

# Cisco

## Exam Questions 100-150

Cisco Certified Support Technician (CCST) Networking



### NEW QUESTION 1

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<sup>1</sup>.

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 2

A user initiates a trouble ticket stating that an external web page is not loading. You determine that other resources both internal and external are still reachable. Which command can you use to help locate where the issue is in the network path to the external web page?

- A. ping -t
- B. tracert
- C. ipconfig/all
- D. nslookup

**Answer: B**

#### Explanation:

The tracert command is used to determine the route taken by packets across an IP network. When a user reports that an external web page is not loading, while other resources are accessible, it suggests there might be an issue at a certain point in the network path to the specific web page. The tracert command helps to diagnose where the breakdown occurs by displaying a list of routers that the packets pass through on their way to the destination. It can identify the network segment where the packets stop progressing, which is valuable for pinpointing where the connectivity issue lies. References := Cisco CCST Networking Certification FAQs – CISCONET Training Solutions, Command Prompt (CMD): 10 network-related commands you should know, Network Troubleshooting Commands Guide: Windows, Mac & Linux - Comparitech, How to Use the Traceroute and Ping Commands to Troubleshoot Network, Network Troubleshooting Techniques: Ping, Traceroute, PathPing.

•tracert Command: This command is used to determine the path packets take to reach a destination. It lists all the hops (routers) along the way and can help identify where the delay or failure occurs.

•ping -t: This command sends continuous ping requests and is useful for determining if a host is reachable but does not provide path information.

•ipconfig /all: This command displays all current TCP/IP network configuration values and can be used to verify network settings but not to trace a network path.

•nslookup: This command queries the DNS to obtain domain name or IP address mapping, useful for DNS issues but not for tracing network paths. References:

•Microsoft tracert Command: tracert Command Guide

•Troubleshooting Network Issues with tracert: Network Troubleshooting Guide

### NEW QUESTION 3

An engineer configured a new VLAN named VLAN2 for the Data Center team. When the team tries to ping addresses outside VLAN2 from a computer in VLAN2, they are unable to reach them. What should the engineer configure?

- A. Additional VLAN
- B. Default route
- C. Default gateway
- D. Static route

**Answer: C**

#### Explanation:

When devices within a VLAN are unable to reach addresses outside their VLAN, it typically indicates that they do not have a configured path to external networks. The engineer should configure a default gateway for VLAN2. The default gateway is the IP address of the router's interface that is connected to the VLAN, which will route traffic from the VLAN to other networks<sup>12</sup>.

References :=

•Understanding and Configuring VLAN Routing and Bridging on a Router Using the IRB Feature

•VLAN 2 not able to ping gateway - Cisco Community

=====

•VLANs: Virtual Local Area Networks (VLANs) logically segment network traffic to improve security and performance. Devices within the same VLAN can communicate directly.

•Default Gateway: For devices in VLAN2 to communicate with devices outside their VLAN, they need a default gateway configured. The default gateway is typically a router or Layer 3 switch that routes traffic between different VLANs and subnets.

- Additional VLAN: Not needed in this scenario as the issue is related to routing traffic outside VLAN2, not creating another VLAN.
  - Default Route: While a default route on the router may be necessary, the primary issue for devices within VLAN2 is to have a configured default gateway.
  - Static Route: This is used on routers to manually specify routes to specific networks but does not address the need for a default gateway on the client devices.
- References:
- Cisco VLAN Configuration Guide: Cisco VLAN Configuration
  - Understanding and Configuring VLANs: VLANs Guide

#### 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 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.

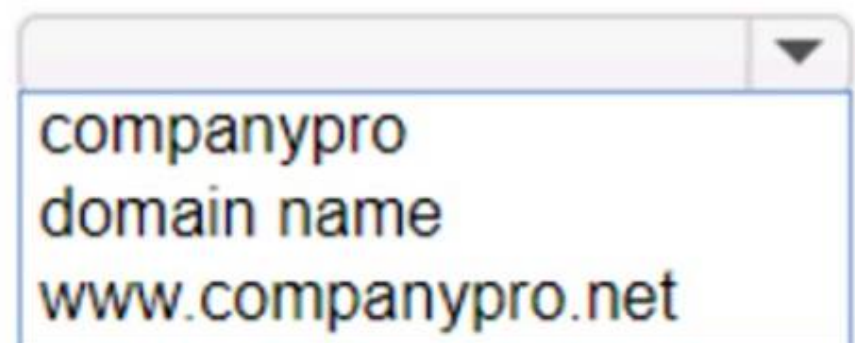
References :=

- ? IT Help Desk Best Practices
- ? Prioritizing IT Support Tickets

#### NEW QUESTION 6

##### HOTSPOT

You want to list the IPv4 addresses associated with the host name `www.companypro.net`.



- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

To list the IPv4 addresses associated with the host name `www.companypro.net`, you should use the following command:  
`nslookup www.companypro.net`  
This command will query the DNS servers to find the IP address associated with the hostname provided. If you want to ensure that it returns the IPv4 address, you can specify the `-type=A` option, which stands for Address records that hold IPv4 addresses<sup>1</sup>. However, the `nslookup` command by default should return the IPv4 address if available.  
To list the IPv4 addresses associated with the host name `www.companypro.net`, you should use the `nslookup` command.  
? Command: `nslookup`  
? Target: `www.companypro.net` So, the completed command is:  
? `nslookup www.companypro.net`  
? `nslookup`: This command is used to query the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.  
? `www.companypro.net`: This is the domain name you want to query to obtain its associated IP addresses. References:  
? Using `nslookup`: `nslookup` Command Guide

**NEW QUESTION 7**  
For each statement about bandwidth and throughput, select True or False.  
Note: You will receive partial credit for each correct selection.

For each statement about bandwidth and throughput, select **True** or **False**.

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

Answer Area		True	False
Low bandwidth can increase network latency.		<input type="radio"/>	<input type="radio"/>
High levels of network latency decrease network bandwidth.		<input type="radio"/>	<input type="radio"/>
You can increase throughput by decreasing network latency.		<input type="radio"/>	<input type="radio"/>

- 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 8**  
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

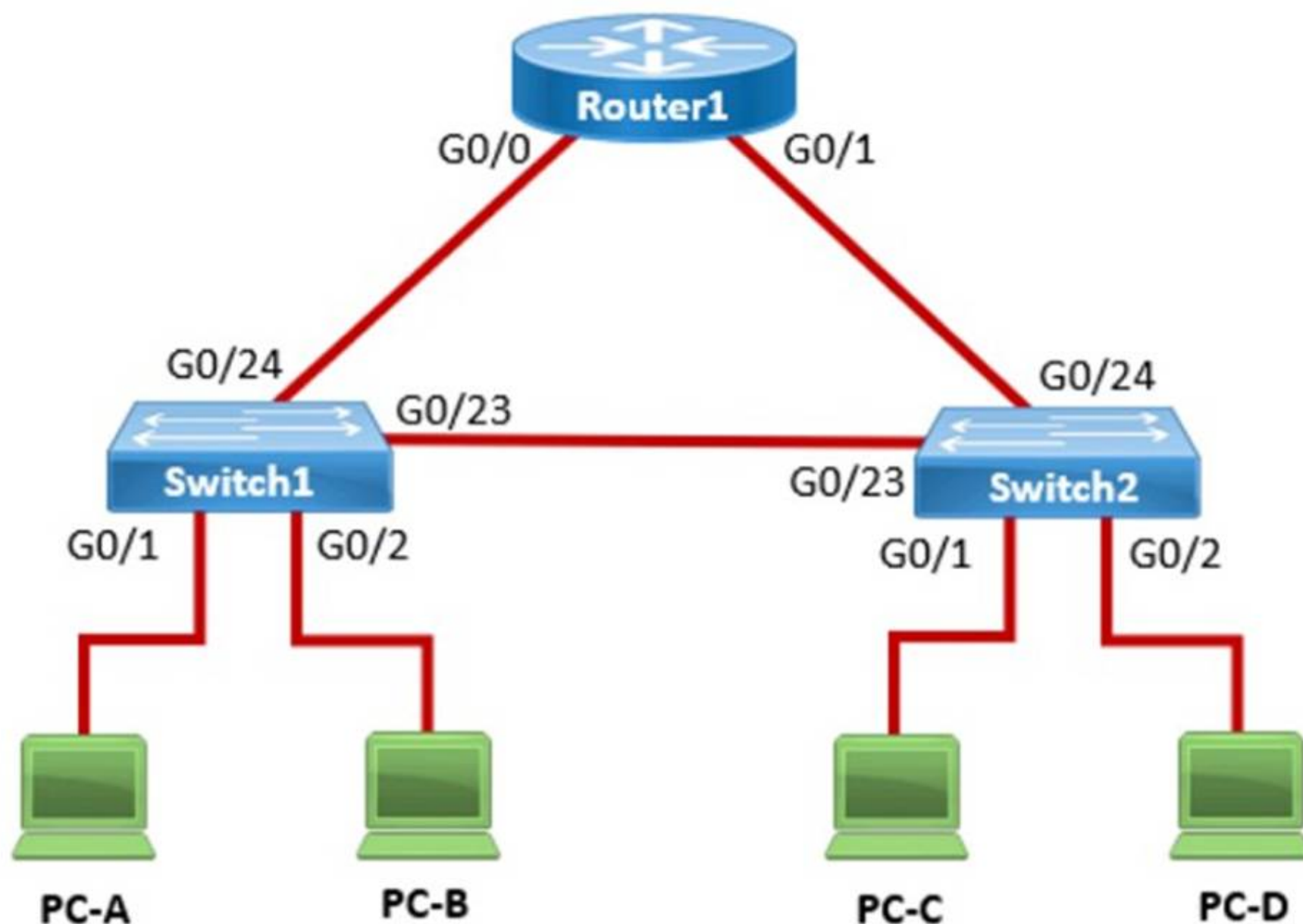
**Answer:** A

**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 9**

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 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  
=====

**NEW QUESTION 10**  
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.

netstat  
ping  
ftp  
nslookup

companypro.net  
192.168.0.1  
localhost  
8.8.8.8

- 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

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.

Protocols

TCPIPFTP Ethernet

TCP Model Layer

Application

Transport

Internetwork

Network

Protocol

Protocol

Protocol

Protocol



- 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 the Transport layer, which is responsible for providing communication between applications on different hosts<sup>1</sup>.

? IP (Internet Protocol): IP is part of the Internet layer, which is tasked with routing packets across network boundaries to their destination<sup>1</sup>.

? FTP (File Transfer Protocol): FTP operates at the Application layer, which supports application and end-user processes. It is used for transferring files over the network<sup>1</sup>.

? Ethernet: While not a protocol within the TCP/IP stack, Ethernet is associated with the Network Interface layer, which corresponds to the link layer of the TCP/IP model and is responsible for the physical transmission of data<sup>1</sup>.

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 process<sup>1</sup>.

? 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.

? Internet 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 18**

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**

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 GHz<sup>1</sup>. 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 21**

.....



## 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

### 100-150 Practice Exam Features:

- \* 100-150 Questions and Answers Updated Frequently
- \* 100-150 Practice Questions Verified by Expert Senior Certified Staff
- \* 100-150 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* 100-150 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 100-150 Practice Test Here](#)**