CompTIA Network+ N10-009

Quick Exam Refresher

*This is your condensed, high-impact review guide for the CompTIA Network+ N10-009 exam. It's built for **quick recall and confidence-building** right before test day — not deep instruction.*

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

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!

Domain 1: Networking Concepts (23%)

OSI Model & TCP/IP Stack

- 7 Layers: Physical, Data Link, Network, Transport, Session, Presentation, Application
- PDU Types: Bits (L1), Frames (L2), Packets (L3), Segments (L4)
- TCP (reliable) vs UDP (fast, connectionless)

Traffic Types

- **Unicast:** One-to-one
- **Broadcast:** One-to-all (IPv4 only)
- **Multicast:** One-to-many
- **Anycast:** One-to-nearest

Subnetting & IPv4/IPv6

- Private IPv4: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- APIPA: 169.254.0.0/16
- IPv6 Global Unicast, Link-Local, Multicast

Common Protocols

- **DHCP:** Auto IP config
- **DNS:** Name resolution
- **NAT/PAT:** IP address translation
- **SNMP:** Network monitoring
- **NTP:** Time synchronization
- **IPSec, GRE, L2TP:** VPN & tunneling

Cloud & Virtual Networking

- **IaaS, PaaS, SaaS** deployment models
- **VPCs, Direct Connect, NAT Gateway**
- **SDN / SD-WAN / VXLAN / SASE**

Domain 2: Network Implementation (20%)

Switching Technologies

- VLANs: Isolate broadcast domains
- Trunking (802.1Q): Carry multiple VLANs
- STP (Spanning Tree): Prevent loops
- LACP (802.3ad): Link aggregation
- Port Security: MAC address filtering
- PoE: Power over Ethernet (802.3af/at/bt)

Routing Technologies

- Static vs Dynamic
- RIP (hop count), OSPF (cost), BGP (path-vector)
- Longest prefix match wins
- Administrative Distance (lower = preferred)

Wireless Networking

- **Standards:** 802.11a/b/g/n/ac/ax
- **Bands:** 2.4 GHz (longer range), 5 GHz (less interference), 6 GHz (Wi-Fi 6E)
- **Security:** WPA2-Enterprise, WPA3, 802.1X
- **Roaming:** 802.11k/v/r
- **SSID, BSSID, ESSID**

Cabling and Connectors

- Twisted pair (Cat5e/Cat6), Fiber (single/multi-mode)
- Coax (RG-6), RJ-45, LC, ST, SC
- Plenum vs Non-Plenum
- Transceivers: SFP, SFP+, QSFP

Domain 3: Network Operations (19%)

Documentation

- Network Diagrams: Physical (rack), Logical (VLAN, subnets)
- Inventory: Devices, firmware, warranty
- IPAM: IP address planning and tracking
- Change Management: Approval, rollback, tracking

Monitoring Tools

- SNMP (UDP 161/162), Syslog (UDP 514), NetFlow
- Port Mirroring (SPAN), Packet Capture (Wireshark)
- SIEM: Correlates and analyzes logs
- Baselines: Normal behavior reference

Disaster Recovery & Redundancy

- Backup Types: Full, Incremental, Differential
- Sites: Hot (live), Warm (partial), Cold (standby)
- RTO: Max downtime; RPO: Max data loss
- FHRP: VRRP, HSRP, GLBP
- Clustering, Load Balancing, UPS

Remote Access

- VPN Types: Site-to-site, Remote
- Protocols: IPsec, SSL, L2TP, GRE
- Split Tunneling vs Full Tunnel
- RDP (3389), SSH (22), Telnet (23, insecure)

Domain 4: Network Security (14%)

Security Concepts

- **CIA Triad:** Confidentiality, Integrity, Availability
- **AAA:** Authentication, Authorization, Accounting
- **Zero Trust:** Always verify
- **Defense in Depth:** Layered security

Device Hardening

- Disable unused ports/services
- Change default credentials
- Secure protocols: SSH, SNMPv3, HTTPS
- Update firmware and config backups

Access Control

- NAC (802.1X + RADIUS)
- Port security (limit MACs)
- ACLs: IP, port, protocol filtering
- VLAN segmentation

Common Attacks

- MAC Flooding, VLAN Hopping, ARP Poisoning
- Rogue DHCP and Evil Twin APs
- DoS/DDoS (volume, protocol, application layer)
- MITM: Packet interception or spoofing
- DHCP Snooping, Dynamic ARP Inspection: Countermeasures

Wireless Security

- WPA3 (SAE), WPA2 (AES), WEP (deprecated)
- 802.1X with RADIUS for enterprise authentication
- Disable WPS (vulnerable auto-connect feature)

Domain 5: Network Troubleshooting (24%)

Troubleshooting Methodology

1. Identify the problem
2. Establish a theory
3. Test the theory
4. Create a plan
5. Verify functionality
6. Document findings

Common Issues

- **Cabling:** Bad crimps, EMI, exceed distance, miswiring
- **DHCP:** No lease = APIPA (169.254.x.x)
- **DNS:** Can't resolve names → use nslookup
- **Routing:** No internet = check gateway, routing tables
- **Switching:** STP loop, blocked trunk, incorrect VLAN
- **Wireless:** Interference, weak signal, wrong key

Interface Errors

- CRC Errors: Bad cable/interference
- Late Collisions: Duplex mismatch
- High Jitter: Voice/video degradation
- Link Flapping: Faulty port or transceiver

Performance Metrics

- Latency: Delay
- Jitter: Variability
- Packet loss: Missing data
- Bandwidth: Capacity
- Throughput: Actual usage

Tools

- CLI: ping, tracert, ipconfig, netstat, arp, nslookup
- Packet: Wireshark, tcpdump
- Physical: Cable tester, TDR/OTDR, loopback plug
- Discovery: Nmap, SNMP scanners
- Visibility: Flow tools, Syslog, SIEM dashboards

Common Protocols and Port Numbers

Protocol	Port(s)	TCP/UDP	Use
FTP	20, 21	TCP	Insecure file transfer
SFTP	22	TCP	Secure file transfer over SSH
SSH	22	TCP	Secure remote CLI access
Telnet	23	TCP	Insecure remote terminal
SMTP	25	TCP	Sends email
DNS	53	TCP/UDP	Name resolution
DHCP	67, 68	UDP	IP address assignment
TFTP	69	UDP	Simple file transfer
HTTP	80	TCP	Unencrypted web traffic
POP3	110	TCP	Email retrieval
NTP	123	UDP	Time synchronization
IMAP	143	TCP	Email retrieval with folders
SNMP	161, 162	UDP	Network monitoring
LDAP	389	TCP/UDP	Directory access
HTTPS	443	TCP	Encrypted web traffic
SMB	445	TCP	File/printer sharing
LDAPS	636	TCP	Secure directory access
IMAPS	993	TCP	Secure IMAP email access
POP3S	995	TCP	Secure POP3 email retrieval
RDP	3389	TCP	Remote desktop
NetBIOS Name	137	UDP	Name resolution (legacy)
NetBIOS Datagram	138	UDP	File sharing broadcast
NetBIOS Session	139	TCP	Windows file sharing
Kerberos	88	TCP/UDP	Authentication
SMTPS	465	TCP	Secure email sending
Syslog	514	UDP	Device log forwarding