CCST Cisco IT Exam Prep

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Unlock the full bank of 1500 questions
+ unlimited timed mock exams + mistake book

Practice on the web: https://certs.theorypractice.app/ccst
$2.99 / week · $6.99 / month · cancel anytime

What you unlock: all 1500 questions • unlimited timed mock exams • mistake book • instant explanations

Also on iOS & Android — and watch the full Q&A walkthrough on YouTube @CertsQuizPrep

Practice Questions

Try all 30 first, then check the answer key at the back.

1. What is the primary difference between TCP and UDP?

A. TCP is faster than UDP
B. UDP provides guaranteed delivery while TCP does not
C. TCP operates at Layer 2 while UDP operates at Layer 4
D. TCP is connection-oriented while UDP is connectionless

2. Which protocol would be most appropriate for time-sensitive applications like video streaming or online gaming?

A. HTTP
B. ICMP
C. UDP
D. TCP

3. What is the default port number for HTTPS?

A. 25
B. 443
C. 80
D. 21

4. Which protocol is used to automatically assign IP addresses to devices on a network?

A. DHCP
B. DNS
C. ICMP
D. NTP

5. What is the primary purpose of DNS?

A. To assign IP addresses to network devices
B. To synchronize time across network devices
C. To secure web traffic with encryption
D. To translate domain names to IP addresses

6. Which protocol would you use to securely transfer files while maintaining SSH authentication and encryption?

A. TFTP
B. HTTP
C. SFTP
D. FTP

7. What network protocol is primarily used for troubleshooting and is the foundation of the ping command?

A. FTP
B. ICMP
C. NTP
D. DHCP

8. Which of the following protocols offers the LEAST security for file transfers?

A. FTP
B. SFTP
C. HTTPS
D. SCP

9. What is the primary purpose of NTP?

A. To transfer files between systems
B. To resolve domain names to IP addresses
C. To monitor network performance
D. To synchronize time across network devices

10. Which protocol is typically used for simple network management tasks in resource-constrained environments like embedded devices or network bootstrapping?

A. SCP
B. FTPS
C. TFTP
D. SFTP

11. What is a key security improvement that HTTPS provides over HTTP?

A. IP address assignment
B. Data encryption
C. Faster data transmission
D. Automatic error correction

12. Which transport layer protocol does DNS primarily use?

A. UDP
B. TCP
C. ICMP
D. HTTP

13. What is the default port number for standard FTP?

A. 20
B. 22
C. 23
D. 21

14. When a DHCP client first joins a network, what is the first message it sends?

A. DHCP OFFER
B. DHCP ACKNOWLEDGE
C. DHCP DISCOVER
D. DHCP REQUEST

15. Which of the following is a key characteristic of connection-oriented protocols like TCP?

A. They cannot retransmit lost packets
B. They require acknowledgment of received packets
C. They prioritize speed over reliability
D. They do not verify data integrity

16. What protocol would typically be used by a web browser when a user enters 'http://example.com' in the address bar?

A. HTTP on port 80
B. HTTPS on port 443
C. FTP on port 21
D. SMTP on port 25

17. Which protocol is used to report errors and test connectivity in IP networks?

A. TCP
B. UDP
C. HTTP
D. ICMP

18. What happens during the TCP three-way handshake?

A. REQUEST, OFFER, ACKNOWLEDGE packet exchange
B. HELLO, RESPONSE, CONFIRM packet exchange
C. SYN, SYN-ACK, ACK packet exchange
D. DATA, ACK, FIN packet exchange

19. What is a key advantage of UDP over TCP for certain applications?

A. Automatic error correction
B. Lower latency
C. Guaranteed delivery
D. Built-in encryption

20. Which protocol would be used to access a secure website?

A. HTTPS
B. HTTP
C. FTP
D. SFTP

21. Which layer of the OSI model is responsible for logical addressing and routing?

A. Physical Layer (Layer 1)
B. Data Link Layer (Layer 2)
C. Transport Layer (Layer 4)
D. Network Layer (Layer 3)

22. In the TCP/IP model, which layer corresponds to the Network layer in the OSI model?

A. Transport Layer
B. Application Layer
C. Internet Layer
D. Network Access Layer

23. What is the primary difference between a frame and a packet in networking?

A. Frames are larger than packets because they include more overhead
B. A frame operates at Layer 2 with MAC addresses, while a packet operates at Layer 3 with IP addresses
C. Frames are used in wireless networks while packets are used in wired networks
D. Packets contain user data while frames only contain control information

24. What occurs during the encapsulation process in networking?

A. Headers are added to data as it travels down the protocol stack
B. Data is compressed to save bandwidth
C. Checksums are verified to ensure data integrity
D. Data is encrypted for secure transmission

25. Which of the following correctly lists the layers of the TCP/IP model from highest to lowest?

A. Application, Internet, Transport, Network Access
B. Application, Session, Transport, Internet, Network Access
C. Application, Transport, Network, Data Link, Physical
D. Application, Transport, Internet, Network Access

26. What is the primary function of the Data Link layer in the OSI model?

A. Converting bits into signals for transmission across the physical media
B. End-to-end data delivery and flow control
C. Node-to-node data delivery and media access control
D. Logical addressing and determining the best path for data delivery

27. Which addressing method uses 48-bit addresses and operates at the Data Link layer?

A. Socket addressing
B. MAC addressing
C. IP addressing
D. Port addressing

28. What is the purpose of the ARP protocol in networking?

A. To map IP addresses to MAC addresses
B. To assign IP addresses dynamically to network devices
C. To resolve domain names to IP addresses
D. To route packets between different networks

29. Which of the following address types is used to send data to all devices on a local network?

A. Unicast address
B. Multicast address
C. Anycast address
D. Broadcast address

30. Which layer of the OSI model is responsible for establishing, maintaining, and terminating sessions between applications?

A. Presentation Layer (Layer 6)
B. Application Layer (Layer 7)
C. Session Layer (Layer 5)
D. Transport Layer (Layer 4)

Answer Key & Explanations

1. D — TCP is connection-oriented while UDP is connectionless
TCP (Transmission Control Protocol) is connection-oriented, providing reliable, ordered, and error-checked delivery of data packets. UDP (User Datagram Protocol) is connectionless and does not guarantee delivery, order, or error checking, making it faster but less reliable.

2. C — UDP
UDP is preferred for time-sensitive applications because it has lower latency due to no handshaking, acknowledgments, or retransmissions. While some packets might be lost, this is generally preferable to the delays that TCP's reliability mechanisms would introduce.

3. B — 443
HTTPS (HTTP Secure) uses port 443 by default. This is the secure version of HTTP that encrypts the data being transmitted using SSL/TLS.

4. A — DHCP
DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses and other network configuration parameters to devices when they join a network, eliminating the need for manual IP configuration.

5. D — To translate domain names to IP addresses
DNS (Domain Name System) translates human-readable domain names (like www.example.com) into IP addresses that computers use to identify each other on the network.

6. C — SFTP
SFTP (SSH File Transfer Protocol) provides secure file transfer capabilities using SSH encryption and authentication, protecting both credentials and data during transfer.

7. B — ICMP
ICMP (Internet Control Message Protocol) is used for network diagnostics and error reporting. The ping command uses ICMP Echo Request and Echo Reply messages to test connectivity between hosts.

8. A — FTP
FTP (File Transfer Protocol) transmits data and credentials in plaintext without encryption, making it vulnerable to packet sniffing and credential theft. TFTP is even simpler but typically only used in controlled environments.

9. D — To synchronize time across network devices
NTP (Network Time Protocol) is designed to synchronize the clocks of computers over a network to a common time reference, ensuring consistent timestamps across systems.

10. C — TFTP
TFTP (Trivial File Transfer Protocol) is a simplified version of FTP that uses minimal resources and lacks

authentication features, making it suitable for basic file transfers in environments with limited resources or during device initialization.

11. B — Data encryption
HTTPS encrypts the data transmitted between the client and server using SSL/TLS protocols, protecting it from eavesdropping and man-in-the-middle attacks, while standard HTTP transmits data in plaintext.

12. A — UDP
DNS primarily uses UDP for standard queries because it's faster and the overhead of establishing a TCP connection isn't necessary for simple lookups. TCP is used for larger responses or zone transfers.

13. D — 21
FTP uses port 21 for command control and typically uses port 20 for data transfer in active mode. Port 21 is the primary port associated with FTP for establishing the initial connection.

14. C — DHCP DISCOVER
DHCP DISCOVER is the first message sent by a client when joining a network. It's a broadcast message sent to locate available DHCP servers on the network before requesting an IP address.

15. B — They require acknowledgment of received packets
Connection-oriented protocols like TCP establish a connection before data transfer begins, maintain state during the transfer, and ensure all data is delivered reliably with acknowledgments for received packets.

16. A — HTTP on port 80
HTTP (Hypertext Transfer Protocol) is the protocol used when a URL begins with 'http://' and operates on port 80 by default. It's the standard protocol for web browsing without encryption.

17. D — ICMP
ICMP (Internet Control Message Protocol) is designed to report errors, provide network diagnostics, and test connectivity between devices on IP networks. Commands like ping and traceroute use ICMP.

18. C — SYN, SYN-ACK, ACK packet exchange
The TCP three-way handshake establishes a connection through three steps: the client sends SYN, the server responds with SYN-ACK, and the client acknowledges with ACK. This process synchronizes sequence numbers and establishes connection parameters.

19. B — Lower latency
UDP has lower latency than TCP because it doesn't establish connections, doesn't wait for acknowledgments, and doesn't retransmit lost packets. This makes it ideal for time-sensitive applications where some packet loss is acceptable.

20. A — HTTPS
HTTPS (HTTP Secure) is used for secure websites. It combines HTTP with SSL/TLS encryption to provide secure communication over a computer network, protecting the privacy and integrity of exchanged data.

21. D — Network Layer (Layer 3)
Layer 3, the Network layer, handles logical addressing (such as IP addresses) and determines the best path for data to travel through the network via routing.

22. C — Internet Layer
The Internet layer in the TCP/IP model corresponds to the Network layer (Layer 3) in the OSI model. Both handle IP addressing and routing functions.

23. B — A frame operates at Layer 2 with MAC addresses, while a packet operates at Layer 3 with IP addresses
A frame operates at Layer 2 (Data Link) and includes MAC addresses, while a packet operates at Layer 3 (Network) and contains IP addresses. Frames encapsulate packets when data moves down the protocol stack.

24. A — Headers are added to data as it travels down the protocol stack
Encapsulation is the process where data traveling down the protocol stack has headers (and sometimes trailers) added at each layer. Each layer adds its own control information to help the corresponding layer on the receiving end.

25. D — Application, Transport, Internet, Network Access
The TCP/IP model consists of four layers: Application at the top, then Transport, Internet, and Network Access at the bottom. This order represents the flow of data from applications down to the physical network.

26. C — Node-to-node data delivery and media access control
The Data Link layer (Layer 2) is responsible for node-to-node delivery of data, providing framing, physical addressing (MAC addresses), error detection, and access to the media.

27. B — MAC addressing
MAC (Media Access Control) addressing uses 48-bit (6-byte) addresses that are typically expressed in hexadecimal format and operates at Layer 2 (Data Link layer) of the OSI model.

28. A — To map IP addresses to MAC addresses
Address Resolution Protocol (ARP) resolves IP addresses to MAC addresses. When a device needs to communicate with another device on the local network, it uses ARP to discover the MAC address associated with the target IP address.

29. D — Broadcast address
A broadcast address is used to deliver packets to all devices on a local network segment. In IPv4, the broadcast address typically ends with all 1s in the host portion of the address.

30. C — Session Layer (Layer 5)
The Session layer (Layer 5) manages communication sessions between applications, including establishing, maintaining, and terminating these connections. It also provides dialog control and synchronization.

Ready to pass?

Unlock the full CCST Cisco IT Exam Prep bank, every explanation, and unlimited timed mock exams.

Scan to start practising
https://certs.theorypractice.app/ccst

Watch the full video walkthrough on YouTube @CertsQuizPrep