CompTIA Network+ N10-009

100 Questions & Answers

Welcome to your complete Network+ N10-009 ***practice question*** *set.*
This collection is designed not just to quiz you — but to reinforce your understanding and prepare you for real-world performance.

Learning Objectives and Expectations

You'll get:

- **Realistic questions** reflecting the latest CompTIA exam format and phrasing.
- **Structured delivery: 10 questions followed by 10** answers with concise explanations.
- **Exam-relevant explanations** to reinforce why the correct answers are right — and what to remember for test day.

Network+ N10-009 Domains

Each domain is weighted differently on the exam, with Network Troubleshooting being the largest:

- **Domain 1:** Networking Concepts (23%)
- **Domain 2:** Network Implementation (20%)
- **Domain 3:** Network Operations (19%)
- **Domain 4:** Network Security (14%)
- **Domain 5:** Network Troubleshooting (24%)

Quick Reminder: How the Exam Works

- Number of Questions: Up to 90
- Format: Multiple choice + Performance-Based Questions (PBQs)
- Time Limit: 90 minutes
- Passing Score: 720/900 (about 80%)
- Test Provider: Pearson VUE (onsite or online)

Questions By Domain

Domain	Title	Questions Assigned	Question Numbers
Domain 1	Networking Concepts (23%)	23 Questions	Q1, Q2, Q3, Q6, Q10, Q13, Q14, Q16, Q20, Q22, Q25, Q28, Q34, Q38, Q39, Q43, Q47, Q53, Q58, Q61, Q65, Q68, Q87
Domain 2	Network Implementation (20%)	20 Questions	Q4, Q5, Q7, Q12, Q15, Q18, Q21, Q24, Q26, Q29, Q30, Q41, Q50, Q55, Q60, Q63, Q64, Q71, Q84, Q100
Domain 3	Network Operations (19%)	19 Questions	Q8, Q9, Q17, Q23, Q27, Q31, Q36, Q44, Q48, Q49, Q51, Q56, Q59, Q66, Q70, Q72, Q73, Q82, Q98
Domain 4	Network Security (14%)	14 Questions	Q11, Q19, Q33, Q40, Q45, Q52, Q57, Q62, Q74, Q75, Q76, Q78, Q83, Q90
Domain 5	Network Troubleshooting (24%)	24 Questions	Q32, Q35, Q37, Q42, Q46, Q54, Q67, Q69, Q77, Q79, Q80, Q85, Q86, Q88, Q89, Q91, Q92, Q93, Q94, Q95, Q96, Q97, Q99, Q99

Remember — you don’t need to be perfect to pass!

The Security+ passing score is about **80%**. That means you **can miss around 18 questions out of 90** and still pass!

Missing a few tricky questions won't ruin your chances — **stay calm**, trust your preparation, and keep moving forward.

Questions 1–10

Q1.
Which OSI layer is responsible for delivering packets based on IP addressing and selecting best paths?
A) Transport
B) Network
C) Data Link
D) Application

Q2.
Which protocol is used to assign IP addresses dynamically to clients on a network?
A) DNS
B) SNMP
C) DHCP
D) NAT

Q3.
Which device operates primarily at Layer 2 and forwards traffic based on MAC addresses?
A) Router
B) Switch
C) Firewall
D) Access Point

Q4.
Which of the following address types is assigned automatically when a device cannot contact a DHCP server?
A) Public
B) Loopback
C) APIPA
D) Multicast

Q5.
A network technician sees excessive broadcast traffic and suspects a switching loop. Which protocol helps prevent this?
A) OSPF

B) STP
C) RIP
D) ARP

Q6.
Which of the following technologies allows multiple physical links to be treated as a single logical link?
A) STP
B) Trunking
C) LACP
D) VLAN

Q7.
A user can access local network resources but cannot reach the internet. Which setting should be verified FIRST?
A) DNS server address
B) MAC address
C) Default gateway
D) Hostname

Q8.
Which type of cable is MOST appropriate for connecting two switches together in a modern network?
A) Straight-through
B) Rollover
C) Console
D) Crossover

Q9.
What is the purpose of a DHCP relay agent?
A) Translate private to public IP addresses
B) Cache IP-to-hostname mappings
C) Forward DHCP messages between subnets
D) Redirect DNS queries to a different server

Q10.
Which of the following would MOST likely be used to secure management access to a

network switch?
A) Telnet
B) FTP
C) HTTP
D) SSH

Answers 1–10

A1.
Answer: B) Network
Explanation:
The Network layer (Layer 3) handles logical addressing (IP) and routing across networks.

A2.
Answer: C) DHCP
Explanation:
Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses and network settings to clients.

A3.
Answer: B) Switch
Explanation:
A switch operates at Layer 2 and uses MAC addresses to forward frames within a LAN.

A4.
Answer: C) APIPA
Explanation:
If a device cannot contact a DHCP server, it assigns itself an APIPA address (169.254.0.0/16) for local communication only.

A5.
Answer: B) STP
Explanation:
Spanning Tree Protocol prevents switching loops by blocking redundant paths in a Layer 2 network.

A6.
Answer: C) LACP
Explanation:
Link Aggregation Control Protocol allows multiple physical links to act as one logical link for redundancy and performance.

A7.
Answer: C) Default gateway
Explanation:
Without a valid default gateway, a device cannot communicate outside its local subnet, including the internet.

A8.
Answer: A) Straight-through
Explanation:
Modern switches use auto MDI-X and can auto-negotiate, making straight-through cables standard for switch-to-switch connections.

A9.
Answer: C) Forward DHCP messages between subnets
Explanation:
A DHCP relay agent allows clients on different subnets to reach a central DHCP server.

A10.
Answer: D) SSH
Explanation:
Secure Shell (SSH) encrypts command-line sessions and is the preferred method for managing switches securely.

Questions 11–20

Q11.
Which wireless frequency band offers more channels and typically less interference?
A) 2.4 GHz
B) 3.5 GHz
C) 5 GHz
D) 1.8 GHz

Q12.
Which of the following DNS record types maps a domain name to an IPv6 address?
A) A
B) CNAME
C) MX
D) AAAA

Q13.
What is the default port number used by HTTPS?
A) 80
B) 23
C) 443
D) 8080

Q14.
Which protocol provides secure remote CLI management using encryption?
A) FTP
B) Telnet
C) SSH
D) SNMP

Q15.
A technician notices that a workstation cannot obtain an IP address and has a 169.254.x.x address. What is the MOST likely issue?
A) DNS failure
B) Switch port error
C) DHCP server unreachable
D) Duplicate IP address

Q16.
What technology is used to logically separate traffic on a switch at Layer 2?
A) Subnetting
B) STP
C) VLAN
D) NAT

Q17.
Which of the following cable types is LEAST susceptible to electromagnetic interference (EMI)?
A) UTP
B) STP
C) Coaxial
D) Fiber optic

Q18.
Which protocol is responsible for network time synchronization between devices?
A) NTP
B) SNMP
C) DNS
D) DHCP

Q19.
Which of the following BEST describes the function of NAT?
A) Resolving hostnames to IPs
B) Translating internal IPs to public IPs
C) Authenticating remote users
D) Encrypting data in transit

Q20.
Which device connects different IP networks and makes forwarding decisions based on IP addresses?
A) Switch
B) Router
C) Bridge
D) Access Point

Answers 11–20

A11.
Answer: C) 5 GHz
Explanation:
The 5 GHz band has more non-overlapping channels and less interference than 2.4 GHz.

A12.
Answer: D) AAAA
Explanation:
AAAA records map domain names to IPv6 addresses.

A13.
Answer: C) 443
Explanation:
HTTPS uses port 443 for encrypted web traffic.

A14.
Answer: C) SSH
Explanation:
Secure Shell (SSH) provides encrypted remote CLI access.

A15.
Answer: C) DHCP server unreachable
Explanation:
A 169.254.x.x APIPA address indicates the client could not reach a DHCP server.

A16.
Answer: C) VLAN
Explanation:
VLANs segment broadcast domains on a Layer 2 switch.

A17.
Answer: D) Fiber optic
Explanation:
Fiber is immune to EMI because it transmits light, not electrical signals.

A18.
Answer: A) NTP
Explanation:
Network Time Protocol (NTP) synchronizes clocks across devices.

A19.
Answer: B) Translating internal IPs to public IPs
Explanation:
NAT converts private internal addresses to public ones for internet access.

A20.
Answer: B) Router
Explanation:
Routers forward packets between different networks based on IP addresses.

Questions 21–30

Q21.
Which of the following cable types supports the longest transmission distances?
A) Cat5e
B) Cat6
C) Multimode Fiber
D) Single-mode Fiber

Q22.
Which protocol is used to send log messages from network devices to a centralized server?
A) SNMP
B) Syslog
C) RADIUS
D) NetFlow

Q23.
Which protocol uses port 161 and allows monitoring of device statistics?
A) LDAP
B) RADIUS
C) SNMP
D) NTP

Q24.
Which of the following is a benefit of link aggregation?
A) Allows dynamic VLAN assignments
B) Provides fault tolerance and higher throughput
C) Prioritizes VoIP traffic over web traffic
D) Prevents switching loops

Q25.
Which layer of the OSI model is responsible for end-to-end delivery and flow control?
A) Network
B) Transport
C) Data Link
D) Application

Q26.
Which command would you use to view the current IP configuration on a Windows device?
A) ping
B) netstat
C) ipconfig
D) tracert

Q27.
A technician wants to identify the route a packet takes to reach a remote host. Which command should be used?
A) netstat
B) nslookup
C) arp
D) tracert

Q28.
What is the function of the default gateway in a network?
A) Assigns IP addresses
B) Maps domain names to IPs
C) Provides access to external networks
D) Blocks incoming traffic

Q29.
Which type of network topology involves devices connecting to a central point?
A) Mesh
B) Bus
C) Star
D) Ring

Q30.
Which technology prevents Layer 2 switching loops?
A) BGP
B) NAT
C) STP
D) OSPF

Answers 21–30

A21.
Answer: D) Single-mode Fiber
Explanation:
Single-mode fiber supports the longest distances, often over 10 km, using a single light path.

A22.
Answer: B) Syslog
Explanation:
Syslog collects and forwards log data from devices to a central server.

A23.
Answer: C) SNMP
Explanation:
Simple Network Management Protocol (SNMP) uses port 161 to monitor and manage devices.

A24.
Answer: B) Provides fault tolerance and higher throughput
Explanation:
Link aggregation (LACP) combines multiple links to increase bandwidth and provide redundancy.

A25.
Answer: B) Transport
Explanation:
The Transport layer (Layer 4) ensures reliable delivery and flow control (TCP/UDP).

A26.
Answer: C) ipconfig
Explanation:
The `ipconfig` command displays IP configuration on Windows systems.

A27.
Answer: D) tracert
Explanation:
tracert (trace route) identifies the hops a packet takes to reach its destination.

A28.
Answer: C) Provides access to external networks
Explanation:
A default gateway routes traffic from the local network to other networks, like the internet.

A29.
Answer: C) Star
Explanation:
In a star topology, all devices connect to a central device (e.g., a switch).

A30.
Answer: C) STP
Explanation:
Spanning Tree Protocol (STP) prevents switching loops in a Layer 2 network.

Questions 31–40

Q31.
Which of the following IP addresses is a valid private address?
A) 8.8.8.8
B) 172.32.0.1
C) 10.0.0.1
D) 192.0.2.1

Q32.
Which protocol uses a three-way handshake to establish a reliable connection?
A) UDP
B) TCP
C) ICMP
D) FTP

Q33.
A user is complaining of slow network speeds. The technician notices a high rate of CRC errors on the interface. What is the MOST likely cause?
A) DNS misconfiguration
B) Duplex mismatch
C) Bad cable or connector
D) IP address conflict

Q34.
Which record type is used in DNS to direct email traffic to the appropriate mail server?
A) A
B) CNAME
C) PTR
D) MX

Q35.
What is the primary purpose of port security on a switch?
A) Prevent IP conflicts
B) Restrict MAC address access per port
C) Filter web traffic
D) Block UDP flooding

Q36.
Which of the following is a Layer 1 device?
A) Router
B) Bridge
C) Hub
D) Switch

Q37.
What command can be used to determine whether DNS resolution is functioning properly?
A) tracert
B) arp
C) netstat
D) nslookup

Q38.
Which protocol is responsible for identifying reachable networks and selecting optimal paths?
A) SNMP
B) DNS
C) Routing protocol
D) NTP

Q39.
Which class of IP addresses provides the fewest hosts per network?
A) Class A
B) Class B
C) Class C
D) Class D

Q40.
A technician wants to enable remote management of a router using a secure CLI. Which protocol should be used?
A) Telnet
B) FTP
C) SSH
D) SNMP

Answers 31–40

A31.
Answer: C) 10.0.0.1
Explanation:
10.0.0.0/8 is a reserved private IP range.

A32.
Answer: B) TCP
Explanation:
TCP uses a SYN, SYN-ACK, ACK three-way handshake to establish connections.

A33.
Answer: C) Bad cable or connector
Explanation:
High CRC errors are often due to physical layer issues like damaged cables or connectors.

A34.
Answer: D) MX
Explanation:
Mail Exchange (MX) records specify the mail server responsible for a domain.

A35.
Answer: B) Restrict MAC address access per port
Explanation:
Port security limits the number or specific MAC addresses allowed on a switch port.

A36.
Answer: C) Hub
Explanation:
Hubs operate at Layer 1 and simply repeat electrical signals to all connected ports.

A37.
Answer: D) nslookup
Explanation:
nslookup tests DNS functionality by querying name resolution.

A38.
Answer: C) Routing protocol
Explanation:
Routing protocols like OSPF and RIP determine reachability and optimal paths.

A39.
Answer: C) Class C
Explanation:
Class C networks (default /24 mask) support 254 hosts, the fewest among A–C.

A40.
Answer: C) SSH
Explanation:
Secure Shell (SSH) allows encrypted remote CLI access.

Questions 41–50

Q41.
Which technology allows multiple VLANs to traverse a single physical link between switches?
A) Port Mirroring
B) LACP
C) 802.1Q
D) STP

Q42.
Which tool would a technician MOST likely use to locate the physical path of a network cable in a patch panel?
A) TDR
B) Multimeter
C) Loopback plug
D) Tone generator and probe

Q43.
Which address type is used for one-to-many communication in IPv4?
A) Unicast
B) Broadcast
C) Multicast
D) Anycast

Q44.
What happens when a switch receives a frame with a destination MAC address not in its CAM table?
A) The frame is dropped
B) The frame is sent to the router
C) The frame is flooded to all ports
D) The frame is queued for resolution

Q45.
Which device is used to separate broadcast domains?
A) Hub
B) Switch

C) Router
D) Bridge

Q46.
Which of the following is a typical use case for a reverse DNS (PTR) record?
A) Forwarding email
B) Resolving MAC addresses
C) Tracing IP ownership
D) Mapping IPs to hostnames

Q47.
What feature of wireless networks allows users to roam between APs with minimal disconnection?
A) WPA2-Enterprise
B) Band steering
C) Fast roaming (802.11r)
D) Beacon frame

Q48.
Which of the following would BEST help reduce the risk of a rogue DHCP server?
A) Port security
B) DHCP snooping
C) NAT
D) Trunking

Q49.
A technician notices high latency and jitter on a VoIP call. Which solution would BEST improve performance?
A) Apply VLAN tagging
B) Enable port mirroring
C) Configure QoS
D) Increase subnet size

Q50.
Which protocol allows for automated IP configuration across different subnets using a router?
A) DHCP snooping

B) DHCP relay
C) NAT
D) ARP

Answers 41–50

A41.
Answer: C) 802.1Q
Explanation:
802.1Q enables VLAN tagging to allow multiple VLANs on a single trunk port.

A42.
Answer: D) Tone generator and probe
Explanation:
This tool helps trace a cable's physical path through walls or patch panels.

A43.
Answer: C) Multicast
Explanation:
Multicast sends traffic from one source to multiple recipients in a group (224.0.0.0/4 range in IPv4).

A44.
Answer: C) The frame is flooded to all ports
Explanation:
Switches flood unknown unicast frames out all ports except the one they came from.

A45.
Answer: C) Router
Explanation:
Routers divide broadcast domains by segmenting Layer 3 networks.

A46.
Answer: D) Mapping IPs to hostnames

Explanation:
PTR records perform reverse DNS lookups, mapping IP addresses back to hostnames.

A47.
Answer: C) Fast roaming (802.11r)
Explanation:
802.11r allows seamless transition between APs in enterprise Wi-Fi environments.

A48.
Answer: B) DHCP snooping
Explanation:
DHCP snooping identifies and blocks unauthorized DHCP servers on a switch.

A49.
Answer: C) Configure QoS
Explanation:
Quality of Service prioritizes VoIP and critical traffic, reducing jitter and delay.

A50.
Answer: B) DHCP relay
Explanation:
DHCP relay forwards DHCP requests across subnets to a centralized server.

Questions 51–60

Q51.
Which type of routing protocol shares the entire routing table periodically with neighbors?
A) Link-state
B) Path-vector
C) Distance-vector
D) Static

Q52.
Which command on a Windows system displays current TCP connections and listening ports?
A) tracert
B) netstat
C) ipconfig
D) ping

Q53.
Which of the following technologies is used in virtualized data centers to create thousands of Layer 2 overlays over Layer 3 infrastructure?
A) STP
B) VXLAN
C) MPLS
D) SD-WAN

Q54.
Which routing protocol is considered a path-vector protocol and is used between ISPs?
A) RIP
B) EIGRP
C) OSPF
D) BGP

Q55.
A technician finds that a trunk port is not passing VLAN 30 between switches. What is the MOST likely cause?
A) STP block on VLAN 30

B) VLAN 30 is not created on both switches
C) MAC address conflict
D) Port is set to access mode

Q56.
Which protocol enables authentication and dynamic VLAN assignment for users connecting to a switch?
A) SNMP
B) 802.1Q
C) 802.1X
D) RADIUS

Q57.
Which of the following ports is used by RDP?
A) 3389
B) 80
C) 161
D) 443

Q58.
Which type of address is used to communicate with all nodes on a local network in IPv4?
A) Broadcast
B) Unicast
C) Multicast
D) Loopback

Q59.
Which network appliance stores frequently accessed content to reduce bandwidth usage and improve load times?
A) Firewall
B) Load balancer
C) Proxy server
D) VPN concentrator

Q60.
Which of the following is an advantage of using fiber optic cabling over copper?

A) Lower cost
B) Simpler termination
C) Immunity to EMI
D) Better PoE support

Answers 51–60

A51.
Answer: C) Distance-vector
Explanation:
Distance-vector protocols (like RIP) periodically share their entire routing tables with neighbors.

A52.
Answer: B) netstat
Explanation:
The netstat command shows current TCP/UDP sessions and listening ports.

A53.
Answer: B) VXLAN
Explanation:
VXLAN is used in large virtualized networks to extend Layer 2 networks across Layer 3 infrastructure.

A54.
Answer: D) BGP
Explanation:
Border Gateway Protocol (BGP) is a path-vector protocol used for routing between autonomous systems.

A55.
Answer: B) VLAN 30 is not created on both switches
Explanation:
A VLAN must exist on both switches to be allowed over a trunk. If it's missing on one side, traffic is dropped.

A56.
Answer: C) 802.1X
Explanation:
802.1X enables port-based authentication and can dynamically assign VLANs based on user identity.

A57.
Answer: A) 3389
Explanation:
Remote Desktop Protocol (RDP) uses TCP port 3389.

A58.
Answer: A) Broadcast
Explanation:
A broadcast address (e.g., 255.255.255.255 or the subnet's broadcast) targets all devices on a local subnet.

A59.
Answer: C) Proxy server
Explanation:
Proxy servers cache content and filter requests, reducing WAN usage and speeding up access.

A60.
Answer: C) Immunity to EMI
Explanation:
Fiber optic cables use light, not electricity, so they are immune to electromagnetic interference.

Questions 61–70

Q61.
Which protocol is primarily used to monitor and manage network devices and collects metrics like bandwidth and uptime?
A) SNMP
B) LDAP
C) ICMP
D) NTP

Q62.
Which of the following would BEST ensure consistent network configurations across multiple devices?
A) SSH
B) Firmware updates
C) Configuration baseline
D) DNS reservation

Q63.
Which wireless encryption protocol has been deprecated due to its weak security?
A) WPA2
B) WPA3
C) WEP
D) 802.1X

Q64.
Which port number is used by the DNS protocol?
A) 80
B) 53
C) 443
D) 25

Q65.
Which network topology involves each device being connected to every other device?
A) Star
B) Bus

C) Ring
D) Mesh

Q66.
Which device is used to connect two different network types and operates at Layer 3 of the OSI model?
A) Switch
B) Bridge
C) Router
D) Hub

Q67.
Which of the following allows a technician to remotely access a device's GUI securely over the internet?
A) SSH
B) Telnet
C) HTTPS
D) SNMP

Q68.
Which IPv6 address type is similar in function to a public IPv4 address?
A) Link-local
B) Loopback
C) Multicast
D) Global unicast

Q69.
Which of the following is MOST likely to help reduce network congestion caused by broadcast traffic?
A) Using static routing
B) Implementing VLANs
C) Using dynamic NAT
D) Increasing MTU

Q70.
What is the purpose of a demilitarized zone (DMZ) in a network architecture?
A) To connect remote offices

B) To isolate guest wireless devices
C) To separate internal LAN from public-facing servers
D) To act as a failover path

Answers 61–70

A61.
Answer: A) SNMP
Explanation:
Simple Network Management Protocol allows administrators to monitor and manage network devices using metrics and alerts.

A62.
Answer: C) Configuration baseline
Explanation:
Baselines define standard configurations, ensuring consistency across systems and simplifying troubleshooting.

A63.
Answer: C) WEP
Explanation:
Wired Equivalent Privacy (WEP) is outdated and insecure due to easily cracked encryption.

A64.
Answer: B) 53
Explanation:
The Domain Name System (DNS) uses port 53 for both TCP and UDP traffic.

A65.
Answer: D) Mesh
Explanation:
In a mesh topology, every node connects to every other node, providing high redundancy.

A66.
Answer: C) Router
Explanation:
Routers connect different IP networks and route packets between them using Layer 3 logic.

A67.
Answer: C) HTTPS
Explanation:
HTTPS provides secure, encrypted GUI access through web browsers.

A68.
Answer: D) Global unicast
Explanation:
Global unicast addresses in IPv6 are equivalent to public IPv4 addresses and are routable on the internet.

A69.
Answer: B) Implementing VLANs
Explanation:
VLANs reduce broadcast domains by logically segmenting a network, lowering broadcast traffic and congestion.

A70.
Answer: C) To separate internal LAN from public-facing servers
Explanation:
DMZs place public services like web or mail servers in a segregated network zone to isolate them from internal systems.

Questions 71–80

Q71.
Which wireless feature helps automatically direct compatible clients to the 5 GHz band instead of 2.4 GHz?
A) Channel bonding
B) Band steering
C) Beamforming
D) Roaming

Q72.
A technician uses ping to test a server and receives a “Destination Host Unreachable” message. What is the MOST likely issue?
A) DNS misconfiguration
B) DHCP server failure
C) Routing or gateway issue
D) ICMP disabled on the technician’s PC

Q73.
Which term describes the delay in data transmission across a network?
A) Throughput
B) Latency
C) Jitter
D) Bandwidth

Q74.
Which of the following is a function of a proxy server?
A) Assign IP addresses
B) Resolve MAC addresses
C) Cache web content and filter traffic
D) Convert public IPs to private

Q75.
What is the main benefit of using STP in a network?
A) Increases routing speed
B) Prevents IP spoofing

C) Avoids switching loops
D) Allows multiple DHCP servers

Q76.
What does the tracert command help a network technician determine?
A) Local subnet mask
B) DNS records for a domain
C) Path packets take to a destination
D) Number of VLANs on a switch

Q77.
Which address format is used for identifying groups of devices for delivery of the same content simultaneously?
A) Unicast
B) Multicast
C) Broadcast
D) Anycast

Q78.
Which of the following authentication services is most often used with 802.1X for port-based security?
A) DHCP
B) LDAP
C) SNMP
D) RADIUS

Q79.
Which term describes the amount of data that can be transferred over a network in a given time?
A) Jitter
B) Latency
C) Bandwidth
D) MTU

Q80.
Which type of fiber optic cable is typically used for long-distance transmission (tens of kilometers)?

A) Multimode
B) Twinax
C) Coaxial
D) Single-mode

Answers 71–80

A71.
Answer: B) Band steering
Explanation:
Band steering pushes capable devices to use 5 GHz, reducing congestion on 2.4 GHz.

A72.
Answer: C) Routing or gateway issue
Explanation:
This message often indicates that no route to the destination exists or the default gateway is misconfigured.

A73.
Answer: B) Latency
Explanation:
Latency measures the delay between a request and a response in data transmission.

A74.
Answer: C) Cache web content and filter traffic
Explanation:
Proxies cache commonly requested content and can enforce content filtering rules.

A75.
Answer: C) Avoids switching loops
Explanation:
Spanning Tree Protocol prevents loops in Layer 2 networks by blocking redundant paths.

A76.
Answer: C) Path packets take to a destination
Explanation:
tracert identifies each hop between the source and destination, useful for routing issues.

A77.
Answer: B) Multicast
Explanation:
Multicast delivers data to multiple devices that are members of a multicast group.

A78.
Answer: D) RADIUS
Explanation:
RADIUS works with 802.1X for centralized authentication of network access.

A79.
Answer: C) Bandwidth
Explanation:
Bandwidth is the maximum data transfer capacity of a network connection.

A80.
Answer: D) Single-mode
Explanation:
Single-mode fiber is designed for long-range communication over long distances with laser light.

Questions 81–90

Q81.
Which of the following WAN technologies uses label-switching for fast packet forwarding and supports QoS?
A) Frame Relay
B) MPLS
C) ISDN
D) DSL

Q82.
Which type of address does a router use to forward packets across networks?
A) MAC address
B) Port number
C) IP address
D) Hostname

Q83.
Which tool can capture and analyze packets in real-time to troubleshoot network issues?
A) Netstat
B) Wireshark
C) Ping
D) SNMP

Q84.
Which wireless standard operates in the 5 GHz band and supports multi-gigabit speeds using MU-MIMO?
A) 802.11b
B) 802.11g
C) 802.11ac
D) 802.11n

Q85.
Which type of network device uses NAT to allow multiple devices to share a single public IP address?
A) Router

B) Bridge
C) Switch
D) Repeater

Q86.
Which of the following is MOST likely to result from a speed/duplex mismatch between two devices?
A) Broadcast storm
B) High jitter
C) VLAN hopping
D) Late collisions

Q87.
What term refers to the maximum size of a single packet that can be transmitted over a network?
A) MSS
B) MTU
C) CRC
D) TTL

Q88.
Which protocol does Secure Copy Protocol (SCP) use for secure file transfers?
A) FTP
B) SSH
C) HTTPS
D) RDP

Q89.
Which DNS record is used to create an alias for another domain name?
A) MX
B) A
C) CNAME
D) PTR

Q90.
Which component of a switch keeps a dynamic list of MAC address-to-port mappings?
A) NAT table

B) ARP cache
C) CAM table
D) Routing table

Answers 81–90

A81.
Answer: B) MPLS
Explanation:
Multiprotocol Label Switching (MPLS) uses labels to route traffic efficiently and supports QoS.

A82.
Answer: C) IP address
Explanation:
Routers use IP addresses to route packets between different networks (Layer 3).

A83.
Answer: B) Wireshark
Explanation:
Wireshark captures and analyzes real-time packet data for protocol and traffic analysis.

A84.
Answer: C) 802.11ac
Explanation:
802.11ac operates on 5 GHz and supports multi-gigabit speeds using MU-MIMO.

A85.
Answer: A) Router
Explanation:
Routers perform NAT to allow multiple private IPs to share one public IP address.

A86.
Answer: D) Late collisions

Explanation:
Speed/duplex mismatches can lead to late collisions and degraded performance.

A87.
Answer: B) MTU
Explanation:
Maximum Transmission Unit (MTU) is the largest frame or packet size that can be sent.

A88.
Answer: B) SSH
Explanation:
SCP uses SSH to securely transfer files over the network.

A89.
Answer: C) CNAME
Explanation:
A CNAME record maps an alias to a canonical domain name.

A90.
Answer: C) CAM table
Explanation:
Switches use a Content Addressable Memory (CAM) table to map MAC addresses to ports.

Questions 91–100

Q91.
Which protocol is responsible for resolving IP addresses to MAC addresses in a local network?
A) DNS
B) ARP
C) DHCP
D) ICMP

Q92.
Which WAN technology provides a dedicated, symmetric, point-to-point connection with fixed bandwidth?
A) Cable
B) MPLS
C) Leased line
D) DSL

Q93.
What is the purpose of a loopback interface on a router?
A) To isolate VLANs
B) To provide a testable internal interface
C) To forward multicast packets
D) To prioritize VoIP traffic

Q94.
Which cable type uses a single copper conductor and is typically used in cable TV or broadband?
A) UTP
B) STP
C) Coaxial
D) Fiber

Q95.
Which of the following protocols uses port 25 to send email?
A) POP3
B) SMTP

C) IMAP
D) SFTP

Q96.
Which concept ensures users are granted only the permissions necessary to perform their job?
A) Least Privilege
B) RBAC
C) MAC
D) SSO

Q97.
Which wireless security protocol replaced WPA and introduced AES encryption?
A) WEP
B) WPA2
C) WPA3
D) 802.1X

Q98.
Which of the following tools can help a technician determine if a user's PC is communicating with a known malicious IP address?
A) ARP
B) ipconfig
C) NetFlow
D) TDR

Q99.
Which of the following is a common cause of intermittent connectivity on a copper Ethernet link?
A) IP conflict
B) Duplex mismatch
C) Crosstalk or EMI
D) Incorrect MTU

Q100.
Which technology allows multiple virtual networks to operate over the same physical infrastructure in a data center?

A) VLAN
B) Subnetting
C) VXLAN
D) NAT

Answers 91–100

A91.
Answer: B) ARP
Explanation:
Address Resolution Protocol (ARP) maps IP addresses to MAC addresses on a local network.

A92.
Answer: C) Leased line
Explanation:
A leased line provides a dedicated point-to-point connection with fixed bandwidth, often used between business sites.

A93.
Answer: B) To provide a testable internal interface
Explanation:
Loopback interfaces are logical interfaces used for testing and network diagnostics.

A94.
Answer: C) Coaxial
Explanation:
Coaxial cable uses a single copper conductor and is common in broadband internet and television setups.

A95.
Answer: B) SMTP
Explanation:
Simple Mail Transfer Protocol (SMTP) uses port 25 to send email.

A96.
Answer: A) Least Privilege
Explanation:
Least privilege ensures users have only the access required to perform their duties.

A97.
Answer: B) WPA2
Explanation:
WPA2 replaced WPA and uses AES encryption, significantly improving wireless security.

A98.
Answer: C) NetFlow
Explanation:
NetFlow provides visibility into network traffic, including identifying conversations with known malicious IPs.

A99.
Answer: C) Crosstalk or EMI
Explanation:
Intermittent connectivity on copper links is often caused by electromagnetic interference or poor shielding.

A100.
Answer: C) VXLAN
Explanation:
Virtual Extensible LAN (VXLAN) enables the creation of Layer 2 overlays across Layer 3 networks in virtualized environments.