Revised Network+ Examination Objectives

2005 Version

The purpose of this document is to highlight changes from the 2001 version objectives for easy reference. Any item highlighted within in yellow, for example, can be noted as a change from the 2001 objectives. Items noted in red and highlighted, for example, generally made note of items which were removed from the objectives between the 2001 and 2005 versions. Also note that some of the domain headers contain additional notes, also highlighted, which add detail surrounding the changes in ordering or presentation of some of the objectives within that domain. **This document is for reference only. CompTIA encourages all individuals and interested parties to base their studies and plans off the final 2005 version objectives posted on the Network+ pages of www.comptia.org.**

Introduction

The skills and knowledge measured by this examination are derived from an industry-wide Job Task Analysis (JTA) and validated through an industry wide, global survey for which over 2,000 responses were received from Subject Matter Experts (SMEs) in Q2 2004. 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.

The Network+ certification covering the 2005 objectives, certifies that the successful candidates knows the layers of the OSI model, can describe the features and functions of network components and has the skills needed to install, configure, and troubleshoot basic networking hardware peripherals and protocols. A typical candidate should have CompTIA A+ certification or equivalent knowledge, though A+ certification is not required. In addition to A+ certification level knowledge, candidates are encouraged to have at least nine months of work experience in network support or administration.

The 2005 objectives update the Network+ certification exam on new technologies, protocols and cable standards and well as the removal of older and less common versions of the same. The 2005 objectives also include changes to the weightings and presentation of objectives within the domains to reflect changes in the activities of individuals in a networking position. There remains continued emphasis on hands-on experience knowledge needed in the areas of network implementation and network support including troubleshooting scenarios.

This examination document includes exam blueprint, weighting, test objectives and example content. Example concepts are included to clarify the test objectives and should not be construed as a comprehensive listing of the content of the examination.

The table below lists the domains measured by this examination and the extent to which they are represented in the examination.

Network+ Certification Domain Areas		% of Examination
1.0	Media and Topologies	20%
2.0	Protocols and Standards	20%
3.0	Network Implementation	25%
4.0	Network Support	35%
Total		100%

Note: All percentages are approximate and are subject to change.

Revised Network+ Examination Objectives

2005 Version

Domain 1.0 - Media and Topologies – 20%

1.1 Recognize the following logical or physical network topologies given a diagram, schematic or description:
- Star
- Bus
- Mesh
- Ring   Hierarchical and wireless were removed

1.2 Specify the main features of 802.2 (Logical Link Control), 802.3 (Ethernet), 802.5 (token ring), 802.11 (wireless), and FDDI (Fiber Distributed Data Interface) networking technologies, including:
- Speed
- Access method (CSMA / CA (Carrier Sense Multiple Access / Collision Avoidance) and CSMA / CD (Carrier Sense Multiple Access / Collision Detection))
- Topology
- Media   Method was removed

1.3 Specify the characteristics (For example: speed, length, topology, and cable type) of the following cable standards:
- 10BASE-T and 10BASE-FL   802.3, 10BASE2, 10BASE5 and gigabit ethernet were removed
- 100BASE-TX and 100BASE-FX
- 1000BASE-T, 1000BASE-CX, 1000BASE-SX and 1000BASE-LX
- 10GBASE-SR, 10GBASE-LR and 10GBASE-ER

1.4 Recognize the following media connectors and describe their uses:
- RJ-11 (Registered Jack)
- RJ-45 (Registered Jack)
- F-Type
- ST (Straight Tip)   AUI and BNC were removed
- SC (Subscriber Connector or Standard Connector)
- IEEE 1394 (FireWire)
- Fiber LC (Local Connector)
- MT-RJ (Mechanical Transfer Registered Jack)
- USB (Universal Serial Bus)

1.5 Recognize the following media types and describe their uses:
- Category 3, 5, 5e, and 6   Connectors were removed and media types are listed in detail
- UTP (Unshielded Twisted Pair)
- STP (Shielded Twisted Pair)
- Coaxial cable
- SMF (Single Mode Fiber) optic cable
- MMF (Multimode Fiber) optic cable

1.6 Identify the purposes, features and functions of the following network components:
- Hubs
- Switches
- Bridges
- Routers
- Gateways
- CSU / DSU (Channel Service Unit / Data Service Unit)
- NICs (Network Interface Card)
- ISDN (Integrated Services Digital Network) adapters
- WAPs (Wireless Access Point)
- Modems
- Transceivers (media converters)

- Firewalls

1.7 Specify the general characteristics (For example: carrier speed, frequency, transmission type and topology) of the following wireless technologies:
- 802.11 (Frequency hopping spread spectrum)
- 802.11*x* (Direct sequence spread spectrum)
- Infrared
- Bluetooth

1.8 Identify factors which affect the range and speed of wireless service (For example: interference, antenna type and environmental factors).

Domain 2.0 – Protocols and Standards – 20% Order of appearance of some objectives, wording of some objectives have been enhanced and/or changed.

2.1 Identify a MAC (Media Access Control) address and its parts.

2.2 Identify the seven layers of the OSI (Open Systems Interconnect) model and their functions.

2.3 Identify the OSI (Open Systems Interconnect) layers at which the following network components operate:
- Hubs
- Switches
- Bridges
- Routers
- NICs (Network Interface Card)
- WAPs (Wireless Access Point)

2.4 Differentiate between the following network protocols in terms of routing, addressing schemes, interoperability and naming conventions:
- IPX / SPX (Internetwork Packet Exchange / Sequence Packet Exchange)
- NetBEUI (Network Basic Input / Output System Extended User Interface)
- AppleTalk / AppleTalk over IP (Internet Protocol)
- TCP / IP (Transmission Control Protocol / Internet Protocol)

2.5 Identify the components and structure of IP (Internet Protocol) addresses (IPv4, IPv6) and the required setting for connections across the Internet.

2.6 Identify classful IP (Internet Protocol) ranges and their subnet masks (For example: Class A, B and C).

2.7 Identify the purpose of subnetting. Default gateways was removed.

2.8 Identify the differences between private and public network addressing schemes.

2.9 Identify and differentiate between the following IP (Internet Protocol) addressing methods:
- Static
- Dynamic
- Self-assigned (APIPA (Automatic Private Internet Protocol Addressing))

2.10 Define the purpose, function and use of the following protocols used in the TCP / IP (Transmission Control Protocol / Internet Protocol) suite:
- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- FTP (File Transfer Protocol)
- SFTP (Secure File Transfer Protocol)
- TFTP (Trivial File Transfer Protocol)

Continued on next page…
Continued from previous page…
- SMTP (Simple Mail Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)
- HTTPS (Hypertext Transfer Protocol Secure)
- POP3 / IMAP4 (Post Office Protocol version 3 / Internet Message Access Protocol version 4)
- Telnet
- SSH (Secure Shell)
- ICMP (Internet Control Message Protocol)
- ARP/RARP (Address Resolution Protocol/Reverse Address Resolution Protocol)
- NTP (Network Time Protocol)
- NNTP (Network News Transport Protocol)
- SCP (Secure Copy Protocol)
- LDAP (Lightweight Directory Access Protocol)
- IGMP (Internet Group Multicast Protocol)
- LPR (Line Printer Remote)

2.11 Define the function of TCP / UDP (Transmission Control Protocol / User Datagram Protocol) ports.

2.12 Identify the well-known ports associated with the following commonly used services and protocols:
- 20   FTP (File Transfer Protocol)
- 21   FTP (File Transfer Protocol)
- 22   SSH (Secure Shell)
- 23   Telnet
- 25   SMTP (Simple Mail Transfer Protocol)
- 53   DNS (Domain Name Service)
- 69   TFTP (Trivial File Transfer Protocol)
- 80   HTTP (Hypertext Transfer Protocol)
- 110   POP3 (Post Office Protocol version 3)
- 119   NNTP (Network News Transport Protocol)
- 123   NTP (Network Time Protocol)
- 143   IMAP4 (Internet Message Access Protocol version 4)
- 443   HTTPS (Hypertext Transfer Protocol Secure)

2.13 Identify the purpose of network services and protocols (For example: DNS (Domain Name Service), NAT (Network Address Translation), ICS (Internet Connection Sharing), WINS (Windows Internet Name Service), SNMP (Simple Network Management Protocol), NFS (Network File System), Zeroconf (Zero configuration), SMB (Server Message Block), AFP (Apple File Protocol), LPD (Line Printer Daemon) and Samba). Example list updated.

2.14 Identify the basic characteristics (For example: speed, capacity, and media) of the following WAN (Wide Area Networks) technologies:
- Packet switching
- Circuit switching
- ISDN (Integrated Services Digital Network)
- FDDI (Fiber Distributed Data Interface)
- T1 (T Carrier level 1) / E1 / J1
- T3 (T Carrier level 3) / E3 / J3
- OCx (Optical Carrier)
- X.25   Frame relay, ATM and Sonet/SDH removed.

2.15 Identify the basic characteristics of the following internet access technologies:
- xDSL (Digital Subscriber Line)
- Broadband Cable (Cable modem)

- POTS / PSTN (Plain Old Telephone Service / Public Switched Telephone Network)
- Satellite
- Wireless

2.16 Define the function of the following remote access protocols and services:
- RAS (Remote Access Service)   ICA was removed
- PPP (Point-to-Point Protocol)
- SLIP (Serial Line Internet Protocol)
- PPPoE (Point-to-Point Protocol over Ethernet)
- PPTP (Point-to-Point Tunneling Protocol)
- VPN (Virtual Private Network)
- RDP (Remote Desktop Protocol)

2.17 Identify the following security protocols and describe their purpose and function:
- IPSec (Internet Protocol Security)   Kerberos was removed
- L2TP (Layer 2 Tunneling Protocol)
- SSL (Secure Sockets Layer)
- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- 802.1x

2.18 Identify authentication protocols (For example: CHAP (Challenge Handshake Authentication Protocol), MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), PAP (Password Authentication Protocol), RADIUS (Remote Authentication Dial-In User Service), Kerberos and EAP (Extensible Authentication Protocol)).

Domain 3.0 Network Implementation – 25%   Order of appearance of some objectives, wording of some objectives have been enhanced and/or changed. Network attached storage was removed.

3.1 Identify the basic capabilities (For example: client support, interoperability, authentication, file and print services, application support and security) of the following server operating systems to access network resources:
- UNIX/Linux/Mac OS X Server
- Netware   Macintosh was removed.
- Windows
- Appleshare IP (Internet Protocol)

3.2 Identify the basic capabilities needed for client workstations to connect to and use network resources (For example: media, network protocols and peer and server services).

3.3 Identify the appropriate tool for a given wiring task (For example: wire crimper, media tester / certifier, punch down tool or tone generator). Moved from domain 4.0 domain 3.0.

3.4 Given a remote connectivity scenario comprised of a protocol, an authentication scheme, and physical connectivity, configure the connection. Includes connection to the following servers:
- UNIX / Linux / MAC OS X Server
- Netware   This objective was derived in part from 3.7 and 3.10 in the 2001 version.
- Windows
- Appleshare IP (Internet Protocol)

3.5 Identify the purpose, benefits and characteristics of using a firewall.

3.6 Identify the purpose, benefits and characteristics of using a proxy service.
3.7 Given a connectivity scenario, determine the impact on network functionality of a particular security implementation (For example: port blocking / filtering, authentication and encryption).

3.8 Identify the main characteristics of VLANs (Virtual Local Area Networks).

3.9 Identify the main characteristics and purpose of extranets and intranets.

3.10 Identify the purpose, benefits and characteristics of using antivirus software.

3.11 Identify the purpose and characteristics of fault tolerance:
- Power
- Link redundancy
- Storage
- Services

3.12 Identify the purpose and characteristics of disaster recovery:
- Backup / restore
- Offsite storage
- Hot and cold spares
- Hot, warm and cold sites

Domain 4.0 Network Support – 35% Order of appearance of some objectives, wording of some objectives have been enhanced and/or changed.

4.1 Given a troubleshooting scenario, select the appropriate network utility from the following:
- Tracert / traceroute
- ping
- arp
- netstat
- nbtstat
- ipconfig / ifconfig
- winipcfg
- nslookup / dig

4.2 Given output from a network diagnostic utility (For example: those utilities listed in objective 4.1), identify the utility and interpret the output.

4.3 Given a network scenario, interpret visual indicators (For example: link LEDs (Light Emitting Diode) and collision LEDs (Light Emitting Diode)) to determine the nature of a stated problem.

4.4 Given a troubleshooting scenario involving a client accessing remote network services, identify the cause of the problem (For example: file services, print services, authentication failure, protocol configuration, physical connectivity and SOHO (Small Office / Home Office) router). Re-worded. Examples expanded.

4.5 Given a troubleshooting scenario between a client and the following server environments, identify the cause of a stated problem:
- UNIX / Linux / Mac OS X Server
- Netware   Macintosh was removed.
- Windows
- Appleshare IP (Internet Protocol)

Revised Network+ Examination Objectives
2005 Version

4.6 Given a scenario, determine the impact of modifying, adding or removing network services (For example: DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name Service) and WINS (Windows Internet Name Service)) for network resources and users.

4.7 Given a troubleshooting scenario involving a network with a particular physical topology (For example: bus, star, mesh or ring) and including a network diagram, identify the network area affected and the cause of the stated failure. Hierarchical and wireless were removed.

4.8 Given a network troubleshooting scenario involving an infrastructure (For example: wired or wireless) problem, identify the cause of a stated problem (For example: bad media, interference, network hardware or environment). Derived in part from 4.2 and 4.7 from 2001 objectives.

4.9 Given a network problem scenario, select an appropriate course of action based on a logical troubleshooting strategy. This strategy can include the following steps: Steps clarified.
    1. Identify the symptoms and potential causes
    2. Identify the affected area
    3. Establish what has changed
    4. Select the most probable cause
    5. Implement an action plan and solution including potential effects
    6. Test the result
    7. Identify the results and effects of the solution
    8. Document the solution and process