



Cisco

Exam Questions 100-150

Cisco Certified Support Technician (CCST) Networking

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

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.

Answer: BD

Explanation:

- 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.

References:

- Cisco Default Gateway Configuration: Cisco Default Gateway

NEW QUESTION 2

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 3

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

The show running-config command 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. Unlike show startup-config, which shows the saved configuration that the router will use on the next reboot, show running-config reflects the live, current configuration in use.

References := The information is supported by multiple sources that detail the use of Cisco commands, particularly the show running-config command 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 4

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 5

A local company requires two networks in two new buildings. The addresses used in these networks must 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 172.31.255.255 falls within the Class B private range.

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

A and D. References :=

? Reserved IP addresses on Wikipedia

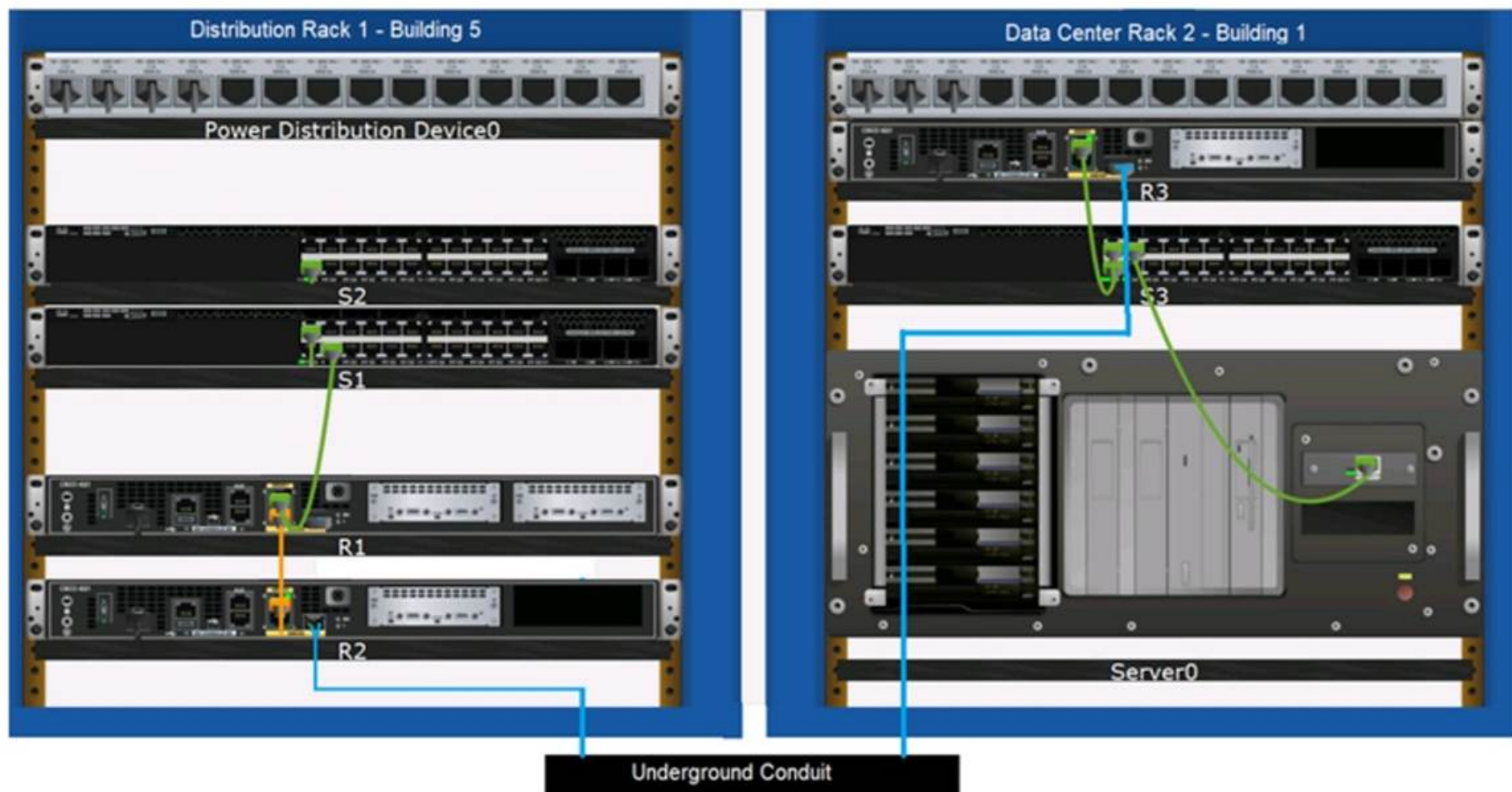
? Private IP Addresses in Networking - GeeksforGeeks

? Understanding Private IP Ranges, Uses, Benefits, and Warnings

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

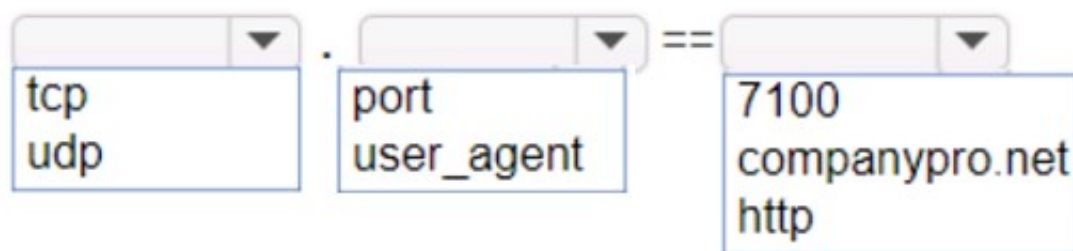
NEW QUESTION 7

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.



The diagram illustrates the Wireshark filter syntax: [Protocol] [Filter Type] == [Value]. The first dropdown menu contains 'tcp' and 'udp'. The second dropdown menu contains 'port' and 'user_agent'. The third dropdown menu contains '7100', 'companypro.net', and 'http'.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To capture packets sent to and received from the URL <https://www.companypro.net:7100/api> using Wireshark, you would use the following filter options:

? Protocol: tcp

? Filter Type: port

? Port Number: 7100

This filter setup in Wireshark will display all TCP packets that are sent to or received from port 7100, which is the port specified in the URL for the API service. Since HTTPS typically uses TCP as the transport layer protocol, filtering by TCP and the specific port number will help isolate the relevant packets for troubleshooting the app's data download issues.

? cp: The app is using HTTPS, which relies on the TCP protocol for communication.

? port: The specific port number used by the application, which in this case is 7100.

? 7100: This is the port specified in the URL (<https://www.companypro.net:7100/api>). This filter will capture all TCP traffic on port 7100, allowing you to analyze the packets related to the application's data download.

References:

? Wireshark Filters: Wireshark Display Filters

NEW QUESTION 8

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 9

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.

	True	False
A firewall can direct all web traffic to a specific IP address.	<input type="radio"/>	<input type="radio"/>
A firewall can block traffic to specific ports on internal computers.	<input type="radio"/>	<input type="radio"/>
A firewall can prevent specific apps from running on a computer.	<input type="radio"/>	<input type="radio"/>

- 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.

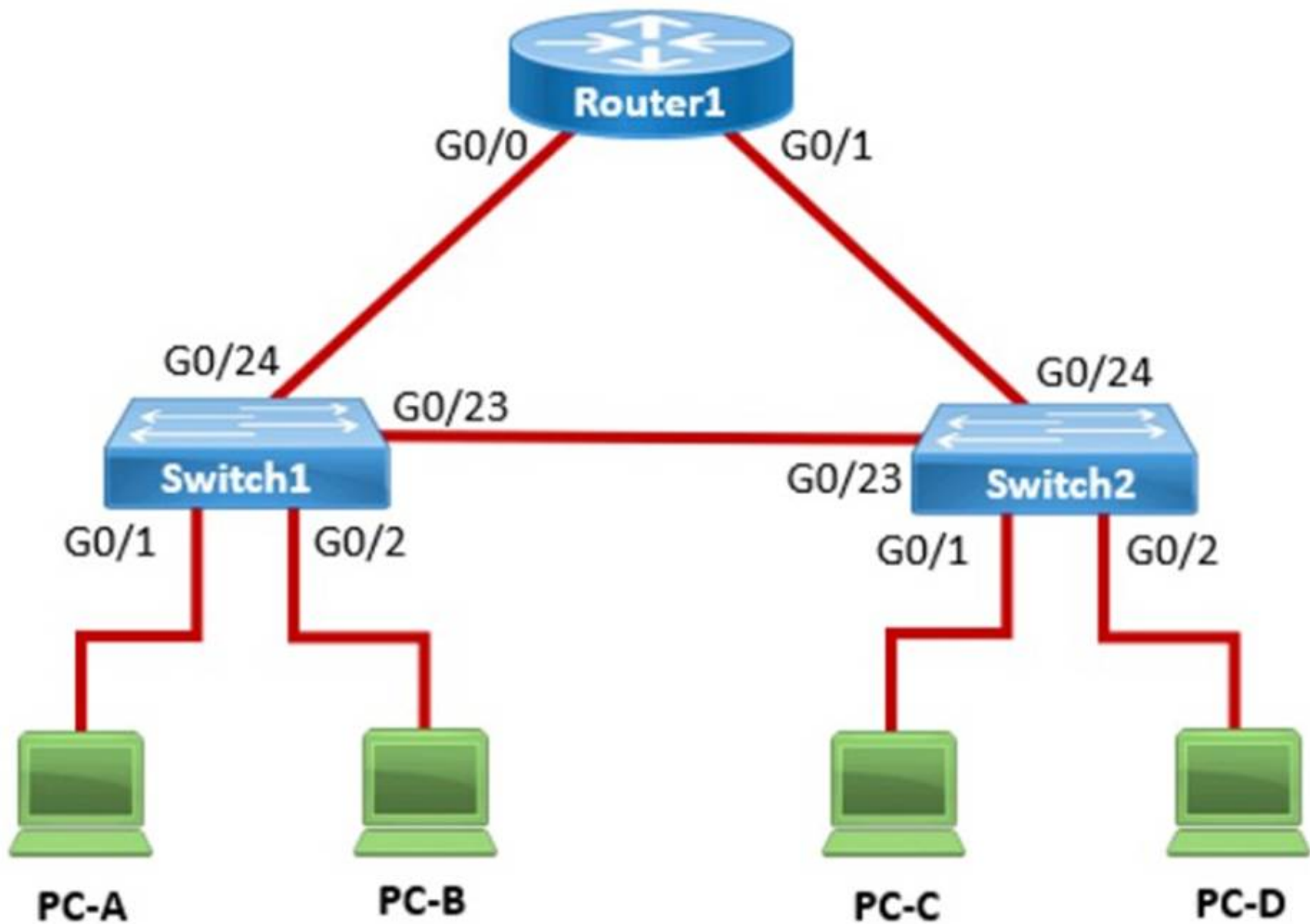
? Application Control: While firewalls manage network traffic, preventing applications from running typically requires software specifically designed for endpoint protection and application management.

References:

? Understanding Firewalls: Firewall Capabilities

NEW QUESTION 10

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: C

Explanation:

Understanding How Layer 2 Switches Handle Unknown MAC Addresses Switches operate at Layer 2 (Data Link Layer) of the OSI model and maintain a MAC address table (CAM table) to forward frames efficiently.

? When a switch receives a frame, it checks its MAC address table to see if it knows the destination MAC address.

? If the destination MAC address is not in the table (meaning the switch does not know which port leads to PC-C), the switch follows the flooding behavior.

What Happens When Switch1 Receives a Frame from PC-A to PC-C?

? Switch1 checks its MAC table:

? Switch1 does not know where PC-C is:

? Switch2 receives the frame and follows the same process:

? Once PC-C responds, Switch1 and Switch2 learn its MAC address and update their tables.

Why Other Options Are Incorrect:

* A. Switch1 queries Switch2 for the MAC address of PC-C.

? Incorrect: Switches do not query other switches directly for MAC addresses.

Instead, they rely on learning MAC addresses dynamically through frame forwarding.

* B. Switch1 drops the frame and sends an error message back to PC-A.

? Incorrect: Switches do not drop frames for unknown MAC addresses. Instead, they flood the frames out all ports except the incoming port.

* D. Switch1 sends an ARP request to obtain the MAC address of PC-C.

? Incorrect:

Conclusion

Since Switch1 does not know the destination MAC address, it floods the frame out all active ports except the port it was received on. This is the default behavior of Layer 2 switches when they encounter an unknown MAC address.

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

References

? Cisco CCNA 200-301 Official Guide – MAC Address Table & Frame Forwarding

? RFC 894 – Standard for Ethernet Frame Forwarding

? Cisco Networking Essentials – Switch Flooding Behavior

NEW QUESTION 10

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

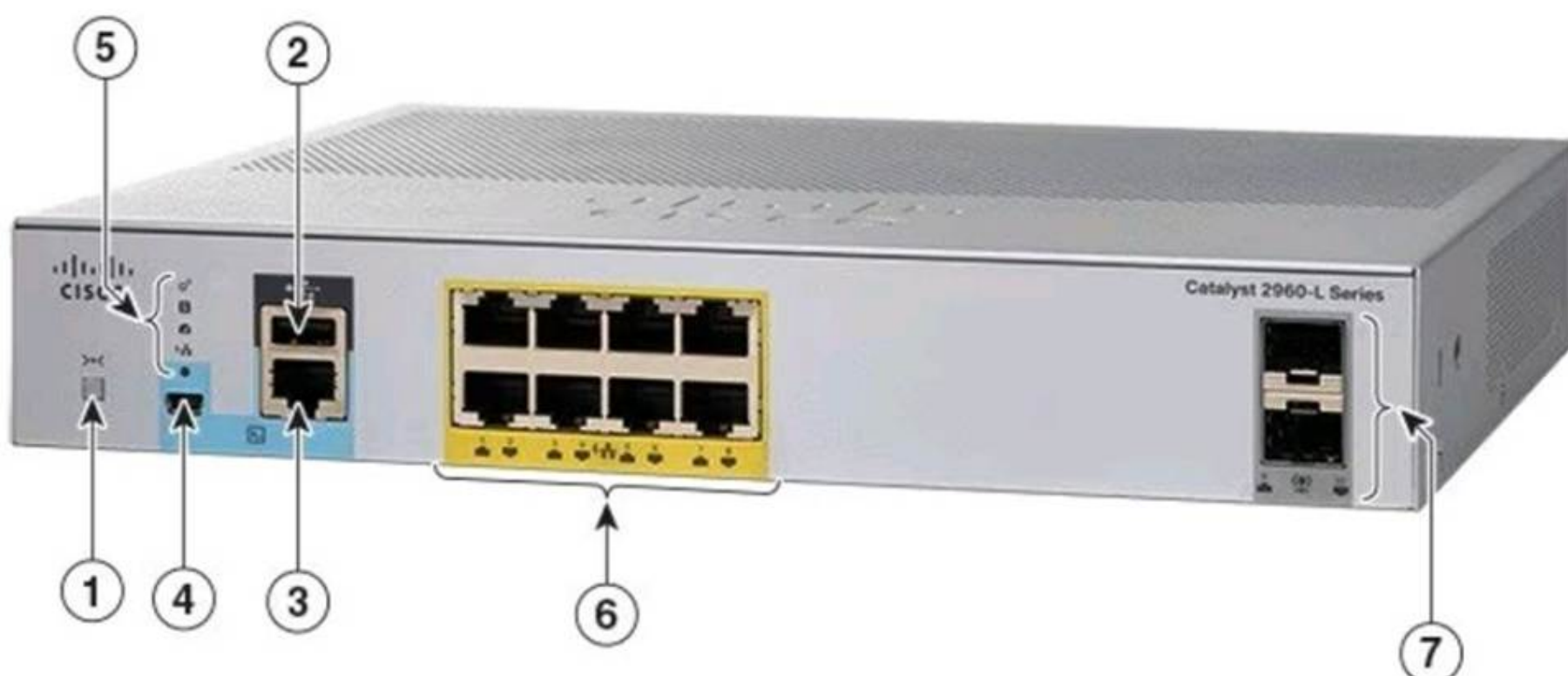
•Count the number of consecutive 1s in the binary form: There are 22 ones.

•Therefore, the CIDR notation is /22. References:

•Understanding Subnetting and CIDR: Cisco CIDR Guide

NEW QUESTION 14

A Cisco PoE switch is shown in the following image. Which type of port will provide both data connectivity and power to an IP phone?



- A. Port identified with number 2
- B. Ports identified with numbers 3 and 4
- C. Ports identified with number 6
- D. Ports identified with number 7

Answer: C

Explanation:

In the provided image of the Cisco PoE switch, the ports identified with number 6 are the standard RJ-45 Ethernet ports typically found on switches that provide both data connectivity and Power over Ethernet (PoE). PoE ports are designed to supply power to devices such as IP phones, wireless access points, and other PoE-enabled devices directly through the Ethernet cable.

- Ports:
- 2: Console port (for management and configuration)
 - 3 and 4: Specific function ports (often for management)
 - 6: RJ-45 Ethernet ports (capable of providing PoE)
 - 7: SFP ports (for fiber connections, typically do not provide PoE) Thus, the correct answer is C. Ports identified with number 6. References :=
 - Cisco Catalyst 2960-L Series Switches Data Sheet
 - Cisco PoE Overview

NEW QUESTION 15

HOTSPOT

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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- ? The two interfaces are administratively shut down:
 - ? The two interfaces have default IP addresses assigned:
 - ? The two interfaces can communicate over Layer 2:
 - ? Interface Status: The absence of the "shutdown" command means the interfaces are not administratively shut down.
 - ? IP Address Assignment: There is no evidence in the output that IP addresses have been assigned to the interfaces, which would typically be shown as "ip address" entries.
 - ? Layer 2 Communication: Switch interfaces in their default state operate at Layer 2, enabling them to forward Ethernet frames and participate in Layer 2 communication.
- References:
- ? Cisco IOS Interface Configuration: Cisco Interface Configuration
 - ? Understanding Cisco Switch Interfaces: Cisco Switch Interfaces

NEW QUESTION 16

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 17

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 connect.

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 18

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 22

A user reports that a company website is not available. The help desk technician issues a tracert command to determine if the server hosting the website is reachable over the network. The output of the command is shown as follows:

```
C:\>tracert 192.168.1.10
Tracing route to 192.168.1.10 over a maximum of 30 hops:
 0  ms  0  ms  1  ms  192.168.5.1
 1  ms  0  ms  0  ms  10.0.1.1
 3 *      *      *      Request timed out.
 4  ms  1  ms  0  ms  10.0.0.2
 5  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 reachable.

12. References :=

- How to Use Traceroute Command to Read Its Results
- How to Use the Tracert Command in Windows

NEW QUESTION 24

.....

Relate Links

100% Pass Your 100-150 Exam with Exambible Prep Materials

<https://www.exambible.com/100-150-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/>