Certification Exam Objectives: N10-005

INTRODUCTION

The CompTIA Network+ certification is an internationally recognized validation of the technical knowledge required of foundation-level IT network practitioners.

Test Purpose: This exam will certify that the successful candidate has the knowledge and skills required to implement a defined network architecture with basic network security. Furthermore, a successful candidate will be able to configure, maintain, and troubleshoot network devices using appropriate network tools and understand the features and purpose of network technologies. Candidates will be able to make basic solution recommendations, analyze network traffic, and be familiar with common protocols and media types.

CompTIA Network+ is accredited by ANSI to show compliance with the ISO 17024 Standard and, as such, undergoes regular reviews and updates to the exam objectives.

It is recommended for CompTIA Network+ candidates to have the following:

- CompTIA A+ certification or equivalent knowledge, though CompTIA A+ certification is not required.
- Have at least 9 to 12 months of work experience in IT networking.

The table below lists the domains measured by this examination and the extent to which they are represented. CompTIA Network+ exams are based on these objectives.

Domain	% of Examination
1.0 Network Concepts	21%
2.0 Network Installation and Configuration	23%
3.0 Network Media and Topologies	17%
4.0 Network Management	20%
5.0 Network Security	19%
Total	**100%**

**Note: The bulleted lists below each objective are not exhaustive lists. Even though they are not included in this document, other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam.

(A list of acronyms used in these objectives appears at the end of this document.)

1.0 Networking Concepts

1.1 Compare the layers of the OSI and TCP/IP models.

- OSI model:
  - Layer 1 – Physical
  - Layer 2 – Data link
  - Layer 3 – Network
  - Layer 4 – Transport
  - Layer 5 – Session
  - Layer 6 – Presentation
  - Layer 7 – Application
- TCP/IP model:
  - Network Interface Layer
  - Internet Layer
  - Transport Layer
  - Application Layer
    - (Also described as: Link Layer, Internet Layer, Transport Layer, Application Layer)

1.2 Classify how applications, devices, and protocols relate to the OSI model layers.

- MAC address
- IP address
- EUI-64
- Frames
- Packets
- Switch
- Router
- Multilayer switch
- Hub
- Encryption devices
- Cable
- NIC
- Bridge

1.3 Explain the purpose and properties of IP addressing.

- Classes of addresses
  - A, B, C and D
  - Public vs. Private
- Classless (CIDR)
- IPv4 vs. IPv6 (formatting)

- MAC address format
- Subnetting
- Multicast vs. unicast vs. broadcast
- APIPA

1.4 Explain the purpose and properties of routing and switching.

- EIGRP
- OSPF
- RIP
- Link state vs. distance vector vs. hybrid
- Static vs. dynamic
- Routing metrics
    - Hop counts
    - MTU, bandwidth
    - Costs
    - Latency
- Next hop
- Spanning-Tree Protocol
- VLAN (802.1q)
- Port mirroring
- Broadcast domain vs. collision domain
- IGP vs. EGP
- Routing tables
- Convergence (steady state)

1.5 Identify common TCP and UDP default ports.

- SMTP – 25
- HTTP – 80
- HTTPS – 443
- FTP – 20, 21
- TELNET – 23
- IMAP – 143
- RDP – 3389
- SSH – 22
- DNS – 53
- DHCP – 67, 68

1.6 Explain the function of common networking protocols.

- TCP
- FTP
- UDP
- TCP/IP suite

- DHCP
- TFTP
- DNS
- HTTPS
- HTTP
- ARP
- SIP (VoIP)
- RTP (VoIP)
- SSH
- POP3
- NTP
- IMAP4
- Telnet
- SMTP
- SNMP2/3
- ICMP
- IGMP
- TLS

1.7 Summarize DNS concepts and its components.

- DNS servers
- DNS records (A, MX, AAAA, CNAME, PTR)
- Dynamic DNS

1.8 Given a scenario, implement the following network troubleshooting methodology:

- Identify the problem:
  - Information gathering
  - Identify symptoms
  - Question users
  - Determine if anything has changed
- Establish a theory of probable cause
  - Question the obvious
- Test the theory to determine cause:
  - Once theory is confirmed determine next steps to resolve problem.
  - If theory is not confirmed, re-establish 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 if applicable implement preventative measures
- Document findings, actions and outcomes

1.9 Identify virtual network components.

- Virtual switches
- Virtual desktops
- Virtual servers
- Virtual PBX
- Onsite vs. offsite
- Network as a Service (NaaS)

2.0 Network Installation and Configuration

2.1 Given a scenario, install and configure routers and switches.

- Routing tables
- NAT
- PAT
- VLAN (trunking)
- Managed vs. unmanaged
- Interface configurations
  - Full duplex
  - Half duplex
  - Port speeds
  - IP addressing
  - MAC filtering
- PoE
- Traffic filtering
- Diagnostics
- VTP configuration
- QoS
- Port mirroring

2.2 Given a scenario, install and configure a wireless network.

- WAP placement
- Antenna types
- Interference
- Frequencies
- Channels
- Wireless standards
- SSID (enable/disable)

- Compatibility (802.11 a/b/g/n)

2.3 Explain the purpose and properties of DHCP.

- Static vs. dynamic IP addressing
- Reservations
- Scopes
- Leases
- Options (DNS servers, suffixes)

2.4 Given a scenario, troubleshoot common wireless problems.

- Interference
- Signal strength
- Configurations
- Incompatibilities
- Incorrect channel
- Latency
- Encryption type
- Bounce
- SSID mismatch
- Incorrect switch placement

2.5 Given a scenario, troubleshoot common router and switch problems.

- Switching loop
- Bad cables/improper cable types
- Port configuration
- VLAN assignment
- Mismatched MTU/MUT black hole
- Power failure
- Bad/missing routes
- Bad modules (SFPs, GBICs)
- Wrong subnet mask
- Wrong gateway
- Duplicate IP address
- Wrong DNS

2.6 Given a set of requirements, plan and implement a basic SOHO network.

- List of requirements
- Cable length
- Device types/requirements
- Environment limitations
- Equipment limitations
- Compatibility requirements

3.0 Network Media and Topologies

3.1 Categorize standard media types and associated properties.

- Fiber:
  - Multimode
  - Singlemode
- Copper:
  - UTP
  - STP
  - CAT3
  - CAT5
  - CAT5e
  - CAT6
  - CAT6a
  - Coaxial
  - Crossover
  - T1 Crossover
  - Straight-through
- Plenum vs. non-plenum
- Media converters:
  - Singlemode fiber to Ethernet
  - Multimode fiber to Ethernet
  - Fiber to Coaxial
  - Singlemode to multimode fiber
- Distance limitations and speed limitations
- Broadband over powerline

3.2 Categorize standard connector types based on network media.

- Fiber:
  - ST
  - SC
  - LC
  - MTRJ
- Copper:
  - RJ-45
  - RJ-11
  - BNC
  - F-connector
  - DB-9 (RS-232)

    - Patch panel
    - 110 block (T568A, T568B)

3.3 Compare and contrast different wireless standards.

- 802.11 a/b/g/n standards
    - Distance
    - Speed
    - Latency
    - Frequency
    - Channels
    - MIMO
    - Channel bonding

3.4 Categorize WAN technology types and properties.

- Types:
    - T1/E1
    - T3/E3
    - DS3
    - OCx
    - SONET
    - SDH
    - DWDM
    - Satellite
    - ISDN
    - Cable
    - DSL
    - Cellular
    - WiMAX
    - LTE
    - HSPA+
    - Fiber
    - Dialup
    - PON
    - Frame relay
    - ATMs
- Properties:
    - Circuit switch
    - Packet switch
    - Speed
    - Transmission media
    - Distance

3.5 Describe different network topologies.

- MPLS
- Point-to-point
- Point-to-multipoint
- Ring
- Star
- Mesh
- Bus
- Peer-to-peer
- Client-server
- Hybrid

3.6 Given a scenario, troubleshoot common physical connectivity problems.

- Cable problems:
  - Bad connectors
  - Bad wiring
  - Open, short
  - Split cables
  - dB loss
  - TXRX reversed
  - Cable placement
  - EMI/Interference
  - Distance
  - Cross-talk

3.7 Compare and contrast different LAN technologies.

- Types:
  - Ethernet
  - 10BaseT
  - 100BaseT
  - 1000BaseT
  - 100BaseTX
  - 100BaseFX
  - 1000BaseX
  - 10GBaseSR
  - 10GBaseLR
  - 10GBaseER
  - 10GBaseSW
  - 10GBaseLW
  - 10GBaseEW
  - 10GBaseT
- Properties:
  - CSMA/CD

    - CSMA/CA
    - Broadcast
    - Collision
    - Bonding
    - Speed
    - Distance

3.8 Identify components of wiring distribution.

- IDF
- MDF
- Demarc
- Demarc extension
- Smart jack
- CSU/DSU

4.0 Network Management

4.1 Explain the purpose and features of various network appliances.

- Load balancer
- Proxy server
- Content filter
- VPN concentrator

4.2 Given a scenario, use appropriate hardware tools to troubleshoot connectivity issues.

- Cable tester
- Cable certifier
- Crimper
- Butt set
- Toner probe
- Punch down tool
- Protocol analyzer
- Loop back plug
- TDR
- OTDR
- Multimeter
- Environmental monitor

4.3 Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

- Protocol analyzer
- Throughput testers

- Connectivity software
- Ping
- Tracert/traceroute
- Dig
- Ipconfig/ifconfig
- Nslookup
- Arp
- Nbtstat
- Netstat
- Route

4.4 Given a scenario, use the appropriate network monitoring resource to analyze traffic.

- SNMP
- SNMPv2
- SNMPv3
- Syslog
- System logs
- History logs
- General logs
- Traffic analysis
- Network sniffer

4.5 Describe the purpose of configuration management documentation.

- Wire schemes
- Network maps
- Documentation
- Cable management
- Asset management
- Baselines
- Change management

4.6 Explain different methods and rationales for network performance optimization.

- Methods:
  - QoS
  - Traffic shaping
  - Load balancing
  - High availability
  - Caching engines
  - Fault tolerance
  - CARP

- Reasons:
    - Latency sensitivity
    - High bandwidth applications (VoIP, video applications, unified communications)
    - Uptime

5.0 Network Security

5.1 Given a scenario, implement appropriate wireless security measures.

- Encryption protocols:
    - WEP
    - WPA
    - WPA2
    - WPA Enterprise
- MAC address filtering
- Device placement
- Signal strength

5.2 Explain the methods of network access security.

- ACL:
    - MAC filtering
    - IP filtering
    - Port filtering
- Tunneling and encryption:
    - SSL VPN
    - VPN
    - L2TP
    - PPTP
    - IPSec
    - ISAKMP
    - TLS
    - TLS1.2
    - Site-to-site and client-to-site
- Remote access:
    - RAS
    - RDP
    - PPPoE
    - PPP
    - ICA
    - SSH

5.3 Explain methods of user authentication.

    - PKI
    - Kerberos
    - AAA (RADIUS, TACACS+)
    - Network access control (802.1x, posture assessment)
    - CHAP
    - MS-CHAP
    - EAP
    - Two-factor authentication
    - Multifactor authentication
    - Single sign-on

5.4 Explain common threats, vulnerabilities, and mitigation techniques.

- Wireless:
    - War driving
    - War chalking
    - WEP cracking
    - WPA cracking
    - Evil twin
    - Rogue access point
- Attacks:
    - DoS
    - DDoS
    - Man in the middle
    - Social engineering
    - Virus
    - Worms
    - Buffer overflow
    - Packet sniffing
    - FTP bounce
    - Smurf
- Mitigation techniques:
    - Training and awareness
    - Patch management
    - Policies and procedures
    - Incident response

5.5 Given a scenario, install and configure a basic firewall.

- Types:
    - Software and hardware firewalls
- Port security
- Stateful inspection vs. packet filtering
- Firewall rules:

    - Block/allow
    - Implicit deny
    - ACL
- NAT/PAT
- DMZ

5.6 Categorize different types of network security appliances and methods.

- IDS and IPS:
    - Behavior based
    - Signature based
    - Network based
    - Host based
- Vulnerability scanners:
    - Nessus
    - Nmap
- Methods:
    - Honeypots
    - Honeynets

Network+ Acronym List

AAA	Authentication Authorization and Accounting
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AH	Authentication Header
AM	Amplitude Modulation
APIPA	Automatic Private Internet Protocol Addressing
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
BERT	Bit-Error Rate Test
BGP	Border Gateway Protocol
BNC	British Naval Connector / Bayonet Niell-Concelman
BootP	Boot Protocol /Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CARP	Common Address Redundancy Protocol
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless inter domain routing
CNAME	Canonical Name
CRAM-MD5	Challenge-Response Authentication Mechanism – Message Digest 5
CSMA / CA	Carrier Sense Multiple Access / Collision Avoidance
CSMA / CD	Carrier Sense Multiple Access / Collision Detection
CSU	Channel Service Unit
dB	decibels
DHCP	Dynamic Host Configuration Protocol
DLC	Data Link Control

DMZ	Demilitarized Zone
DNS	Domain Name Service / Domain Name Server / Domain Name System
DOCSIS	Data-Over-Cable Service Interface Specification
DoS	Denial of Service
DDoS	Distributed Denial of Service
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
DSU	Data Service Unit
DWDM	Dense Wavelength Division Multiplexing
E1	E-Carrier Level 1
EAP	Extensible Authentication Protocol
EDNS	Extension Mechanisms for DNS
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
ESSID	Extended Service Set Identifier
ESP	Encapsulated security packets
FDDI	Fiber Distributed Data Interface
FDM	Frequency Division Multiplexing
FHSS	Frequency Hopping Spread Spectrum
FM	Frequency Modulation
FQDN	Fully Qualified Domain Name / Fully Qualified Distinguished Name
FTP	File Transfer Protocol
GBIC	Gigabit Interface Converter
Gbps	Giga bits per second
GPG	GNU Privacy Guard
HDLC	High-Level Data Link Control
HIDS	Host Intrusion Detection System

HIPS	Host Intrusion Prevention System
HSPA	High Speed Packet Access
HSRP	Hot Standby Router Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
Hz	Hertz
IANA	Internet Assigned Numbers Authority
ICA	Independent Computer Architecture
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
ICS	Internet Connection Sharing
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Multicast Protocol
IGP	Interior Gateway Protocol
IIS	Internet Information Services
IKE	Internet Key Exchange
IMAP4	Internet Message Access Protocol version 4
InterNIC	Internet Network Information Center
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology

IV	Initialization Vector
Kbps	Kilobits per second
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LACP	Link aggregation control protocol
LAN	Local Area Network
LC	Local Connector
LDAP	Lightweight Directory Access Protocol
LEC	Local Exchange Carrier
LED	Light Emitting Diode
LLC	Logical Link Control
MAC	Media Access Control / Medium Access Control
Mbps	Megabits per second
MBps	Megabytes per second
MDF	Main Distribution Frame
MDI	Media Dependent Interface
MDIX	Media Dependent Interface Crossover
MIB	Management Information Base
MIMO	Multiple Input, Multiple Output
MMF	Multimode Fiber
MPLS	Multi-Protocol Label Switching
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MT-RJ	Mechanical Transfer-Registered Jack
MX	Mail Exchanger
NAC	Network Access Control
NaaS	Network as a Service
NAS	Network Attached Storage
NAT	Network Address Translation
NCP	Network Control Protocol

NetBEUI	Network Basic Input / Output Extended User Interface
NetBIOS	Network Basic Input / Output System
NFS	Network File Service
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
nm	Nanometer
NNTP	Network News Transport Protocol
NTP	Network Time Protocol
NWLINK	Microsoft IPX/SPX Protocol
OCx	Optical Carrier
OS	Operating Systems
OSI	Open Systems Interconnect
OSPF	Open Shortest Path First
OTDR	Optical Time Domain Reflectometer
PAP	Password Authentication Protocol
PAT	Port Address Translation
PC	Personal Computer
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PoE	Power over Ethernet
POP3	Post Office Protocol version 3
POTS	Plain Old Telephone System
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network

PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RARP	Reverse Address Resolution Protocol
RAS	Remote Access Service
RDP	Remote Desktop Protocol
RFI	Radio Frequency Interface
RG	Radio Guide
RIP	Routing Internet Protocol
RJ	Registered Jack
RSA	Rivest, Shamir, Adelman
RSH	Remote Shell
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
RTT	Round Trip Time or Real Transfer Time
SA	Security Association
SC	Standard Connector / Subscriber Connector
SCP	Secure Copy Protocol
SDSL	Symmetrical Digital Subscriber Line
SFTP	Secure File Transfer Protocol
SFP	Small Form-factor Pluggable
SIP	Session Initiation Protocol
SLIP	Serial Line Internet Protocol
SMF	Single Mode Fiber
SMTP	Simple Mail Transfer Protocol
SNAT	Static Network Address Translation
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOA	Start of Authority

SOHO	Small Office / Home Office
SONET	Synchronous Optical Network
SPS	Standby Power Supply
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
ST	Straight Tip or Snap Twist
STP	Spanning Tree Protocol
STP	Shielded Twisted Pair
SVC	Switched Virtual Connection
T1	T-Carrier Level 1
TA	Terminal Adaptor
TACACS+	Terminal Access Control Access Control System+
TCP	Transmission Control Protocol
TCP / IP	Transmission Control Protocol / Internet Protocol
TDM	Time Division Multiplexing
TDR	Time Domain Reflectometer
Telco	Telephone Company
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time to Live
UDP	User Datagram Protocol
UNC	Universal Naming Convention
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VDSL	Variable Digital Subscriber Line

VLAN	Virtual Local Area Network
VNC	Virtual Network Connection
VoIP	Voice over IP
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
VTC	Video Teleconference
VTP	Virtual Trunk Protocol
WAN	Wide Area Network
WAP	Wireless Application Protocol / Wireless Access Point
WEP	Wired Equivalent Privacy
WINS	Window Internet Name Service
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
www	World Wide Web
X.25	CCITT Packet Switching Protocol
XML	eXtensible Markup Language
XDSL	Extended Digital Subscriber Line
Zeroconf	Zero Configuration

Network+ Proposed Hardware and Software List

** CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Network+ exam. This list may also be helpful for training companies who wish to create a lab component to their training offering. The bulleted lists below each topic are a sample list and not exhaustive.

Equipment

- Patch Panels
- Punch downs blocks
- Layer 3 Switch

- Router
- Firewall
- Two basic PCs
- Access point
- Media converters
- Configuration terminal (with telnet and SSH)

Spare hardware
- NICs
- Power supplies
- GBICs
- SFPs

Spare parts
- Patch cables
- RJ-45 connectors, modular jacks
- RJ-11 connectors
- Cable spool
- Coaxial cable spool
- F-connectors

Tools
- Telco/network crimper
- Cable tester
- Punch down tool
- Cable striper
- Coaxial crimper
- Wire cutter
- Tone generator

Software
- Packet Sniffer
- Protocol Analyzer
- Terminal Emulation Software
- Linux/Windows OSs
- Software Firewall
- Software IDS / IPS
- Network mapper
- Virtual network environment

Other

- Sample network documentation
- Sample logs
- Defective cables

Version 2.0