

CompTIA Network+ (2009 Edition) Certification Examination Objectives

DRAFT

INTRODUCTION

The CompTIA Network+ (2009 Edition) certification is an internationally recognized validation of the technical knowledge required of foundation-level IT network practitioners.

The CompTIA Network+ (2009 Edition) certification ensures that the successful candidate has the important knowledge and skills necessary to manage, maintain, troubleshoot, install, operate and configure basic network infrastructure, describe networking technologies, basic design principles, and adhere to wiring standards and use testing tools.

The skills and knowledge measured by this examination were derived from an industry-wide job task analysis and validated through an industry-wide global survey in Q2 2008. The results of this survey were used in weighing the domains and ensuring that the weighting is representative of the relative importance of the content.

It is recommended for CompTIA Network+ (2009 Edition) 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+ (2009 Edition) exams are based on these objectives.

Domain	% of Examination
1.0 Network Technologies	20%
2.0 Network Media and Topologies	20%
3.0 Network Devices	17%
4.0 Network Management	20%
5.0 Network Tools	12%
6.0 Network Security	11%
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 Network Technologies

1.1 *Explain the function of common networking protocols*

- TCP
- FTP
- UDP
- TCP/IP suite
- DHCP
- TFTP
- DNS
- HTTP(S)
- ARP
- SIP (VoIP)
- RTP (VoIP)
- SSH
- POP3
- NTP
- IMAP4
- Telnet
- SMTP
- SNMP2/3
- ICMP
- IGMP
- TLS

1.2 *Identify commonly used TCP and UDP default ports*

TCP ports

- FTP – 20, 21
- SSH – 22
- TELNET – 23
- SMTP – 25
- DNS – 53
- HTTP – 80
- POP3 – 110
- NTP – 123
- IMAP4 – 143
- HTTPS – 443

UDP ports

- TFTP – 69
- DNS – 53
- BOOTPS/DHCP – 67
- SNMP – 161

1.3 *Identify the following address formats*

- IPv6
- IPv4
- MAC addressing

1.4 Given a scenario, evaluate the proper use of the following addressing technologies and addressing schemes

Addressing Technologies

- Subnetting
- Classful vs. classless (e.g. CIDR, Supernetting)
- NAT
- PAT
- SNAT
- Public vs. private
- DHCP (static, dynamic APIPA)

Addressing schemes

- Unicast
- Multicast
- Broadcast

1.5 Identify common IPv4 and IPv6 routing protocols

Link state

- OSPF
- IS-IS

Distance vector

- RIP
- RIPv2
- BGP

Hybrid

- EIGRP

1.6 Explain the purpose and properties of routing

- IGP vs. EGP
- Static vs. dynamic
- Next hop
- Understanding routing tables and how they pertain to path selection
- Explain convergence (steady state)

1.7 Compare the characteristics of wireless communication standards

- 802.11 a/b/g/n
 - Speeds
 - Distance
 - Channels
 - Frequency
- Authentication and encryption
 - WPA
 - WEP
 - RADIUS
 - TKIP

2.0 Network Media and Topologies

2.1 *Categorize standard cable types and their properties*

Type:

- CAT3, CAT5, CAT5e, CAT6
- STP, UTP
- Multimode fiber, single-mode fiber
- Coaxial
 - RG-59
 - RG-6
- Serial
- Plenum vs. Non-plenum

Properties:

- Transmission speeds
- Distance
- Duplex
- Noise immunity (security, EMI)
- Frequency

2.2 *Identify common connector types*

- RJ-11
- RJ-45
- BNC
- SC
- ST
- LC
- RS-232
- RG-59
- RG-6

2.3 *Identify common physical network topologies*

- Star
- Mesh
- Bus
- Ring
- Point to point
- Point to multipoint
- Hybrid

2.4 *Given a scenario, differentiate and implement appropriate wiring standards*

- 568A
- 568B
- Straight vs. cross-over
- Rollover
- Loopback

2.5 Categorize WAN technology types and properties

Type:

- Frame relay
- E1/T1
- ADSL
- SDSL
- VDSL
- Cable modem
- Satellite
- E3/T3
- OC-x
- Wireless
- ATM
- SONET
- MPLS
- ISDN BRI
- ISDN PRI
- POTS
- PSTN

Properties

- Circuit switch
- Packet switch
- Speed
- Transmission media
- Distance

2.6 Categorize LAN technology types and properties

Types:

- Ethernet
- 10BaseT
- 100BaseTX
- 100BaseFX
- 1000BaseT
- 1000BaseX
- 10GBaseSR
- 10GBaseLR
- 10GBaseER
- 10GBaseSW
- 10GBaseLW
- 10GBaseEW
- 10GBaseT

Properties

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

2.7 Explain common logical network topologies and their characteristics

- Peer to peer
- Client/server
- VPN
- VLAN

2.8 Install components of wiring distribution

- Vertical and horizontal cross connects
- Patch panels
- 66 block
- MDFs
- IDFs
- 25 pair
- 100 pair
- 110 block
- Demarc
- Demarc extension
- Smart jack
- Verify wiring installation
- Verify wiring termination

3.0 Network Devices

3.1 Install, configure and differentiate between common network devices

- Hub
- Repeater
- Modem
- NIC
- Media converters
- Basic switch
- Bridge
- Wireless access point
- Basic router
- Basic firewall
- Basic DHCP server

3.2 Identify the functions of specialized network devices

- Multilayer switch
- Content switch
- IDS/IPS
- Load balancer
- Multifunction network devices
- DNS server
- Bandwidth shaper
- Proxy server
- CSU/DSU

3.3 Explain the advanced features of a switch

- PoE
- Spanning tree
- VLAN
- Trunking
- Port mirroring
- Port authentication

3.4 Implement a basic wireless network

- Install client
- Access point placement
- Install access point
 - Configure appropriate encryption
 - Configure channels and frequencies
 - Set ESSID and beacon
- Verify installation

4.0 Network Management

4.1 Explain the function of each layer of the OSI model

- Layer 1 – physical
- Layer 2 – data link
- Layer 3 – network
- Layer 4 – transport
- Layer 5 – session
- Layer 6 – presentation
- Layer 7 – application

4.2 Identify types of configuration management documentation

- Wiring schematics
- Physical and logical network diagrams
- Baselines
- Policies, procedures and configurations
- Regulations

4.3 Given a scenario, evaluate the network based on configuration management documentation

- Compare wiring schematics, physical and logical network diagrams, baselines, policies and procedures and configurations to network devices and infrastructure
- Update wiring schematics, physical and logical network diagrams, configurations and job logs as needed

4.4 Conduct network monitoring to identify performance and connectivity issues using the following:

- Network monitoring utilities (e.g. packet sniffers, connectivity software, load testing, throughput testers)
- System logs, history logs, event logs

4.5 Explain different methods and rationales for network performance optimization

Methods:

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

Reasons:

- Latency sensitivity
- High bandwidth applications
 - VoIP
 - Video applications
- Uptime

4.6 Given a scenario, implement the following network troubleshooting methodology

- Information gathering – identify symptoms and problems
- Identify the affected areas of the network
- Determine if anything has changed
- Establish the most probable cause
- Determine if escalation is necessary
- Create an action plan and solution identifying potential effects
- Implement and test the solution
- Identify the results and effects of the solution
- Document the solution and the entire process

4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution

Physical issues:

- Cross talk
- Nearing cross talk
- Attenuation
- Collisions
- Shorts
- Open impedance mismatch (echo)
- Interference

Logical issues:

- Port speed
- Port duplex mismatch
- Incorrect VLAN
- Incorrect IP address
- Wrong gateway
- Wrong DNS
- Wrong subnet mask

Issues that should be identified but escalated:

- Switching loop
- Routing loop
- Route problems
- Proxy arp
- Broadcast storms

Wireless Issues:

- Interference (bleed, environmental factors)
- Incorrect encryption
- Incorrect channel
- Incorrect frequency
- ESSID mismatch
- Standard mismatch (802.11 a/b/g/n)
- Distance
- Bounce
- Incorrect antenna placement

5.0 Network Tools

5.1 Given a scenario, select the appropriate command line interface tool and interpret the output to verify functionality

- Traceroute
- Ipconfig
- Ifconfig
- Ping
- Arp ping
- Arp
- Nslookup
- Host
- Dig
- Mtr
- Route
- Nbtstat
- Netstat

5.2 Explain the purpose of network scanners

- Packet sniffers
- Intrusion detection software
- Intrusion prevention software
- Port scanners

5.3 Given a scenario, utilize the appropriate hardware tools

- Cable testers
- Protocol analyzer
- Certifiers
- TDR
- OTDR
- Multimeter
- Toner probe
- Butt set
- Punch down tool
- Cable stripper
- Snips
- Voltage event recorder
- Temperature monitor

6.0 Network Security

6.1 *Explain the function of hardware and software security devices*

- Network based firewall
- Host based firewall
- IDS
- IPS
- VPN concentrator

6.2 *Explain common features of a firewall*

- Application layer vs. network layer
- Stateful vs. stateless
- Scanning services
- Content filtering
- Signature identification
- Zones

6.3 *Explain the methods of network access security*

Filtering:

- ACL
 - MAC filtering
 - IP filtering
- Tunneling and encryption
 - SSL VPN
 - VPN
 - L2TP
 - PPTP
 - IPSEC
- Remote access
 - RAS
 - RDP
 - PPPoE
 - PPP
 - VNC
 - ICA

6.4 *Explain methods of user authentication*

- PKI
- Kerberos
- AAA
 - RADIUS
 - TACACS+
- Network access control
 - 802.1x
- CHAP
- MS-CHAP
- EAP

6.5 Explain issues that affect device security

- Physical security
- Restricting local and remote access
- Secure methods vs. unsecure methods
 - SSH, HTTPS, SNMPv3, SFTP, SCP
 - TELNET, HTTP, FTP, RSH, RCP, SNMPv1/2

6.6 Identify common security threats and mitigation techniques

Security threats

- DoS
- Viruses
- Worms
- Attackers
- Man in the middle
- Smurf
- Rogue access points
- Social engineering (phishing)

Mitigation techniques

- Policies and procedures
- User training
- Patches and updates

NETWORK+ ACRONYMS

AAA	Authentication Authorization and Accounting
ACL	Access Control List
ADF	Automatic Document Feeder
ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
AM	Amplitude Modulation
AMI	Alternate Mark Inversion
APIPA	Automatic Private Internet Protocol Addressing
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BDF	Building Distribution Frame
BERT	Bit-Error Rate Test
BGP	Border Gateway Protocol
BNC	British Naval Connector / Bayonet Niell-Concelman
BootP	Boot Protocol /Bootstrap Protocol
BRI	Basic Rate Interface
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
DNS	Domain Name Service / Domain Name Server / Domain Name System
DoS	Denial of Service
DDoS	Distributed Denial of Service
DSL	Digital Subscriber Line
DSU	Data Service Unit
E1	E-Carrier Level 1
EAP	Extensible Authentication Protocol
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
EMI	Electromagnetic Interference
ESSID	Enhanced Service Set Identifier
ESP	Encapsulated security packets
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
HDLC	High-Level Data Link Control
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
Hz	Hertz

IANA	Internet Assigned Numbers Authority
ICA	Independent Computer Architecture
ICMP	Internet Control Message Protocol
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Multicast Protocol
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IMAP4	Internet Message Access Protocol version 4
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System - Intermediate system
ISP	Internet Service Provider
IT	Information Technology
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
MMF	Multimode Fiber
MPLS	Multi-Protocol Label Switching
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MT-RJ	Mechanical Transfer-Registered Jack
MX	Mail Exchanger
NAT	Network Address Translation
NetBEUI	Network Basic Input / Output Extended User Interface
NetBIOS	Network Basic Input / Output System
NIC	Network Interface Card
nm	nanometer
NNTP	Network News Transport Protocol
NTP	Network Time 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
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
SC	Standard Connector / Subscriber Connector
SCP	Secure Copy Protocol
SDSL	Symmetrical Digital Subscriber Line
SFTP	Secure File Transfer Protocol
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
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
STP	Shielded Twisted Pair
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
tcsh	turbo C shell
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
VTP	Virtual Trunk Protocol
WAN	Wide Area Network
WAP	Wireless Application Protocol / Wireless Access Point
WEP	Wired Equivalent Privacy
WINS	Window Internet Name Service
WPA	Wi-Fi Protected Access
www	World Wide Web
Zeroconf	Zero Configuration