Global Knowledge®

Expert Reference Series of White Papers

What's New in the CompTIA Network (N10-006) Exam

What's New in the CompTIA Network (N10-006) Exam

George Mays, CCNA, A+, Network+, Security+, CTT+, I-Net+

Introduction

CompTIA is fond of making changes periodically to their various certifications, and Network+ is no exception. Recent changes on February 28, 2015, have begun affecting prospective candidates.

When changes are made, they not only affect the exam itself but also the books and training materials in the marketplace that need to "catch up" and reflect the new requirements. With that in mind, CompTIA provides a grace period in which the old and new requirements overlap one another. Until August 31, 2015, the previous exam is still offered, as is the new one. (Note: These dates are for the English-language version of the exams.) So, the big question is, "How is the new exam different from the old one?"

Let us start with the basics. While each exam runs 90 minutes and has the same passing score of 720 (on a 100–900 scale), the designations have changed: the old exam is now referred to as the N10-005 exam, while the new one is the N10-006 exam.

The number of questions has also changed. The old exam specified a maximum of 100 questions, whereas the new exam is limited to ninety questions. In practice, the old exam was usually around 92 questions or so, a mixture of "performance-based" questions (e.g., 8 questions) and multiple-choice questions (e.g., 84 questions). If one were to guess about the future direction in this regard, it seems likely that there will be more emphasis on the performance-based questions.

The performance-based questions are simply simulations of practical scenarios that pop up in networking. For example, you might be presented with a diagram of two interconnected networks with various computers attached. Your task might be to change the configuration settings on a computer that is having difficulty communicating with others.

Methodology

To evaluate the changes in the exam objectives, I performed a side-by-side comparison of the documentation provided by CompTIA. I noticed that the five "domains" of knowledge had changed, so I mapped the old topics to the new structure to get a sense of how things have moved around. This also revealed things that were dropped. Finally, I isolated the topics that are new to the revised exam.

The Five Domains of Knowledge

Old Objectives (N10-005)		New Objectives (N10-006)
Network Concepts	1	Network Architecture
Network Installation & Configuration	2	Network Operations
Network Media & Topologies	3	Network Security
Network Management	4	Troubleshooting
Network Security	5	Industry Standards, Practices, and Network Theory

These domains of knowledge are simply different subject areas that lend structure to the material covered by the Network+ exam.

Seemingly, the only domain to remain intact is Network Security. One might guess that the Network Media and Topologies equates roughly with the new Network Architecture domain. This leads to questions such as "Are Network Operations derived from Network Management?" and "Are the Network Concepts now part of Industry Standards, Practices, and Network Theory?" The following is a closer examination of the objectives for the new domains to help address some of these questions.

- **Network Architecture**
  The new Network Architecture domain seems to draw largely from the old Network Concepts. IP addressing, MAC addressing, Subnetting, Routing, and DNS are transplanted here. Topics such as NAT, QoS, and DHCP come from the old Installation and Configuration domain. Cable and connector types are taken from the old Media and Topologies, as are WAN Concepts and network topologies. Devices such as proxies, VPN concentrators, and content filters come from the old Network Management domain, along with traffic shaping, load balancing, and high availability. Lastly, VPN concepts and IPsec and NAT derive from the old Network Security domain.

- **Network Operations**
  The new Network Operations domain derives largely from the old Installation and Configuration material. Most of the wireless stuff ends up here. Spanning Tree and VLAN concepts are drawn from the old Network Concepts. A few things like Asset Management and Baselines come from the old Network Management. Nothing to do with Network Security lands here.

- **Network Security**
  Naturally the new Network Security domain contains most of the information from the previous Network Security domain. However, a surprising amount has been added. For example, disaster recovery, penetration testing, TEMPEST, SNMPv3, and unified threat management are new. Greater emphasis is placed on physical security topics such as mantraps, door access controls, and cipher locks. Also, some understanding of forensics is now required.

- **Troubleshooting**
  A good deal moves from the old Installation and Configuration domain to the new Troubleshooting. This includes port configuration issues, VLAN assignments, bad or missing routes, bad mask or gateway, etc. The troubleshooting methodology that CompTIA has promoted for many years comes from the old Network Concepts domain. Troubleshooting hardware and software tools are moved here from the old Network Management, as is the topic of protocol analyzers. Access point placement and signal strength and packet sniffing are drawn from the old Network Security domain.

- **Industry Standards, Practices, and Theory Domain**
  This new domain is derived primarily from two places. First, the OSI and TCP/IP models move over from the old Network Concepts domain, which is not a surprise. Second, all of the "flavors" of Ethernet as well as the difference between CSMA/CD and CSMA/CA come from the old Media and Topologies domain. Cable management and change management are borrowed from the old Network Management domain.

Intermediate Summary

It seems that CompTIA effectively "shuffled the deck" on us. Many topics moved around as part of these newly reorganized exam objectives. Despite this reorganization, almost all of the old topics can be found in the new objectives. Some, however, have disappeared.

Topics No Longer Enumerated in the New Objectives

The following is a list of items that used to be on the old exam that are not explicitly mentioned for the new one. It is ordered roughly in accordance with the sequence of old domains:*

1. Classifying things in accordance with the OSI model
2. Traffic analysis
3. Wire schemes
4. Network maps
5. Caching engines
6. Fault tolerance
7. Common Address Redundancy Protocol (CARP)
8. Remote access
9. Public Key Infrastructure (PKI)
10. Viruses vs. worms
11. Buffer overflow
12. FTP bounce
13. Incident response

**A cautionary note*: The items in this list should not be simply overlooked and ignored. Just because something is not clearly referred to in the new objectives document does not mean that the topic in question is not implied within another area of study that you need to understand. For example, PKI is closely associated with SSL/TLS, and remote access is necessarily akin to VPNs.

What Is New?

Through my research, I was able to determine there are 169 new topics. While this number may not be precise, it is representative of the magnitude of changes made to the new objectives. The following is a list roughly in the order of the new objectives document:

Domain 1: Network Architecture

Unified voice services	ICS server
Network controllers	Distributed Control System (DCS) / closed network
Reverse proxy	Remote terminal unit
Secure network address translation (SNAT) and dynamic network address translation (DNAT)	Programmable logic controller
Defense wavelength division multiplexing (DWDM) and course wavelength division multiplexing (CWDM)	Medianets
GSM/CSMA	Video teleconferencing (VTC) for ISDN, IP/SIP
LTE/4G	IPv6 new topics: - IPv6 autoconfiguration - DHCP6 - Transition tunneling – 6to5, 4to6, Teredo, Miredo
HSPA+	VRRP, HSRP, Virtual IP
3G	Shortest path bridging (SPB)
Edge	Unified communications topics: - Video - Real-time services – presence awareness - UC servers - UC devices - UC gateways
Metro Ethernet	Software-Defined Networks (SDN)
UTP and BNC couplers	Storage area network (SAN)
66 block	Cloud computing concepts extended
FC and "fiber coupler" connectors	
APC vs. UPC fiber cables	
Near field communication (NFC) and radio frequency identification (RFID)	
Supervisory Control and Data Acquisition (SCADA) / Industrial Control Systems (ICS)	

Domain 2: Network Operations

SNMP details	Switch AAA configuration
Alerts via email or SMS	Switch management via virtual terminals
Packet flow monitoring	In-band vs. Out-of-band management
Integrated log management (SIEM)	Managed vs. unmanaged devices
Wireless survey tools	Wireless controllers (VLAN pooling, Lightweight Access Point Protocol [LWAPP])
Wireless analyzers	Goodput
Monitoring and tracking performance tools	MUMIMO
Archives	Wireless Mesh topologies
On-boarding and off-boarding mobile devices	Mobile devices (phone, laptop, tablet, gaming, media)
Network segmentation	

Domain 3: Network Security

Disaster recovery	Biometrics
Business continuity planning	Keypad and cipher locks
First responders	Security guards
Data breaches	Unified threat management (UTM)
Single points of failure	Virtual wire vs. routed
Penetration testing	Network access control models
VLAN hopping	Posture assessments
Comprised systems	Quarantine network
Effects of malware on networks	Edge vs. access control
Zero-day attacks	Forensic concepts
Vulnerabilities including: - Unnecessary running services - Open ports - Unpatched legacy systems - Unencrypted channels - Clear text credentials - Unsecure protocols (Telnet, Web, FTP, SNMP) - TEMPEST / RF emanation	First responders
Anti-malware software – cloud/server based	Secure the area, escalate as needed
SNMPv3 Guest network Persistent vs. non-persistent agents	Document the scene
Hashes (MD5 and SHA)	e-Discovery
Physical security controls	Evidence/data collection
Mantraps	Chain of custody
Network closets	Data transport
Video monitoring (IP cameras, CCTV)	Forensics report
Door access controls	Legal hold
Proximity readers and key fobs	

Domain 4: Troubleshooting

Light meters	Fiber type mismatch
Speed test sites	Bend radius limitations
Looking Glass sites	NIC teaming misconfiguration (active vs. passive)
Wi-Fi analyzer	Resolving common security issues, including: - Misconfigured firewall - Ping of death - Improper access/backdoor access - Banner grabbing/OUI - Domain/local group configurations - Jamming
AP configuration (LWAPP, thing vs. thick)	Smart jack/NIU
Wireless environmental factors	Channel service unit (CSU)/data service unit (DSU)
Gigabit interface converters (GBICs) and small form-factor pluggables (SFPs)	Copper line drivers/repeaters
Wavelength mismatch	Company security policy (throttling, blocking)

Domain 5: Industry Standards, Practices, and Network Theory

Bit rate vs. baud rate	Emergency procedures, including: - Building layout - Fire escape plan - Safety/emergency exits - Fail open vs. fail close - Emergency alert system
Sampling size	Fire suppression systems
IEEE 802.11ac	HVAC
Ethernet over HDMI	Power management, including: - Power converters - Circuits - UPS - Inverters - Power redundancy
Ethernet over power line	Air flow
Broadband (cable) standards - DOCSIS	Rack systems (server rail racks, two vs. four posts)
Security policies – consent to monitoring	Labeling (ports, systems, circuits, patch panels)
Standard business docs (SLA, MOU, MSA, SOW)	Rack monitoring and security
Installation safety, including: - Lifting equipment - Rack installation - Placement - Tool safety	Change management
MSDS	New ports and protocols: - SIP, 5060/5061 - MGCP, 2427/2727 - RTP. 5004/5005 - H.323, 1720

Be aware that some of these items were implied but not explicitly mentioned in the old objectives. For example, 66 blocks are a required part of understanding EIA / TIA 568. So, not everything is entirely new.

Conclusion

The new Network+ certification will certainly be different than the old one. You will be held accountable for almost all of the old material as well as an extensive list of new topics. Much of the new content has to do with security, cloud, data-center and operational concerns, and troubleshooting. Add to that a greater emphasis on wireless networking and VoIP, and you can see the changes are significant. Do not think for a moment that, if you prepared for the old exam you can pass the new one without expanding your studies. CompTIA has raised the bar on Network+ candidates.

Good luck and best wishes with the new exam.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

Network+ Prep Course (N10-006)

Visit www.globalknowledge.com or call 1-800-COURSES (1-800-268-7737) to speak with a Global Knowledge training advisor.

About the Author

George Mays is the president of G.W. Mays & Associates, Inc. based in San Antonio, Texas. George co-authored Villanova University's Mastering IS Security+ course and their CISSP and CASP courses. Additionally, he wrote ANRC's Network Traffic Analysis and Advanced Network Traffic Analysis courses, which he taught on a regular basis to security agencies in the United States. George has over 45 years of experience in computing, data communications, and networking.