Cisco

Exam Questions CCST-Networking

Cisco Certified Support Technician (CCST) NetworkingExam

NEW QUESTION 1
Which command will display all the current operational settings configured on a Cisco router?

A. show protocols
B. show startup-config
C. show version
D. show running-config

Answer: D

Explanation:

Router
Theshow running-configcommand is used on a Cisco router to display the current operational settings that are actively configured in the router??s RAM. This command outputs all the configurations that are currently being executed by the router, which includes interface configurations, routing protocols, access lists, and other settings. Unlikeshow startup-config, which shows the saved configuration that the router will use on the next reboot,show running-configreflects the live, current configuration in use.
References:= The information is supported by multiple sources that detail the use of Cisco commands, particularly theshow running-configcommand as the standard for viewing the active configuration on a Cisco device123.
? show running-config: This command displays the current configuration running on the router. It includes all the operational settings and configurations applied to the router.
? show protocols: This command shows the status of configured protocols on the
router but not the entire configuration.
? show startup-config: This command displays the configuration saved in NVRAM, which is used to initialize the router on startup, but not necessarily the current running configuration.
? show version: This command provides information about the router's software version, hardware components, and uptime but does not display the running configuration.
References:
? Cisco IOS Commands: Cisco IOS Commands

NEW QUESTION 2
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

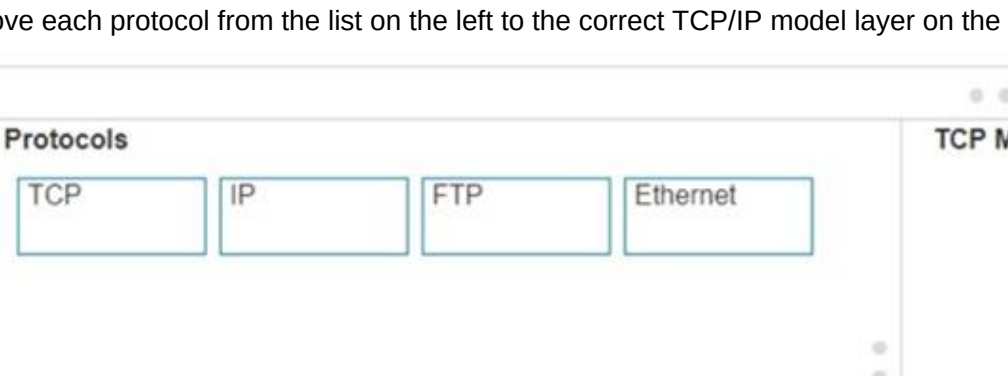
Answer: D

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 3
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:
? 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 4
DRAG DROP
Move each protocol from the list on the left to the correct TCP/IP model layer on the right. Note: You will receive partial credit for each correct match.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Here??s how each protocol aligns with the correct TCP/IP model layer:
? TCP (Transmission Control Protocol): This protocol belongs to 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 5
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

Answer: AD

Explanation:
The private IP address ranges that are set aside specifically for use within private networks and not routable on the internet are as follows:
? Class A: 10.0.0.0 to 10.255.255.255
? Class B: 172.16.0.0 to 172.31.255.255
? Class C: 192.168.0.0 to 192.168.255.255
These ranges are defined by the Internet Assigned Numbers Authority (IANA) and are used
for local communications within a private network123.
Given the options: A.172.16.0.0 to 172.31.255.255falls 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

NEW QUESTION 6
Which address is included in the 192.168.200.0/24 network?

A. 192.168.199.13
B. 192.168.200.13
C. 192.168.201.13
D. 192.168.1.13

Answer: B

Explanation:
•192.168.200.0/24 Network: This subnet includes all addresses from 192.168.200.0 to 192.168.200.255. The /24 indicates a subnet mask of 255.255.255.0, which allows for 256 addresses.
•192.168.199.13: This address is in the 192.168.199.0/24 subnet, not the 192.168.200.0/24 subnet.
•192.168.200.13: This address is within the 192.168.200.0/24 subnet.
•192.168.201.13: This address is in the 192.168.201.0/24 subnet, not the 192.168.200.0/24 subnet.
•192.168.1.13: This address is in the 192.168.1.0/24 subnet, not the 192.168.200.0/24 subnet.
References:
•Subnetting Guide: Subnetting Basics

NEW QUESTION 7
You need to connect a computer's network adapter to a switch using a 1000BASE-T cable. Which connector should you use?

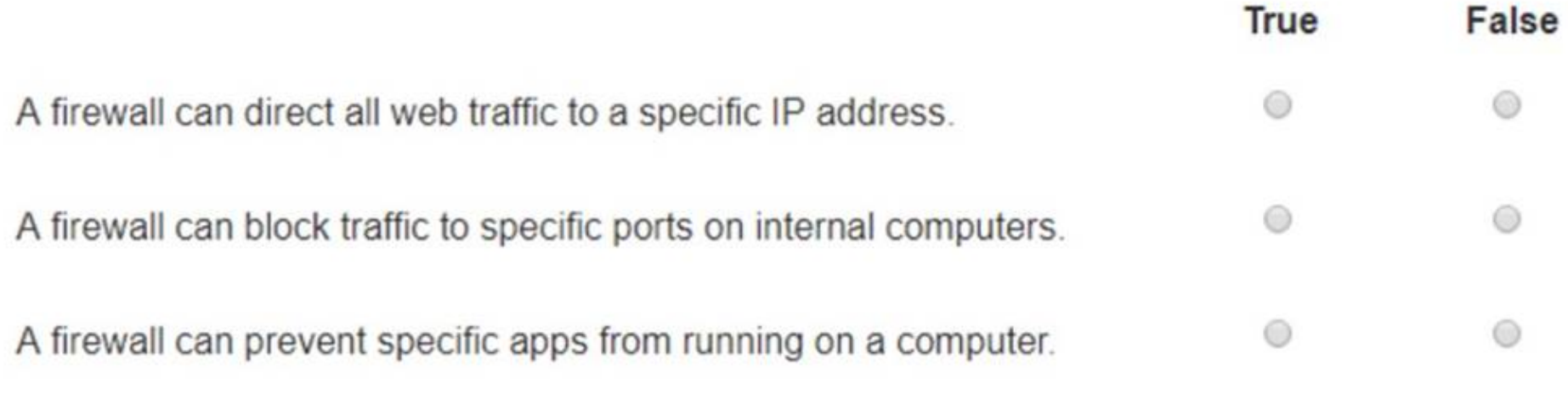
A. Coax
B. RJ-11
C. OS2 LC
D. RJ-45

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 8
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.

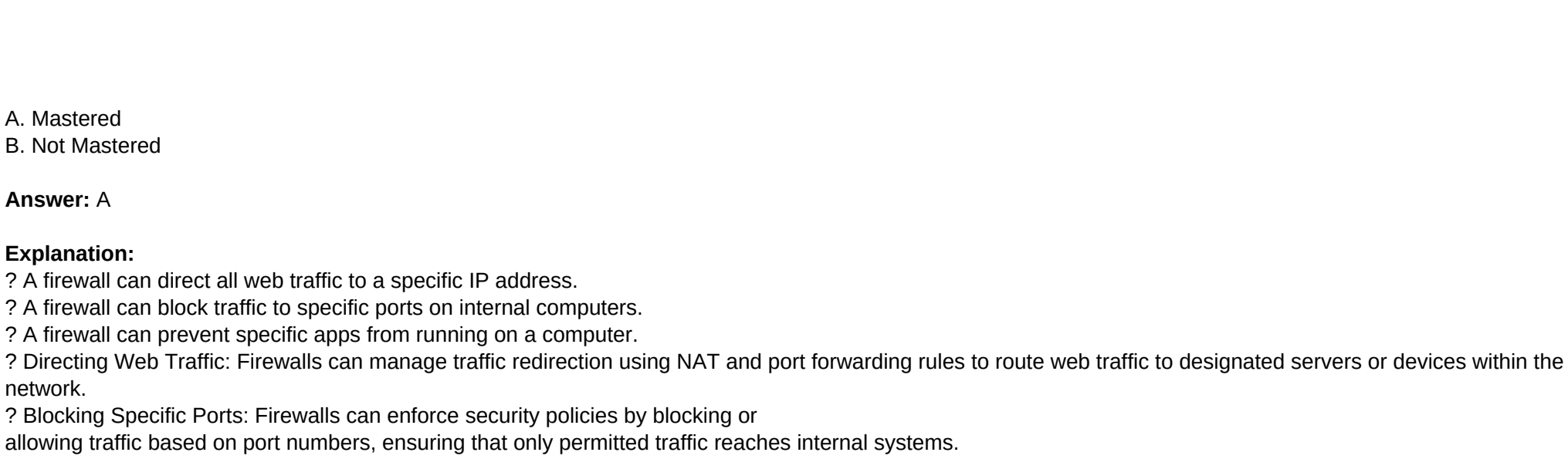


A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 9
DRAG DROP
Move each protocol from the list on the left to its correct example on the right.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The correct matching of the protocols to their examples is as follows:
? DHCP: Assign the reserved IP address 10.10.10.200 to a web server at your company.
? DNS: Perform a query to translate companypro.net to an IP address.
? ICMP: Perform a ping to ensure that a server is responding to network connections.
Here??s how each protocol corresponds to its example:
? DHCP (Dynamic Host Configuration Protocol)is used to assign IP addresses to devices on a network. In this case, DHCP would be used to assign the reserved IP address 10.10.10.200 to a web server.
? DNS (Domain Name System)is used to translate domain names into IP addresses.
Therefore, to translate companypro.net to an IP address, DNS would be utilized.
? ICMP (Internet Control Message Protocol)is used for sending error messages and operational information indicating success or failure when communicating with another IP address. An example of this is using the ping command to check if a server is responding to network connections.
These protocols are essential for the smooth operation of networks and the internet.
? Perform a query to translate companypro.net to an IP address.
? Assign the reserved IP address 10.10.10.200 to a web server at your company.
? Perform a ping to ensure that a server is responding to network connections.
? DNS (Domain Name System): DNS translates human-friendly domain names like "companypro.net" into IP addresses that computers use to identify each other on the network.
? DHCP (Dynamic Host Configuration Protocol): DHCP automatically assigns IP addresses to devices on a network, ensuring that no two devices have the same IP address.
? ICMP (Internet Control Message Protocol): ICMP is used for diagnostic or control purposes, and the ping command uses ICMP to test the reachability of a host on an IP network.
References:
? DNS Basics: What is DNS?
? DHCP Overview: What is DHCP?
? ICMP and Ping: Understanding ICMP

NEW QUESTION 10
Which command will display the following output?

Image is command output that states the following.

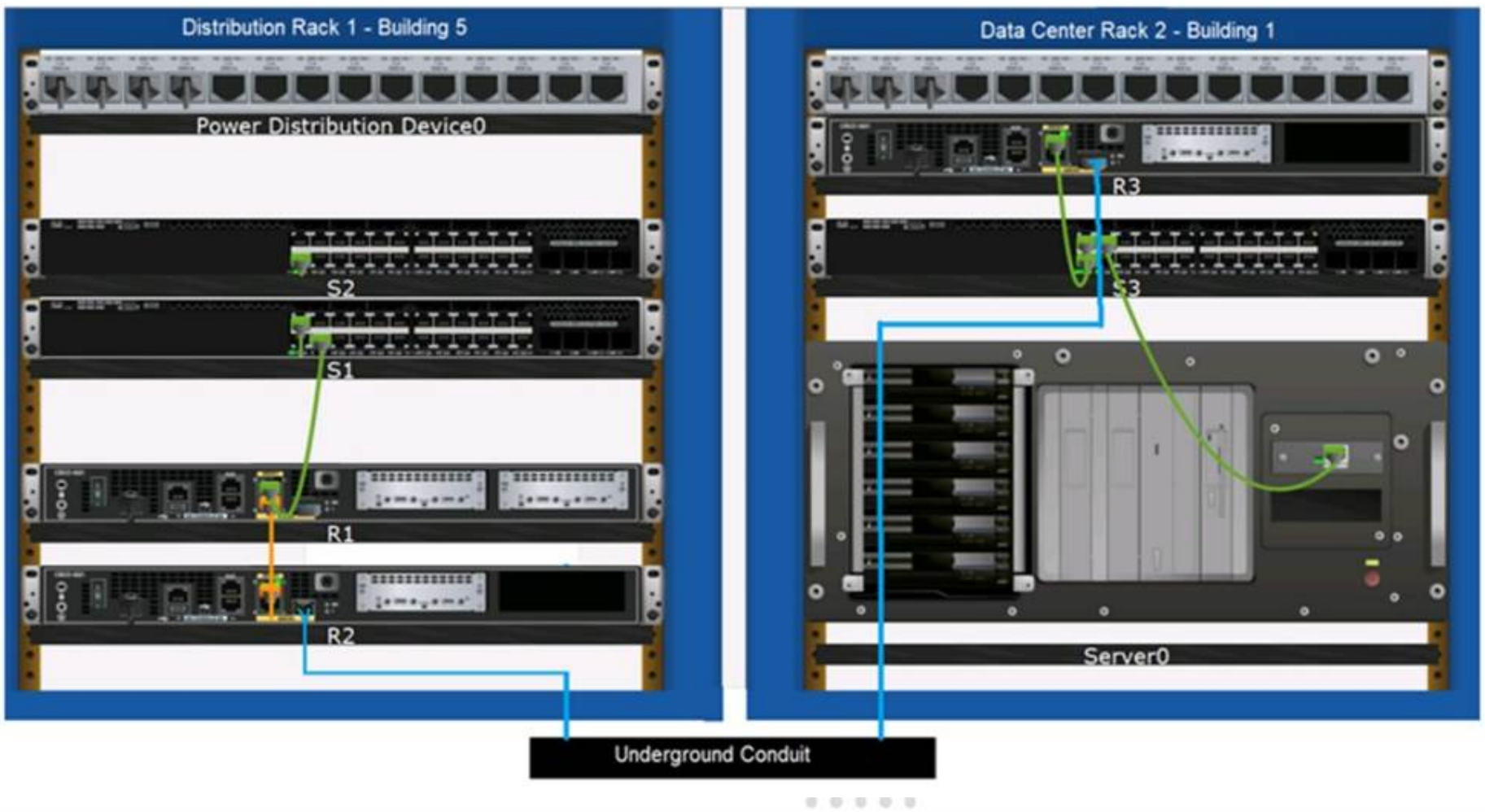
```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
esxi             Gig 0/5           177              S    VMware ES vmnic0
esxi             Gig 0/7           177              S    VMware ES vmnic1
esxi             Gig 0/6           177              S    VMware ES vmnic2
981888fc23a7     Gig 0/47          160            R S    Meraki MR Port 0
3456fecd1d08     Gig 0/1           178              S    MS120-8LP Port 9"
```

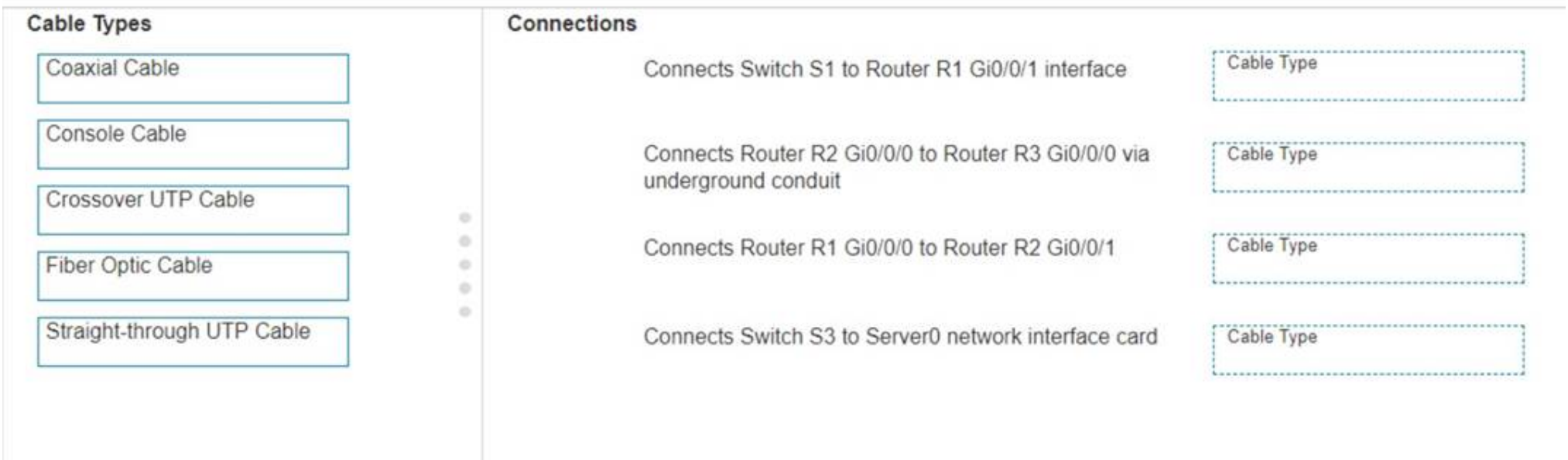
A. show mac-address-table
B. show cdp neighbor
C. show inventory
D. show ip interface

Answer: B

Explanation:
The command that will display the output provided, which includes capability codes, local interface details, device IDs, hold times, and platform port ID capabilities, is the show cdp neighbor command. This command is used in Cisco devices to display current information about neighboring devices detected by Cisco Discovery Protocol (CDP), which includes details such as the interface through which the neighbor is connected, the type of device, and the port ID of the device1.
References :=
•Cisco - show cdp neighbors
The provided output is from the Cisco Discovery Protocol (CDP) neighbor table. The show cdp neighbor command displays information about directly connected Cisco devices, including Device ID, Local Interface, Holdtime, Capability, Platform, and Port ID.
•A. show mac-address-table: Displays the MAC address table on the switch.
•C. show inventory: Displays information about the hardware inventory of the device.
•D. show ip interface: Displays IP interface status and configuration. Thus, the correct answer is B. show cdp neighbor.
References :=
•Cisco CDP Neighbor Command
•Understanding CDP

NEW QUESTION 10
DRAG DROP
Examine the connections shown in the following image. Move the cable types on the right to the appropriate connection description on the left. You may use each cable type more than once or not at all.





A. Mastered
B. Not Mastered

Answer: A

Explanation:
Based on the image description provided, here are the cable types matched with the appropriate connection descriptions:
Connects Switch S1 to Router R1 Gi0/0/1 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 12
Which standard contains the specifications for Wi-Fi networks?

A. GSM
B. LTE
C. IEEE 802.11
D. IEEE 802.3
E. EIA/TIA 568A

Answer: C

Explanation:
The IEEE 802.11 standard contains the specifications for Wi-Fi networks. It is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in various frequencies, including but not limited to 2.4 GHz, 5 GHz, and 6 GHz1. This standard is maintained by the Institute of Electrical and Electronics Engineers (IEEE) and is commonly referred to as Wi-Fi. The standard has evolved over time to include several amendments that improve speed, range, and reliability of wireless networks.
References :=
•The Most Common Wi-Fi Standards and Types, Explained
•802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a
•Wi-Fi Standards Explained - GeeksforGeeks
==========

NEW QUESTION 15
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 18
A help desk technician receives the four trouble tickets listed below. Which ticket should receive the highest priority and be addressed first?

A. Ticket 1: A user requests relocation of a printer to a different network jack in the same offic
B. The jack must be patched and made active.
C. Ticket 2: An online webinar is taking place in the conference roo
D. The video conferencing equipment lost internet access.
E. Ticket 3: A user reports that response time for a cloud-based application is slower than usual.
F. Ticket 4: Two users report that wireless access in the cafeteria has been down for the last hour.

Answer: B

Explanation:
When prioritizing trouble tickets, the most critical issues affecting business operations or high-impact activities should be addressed first. Here's a breakdown of the tickets:
? Ticket 1: Relocation of a printer, while necessary, is not urgent and does not

impact critical operations.
? Ticket 2: An ongoing webinar losing internet access is critical, especially if the webinar is time-sensitive and involves multiple participants.
? Ticket 3: Slower response time for a cloud-based application is important but typically not as urgent as a complete loss of internet access for a live event.
? Ticket 4: Wireless access down in the cafeteria affects users but does not have the same immediate impact as a live webinar losing connectivity.
Thus, the correct answer is B. Ticket 2: An online webinar is taking place in the conference
room. The video conferencing equipment lost internet access.
References:=
? IT Help Desk Best Practices
? Prioritizing IT Support Tickets

NEW QUESTION 21
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 aserver. 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 26
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 27
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

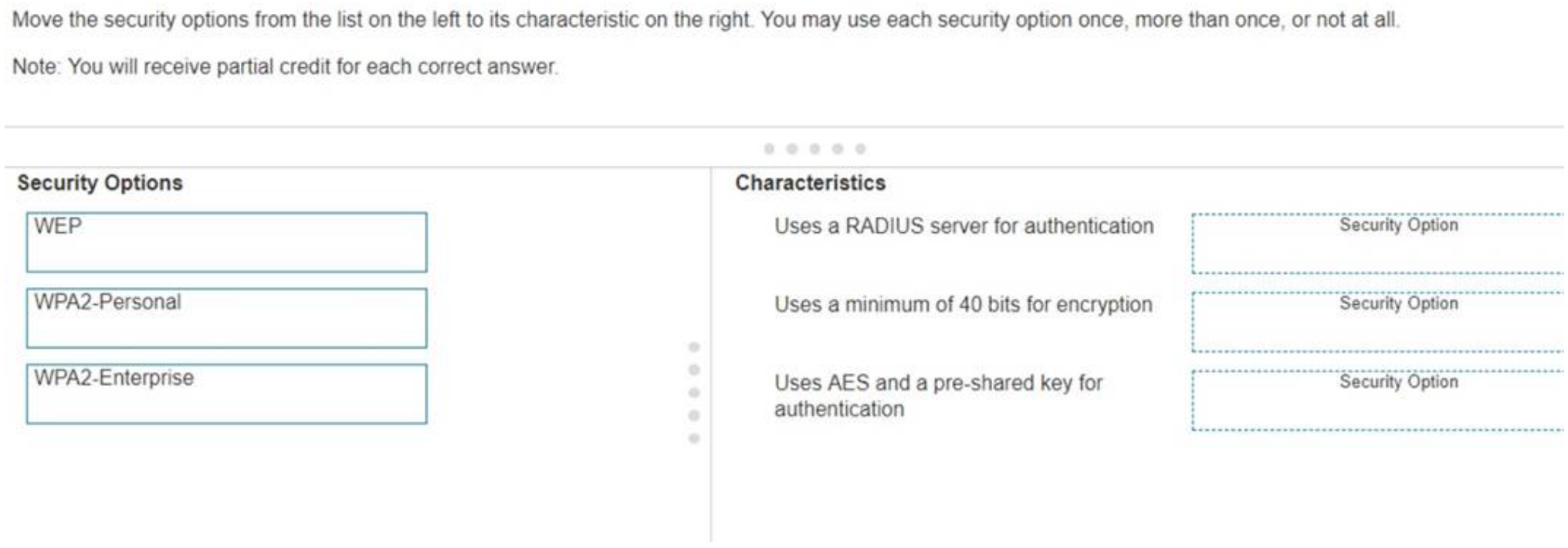
NEW QUESTION 31
Which wireless security option uses a pre-shared key to authenticate clients?

A. WPA2-Personal
B. 802.1x
C. 802.1q
D. WPA2-Enterprise

Answer: A

Explanation:
WPA2-Personal, also known as WPA2-PSK (Pre-Shared Key), is the wireless security option that uses a pre-shared key to authenticate clients. This method is designed for home and small office networks and doesn??t require an authentication server. Instead, every user on the network uses the same key or passphrase to connect1.
References :=
•What is a Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)?
•Exploring WPA-PSK and WiFi Security
==========
•WPA2-Personal: This wireless security option uses a pre-shared key (PSK) for authentication. Each client that connects to the network must use this key to gain access. It is designed for home and small office networks where simplicity and ease of use are important.
•WPA2-Enterprise: Unlike WPA2-Personal, WPA2-Enterprise uses 802.1x authentication with an authentication server (such as RADIUS) and does not rely on a pre-shared key.
•802.1x: This is a network access control protocol for LANs, particularly wireless LANs. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
•802.1q: This is a networking standard that supports VLAN tagging on Ethernet networks and is not related to wireless security.
References:
•Cisco Documentation on WPA2 Security: Cisco WPA2
•Understanding Wireless Security: Wireless Security Guide

NEW QUESTION 34
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-Enterpriseuses 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 39

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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 FirstTry

* CCST-Networking Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year