Connects devices within the range of an individual person, such as connecting a phone to a Bluetooth headset.
- ? WAN (Wide Area Network): Spans large geographical areas, connecting multiple LANs across cities, countries, or continents.

References:

- ? Network Types Overview: Cisco Networking Basics
- ? Understanding Different Network Types: Network Types Guide

NEW QUESTION 38

.....

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CCST-Networking Practice Exam Features:

- * CCST-Networking Questions and Answers Updated Frequently
- * CCST-Networking Practice Questions Verified by Expert Senior Certified Staff
- * CCST-Networking Most Realistic Questions that Guarantee you a Pass on Your First Try
- * CCST-Networking Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CCST-Networking Practice Test Here](#)