



Cisco

Exam Questions CCST-Networking

Cisco Certified Support Technician (CCST) NetworkingExam

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

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

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 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 3

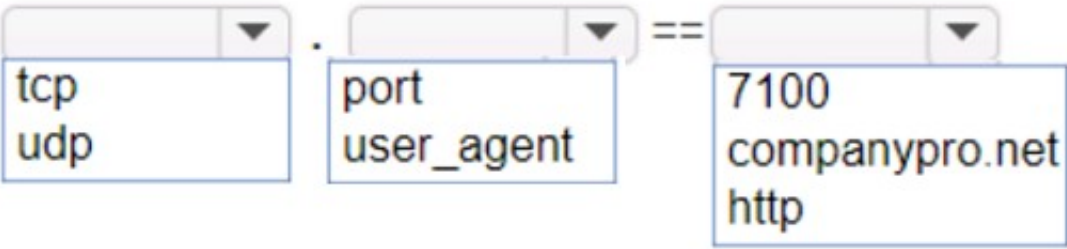
HOTSPOT

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 4

DRAG DROP

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

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

Protocols

DHCP

DNS

ICMP

Examples

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.

Protocol

Protocol

Protocol

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.

Your Partner of IT Exam

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

? 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 5

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 switch1.

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 6

DRAG DROP

Move the MFA factors from the list on the left to their correct examples on the right. You may use each factor once, more than once, or not at all.

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

Factors

Inference

Knowledge

Possession

Examples

Entering a one-time security code sent to your device after logging in

Holding your phone to your face to be recognized

Specifying your user name and password to log on to a service

Factor

Factor

Factor

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The correct matching of the MFA factors to their examples is as follows:

- ? Entering a one-time security code sent to your device after logging in: Possession
- ? Holding your phone to your face to be recognized: Inherence
- ? Specifying your user name and password to log on to a service: Knowledge Here's why each factor matches the example:
- ? Possession: This factor is something the user has, like a mobile device. A one-time security code sent to this device falls under this category.
- ? Inherence: This factor is something the user is, such as a biometric characteristic. Facial recognition using a phone is an example of this factor.
- ? Knowledge: This factor is something the user knows, like a password or PIN. Multi-Factor Authentication (MFA) enhances security by requiring two or more of these factors to verify a user's identity before granting access.
- ? Entering a one-time security code sent to your device after logging in.
- ? Holding your phone to your face to be recognized.
- ? Specifying your username and password to log on to a service.
- ? Possession Factor: This involves something the user has in their possession. Receiving a one-time security code on a device (e.g., phone) is an example of this.
- ? Inference Factor (Inherence/Biometric): This involves something inherent to the user, such as biometric verification (e.g., facial recognition or fingerprint scanning).

? Knowledge Factor: This involves something the user knows, such as login credentials (username and password).

References:

? Multi-Factor Authentication (MFA) Explained: MFA Guide

? Understanding Authentication Factors: Authentication Factors

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

Cable Types

Coaxial Cable

Console Cable

Crossover UTP Cable

Fiber Optic Cable

Straight-through UTP Cable

Connections

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

Cable Type

Cable Type

Cable Type

Cable Type

- 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 interfaceCable Type: = Straight-through UTP Cable

Connects Router R2 Gi0/0/0 to Router R3 Gi0/0/0 via underground conduitCable Type

: = Fiber Optic Cable

Connects Router R1 Gi0/0/0 to Router R2 Gi0/0/1Cable Type: = Crossover UTP Cable

Connects Switch S3 to Server0 network interface cardCable Type: = Straight-through UTP Cable

The choices are based on standard networking practices where:

? Straight-through UTP cablesare typically used to connect a switch to a router or a network interface card.

? Fiber optic cablesare ideal for long-distance, high-speed data transmission, such as connections through an underground conduit.

? Crossover UTP cablesare 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.

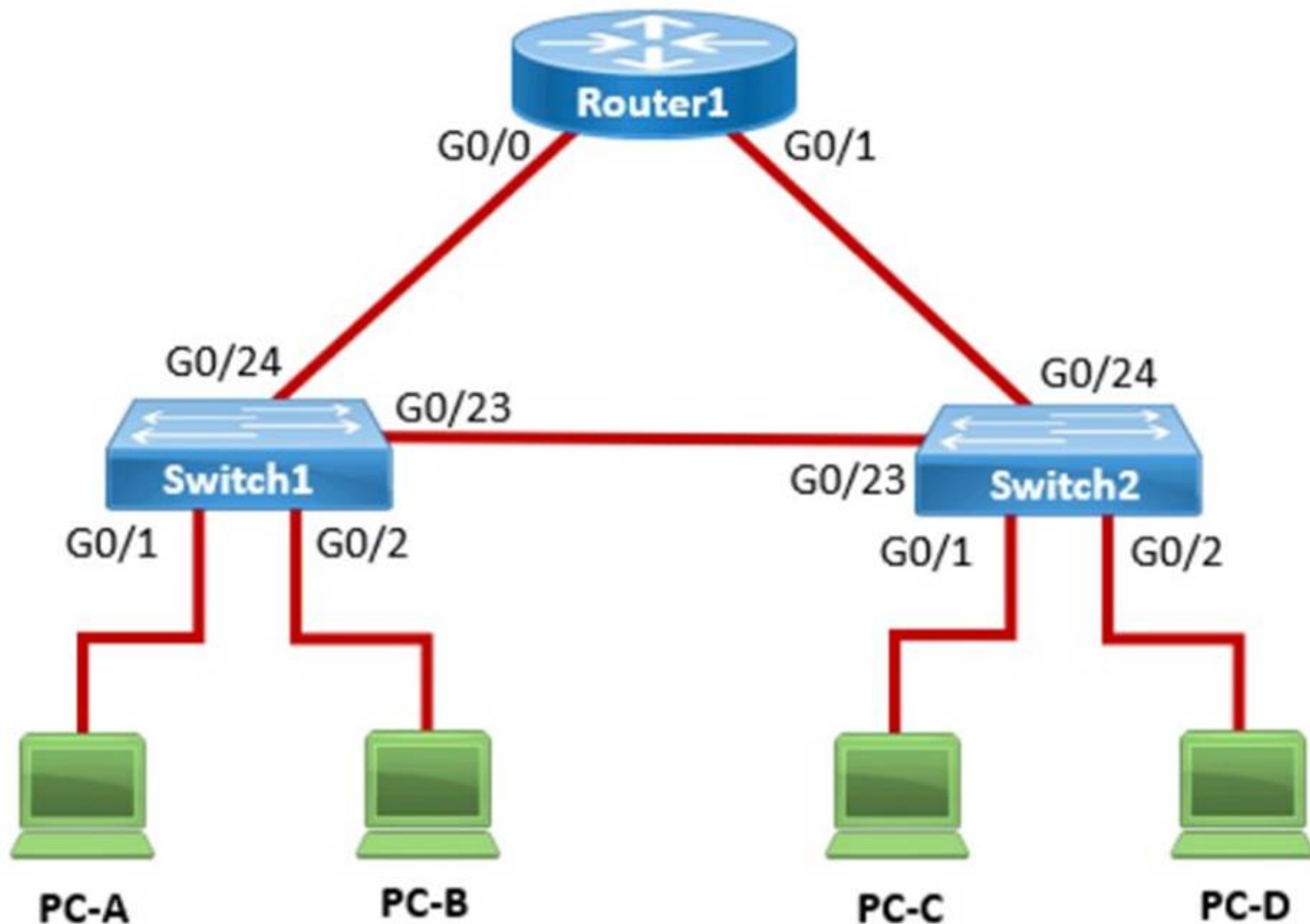
References:

? Network Cable Types and Uses: Cisco Network Cables

? Understanding Ethernet Cabling: Ethernet Cable Guide

NEW QUESTION 8

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



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

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

Answer: B

Explanation:

In a network, when a Layer 2 switch (like Switch1) receives a frame destined for a MAC address that is not in its MAC address table, it performs a flooding operation. This means the switch will send the frame out of all ports except the port on which the frame was received. This flooding ensures that if the destination device is connected to one of the other ports, it will receive the frame and respond, allowing the switch to learn its MAC address.

? A. Switch1 queries Switch2 for the MAC address of PC-C: This does not happen in Layer 2 switches; they do not query other switches for MAC addresses.

? A. Switch1 drops the frame and sends an error message back to PC-A: This is not the default behavior for unknown unicast frames.

? D. Switch1 sends an ARP request to obtain the MAC address of PC-C: ARP is used by devices to map IP addresses to MAC addresses, not by switches to find unknown MAC addresses.

Thus, the correct answer is B. Switch1 floods the frame out all active ports except port G0/1.

References:=-

? Cisco Layer 2 Switching Overview

? Switching Mechanisms (Cisco)

NEW QUESTION 9

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

TrueFalse

Low bandwidth can increase network latency.



High levels of network latency decrease network bandwidth.



You can increase throughput by decreasing network latency.



- 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 10

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 networks.

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 10

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 office.
B. The jack must be patched and made active.
C. Ticket 2: An online webinar is taking place in the conference room.
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

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 18

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 22

.....

Relate Links

100% Pass Your CCST-Networking Exam with ExamBible Prep Materials

<https://www.exambible.com/CCST-Networking-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/>