STRANDS AND STANDARDS
NETWORK FUNDAMENTALS

Course Description

Utah's Network Fundamentals are based on CompTIA Exam Number N10-007 Network+ Objectives. The CompTIA Network+ certification is an internationally recognized validation of the technical knowledge required of foundation-level IT network practitioners.

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.

It is recommended for CompTIA Network+ candidates to have the following: CompTIA A+ certification or equivalent knowledge and at least 9 to 12 months of work experience in IT networking.

ADA Compliant: December 2020

Intended Grade Level	10-12
Units of Credit	0.5
Core Code	35.01.00.00.030
Concurrent Enrollment Core Code	35.01.00.13.030
Prerequisite	Suggested – Computer Systems 1 and 2, Cisco Certified Networking Associate (CCNA), or Teacher Approval
Skill Certification Test Number	State Skills Exam #888 981 - MTA Networking Fundamentals (98-366) 982 – CompTIA Network+ (N10-007) 9821 – TestOut Network Pro
Test Weight	0.5
License Type	CTE and/or Secondary Education 6-12
Required Endorsement(s)	
Endorsement 1 or	OR Cybersecurity
Endorsement 2	OR Information Technology Systems

CompTIA Network+ Certification Exam Objectives:

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

Doman Network+ (N10-007)	Percentage of Exam
1.0 Networking Concepts	23%
2.0 Infrastructure	18%
3.0 Network Operations	17%
4.0 Network Security	20%
5.0 Network Troubleshooting and Tools	22%
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.

STRAND 1

Networking Concepts

Standard 1

Understand the purposes and uses of ports and protocols.

- Protocols and ports
  - SSH 22
  - DNS 53
  - SMTP 25
  - SFTP 22
  - FTP 20, 21
  - TFTP 69
  - TELNET 23
  - DHCP 67, 68
  - HTTP 80
  - HTTPS 443
  - SNMP 161
  - RDP 3389
  - NTP 123
  - SIP 5060, 5061
  - SMB 445
  - POP 110
  - IMAP 143
  - LDAP 389
  - LDAPS 636
  - H.323 1720
- Protocol types
  - ICMP
  - UDP
  - TCP
  - IP
- Connection-oriented vs. connectionless

Standard 2

Identify devices, applications, protocols and services and which layer of the OSI model they operate at.

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

Standard 3

Identify the characteristics of routing and switching.

- Properties of network traffic
  - Broadcast domains
  - CSMA/CD
  - CSMA/CA
  - Collision domains
  - Protocol data units
  - MTU
  - Broadcast
  - Multicast
  - Unicast

- Segmentation and interface properties
  - VLANs
  - Trunking (802.1q)
  - Tagging and untagging ports
  - Port mirroring
  - Switching loops/spanning tree
  - PoE and PoE+ (802.3af, 802.3at)
  - DMZ
  - MAC Table
  - ARP table
- Routing
  - Routing protocols (IPv4 and IPv6)
    - Distance-vector routing protocols
      - RIP
      - EIGRP
    - Link-state routing protocols
      - OSPF
    - Hybrid
      - BGP
  - Routing types
    - Static
    - Dynamic
    - Default
- IPv6 concepts
  - Addressing
  - Tunneling
  - Dual stack
  - Router advertisement
  - Neighbor discovery

- Performance concepts
    - Traffic shaping
    - QoS
    - Diffserv
    - CoS
- NAT/PAT
- Port Forwarding
- Access control list
- Distributed switching
- Packet-switched vs. circuit-switched network
- Software-defined networking

Standard 4

Demonstrate the configuration of appropriate IP addressing components.

- Private vs. public
- Loopback and reserved
- Default gateway
- Virtual IP
- Subnet mask
- Subnetting
    - Classful
        - Classes A, B, C, D, and E
    - Classless
        - VLSM
        - CIDR notation (IPv4 vs. IPv6)
- Address assignments
    - DHCP
    - DHCPv6
    - Static
    - APIPA
    - EUI64
    - IP reservations

Standard 5

Understand network topologies, types, and technologies.

- Wired topologies
    - Logical vs. physical
    - Star
    - Ring
    - Mesh
    - Bus

- Wireless topologies
  - Mesh
  - Ad hoc
  - Infrastructure
- Types
  - LAN
  - WLAN
  - MAN
  - WAN
  - CAN
  - SAN
  - PAN
- Technologies that facilitate the Internet of Things (IoT)
  - Z-Wave
  - Ant+
  - Bluetooth
  - NFC
  - IR
  - RFID
  - 802.11

Standard 6

Understand wireless technologies and configurations.

- 802.11 standards
  - a
  - b
  - g
  - n
  - ac
- Cellular
  - GSM
  - TDMA
  - CDMA
- Frequencies
  - 2.4GHz
  - 5.0GHz
- Speed and distance requirements
- Channel bandwidth
- Channel bonding
- MIMO/MU-MIMO
- Unidirectional/omnidirectional
- Site surveys

Standard 7

Understand cloud concepts and their purpose.

- Types of services
  - SaaS
  - PaaS
  - IaaS
- Cloud delivery models
  - Private
  - Public
  - Hybrid
- Connectivity methods
- Security implications/considerations
- Relationship between local and cloud resources

Standard 8

Understand the functions of network services.

- DNS service
  - Record types
    - A, AAA
    - TXT (SPF, DKIM)
    - SRV
    - MX
    - CNAME
    - NS
    - PTR
  - Internal vs. external DNS
  - DNSSEC
  - Third-party/cloud-hosted DNS
  - Hierarchy
  - Forward vs. reverse zone
- DHCP service
  - MAC reservations
  - Pools
  - IP exclusions
  - Scope options
  - Lease time
  - TTL
  - DHCP relay/IP helper
- NTP
- IPAM

STRAND 2

Infrastructure

Standard 1

Understand appropriate network cabling solutions.

- Media types
  - Cooper
    - UTP
    - STP
    - Coaxial
  - Fiber
    - Single-mode
    - Multimode
- Plenum vs. PVC
- Connector types
  - Cooper
    - RJ-45
    - RJ-11
    - BNC
    - DB-9
    - DB-25
    - F-type
  - Fiber
    - LC
    - ST
    - SC
      - APC
      - UPC
      - MTRJ
- Transceivers
  - SFP
  - GBIC
  - SFP+
  - QSFP
  - Characteristics of fiber transceivers
    - Bidirectional
    - Duplex
- Termination points
  - 66 block
  - 110 block
  - Patch panel
  - Fiber distribution panel

- Copper cable standards
  - Cat 3
  - Cat 5
  - Cat 5e
  - Cat 6
  - Cat 6a
  - Cat 7
  - Cat 8
  - RG-6
  - RG-59
- Copper termination standards
  - TIA/EIA 568a
  - TIA/EIA 568b
  - Crossover
  - Straight-through
- Ethernet deployment standards
  - 100BaseT
  - 1000BaseT
  - 1000BaseLX
  - 1000BaseSX
  - 10GBaseT

Standard 2

Diagram the appropriate placement of networking devices on a network.

- Firewall
- Router
- Switch
- Hub
- Bridge
- Modems
- Wireless access point
- Media converter
- Wireless range extender
- VoIP endpoint

Standard 3

Identify the use cases for advanced networking devices.

- Multilayer switch
- Layer 3 Switch
- Wireless controller
- Load balancer
- IDS/IPS
- Proxy server
- Reverse Proxy server

- VPN concentrator
- AAA/RADIUS server
- UTM appliance
- NGFW/Layer 7 firewall
- VoIP PBX
- VoIP gateway
- Content filter

Standard 4

Identify the purposes of virtualization and network storage technologies.

- Virtual networking components
  - Virtual switch
  - Virtual firewall
  - Virtual NIC
  - Virtual router
  - Hypervisor
- Network storage types
  - NAS
  - SAN
  - JBOD
- Connection type
  - FCoE
  - Fiber Channel
  - iSCSI
  - InfiniBand
- Jumbo frame

Standard 5

Understand WAN technologies.

- Service type
  - ISDN
  - - T1/T3
  - - E1/E3
  - - OC-3 – OC-192
  - DSL
  - Metropolitan Ethernet
  - Cable broadband
  - Dial-up
  - PRI
- Transmission mediums
  - Satellite
  - Copper
  - Fiber
  - Wireless

- Characteristics of service
  - MPLS
  - ATM
  - Frame relay
  - PPPoE
  - PPP
  - DMVPN
  - SIP trunk
- Termination
  - Demarcation point
  - CSU/DSU
  - Smart jack

STRAND 3

Network Operations

Standard 1

Create appropriate documentation and diagrams to manage the network.

- Diagram symbols
- Standard operating procedures/work instructions
- Logical vs. physical diagrams
- Rack diagrams
- Change management documentation
- Wiring and port locations
- IDF/MDF documentation
- Labeling
- Network configuration and performance baselines
- Inventory management

Standard 2

Understand business continuity and disaster recovery concepts.

- Availability concepts
  - Fault tolerance
  - High availability
  - Load balancing
  - NIC teaming
  - Port aggregation
  - Clustering
  - Power management
    - Battery backups/UPS
    - Power generators
    - Dual power supplies
    - Redundant circuits

- Recovery
    - Cold sites
    - Warm sites
    - Hot sites
    - Backups
        - Full
        - Differential
        - Incremental
    - Snapshots
- MTTR
- MTBF
- SLA requirements

Standard 3

Understand common scanning, monitoring and patching processes and summarizetheir expected outputs.

- Processes
    - Log reviewing
    - Port scanning
    - Vulnerability scanning
    - Patch management
        - Rollback
    - Reviewing baselines
    - Packet/traffic analysis
- Event management
    - Notifications
    - Alerts
    - SIEM
- SNMP monitors
    - MIB
- Metrics
    - Error rate
    - Utilization
    - Packet drops
    - Bandwidth/throughput

Standard 4

Identity remote access methods.

- VPN
    - IPSec
    - SSL/TLS/DTLS
    - Site-to-site
    - Client-to-site
- RDP
- SSH
- VNC

- Telnet
- HTTPS/management URL
- Remote file access
    - FTP/FTPS
    - SFTP
    - TFTP
- Out-of-band management
    - Modem
    - Console router

Standard 5

Identify enterprise network policies and best practices.

- Privileged user agreement
- Password policy
- On-boarding/off-boarding procedures
- Licensing restrictions
- International export controls
- Data loss prevention
- Remote access policies
- Incident response policies
- BYOD
- AUP
- NDA
- System life cycle
    - Asset disposal
- Safety procedures and policies

STRAND 4

Network Security

Standard 1

Understand the purpose of physical security devices.

- Detection
    - Motion detection
    - Video surveillance
    - Asset tracking tags
    - Tamper detection
- Prevention
    - Badges
    - Biometrics
    - Smart cards
    - Key fob
    - Locks

Standard 2

Explain authentication and access controls.

- Authorization, authentication, and accounting
  - RADIUS
  - TACACS+
  - Kerberos
  - Single sign-on
  - Local authentication
  - LDAP
  - Certificates
  - Auditing and logging
- Multifactor authentication
  - Something you know
  - Something you have
  - Something you are
  - Somewhere you are
  - Something you do
- Access control
  - 802.1x
  - NAC
  - Port security
  - MAC filtering
  - Captive portal
  - Access control lists

Standard 3

Understand basic wireless network security protocols.

- WPA
- WPA2
- TKIP-RC4
- CCMP-AES
- Authentication and authorization
  - EAP
    - PEAP
    - EAP-FAST
    - EAP-TLS
  - Shared or open
  - Preshared key
  - MAC filtering
- Geofencing

Standard 4

Identify common networking attacks.

- DoS
    - Reflective
    - Amplified
    - Distributed
- Social engineering
- Insider threat
- Logic bomb
- Rogue access point
- Evil twin
- War-driving
- Phishing
- Pharming
- Ransomware
- DNS poisoning
- ARP poisoning
- Spoofing
- Deauthentication
- Brute force
- VLAN hopping
- Man-in-the-middle
- Exploits vs. vulnerabilities

Standard 5

Understand network device hardening.

- Changing default credentials
- Avoiding common passwords
- Upgrading firmware
- Patching and updates
- File hashing
- Disabling unnecessary services
- Using secure protocols
- Generating new keys
- Disabling unused ports
    - IP ports
    - Device ports (physical and virtual)

Standard 6

Explain common mitigation techniques and their purpose.

- Signature management
- Device hardening
- Change native VLAN

- Switch port protection
    - Spanning tree
    - Flood guard
    - BPDU guard
    - Root guard
    - DHCP snooping
- Network segmentation
    - DMZ
    - VLAN
- Privileged user account
- File integrity monitoring
- Role separation
- Restricting access via ACLs
- Honeypot/honeynet
- Penetration testing

STRAND 5

Network Troubleshooting and Tools

Standard 1

Understand network troubleshooting methodology.

- Identify the problem
    - Gather information
    - Duplicate the problem, if possible
    - Question users
    - Identify symptoms
    - Determine if anything has changed
    - Approach multiple problems individually
- Establish a theory of probable cause
    - Question the obvious
    - Consider multiple approaches
        - Top-to-bottom/bottom-to-top OSI model
        - Divide and conquer
- Test the theory to determine the cause
    - Once the theory is confirmed, determine the next steps to resolve the problem
    - If the theory is not confirmed, reestablish 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, if applicable, implement preventive measures
- Document findings, actions, and outcomes

Standard 2

Demonstrate the use of appropriate networking tools.

- Hardware tools
  - Crimper
  - Cable tester
  - Punchdown tool
  - OTDR
  - Light meter
  - Tone generator
  - Loopback adapter
  - Multimeter
  - Spectrum analyzer
- Software tools
  - Packet sniffer
  - Port scanner
  - Protocol analyzer
  - WiFi analyzer
  - Bandwidth speed tester
  - Command line
    - ping
    - tracert, traceroute
    - nslookup
    - ipconfig
    - ifconfig
    - iptables
    - netstat
    - tcpdump
    - pathping
    - nmap
    - route
    - arp
    - dig

Standard 3

Identify troubleshooting methods for common wired connectivity and performance issues.

- Attenuation
- Latency
- Jitter
- Crosstalk
- EMI
- Open/short
- Incorrect pin-out

- Incorrect cable type
- Bad port
- Transceiver mismatch
- TX/RX reverse
- Duplex/speed mismatch
- Damaged cables
- Bent pins
- Bottlenecks
- VLAN mismatch
- Network connection LED status indicators

Standard 4

Identity troubleshooting methods for common wireless connectivity and performance issues.

- Reflection
- Refraction
- Absorption
- Latency
- Jitter
- Attenuation
- Incorrect antenna type
- Interference
- Incorrect antenna placement
- Channel overlap
- Overcapacity
- Distance limitations
- Frequency mismatch
- Wrong SSID
- Wrong passphrase
- Security type mismatch
- Power levels
- Signal-to-noise ratio

Standard 5

Identity troubleshooting methods for common network service issues.

- Names not resolving
- Incorrect gateway
- Incorrect netmask
- Duplicate IP addresses
- Duplicate MAC addresses
- Expired IP address
- Rogue DHCP server
- Untrusted SSL certificate

- Incorrect time
- Exhausted DHCP scope
- Blocked TCP/UDP ports
- Incorrect host-based firewall settings
- Incorrect ACL settings
- Unresponsive service
- Hardware failure

Skill Certificate Test Points by Strand

Test Name	Test #	Number of Test Points by Strand										Total Points	Total Questions
		1	2	3	4	5	6	7	8	9	10		
Network Fundamentals	888	27	7	18	13	7						72	72