



COMPTIA

Network+ N10-009 — CompTIA

Network+

Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

BEGINNER

40 HOURS

5 DAYS

At a glance

COURSE	Network+ N10-009 — CompTIA Network+
TRACK	CompTIA
DOMAIN	Cyber Security
LEVEL	Beginner
DURATION	40 hours (about 5 days)
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is a beginner course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Five domains, mapped one-for-one to the CompTIA Network+ N10-009 exam objectives and taught in the same order, so nothing on the exam is left uncovered.

N10-009 is the current version. It launched on 20 June 2024 and has not been superseded; CompTIA retires an exam version roughly three years after launch, so N10-009 remains the exam you sit. Anything taught here is examinable.

The shape of N10-009 says something about the job. Troubleshooting is the heaviest domain at 24%, ahead of concepts, because the work is diagnosing a network somebody else built. Security has its own domain rather than being scattered, and cloud and software-defined networking now sit inside the core concepts instead of being treated as an advanced afterthought. Each domain below carries its published weighting, and we give it classroom time in proportion.

Roughly half the classroom time is hands-on. A meaningful share of the exam is performance-based — configuration and diagnosis in a simulated environment — so we practise in one rather than describing one.

Domain 01 — Networking Concepts

The model, the hardware, the addressing and the protocols that the other four domains all assume you already know. 23% of the exam.

- The OSI model layer by layer, and using it to place a fault or a control rather than to recite it
- Networking appliances: routers, switches, firewalls, IDS and IPS, load balancers, proxies, NAS and SAN
- Applications and functions — VPN headends, content delivery networks, quality of service, time to live
- Cloud concepts: network functions virtualisation, virtual private cloud, network security groups and lists, cloud gateways
- Deployment models — public, private, hybrid — and service models: SaaS, IaaS and PaaS
- Ports and protocols in common use, including FTP, SFTP, SSH, SMTP, DNS, DHCP, HTTP, HTTPS, SNMP, LDAP, RDP and SIP
- Traffic types — unicast, multicast, anycast and broadcast — and transmission media and transceivers from single-mode and multimode fibre to twisted pair and coaxial
- Network topologies and architectures: three-tier hierarchy, spine and leaf, collapsed core, and traffic flows
- IPv4 addressing, subnetting and CIDR, public against private ranges, APIPA and loopback, and IPv6 addressing concepts
- Modern network environments: SDN, SD-WAN, VXLAN, zero trust architecture and infrastructure as code

Domain 02 — Network Implementation

Actually building it: routing, switching, wireless and the physical layer underneath all of them. 20% of the exam.

- Routing technologies: static and dynamic routing, default routes, route selection and administrative distance
- Routing protocols — BGP, EIGRP, OSPF, RIP — and what distinguishes them in practice
- Address translation with NAT and PAT, and first hop redundancy protocols
- Virtual IP addressing, subinterfaces, and route summarisation
- Switching technologies: VLANs, trunking with 802.1Q, native VLANs and voice VLANs
- Spanning tree, link aggregation, port speed and duplex, MTU and jumbo frames
- Wireless standards and frequencies, channels and channel width, and regulatory impacts

- Wireless network types — mesh, ad hoc, point to point, infrastructure — and guest and captive portal deployment
- Antenna types, encryption standards, service set identifiers and BSSID, and RF profile planning
- Physical installations: cabling, patch panels, racks, power distribution, environmental controls and locking mechanisms

Domain 03 — Network Operations

Keeping a running network documented, monitored, patched and recoverable. 19% of the exam.

- Documentation: physical and logical diagrams, rack and wiring diagrams, IP address management, asset inventory and baseline configurations
- Site surveys, heat maps, and audit and assessment reports
- Lifecycle management: end of life, end of support, software management, and decommissioning
- Change management: request process, approval, implementation, validation and rollback
- Configuration management, version control, and keeping the documented state and the real state the same
- Network monitoring: SNMP, flow data, packet capture, log aggregation, and thresholds that generate useful alerts rather than noise
- Disaster recovery concepts: recovery time and recovery point objectives, mean time to repair and mean time between failures
- Recovery sites — cold, warm, hot and active-active — and testing the failover
- Network services: DHCP scopes and reservations, DNS record types and resolution, NTP and precision time protocol
- Access and management methods: VPN, SSH, graphical interfaces, API integration, console access, and in-band against out-of-band management

Domain 04 — Network Security

The smallest domain by weighting, and the one whose absence is most expensive. 14% of the exam.

- Logical security: encryption at rest and in transit, certificates, identity and access management
- Authentication methods and multifactor authentication, single sign-on, RADIUS, LDAP, SAML and TACACS+
- Authorisation models and least privilege applied to network devices
- Physical security: cameras, locks, and controlling access to network equipment
- Deception technologies — honeypots and honeynets — and what they are actually for
- Common security terminology: risk, vulnerability, exposure, threat, and the difference between them
- Audits, regulatory compliance, and data locality requirements
- Network segmentation and its uses: IoT and industrial systems, guest access, and screened subnets
- Attack types: denial of service and distributed denial of service, VLAN hopping, ARP spoofing, DNS poisoning, rogue access points, evil twin, on-path attacks, social engineering, malware
- Defence techniques: device hardening, network access control, port security, 802.1X, MAC filtering, key management and disabling unused services

Domain 05 — Network Troubleshooting

The heaviest domain, because diagnosing a network you did not build is the job. 24% of the exam.

- A structured troubleshooting methodology — identify, theorise, test, implement, verify, document — and why guessing costs more time than it saves

- Cable and physical interface issues: attenuation, interference, decibel loss, incorrect pinout, bad ports, opens and shorts
- Transceiver, duplex and speed mismatches, and reading interface counters as evidence
- Hardware faults, power over Ethernet problems and environmental causes
- Network service issues: DHCP scope exhaustion, incorrect gateway or subnet mask, DNS resolution failures, duplicate addresses and duplicate MAC addresses
- Performance issues: latency, jitter, packet loss, bottlenecks, and blocked or filtered traffic
- Routing and switching problems: routing loops, switching loops, missing routes, VLAN assignment and misconfigured ACLs
- Wireless issues: interference, channel overlap, insufficient coverage, client capability mismatch and roaming misconfiguration
- Hardware and software tools: protocol analysers, cable testers, toners, taps, Wi-Fi analysers and spectrum analysers
- Command line diagnostics — ping, traceroute, nslookup and dig, netstat, arp, ipconfig and ifconfig, tcpdump — and reading their output properly

Who should take this

Help desk and desktop support staff moving into infrastructure, junior network administrators and network support technicians, and anyone heading into security who needs the network fundamentals underneath it first. It also suits developers and cloud engineers who can build on a network but cannot diagnose one.

CompTIA recommends holding A+ first, plus nine to twelve months of hands-on experience in a junior network administrator or network support role. These are recommendations, not requirements — nothing prevents you from booking the exam without them. In practice, you will get more out of the week if you are already comfortable with basic PC and operating system administration.

The exam

The Network+ is set and awarded by CompTIA, and delivered at a Pearson VUE test centre or by online proctor.

- A maximum of 90 questions, 90 minutes
- Multiple-choice and performance-based questions, the latter scored on what you do in a simulated environment
- A scaled score of 720 out of 100 to 900 is required to pass
- Available in English, German, Japanese, Portuguese and Spanish

The exam voucher is purchased separately from CompTIA. We arrange it on your behalf and send you the code, and you book your own exam date. The certification is valid for three years and is renewed through CompTIA's continuing education programme.

How we deliver it

Five days, classroom or online live, or at your office for a private group. Roughly half the time is hands-on — subnetting drills until they are quick, switch and router configuration, wireless survey work, and fault-finding against a lab estate we have broken on purpose. Dedicated practice at performance-based question formats, domain checkpoints each day, and a full-length timed mock under exam conditions on the final afternoon.

Mapped to the CompTIA Network+ N10-009 exam objectives. Taught from Hacky Security's own curriculum and lab estate by instructors who build and run production networks.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 · info@hackysecurity.com

<https://hackysecurity.com/courses/network-plus/>

CHANDIGARH · SHIMLA · DELHI · DUBAI · LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 11 September 2026.