Printed from LandTechJobs.com – Information Sourced from the CompTIA Website for the Network+ N10-009 Exam

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

CompTIA Network+ Exam Objectives - N10-009

1.0 Networking Fundamentals

1.1 Explain concepts related to the Open Systems Interconnection (OSI) reference model.

- OSI Model
    - Layer 1 – Physical
    - Layer 2 – Data link
    - Layer 3 – Network
    - Layer 4 – Transport
    - Layer 5 – Session
    - Layer 6 – Presentation
    - Layer 7 – Application

1.2 Compare and contrast networking appliances, applications, and functions.

- Physical and virtual appliances
    - - Router
    - - Switch
    - - Firewall
    - - Intrusion detection system (IDS)/intrusion prevention system (IPS)
    - - Load balancer
    - - Proxy
    - - Network-attached storage (NAS)
    - - Storage area network (SAN)
- - Wireless
    - o Access point (AP)
    - o Controller
- • Applications
    - - Content delivery network (CDN)
- • Functions
    - - Virtual private network (VPN)
    - - Quality of service (QoS)
    - - Time to live (TTL)

1.3 Summarize cloud concepts and connectivity options.

Printed from LandTechJobs.com – Information Sourced from the CompTIA Website for the Network+ N10-009 Exam

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- Network functions virtualization
- (NFV)
- • Virtual private cloud (VPC)
- • Network security groups
- • Network security lists
- • Cloud gateways
    - - Internet gateway
    - - Network address translation (NAT) gateway
- • Cloud connectivity options
    - - VPN
    - - Direct Connect
- • Deployment models
    - - Public
    - - Private
    - - Hybrid
- • Service models
    - - Software as a service (SaaS)
    - - Infrastructure as a service (IaaS)
    - - Platform as a service (PaaS)
- • Scalability
- • Elasticity
- • Multitenancy

1.4 Explain common networking ports, protocols, services, and traffic types.

- Protocols Ports
    - File Transfer Protocol (FTP) 20/21
    - Secure File Transfer Protocol (SFTP) 22
    - Secure Shell (SSH) 22
    - Telnet 23
    - Simple Mail Transfer Protocol (SMTP) 25
    - Domain Name System (DNS) 53
    - Dynamic Host Configuration Protocol (DHCP) 67/68
    - Trivial File Transfer Protocol (TFTP) 69
    - Hypertext Transfer Protocol (HTTP) 80
    - Network Time Protocol (NTP) 123
    - Simple Network Management Protocol (SNMP) 161/162
    - Lightweight Directory Access Protocol (LDAP) 389
    - Hypertext Transfer Protocol Secure (HTTPS) 443

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- Server Message Block (SMB) 445
- Syslog 514
- Simple Mail Transfer Protocol Secure (SMTPS) 587
- Lightweight Directory Access Protocol over SSL (LDAPS) 636
- Structured Query Language (SQL) Server 1433
- Remote Desktop Protocol (RDP) 3389
- Session Initiation Protocol (SIP) 5060/5061

- • Internet Protocol (IP) types
  - - Internet Control Message Protocol (ICMP)
  - - Transmission Control Protocol (TCP)
  - - User Datagram Protocol (UDP)
  - - Generic Routing Encapsulation (GRE)
  - - Internet Protocol Security (IPSec)
    - o Authentication Header (AH)
    - o Encapsulating Security Payload (ESP)
    - o Internet Key Exchange (IKE)
- • Traffic types
  - - Unicast
  - - Multicast
  - - Anycast
  - - Broadcast

1.5 Compare and contrast transmission media and transceivers.

- • Wireless
  - - 802.11 standards
  - - Cellular
  - - Satellite
- • Wired
  - - 802.3 standards
  - - Single-mode vs. multimode fiber
  - - Direct attach copper (DAC) cable
    - o Twinaxial cable
  - - Coaxial cable
  - - Cable speeds
  - - Plenum vs. non-plenum cable
- • Transceivers
  - - Protocol
    - o Ethernet

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

        - o Fibre Channel (FC)
- - Form factors
    - o Small form-factor pluggable (SFP)
    - o Quad small form-factor pluggable (QSFP)
- • Connector types
    - - Subscriber connector (SC)
    - - Local connector (LC)
    - - Straight tip (ST)
    - - Multi-fiber push on (MPO)
    - - Registered jack (RJ)11
    - - RJ45
    - - F-type
    - - Bayonet Neill–Concelman (BNC)

1.6 Compare and contrast network topologies, architectures, and types.

- Mesh
- • Hybrid
- • Star/hub and spoke
- • Spine and leaf
- • Point to point
- • Three-tier hierarchical model
    - - Core
    - - Distribution
    - - Access
- • Collapsed core
- • Traffic flows
    - - North-south
    - - East-west

1.7 Given a scenario, use appropriate IPv4 network addressing.

- Public vs. private
    - - Automatic Private IP Addressing (APIPA)
    - - RFC1918
    - - Loopback/localhost
- • Subnetting
    - - Variable Length Subnet Mask (VLSM)
    - - Classless Inter-domain Routing (CIDR)
- • IPv4 address classes

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- - Class A
- - Class B
- - Class C
- - Class D
- - Class E

1.8 Summarize evolving use cases for modern network environments.

- Software-defined network (SDN) and software-defined wide area network (SD-WAN)
  - - Application aware
  - - Zero-touch provisioning
  - - Transport agnostic
  - - Central policy management
- • Virtual Extensible Local Area Network (VXLAN)
  - - Data center interconnect (DCI)
  - - Layer 2 encapsulation
- • Zero trust architecture (ZTA)
  - - Policy-based authentication
  - - Authorization
  - - Least privilege access
- • Secure Access Secure Edge (SASE)/Security Service Edge (SSE)
- • Infrastructure as code (IaC)
  - - Automation
    - o Playbooks/templates/reusable tasks
    - o Configuration drift/compliance
    - o Upgrades
    - o Dynamic inventories
  - - Source control
    - o Version control
    - o Central repository
    - o Conflict identification
    - o Branching
- • IPv6 addressing
  - - Mitigating address exhaustion
  - - Compatibility requirements
    - o Tunneling
    - o Dual stack
    - o NAT64

2.0 Network Implementation

Printed from LandTechJobs.com – Information Sourced from the CompTIA Website for the Network+ N10-009 Exam

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

2.1 Explain characteristics of routing technologies.

- Static routing
- • Dynamic routing
    - - Border Gateway Protocol (BGP)
    - - Enhanced Interior Gateway Routing Protocol (EIGRP)
    - - Open Shortest Path First (OSPF)
- • Route selection
    - - Administrative distance
    - - Prefix length
    - - Metric
- • Address translation
    - - NAT
    - - Port address translation (PAT)
- • First Hop Redundancy Protocol (FHRP)
- • Virtual IP (VIP)
- • Subinterfaces

2.2 Given a scenario, configure switching technologies and features.

- Virtual Local Area Network (VLAN)
    - - VLAN database
    - - Switch Virtual Interface (SVI)
- • Interface configuration
    - - Native VLAN
    - - Voice VLAN
    - - 802.1Q tagging
    - - Link aggregation
    - - Speed
    - - Duplex
- • Spanning tree
- • Maximum transmission unit (MTU)
    - - Jumbo frames

2.3 Given a scenario, select and configure wireless devices and Technologies.

- Channels
    - - Channel width
    - - Non-overlapping channels
    - - Regulatory impacts

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

        - o 802.11h
- • Frequency options
    - - 2.4GHz
    - - 5GHz
    - - 6GHz
    - - Band steering
- • Service set identifier (SSID)
    - - Basic service set identifier (BSSID)
    - - Extended service set identifier (ESSID)
- • Network types
    - - Mesh networks
    - - Ad hoc
    - - Point to point
    - - Infrastructure
- • Encryption
    - - Wi-Fi Protected Access 2 (WPA2)
    - - WPA3
- • Guest networks
    - - Captive portals
- • Authentication
    - - Pre-shared key (PSK) vs. Enterprise
- • Antennas
    - - Omnidirectional vs. directional
- • Autonomous vs. lightweight access point

2.4 Explain important factors of physical installations.

- • Important installation implications
    - - Locations
        - o Intermediate distribution frame (IDF)
        - o Main distribution frame (MDF)
- - Rack size
- - Port-side exhaust/intake
- - Cabling
    - o Patch panel
    - o Fiber distribution panel
- - Lockable

- • Power
    - - Uninterruptible power supply (UPS)
    - - Power distribution unit (PDU)

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- - Power load
- - Voltage

- • Environmental factors
  - - Humidity
  - - Fire suppression
  - - Temperature

3.0 Network Operations

3.1 Explain the purpose of organizational processes and procedures

- Documentation
- - Physical vs. logical diagrams
- - Rack diagrams
- - Cable maps and diagrams
- - Network diagrams
  - o Layer 1
  - o Layer 2
  - o Layer 3
- - Asset inventory
  - o Hardware
  - o Software
  - o Licensing
  - o Warranty support
- - IP address management (IPAM)
- - Service-level agreement (SLA)
- - Wireless survey/heat map

- • Life-cycle management
  - - End-of-life (EOL)
  - - End-of-support (EOS)
  - - Software management
    - o Patches and bug fixes
    - o Operating system (OS)
    - o Firmware
- - Decommissioning

- • Change management
  - - Request process tracking/service request

Printed from LandTechJobs.com – Information Sourced from the CompTIA Website for the Network+ N10-009 Exam

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- • Configuration management
    - - Production configuration
    - - Backup configuration
    - - Baseline/golden configuration

3.2 Given a scenario, use network monitoring technologies

- Methods
    - - SNMP
        - o Traps
        - o Management information base (MIB)
        - o Versions
            - o v2c
            - o v3
        - o Community strings
        - o Authentication
- - Flow data
- - Packet capture
- - Baseline metrics
    - o Anomaly alerting/notification
- - Log aggregation
    - o Syslog collector
    - o Security information and event management (SIEM)
- - Application programming interface (API) integration
- - Port mirroring

- • Solutions
    - - Network discovery
        - o Ad hoc
        - o Scheduled
    - - Traffic analysis
    - - Performance monitoring
    - - Availability monitoring
    - - Configuration monitoring

3.3 Explain disaster recovery (DR) concepts

- DR metrics
    - - Recovery point objective (RPO)
    - - Recovery time objective (RTO)
    - - Mean time to repair (MTTR)

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- - Mean time between failures (MTBF)
- • DR sites
  - - Cold site
  - - Warm site
  - - Hot site
- • High-availability approaches
  - - Active-active
  - - Active-passive
- • Testing
  - - Tabletop exercises
  - - Validation tests

3.4 Given a scenario, implement IPv4 and IPv6 network services

- Dynamic addressing
  - - DHCP
    - o Reservations
    - o Scope
    - o Lease time
    - o Options
    - o Relay/IP helper
    - o Exclusions
    - - Stateless address autoconfiguration (SLAAC)

- • Name resolution
  - - DNS
    - o Domain Name Security Extensions (DNSSEC)
    - o DNS over HTTPS (DoH) and DNS over TLS (DoT)
    - o Record types
      - o Address (A)
      - o AAAA
      - o Canonical name (CNAME)
      - o Mail exchange (MX)
      - o Text (TXT)
      - o Nameserver (NS)
      - o Pointer (PTR)
  - o Zone types
    - o Forward
    - o Reverse
  - o Authoritative vs. non-authoritative
  - o Primary vs. secondary

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- o Recursive
- - Hosts file

- • Time protocols
  - - NTP
  - - Precision Time Protocol (PTP)
  - - Network Time Security (NTS)

3.5 Compare and contrast network access management methods

- • Site-to-site VPN
- • Client-to-site VPN
  - - Clientless
  - - Split tunnel vs. full tunnel
- • Connection methods
  - - SSH
  - - Graphical user interface (GUI)
  - - API
  - - Console
- • Jump box/host
- • In-band vs. out-of-band management

4.0 Network Security

4.1 Explain the importance of basic network security concepts.

- Logical security
  - - Encryption
- o Data in transit
- o Data at rest
  - - Certificates
- o Public key infrastructure (PKI)
- o Self-signed
  - - Identity and access management (IAM)
- o Authentication
  - o Multifactor authentication (MFA)
  - o Single sign-on (SSO)
  - o Remote Authentication Dial-in User Service (RADIUS)
  - o LDAP
  - o Security Assertion Markup Language (SAML)
  - o Terminal Access Controller Access Control System Plus (TACACS+)

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

        - o Time-based authentication
- o Authorization
    - o Least privilege
    - o Role-based access control
- - Geofencing

- • Physical security
    - - Camera
    - - Locks

- • Deception technologies
    - - Honeypot
    - - Honeynet

- • Common security terminology
    - - Risk
    - - Vulnerability
    - - Exploit
    - - Threat
    - - Confidentiality, Integrity, and Availability (CIA) triad

- • Audits and regulatory compliance
    - - Data locality
    - - Payment Card Industry Data Security Standards (PCI DSS)
    - - General Data Protection Regulation (GDPR)

- • Network segmentation enforcement
    - - Internet of Things (IoT) and Industrial Internet of Things (IIoT)
    - - Supervisory control and data acquisition (SCADA), industrial control System (ICS), operational technology (OT)
- - Guest
- - Bring your own device (BYOD)

4.2 Summarize various types of attacks and their impact to the network

- Denial-of-service (DoS)/
- distributed denial-of-service
- (DDoS)
- • VLAN hopping
- • Media Access Control (MAC)

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- flooding
- • Address Resolution Protocol
- (ARP) poisoning
- • ARP spoofing
- • DNS poisoning
- • DNS spoofing
- • Rogue devices and services
    - - DHCP
    - - AP
- • Evil twin
- • On-path attack
- • Social engineering
    - - Phishing
    - - Dumpster diving
    - - Shoulder surfing
    - - Tailgating
- • Malware

4.3 Given a scenario, apply network security features, defense techniques, and solutions.

- Device hardening
    - - Disable unused ports and Services
    - - Change default passwords

- • Network access control (NAC)
    - - Port security
    - - 802.1X
    - - MAC filtering

- • Key management
- • Security rules

    - - Access control list (ACL)
    - - Uniform Resource Locator (URL) filtering
    - - Content filtering

- • Zones

    - - Trusted vs. untrusted
    - - Screened subnet

Printed from LandTechJobs.com – Information Sourced from the CompTIA Website for the Network+ N10-009 Exam

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

5.0 Network Security

5.1 Explain the troubleshooting methodology

- • Identify the problem
  - - Gather information
  - - Question users
  - - Identify symptoms
  - - Determine if anything has changed
  - - Duplicate the problem, if possible
  - - Approach multiple problems individually
- • Establish a theory of probable cause
  - - Question the obvious
  - - Consider multiple approaches
    - o Top-to-bottom/bottom-to-top OSI model
    - o Divide and conquer
- • Test the theory to determine the cause
  - - If theory is confirmed, determine next steps to resolve problem
  - - If theory is not confirmed, establish a new theory or escalate
- • Establish a plan of action to resolve the problem and identify potential effects
- • Implement the solution or escalate as necessary
- • Verify full system functionality and implement preventive measures if applicable
- • Document findings, actions, outcomes, and lessons learned throughout the process

5.2 Given a scenario, troubleshoot common cabling and physical interface issues.

- • Cable issues
  - - Incorrect cable
    - o Single mode vs. multimode
    - o Category 5/6/7/8
    - o Shielded twisted pair (STP) vs. unshielded twisted pair (UTP)
  - - Signal degradation
    - o Crosstalk
    - o Interference
    - o Attenuation
  - - Improper termination
  - - Transmitter (TX)/Receiver (RX) transposed
- • Interface issues
  - - Increasing interface counters

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- o Cyclic redundancy check (CRC)
- o Runts
- o Giants
- o Drops
- - Port status
  - o Error disabled
  - o Administratively down
  - o Suspended
- • Hardware issues
  - - Power over Ethernet (PoE)
    - o Power budget exceeded
    - o Incorrect standard
  - - Transceivers
    - o Mismatch
    - o Signal strength

5.3 Given a scenario, troubleshoot common issues with network services.

- Switching issues
  - - STP
    - o Network loops
    - o Root bridge selection
    - o Port roles
    - o Port states
  - - Incorrect VLAN assignment
  - - ACLs
- • Route selection
  - - Routing table
  - - Default routes
- • Address pool exhaustion
- • Incorrect default gateway
- • Incorrect IP address
  - - Duplicate IP address
- • Incorrect subnet mask

5.4 Given a scenario, troubleshoot common performance issues.

- Congestion/contention
- • Bottlenecking
- • Bandwidth

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- - Throughput capacity
- • Latency
- • Packet loss
- • Jitter
- • Wireless
  - - Interference
    - o Channel overlap
- - Signal degradation or loss
- - Insufficient wireless coverage
- - Client disassociation issues
- - Roaming misconfiguration

5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues

- Software tools
  - - Protocol analyzer
  - - Command line
    - o ping
    - o traceroute/tracert
    - o nslookup
    - o tcpdump
    - o dig
    - o netstat
    - o ip/ifconfig/ipconfig
    - o arp
    - - Nmap
    - - Link Layer Discovery Protocol (LLDP)/Cisco Discovery Protocol (CDP)
  - - Speed tester
- • Hardware tools
  - - Toner
  - - Cable tester
  - - Taps
  - - Wi-Fi analyzer
  - - Visual fault locator

- • Basic networking device commands
  - - show mac-address-table
  - - show route
  - - show interface
  - - show config

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- - show arp
- - show vlan
- - show power

ACRONYMS:

- **MAC**
- **MDF**
- **MDIX**
- **MFA**
- **MIB**
- **MPO**
- **MTBF**
- **MTTR**
- **MTU**
- **MX**
- **NAC**
- **NAS**
- **NAT**
- **NFV**
- **NIC**
- **NS**
- **NTP**
- **NTS**

Printed from LandTechJobs.com – Information Sourced from the CompTIA Website for the Network+ N10-009 Exam

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- **OS**
- **OSPF**
- **OSI**
- **OT**
- **PaaS**
- **PAT**
- **PCI DSS**
- **PDU**
- **PKI**
- **PoE**
- **PSK**
- **PTP**
- **PTR**
- **QoS**
- **QSFP**
- **RADIUS**
- **RDP**
- **RFID**
- **RIP**
- **RJ**

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- **RPO**
- **RSTP**
- **RTO**
- **RX**
- **SaaS**
- **SAML**
- **SAN**
- **SASE**
- **SC**
- **SCADA**
- **SDN**
- **SD-WAN**
- **SFP**
- **SFTP**
- **SIP**
- **SIEM**
- **SLA**
- **SLAAC**
- **SMB**
- **SMTP**
- **SMTPS**

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- **SNMP**
- **SOA**
- **SQL**
- **SSE**
- **SSH**
- **SSID**
- **SSL**
- **SSO**
- **ST**
- **STP**
- **SVI**
- **TACAS+**
- **TCP**
- **TFTP**
- **TTL**
- **TX**
- **TXT**
- **UDP**
- **UPS**
- **URL**

We recommend all candidates write in two to three sentences for each objective, and check them off as they go.

- **USB**
- **UTM**
- **UTP**
- **VIP**
- **VLAN**
- **VLSM**
- **VoIP**
- **VPC**
- **VPN**
- **WAN**
- **WPA Wi-Fi**
- **WPS Wi-Fi**
- **VXLAN**
- **ZTA**