CCST-NETWORKING Q&As

Cisco Certified Support Technician (CCST) NetworkingExam

Pass Cisco CCST-NETWORKING Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

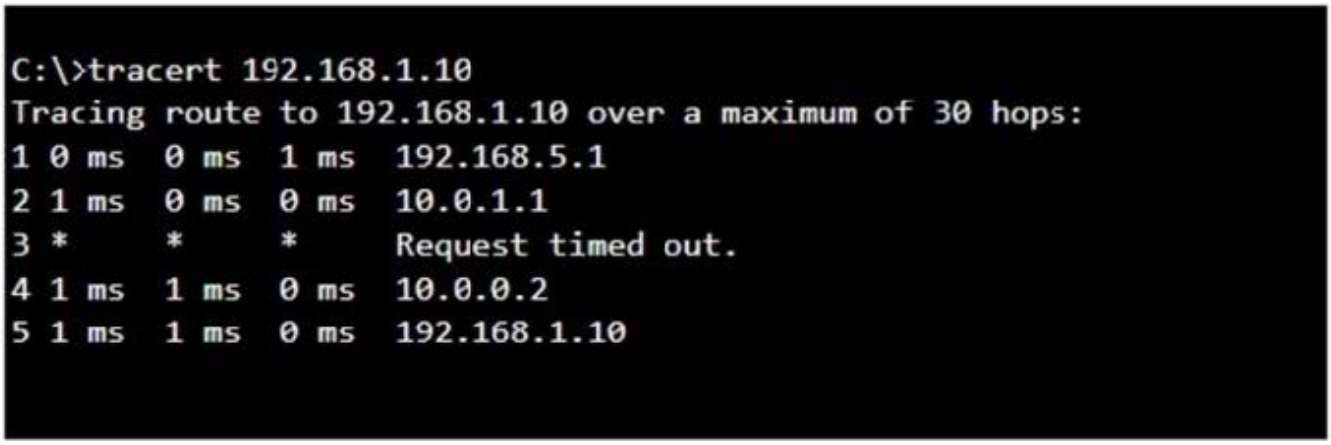
https://www.leads4pass.com/ccst-networking.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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 isreachable over the network. The output of the command is shown as follows:



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.

Correct Answer: C

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 reachable.

References:

-How to Use Traceroute Command to Read Its Results

-How to Use the Tracert Command in Windows

QUESTION 2

A Cisco switch is not accessible from the network. You need to view its running configuration.

Which out-of-band method can you use to access it?

A. SNMP

B. Console

C. SSH

D. Telnet

Correct Answer: B

Out-of-band management

When a Cisco switch is not accessible from the network, the recommended out-of-band method to access its running configuration is through theconsole port. Out-of-band management involves accessing the network device through a

dedicated management channel that is not part of the data network.The console port provides direct access to the switch\\'s Command Line Interface (CLI) without using the network, which is essential when the switch cannot be accessed

remotely via the network12.

References:

Out-of-band (OOB) network interface configuration guidelines Out of band management configuration

==========

If you have any more questions or need further assistance, feel free to ask!

QUESTION 3

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

Correct Answer: C

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

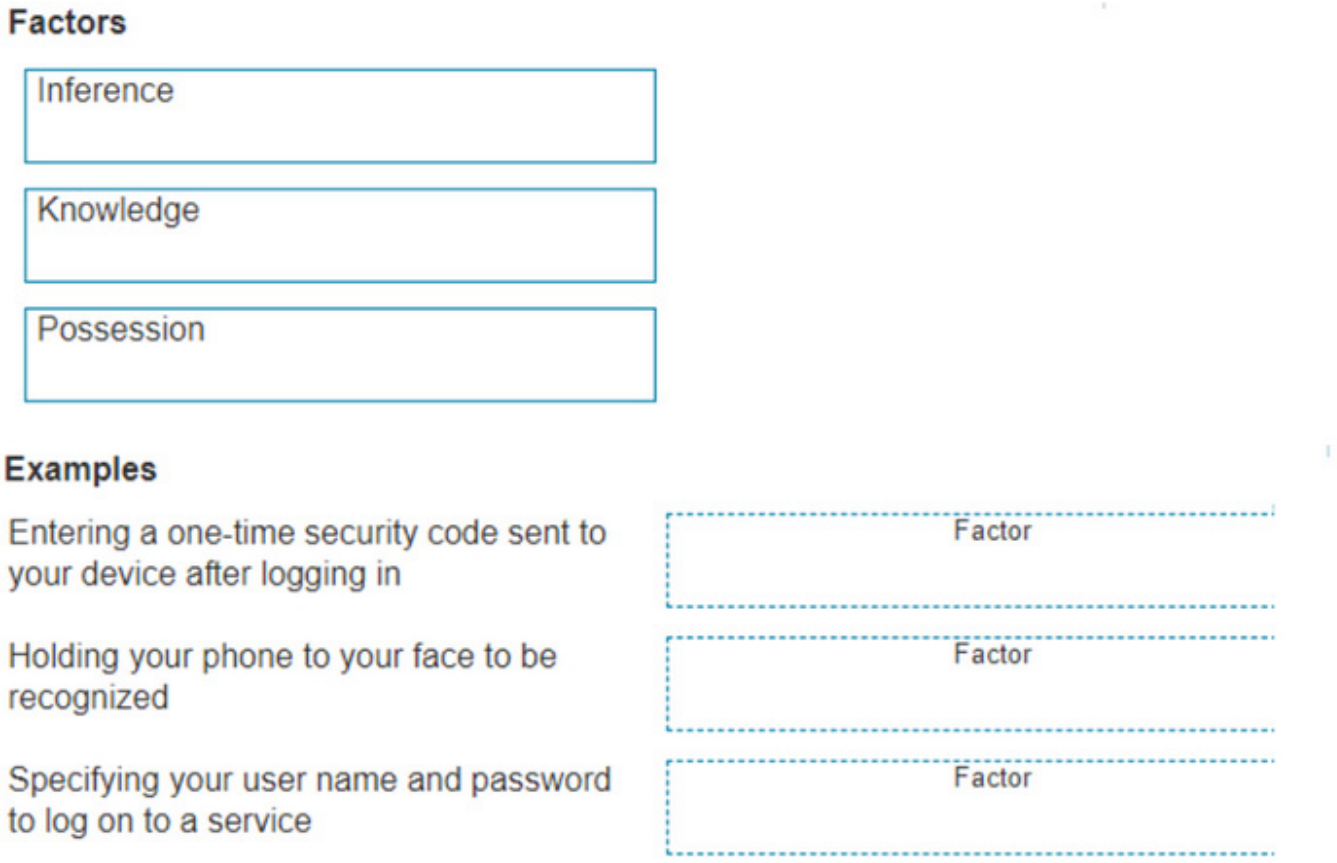
QUESTION 4

DRAG DROP

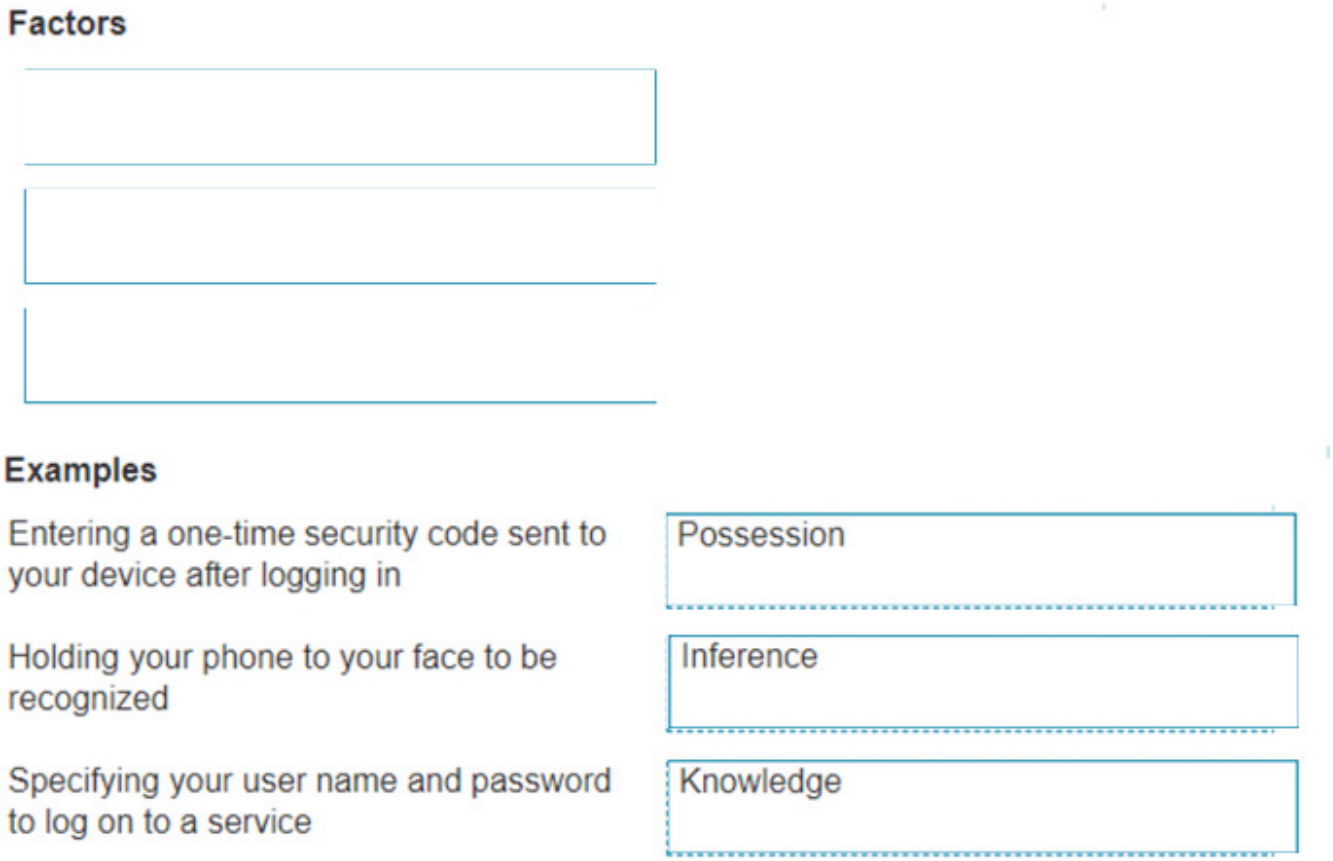
Move the MFA factors from the list on the left to their correct examples on the right. You may use each factor once, more than once, or not at all.

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

Select and Place:



Correct Answer:



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

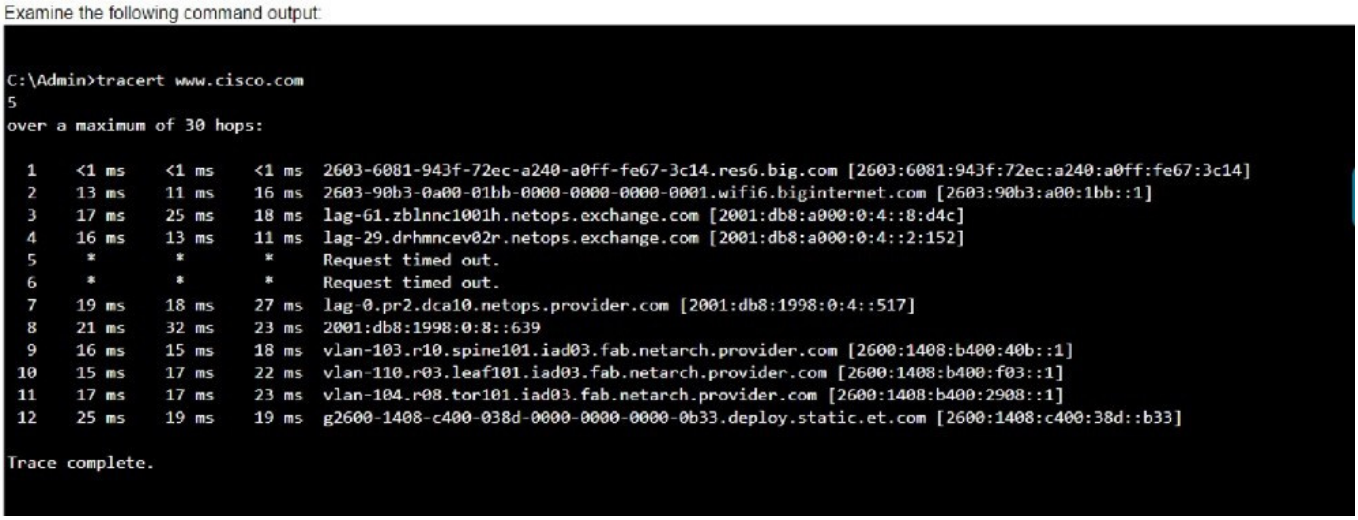
user, such as biometric verification (e.g., facial recognition or fingerprint scanning). Knowledge Factor: This involves something the user knows, such as login credentials (username and password).

References:

Multi-Factor Authentication (MFA) Explained: MFA Guide Understanding Authentication Factors: Authentication Factors

QUESTION 5

Examine the following output:



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.

Correct Answer: AC

-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

QUESTION 6

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

Correct Answer: B

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, Macand; 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

QUESTION 7

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.

Correct Answer: BD

-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.

QUESTION 8

A local company requires two networks in two new buildings. The addresses used in these networksmust 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

Correct Answer: AD

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 172.31.255.255falls within the Class B private range. B.

192.16.0.0 to 192.16.255.255is not a recognized private IP range. C.11.0.0.0 to 11.255.255.255is 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 AandD.

References:

Reserved IP addresses on Wikipedia

Private IP Addresses in Networking - GeeksforGeeks Understanding Private IP Ranges, Uses, Benefits, and Warnings

QUESTION 9

HOTSPOT

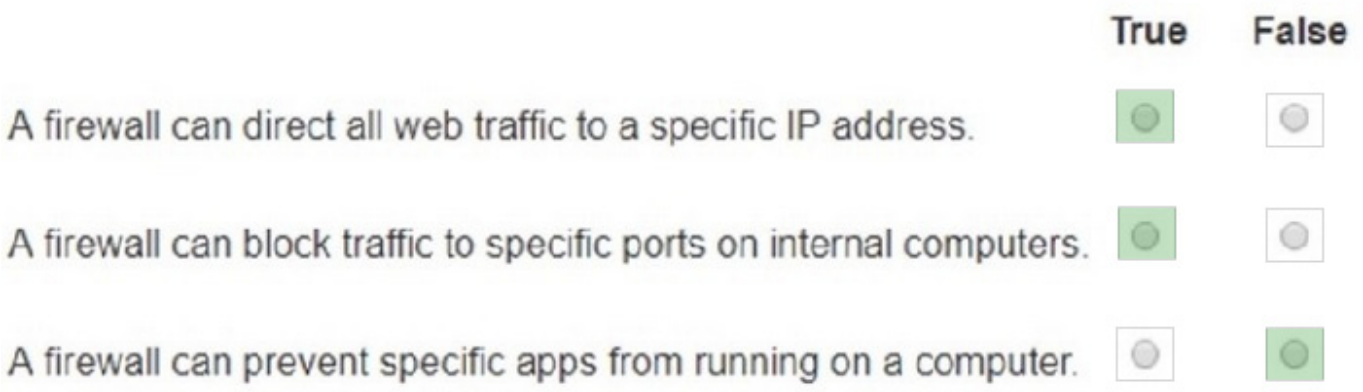
You plan to use a network firewall to protect computers at a small office.

For each statement about firewalls, select True or False.

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

Hot Area:

Correct Answer:



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

Network Security Best Practices: Network Security Guide

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. The jack must be patched and made active.

B. Ticket 2: An online webinar is taking place in the conference room. The video conferencing equipment lost internet access.

C. Ticket 3: A user reports that response time for a cloud-based application is slower than usual.

D. Ticket 4: Two users report that wireless access in the cafeteria has been down for the last hour.

Correct Answer: B

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