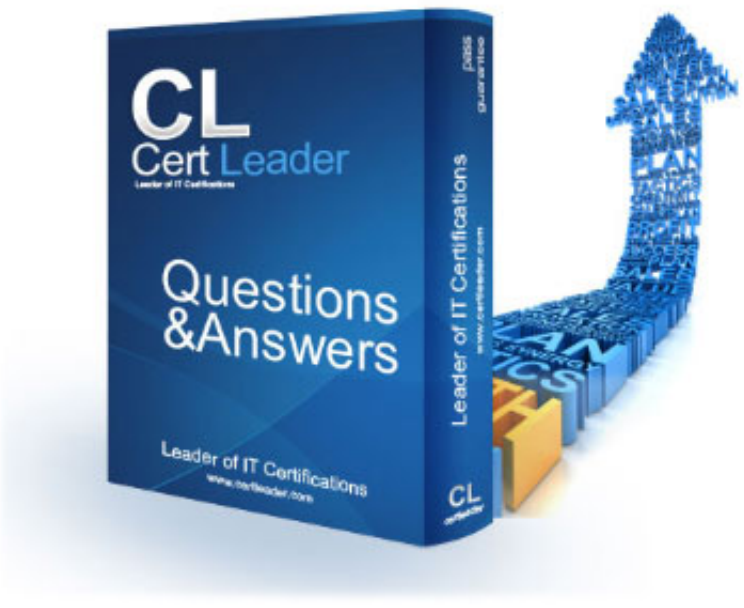
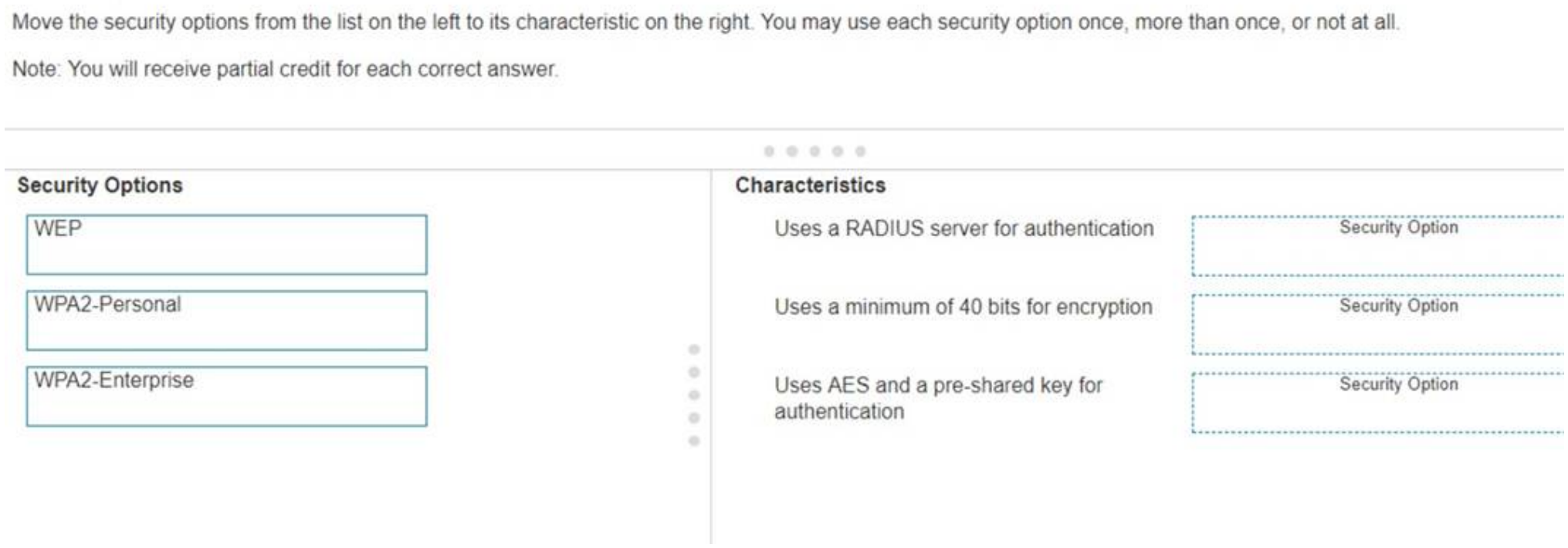
100-150 Dumps

Cisco Certified Support Technician (CCST) Networking

https://www.certleader.com/100-150-dumps.html



NEW QUESTION 1
DRAG DROP
Move the security options from the list on the left to its characteristic on the right. You may use each security option once, more than once, or not at all.
Note: You will receive partial credit for each correct answer.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The correct matching of the security options to their characteristics is as follows:
? WPA2-Enterprise: Uses a RADIUS server for authentication
? WEP: Uses a minimum of 40 bits for encryption
? WPA2-Personal: Uses AES and a pre-shared key for authentication Here??s why each security option matches the characteristic:
? WPA2-Enterprise uses a RADIUS server for authentication, which provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.
? WEP (Wired Equivalent Privacy) is an outdated security protocol that uses a minimum of 40 bits for encryption (and up to 104 bits), which is relatively weak by today??s standards.
? WPA2-Personal (Wi-Fi Protected Access 2 - Personal) uses the Advanced Encryption Standard (AES) for encryption and a pre-shared key (PSK) for authentication, which is shared among users to access the network.
These security options are essential for protecting wireless networks from unauthorized access and ensuring data privacy.

NEW QUESTION 2
You want to store files that will be accessible by every user on your network. Which endpoint device do you need?

A. Access point
B. Server
C. Hub
D. Switch

Answer: B

Explanation:
To store files that will be accessible by every user on a network, you would need a server. A server is a computer system that provides data to other computers. It can serve data to systems on a local network (LAN) or a wide network (WAN) over the internet. In this context, a file server would be set up to store and manage files, allowing users on the network to access them from their own devices1.
References :=
? What is a Server?
? Understanding Servers and Their Functions
A server is a computer designed to process requests and deliver data to other computers over a local network or the internet. In this case, to store files that will be accessible by every user on the network, a file server is the appropriate endpoint device. It provides a centralized location for storing and managing files, allowing users to access and share files easily.
? A. Access point: Provides wireless connectivity to a network.
? C. Hub: A basic networking device that connects multiple Ethernet devices together, making them act as a single network segment.
? D. Switch: A networking device that connects devices on a computer network by using packet switching to forward data to the destination device.
Thus, the correct answer is B. Server.
References :=
? File Server Overview (Cisco)
? Server Roles in Networking (Cisco)

NEW QUESTION 3
Which component of the AAA service security model provides identity verification?

A. Authorization
B. Auditing
C. Authentication

D. Accounting

Answer: C

Explanation:
The AAA service security model consists of three components: Authentication, Authorization, and Accounting.
•Authentication: This is the process of verifying the identity of a user or device. It ensures that only legitimate users can access the network or service.
•Authorization: This determines what an authenticated user is allowed to do or access within the network.
•Auditing/Accounting: This component tracks the actions of the user, including what resources they access and what changes they make.
Thus, the correct answer is C. Authentication. References :=
•Cisco AAA Overview
•Understanding AAA (Authentication, Authorization, and Accounting)

NEW QUESTION 4
Which 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

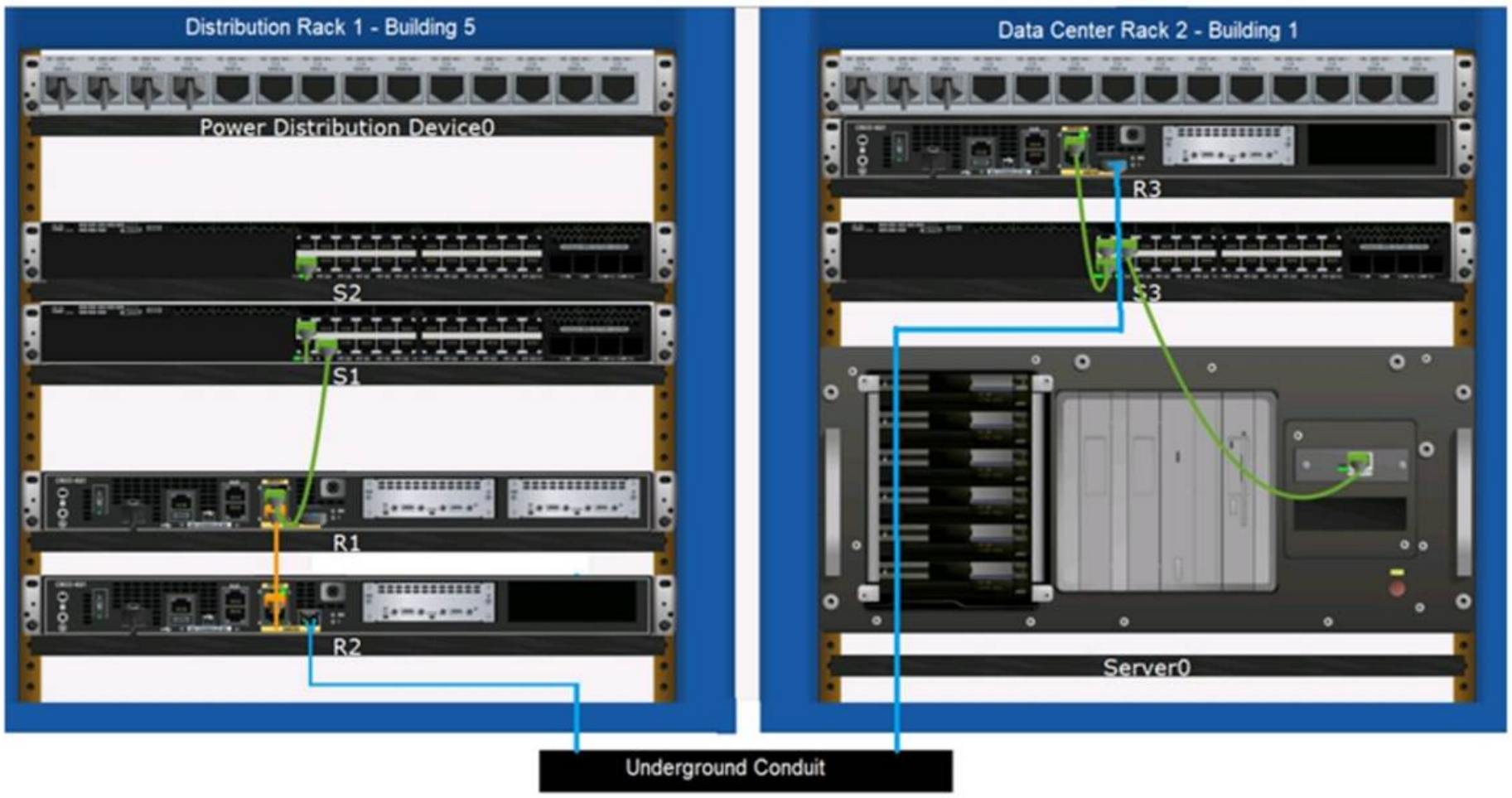
NEW QUESTION 5
A support technician examines the front panel of a Cisco switch and sees 4 Ethernet cables connected in the first four ports. Ports 1, 2, and 3 have a green LED. Port 4 has a blinking green light. What is the state of the Port 4?

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 6
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.

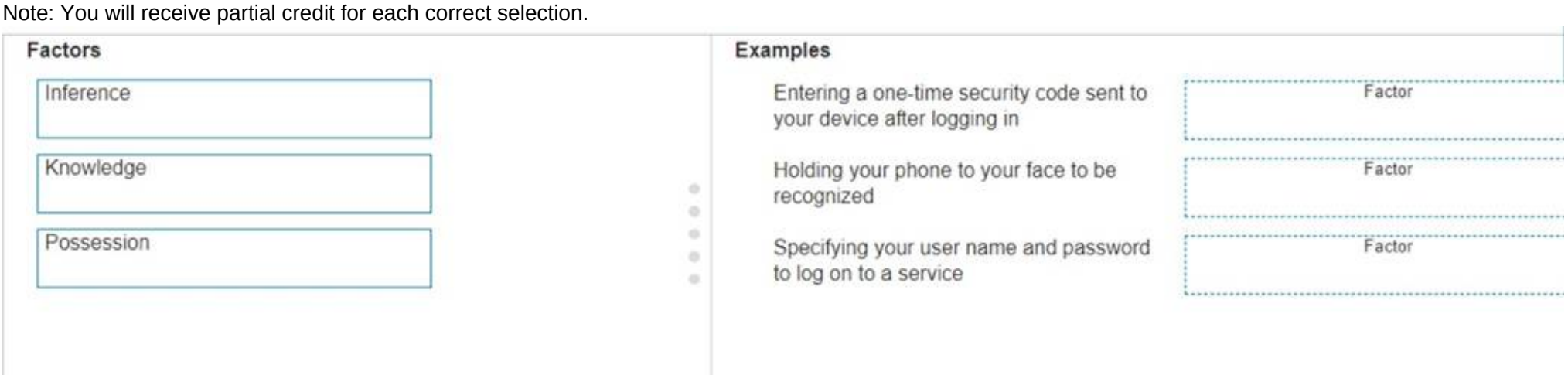


A. Mastered
B. Not Mastered

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 7
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.

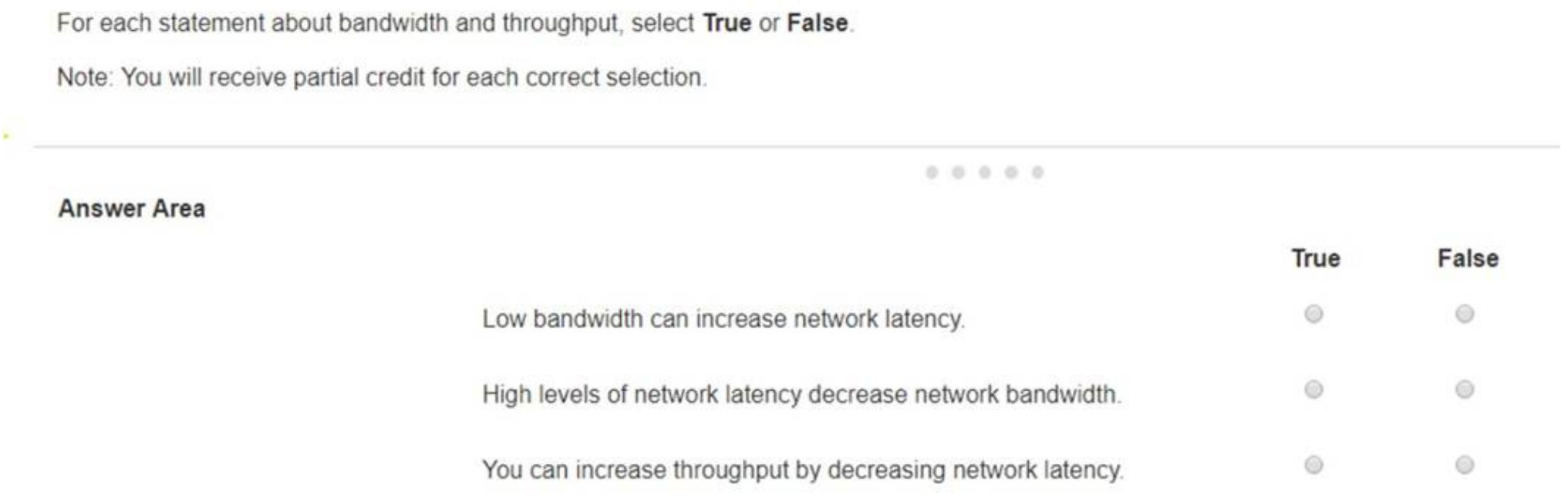


A. Mastered
B. Not Mastered

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 8
For each statement about bandwidth and throughput, select True or False.
Note: You will receive partial credit for each correct selection.



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 9
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 10
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.	○	○
The two interfaces have default IP addresses assigned.	○	○
The two interfaces can communicate over Layer 2.	○	○

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
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.

A. Mastered
B. Not Mastered

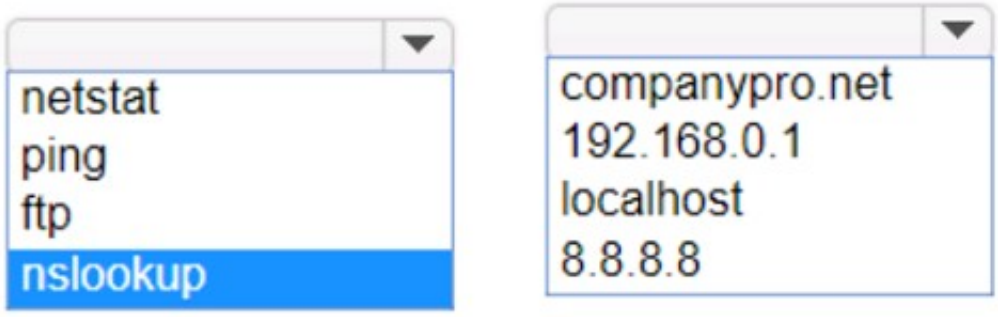
Answer: A

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 13
HOTSPOT
Computers in a small office are unable to access companypro.net. You run the ipconfig command on one of the computers. The results are shown in the exhibit.
You need to determine if you can reach the router.

```
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . . . . . . . : 192.168.0.14(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Sunday, January 8, 2023 11:00:02 AM
Lease Expires . . . . . . . . . . : Sunday, January 8, 2023 12:00:12 PM
Default Gateway . . . . . . . . . : 192.168.0.1
DHCP Server . . . . . . . . . . . : 192.168.0.1
DNS Servers . . . . . . . . . . . : 8.8.8.8
                                   8.8.4.4
NetBIOS over Tcpip. . . . . . . . : Enabled
```

Which command should you use? Complete the command by selecting the correct options from each drop-down lists.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
To determine if you can reach the router, you should use the ping command followed by the IP address of the router. The ping command is a network utility used to test the
reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination

computer.
The Default Gateway in the ipconfig results is typically the router??s IP address in a home or small office network. In this case, the Default Gateway is 192.168.0.1, which is the address you would ping to check connectivity to the router.
References :=
? How to Use the Ping Command
? Testing Network Connectivity with the Ping Command
==========
To determine if you can reach the router, you should use the ping command with the IP address of the router.
? Command: ping
? Target: 192.168.0.1 So, the completed command is:
? ping 192.168.0.1
Step by Step Comprehensive and Detailed Explanation:
? ping: The ping command sends ICMP Echo Request messages to the target IP address and waits for an Echo Reply. It is commonly used to test the reachability of a network device.
? 192.168.0.1: This is the IP address of the default gateway (the router) as shown in the ipconfig output. Pinging this address will help determine if the computer can communicate with the router.
References:
? Using the ping Command: ping Command Guide

NEW QUESTION 14
Which two pieces of information should you include when you initially create a support ticket? (Choose 2.)

A. A detailed description of the fault
B. Details about the computers connected to the network
C. A description of the conditions when the fault occurs
D. The actions taken to resolve the fault
E. The description of the top-down fault-finding procedure

Answer: AC

Explanation:
? Statement A: "A detailed description of the fault." This is essential for support staff to understand the nature of the problem and begin troubleshooting effectively.
? Statement C: "A description of the conditions when the fault occurs." This helps in reproducing the issue and identifying patterns that might indicate the cause of the fault.
? Statement B: "Details about the computers connected to the network." While useful, this is not as immediately critical as understanding the fault itself and the conditions under which it occurs.
? Statement D: "The actions taken to resolve the fault." This is important but typically follows the initial report.
? Statement E: "The description of the top-down fault-finding procedure." This is more of a troubleshooting methodology than information typically included in an initial support ticket.
References:
? Best Practices for Submitting Support Tickets: Support Ticket Guidelines

NEW QUESTION 19
During the data encapsulation process, which OSI layer adds a header that contains MAC addressing information and a trailer used for error checking?

A. Network
B. Transport
C. Data Link
D. Session

Answer: C

Explanation:

OSI model

During the data encapsulation process, the Data Link layer of the OSI model is responsible for adding a header that contains MAC addressing information and a trailer used for error checking. The header typically includes the source and destination MAC addresses, while the trailer contains a Frame Check Sequence (FCS) which is used for error detection1.
The Data Link layer ensures that messages are delivered to the proper device on a LAN using hardware addresses and translates messages from the Network layer into bits for the Physical layer to transmit. It also controls how data is placed onto the medium and is received from the medium through the physical hardware.
References :=
? The OSI Model – The 7 Layers of Networking Explained in Plain English
? OSI Model - Network Direction
? Which layer adds both header and trailer to the data?
? What is OSI Model | 7 Layers Explained - GeeksforGeeks

NEW QUESTION 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 24
You need to connect a computer's network adapter to a switch using a 1000BASE-T cable. Which connector should you use?

A. Coax
B. RJ-11
C. OS2 LC
D. RJ-45

Answer: D

Explanation:

•1000BASE-T Cable: This refers to Gigabit Ethernet over twisted-pair cables (Cat 5e or higher).
•Connector: RJ-45 connectors are used for Ethernet cables, including those used for 1000BASE-T.
•Coax: Used for cable TV and older Ethernet standards like 10BASE2.
•RJ-11: Used for telephone connections.
•OS2 LC: Used for fiber optic connections. References:
•Ethernet Standards and Cables: Ethernet Cable Guide

NEW QUESTION 29
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
```

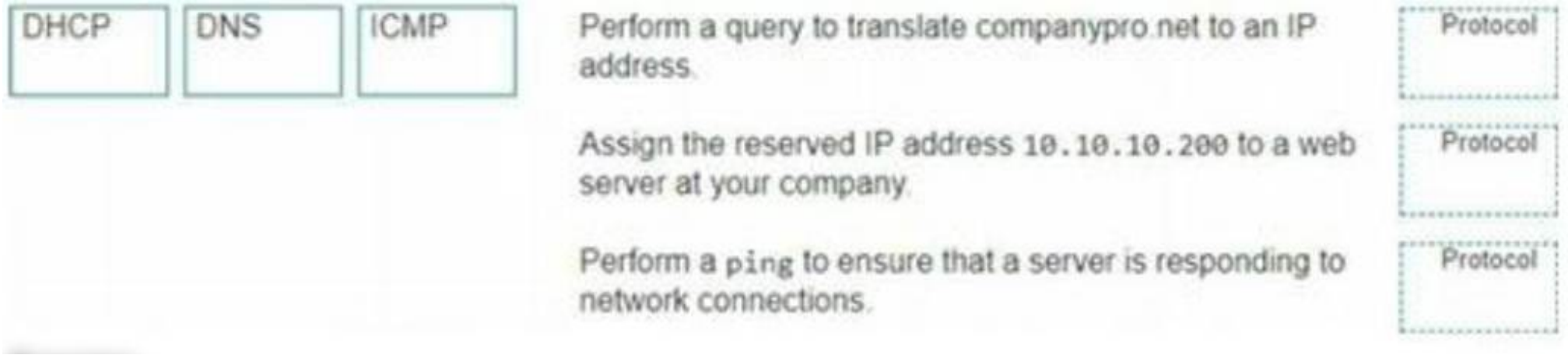
What can you tell from the command output?

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

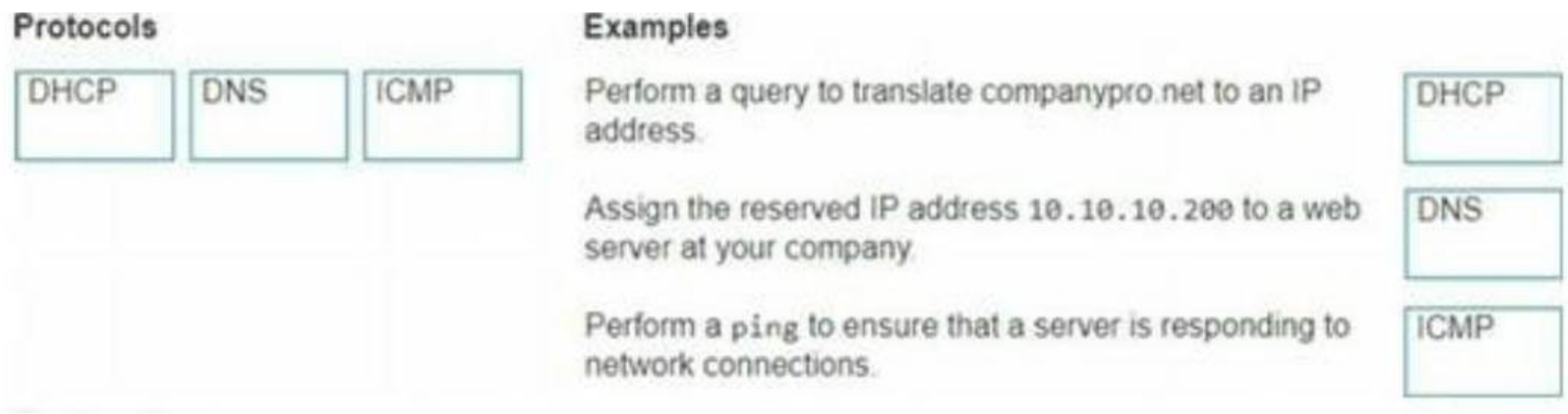
NEW QUESTION 32
DRAG DROP
Move each network type from the list on the left to the correct example on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 34

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 100-150 Exam with Our Prep Materials Via below:

https://www.certleader.com/100-150-dumps.html