



**Cisco**

## **Exam Questions CCST-Networking**

Cisco Certified Support Technician (CCST) NetworkingExam

### NEW QUESTION 1

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 detection.

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 2

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.

tcp udp	.	port user_agent	==	7100 companypro.net 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 3

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 172.31.255.255falls 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 4

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.

	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  
? Network Security Best Practices: Network Security Guide

NEW QUESTION 5

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 6

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
3456fec1d08	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 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.

**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.

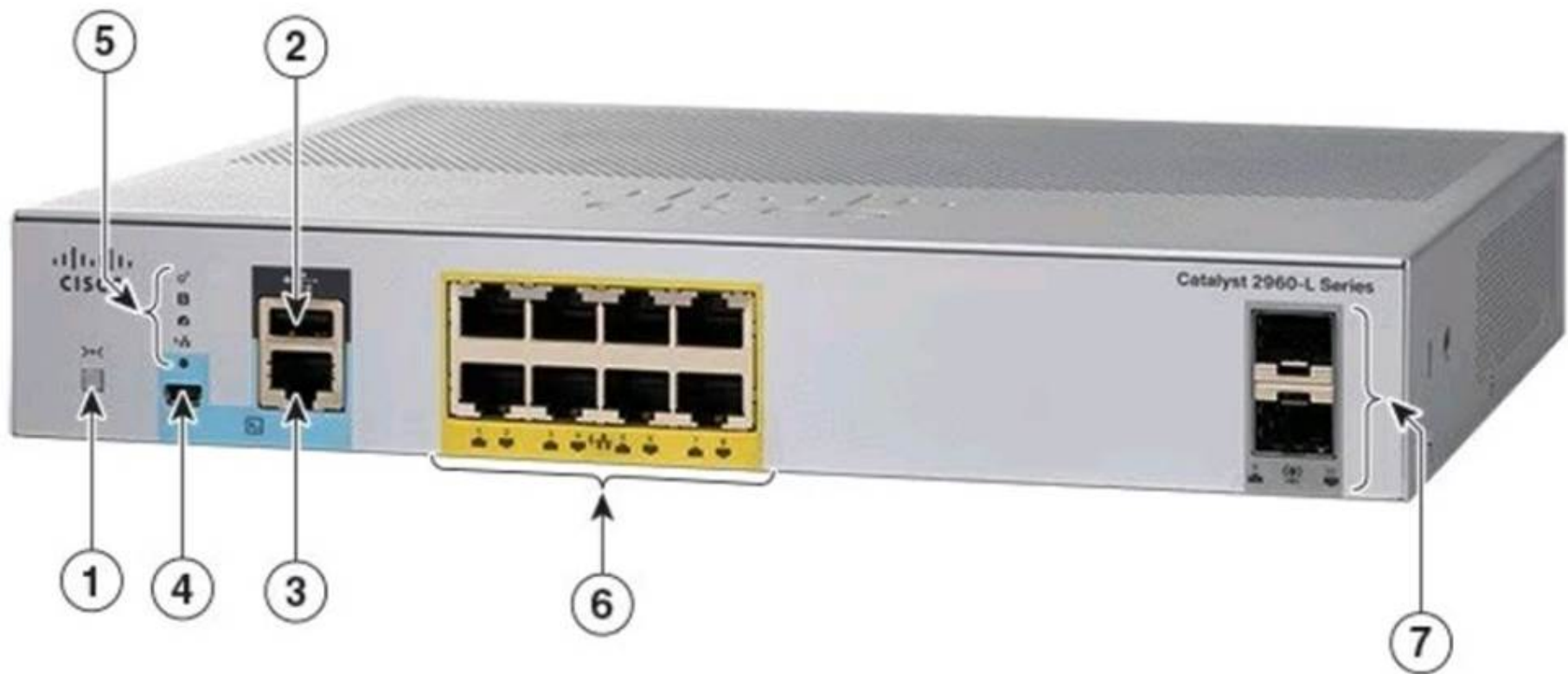
References:

- Cisco Default Gateway Configuration: Cisco Default Gateway

#### NEW QUESTION 8

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 9**

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

**Answer:** B

**Explanation:**



#### 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 the console 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 network.

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!

#### NEW QUESTION 10

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 devices.

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 10

Which device protects the network by permitting or denying traffic based on IP address, port number, or application?

- A. Firewall
- B. Access point
- C. VPN gateway
- D. Intrusion detection system

**Answer: A**

#### Explanation:

? Firewall: A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It permits or denies traffic based on IP addresses, port numbers, or applications.

? Access Point: This is a device that allows wireless devices to connect to a wired network using Wi-Fi. It does not perform traffic filtering based on IP, port, or application.

? VPN Gateway: This device allows for secure connections between networks over the internet, but it is not primarily used for traffic filtering based on IP, port, or application.

? Intrusion Detection System (IDS): This device monitors network traffic for suspicious activity and policy violations, but it does not actively permit or deny traffic.

References:

? Understanding Firewalls: Firewall Basics

## NEW QUESTION 15

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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 First Try
- \* CCST-Networking Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CCST-Networking Practice Test Here](#)**