CompTIA Network+ 2026 Prep

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Unlock the full bank of 1010 questions + unlimited timed mock exams + mistake book

Practice on the web: https://certs.theorypractice.app/comptianetwork

$2.99 / week · $6.99 / month · cancel anytime

What you unlock: all 1010 questions • unlimited timed mock exams • mistake book • instant explanations

Study offline on the free app — search your exam on the App Store or Google Play

Practice Questions

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

1. Which network configuration allows remote users to securely access a company's internal network through the internet?

A. NAT (Network Address Translation)
B. VLAN (Virtual Local Area Network)
C. DMZ (Demilitarized Zone)
D. VPN (Virtual Private Network)

2. Which component of a network cable does the 802.3af PoE (Power over Ethernet) standard affect?

A. The power delivery
B. The color coding
C. The bandwidth
D. The speed

3. In a network, what type of route is manually entered into a router's routing table to define a path for packets destined to an unknown network?

A. Connected route
B. Default route
C. Static route
D. Dynamic route

4. Which of the following is NOT a valid characteristic of an IP address?

A. Subnet mask
B. MAC address
C. Network ID
D. Host ID

5. What is the maximum length supported by a Cat6 cable for 10GBase-T Ethernet?

A. 300 m
B. 10 km
C. 55 m
D. 100 m

6. Which type of IPv6 address range is FC00::/7?

A. Global unicast
B. Link-local unicast
C. Multicast
D. Unique local unicast

7. The Enhanced Interior Gateway Routing Protocol (EIGRP) uses which of the following as a metric for selecting the best path?

A. MTU
B. Reliability and Delay
C. Hop Count
D. Bandwidth

8. Which of the following is a model that allows businesses to lease virtual computing resources from a service provider?

A. PaaS
B. SaaS
C. IaaS
D. DaaS

9. Which type of cloud topology is most prone to data leakage due to its shared infrastructure?

A. Private cloud
B. Hybrid cloud
C. Community cloud
D. Public cloud

10. Which of the following network security audits can be entirely carried out by software without human intervention?

A. Security policy compliance check
B. Risk analysis
C. Automated security audit
D. Manual configuration review

11. Which of the following is NOT primarily an attack on confidentiality?

A. DDoS attack
B. On-path attack
C. Phishing
D. Man-in-the-middle attack

12. Which of the following is NOT a commonly implemented firewall security best practice?

A. Enabling logging and alerting
B. Implementing access control lists (ACLs)
C. Conducting regular vulnerability assessments
D. Disabling stateful inspection

13. What type of attack involves overwhelming a network with excessive traffic causing legitimate users to experience delays or denied access?

A. SQL injection
B. Distributed denial of service
C. Man-in-the-middle
D. Phishing

14. Which of the following security practices helps in preventing an insider threat by ensuring critical tasks are distributed among multiple people?

A. Least privilege
B. Zero trust
C. Role-based access controls
D. Separation of duties

15. Which of the following concepts are associated with ensuring the authenticity and integrity of emails using cryptographic techniques?

A. PGP
B. FTP
C. IPsec
D. SMTP

16. Which of the following tools can be used for creating and managing cryptographic keys for network security?

A. OpenSSL
B. Wireshark
C. Splunk
D. Honeypot

17. Which of the following protocols is utilized to securely exchange keys over an insecure network?

A. RSA (Rivest-Shamir-Adleman)
B. Internet Key Exchange (IKE)
C. Transport Layer Security (TLS)
D. Secure/Multipurpose Internet Mail Extensions (S/MIME)

18. Which of the following is NOT a valid ping command?

A. ping -t
B. ping unknown
C. ping 127.0.0.1
D. ping google.com

19. When fiber optic cables have their glass core fractured, resulting in loss of signal transmission, this is referred to as which of the following?

A. Attenuation
B. Reflection
C. Dispersion
D. Break

20. Which command should you use with the ifconfig utility to bring down a network interface in a Linux system?

A. down
B. disable
C. stop
D. deactivate

21. A small company is using a Linux-based server for authentication, but one of the users cannot log in due to authentication failures. What could be the most likely cause?

A. Incorrect permissions
B. Expired user account
C. Duplicate hostname
D. Misconfigured time settings

22. Which of the following is NOT a common practice for ensuring network security in an enterprise environment?

A. Enforcing strong password policies
B. Conducting regular security audits
C. Regular physical equipment replacement
D. Implementing firewall rules

23. Your organization is planning to enhance its disaster recovery plan by focusing on system availability. Which of the following metrics is MOST relevant for this?

A. RPO
B. RTO
C. MTTR
D. MTBF

24. When configuring a redundant power supply for a critical server, which option provides the most immediate failover but is the costliest?

A. Generator Backup
B. Online UPS
C. Standby UPS
D. Line-Interactive UPS

25. Which of the following stages in the disaster recovery process involves restoring critical business functions and verifying the integrity of restored data?

A. Analysis
B. Containment
C. Recovery
D. Mitigation

26. In the context of wireless networks, which Wi-Fi security protocol observes and monitors for potential threats without allowing client access to the network?

A. WIDS (Wireless Intrusion Detection System)
B. WEP (Wired Equivalent Privacy)
C. WPA2 (Wi-Fi Protected Access 2)
D. WPA3 (Wi-Fi Protected Access 3)

27. In a wireless network, the frequency bands used for Wi-Fi communication are measured in which units?

A. Terahertz
B. Gigahertz
C. Kilohertz
D. Megahertz

28. Which protocol operates on Data Link Layer to automatically configure the switches in a local network?

A. Dynamic Host Configuration Protocol
B. Border Gateway Protocol
C. Spanning Tree Protocol
D. Address Resolution Protocol

29. In the context of wireless networking, which of the following devices always operates in multiple collision domains but a single broadcast domain?

A. Hub
B. Router
C. Wireless Access Point (WAP)
D. Repeater

30. Which of the following Wi-Fi technologies allows simultaneous dual-band operation, enabling devices to use 2.4 GHz and 5 GHz frequencies concurrently?

A. 802.11ac
B. 802.11b
C. 802.11g
D. 802.11a

Answer Key & Explanations

1. D — VPN (Virtual Private Network)
Answer: VPN (Virtual Private Network) A Virtual Private Network (VPN) creates a secure, encrypted connection over the internet between the remote user and the company's internal network. This allows employees to access resources and data securely from any device, ensuring the integrity and confidentiality of the transmitted information. Network Address Translation (NAT), VLAN (Virtual Local Area Network), and DMZ (Demilitarized Zone) all perform distinct networking tasks. NAT translates private IP addresses to a public IP address for internet access. VLAN segments a network into different broadcast domains. DMZ provides an additional layer of security by isolating external services from the internal network.

2. A — The power delivery
The 802.3af PoE standard is specifically designed to supply power over Ethernet cables to power devices such as IP cameras and wireless access points. It does not affect the color coding, bandwidth, or speed of the network cables.

3. C — Static route
Answer: Static route A static route is manually configured by a network administrator to specify the path that packets should take to reach a particular network. This type of route is used when automatic routing is not desired or possible. A dynamic route is learned automatically through routing protocols, a connected route is automatically added for directly connected networks, and a default route specifies the path for any addresses not found in the routing table but is usually not manually configured for specific external networks.

4. B — MAC address
Answer: MAC address An IP address is used to uniquely identify a device on a network. It consists of a Network ID, a Host ID, and is associated with a Subnet mask. A MAC address, on the other hand, is a hardware identifier used at the data link layer for network communication.

5. C — 55 m
Answer: 55 m Cat6 cables can support 10GBase-T Ethernet speeds up to a maximum distance of 55 meters. Beyond this distance, the signal quality degrades and higher category cables, like Cat6a or Cat7, are recommended for longer distances.

6. D — Unique local unicast
Answer: Unique local unicast Unique local addresses are non-routable IPv6 addresses in the FC00::/7 range. They are used within a private network, similar to private IP addresses in IPv4 (e.g., 192.168.x.x). Global unicast addresses are routable on the Internet and are in the range 2000::/3. Link-local unicast addresses are used on a single link and have the prefix FE80::/10. IPv6 multicast addresses, used to send packets to multiple interfaces, are in the FF00::/8 range.

7. B — Reliability and Delay
Answer: Reliability and Delay EIGRP uses a combination of metrics including reliability, delay, load, and bandwidth, with reliability and delay being two of the main factors. In contrast, OSPF uses bandwidth and RIP

uses hop count as their metrics.

8. C — IaaS
Answer: IaaS Infrastructure as a Service (IaaS) is a service model that allows businesses to lease virtualized computing resources from a cloud provider. Desktop as a Service (DaaS) offers a virtual desktop infrastructure managed by a third-party provider. Platform as a Service (PaaS) provides a managed environment for developers to build, test, and deploy software applications. Software as a Service (SaaS) offers software solutions provided over the internet on a subscription basis, such as Microsoft 365 or Google Workspace.

9. D — Public cloud
Public cloud deployments are more prone to data leakage because multiple different organizations share the same infrastructure. Private clouds have dedicated infrastructure, reducing this risk. Hybrid clouds, being a mix of public and private clouds, can have both shared and dedicated components. In a community cloud, infrastructure may be shared only among organizations with similar needs, which may reduce the risk compared to the public cloud.

10. C — Automated security audit
Correct answer: Automated security audit An automated security audit is a type of review performed entirely by software tools to scan and verify the security state of a network without human intervention. Manual configuration reviews, security policy compliance checks, and risk analyses require human input to interpret findings and make decisions based on complex data sets and organizational context.

11. A — DDoS attack
Answer: DDoS attack A DDoS attack targets availability by attempting to overwhelm a network or service, rendering it unavailable to legitimate users. On-path attacks, phishing, and man-in-the-middle attacks are all aimed at compromising confidentiality.

12. D — Disabling stateful inspection
Answer: Disabling stateful inspection Stateful inspection is a core feature of many firewalls that tracks the state of active connections and helps distinguish between legitimate and illegitimate traffic. Other best practices include enabling logging and alerting, implementing ACLs, and conducting regular vulnerability assessments.

13. B — Distributed denial of service
Answer: Distributed denial of service A distributed denial of service (DDoS) attack aims to disrupt normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. Such attacks often use multiple compromised computer systems as sources of attack traffic.

14. D — Separation of duties
Answer: Separation of duties Separation of duties ensures that critical tasks, especially those prone to fraud or misuse, are divided among multiple individuals. This makes it harder for any single user to abuse their access. Least privilege grants users only the permissions necessary for their job functions, thereby minimizing the potential damage from compromised accounts. Zero trust is a security model that requires strict identity verification and assumes that threats could be both inside and outside the network. Role-based access controls assign permissions based on user roles, streamlining access management within an organization.

15. A — PGP
Answer: PGP Pretty Good Privacy (PGP) uses cryptographic techniques to provide security services such as email authentication and integrity verification. FTP is a protocol for transferring files, IPsec is used for securing internet communication, and SMTP is used for sending email, all of which do not directly provide email authentication or integrity.

16. A — OpenSSL
Answer: OpenSSL OpenSSL is an open-source toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. It provides various cryptographic functions including the management of cryptographic keys, certificate generation, and encryption. Wireshark is a network protocol analyzer, not a cryptographic toolkit. Splunk is a security information and event management (SIEM) system. A honeypot is a decoy system designed to detect and distract attackers.

17. B — Internet Key Exchange (IKE)
Answer: Internet Key Exchange (IKE) Internet Key Exchange (IKE) is a protocol used to set up a secure and authenticated communication channel over an insecure network by securely exchanging encryption keys. Transport Layer Security (TLS) ensures data privacy between client and server communication. Secure/Multipurpose Internet Mail Extensions (S/MIME) provides a way to send encrypted email messages. RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem used for secure data transmission.

18. B — ping unknown
Answer: ping unknown ping 127.0.0.1, ping google.com, and ping -t are all valid commands. ping unknown is not a valid command.

19. D — Break
Answer: Break When the glass core of a fiber optic cable is fractured, it results in a 'break', disrupting the signal transmission. An attenuation occurs when the signal strength decreases over distance. A reflection happens when light bounces back towards the source, causing loss of signal clarity. A dispersion is when light pulses spread out over time within the fiber, affecting the signal quality.

20. A — down
Answer: down The down command deactivates a network interface on a Linux system using ifconfig. The commands disable, stop, and deactivate are not valid for the ifconfig utility.

21. D — Misconfigured time settings
Answer: Misconfigured time settings Authentication services often require system clocks to be closely synchronized for security tokens to be validated. A time discrepancy could prevent a user from logging in even if other network services appear to function normally. Incorrect permissions would prevent access to specific resources but would not necessarily block the user from logging in. An expired user account would typically give a clear message about account status. A duplicate hostname might cause network conflicts but would usually not prevent a user from authenticating.

22. C — Regular physical equipment replacement
Answer: Regular physical equipment replacement Securing a network typically involves practices like implementing firewall rules, enforcing strong password policies, and conducting regular security audits. Regular physical equipment replacement is not a standard security practice but rather a maintenance activity for hardware lifecycle management.

23. D — MTBF
Answer: MTBF Mean time between failures (MTBF) measures the average amount of time between failures of a particular component. This is relevant to system availability because it helps in understanding how frequently components are likely to fail, thus aiding in planning for redundancy and maintenance. The recovery point objective (RPO) measures how far back you have to go to fully recover from an outage. The recovery time objective (RTO) defines how long a component can be down without causing unacceptable consequences. Mean time to repair (MTTR) is the average amount of time between a component failing and the system being restored to normal operation; this should be minimized.

24. B — Online UPS
Answer: Online UPS Different types of UPS (Uninterruptible Power Supply) solutions offer varying levels of protection and failover capabilities: Standby UPS: The least expensive type, which only switches to battery power when mains supply fails, causing a brief interruption. Line-Interactive UPS: Offers better regulation against power fluctuations by using an autotransformer, but still has a brief switch-over time. Online UPS: Provides continuous power from its battery, eliminating switchover time entirely. This is the costliest option but offers the most immediate failover capability. Generator Backup: Provides long-term power but has the longest delay before becoming operational.

25. C — Recovery
Answer: Recovery Typical disaster recovery plans include the following stages: Stage Description Preparation **Prepare**: Organizations ensure that they have the resources and plans to handle a potential disaster. Detection **Detect**: Identification of a disaster event. Containment **Contain**: Steps to prevent the disaster from escalating. Mitigation **Mitigate**: Reducing the impact of the disaster through initial response actions. Recovery **Recovery**: Restoring affected systems and data to normal operations, including verification of data integrity. Review **Review**: Analyzing the response to improve future disaster recovery processes.

26. A — WIDS (Wireless Intrusion Detection System)
Answer: WIDS (Wireless Intrusion Detection System) WIDS monitors a wireless network for malicious activity or policy violations but does not allow client access. It observes network traffic and detects potential security issues. WEP is an outdated security protocol that provides minimal protection. WPA2 and WPA3 are current security protocols that offer strong protection by allowing client access while securing the network.

27. B — Gigahertz
Answer: Gigahertz. The frequency bands used in Wi-Fi communication are measured in gigahertz (GHz). Most common Wi-Fi standards use either 2.4 GHz or 5 GHz bands.

28. C — Spanning Tree Protocol
Answer: Spanning Tree Protocol The Spanning Tree Protocol (STP) is used at the Data Link Layer to prevent network loops and ensure efficient and reliable network communications by allowing switches to dynamically learn the network topology. The Address Resolution Protocol (ARP) is used in IPv4 networks to map IP addresses to MAC addresses. The Dynamic Host Configuration Protocol (DHCP) is used to automatically assign IP addresses to hosts. The Border Gateway Protocol (BGP) is used to exchange routing information between autonomous systems on the internet.

29. C — Wireless Access Point (WAP)
Answer: Wireless Access Point (WAP). WAPs create multiple collision domains, as each connected device communicates with the WAP independently. However, the WAP itself maintains a single broadcast domain for

all connected devices. Repeaters operate within a single collision and broadcast domain because they simply amplify signals. Hubs also have a single collision and broadcast domain. Routers have multiple collision domains and can belong to multiple broadcast domains.

30. A — 802.11ac
Answer: 802.11ac The 802.11ac Wi-Fi technology allows for simultaneous dual-band operation, which means devices can use both the 2.4 GHz and 5 GHz frequencies concurrently. This provides higher bandwidth and better performance. 802.11b only operates in the 2.4 GHz band and offers slower speeds. 802.11g also operates in the 2.4 GHz band but offers improved speeds compared to 802.11b. 802.11a operates in the 5 GHz band but does not support dual-band operation.

Ready to pass?

Unlock the full CompTIA Network+ 2026 Prep bank, every explanation, and unlimited timed mock exams.

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

Also on iOS & Android — search your exam name on the App Store or Google Play