STRANDS AND STANDARDS
NETWORK FUNDAMENTALS

Course Description

Utah's Network Fundamentals are based on CompTIA 2011 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, though CompTIA A+ certification is not required. Have at least 9 to12 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.

Intended Grade Level	10-12
Units of Credit	0.5 or 1.0
Core Code	35.01.00.00.030
Concurrent Enrollment Core Code	35.01.00.13.030
Prerequisite	Suggested – A+ (Computer Repair/Maintenance), Cisco Certified Networking Associate (CCNA), Microsoft Certified Professional, or Teacher Approval
Skill Certification Test Number	888, 981, 982
Test Weight	0.5 or 1.0
License Type	CTE and/or Secondary Education 6-12
Required Endorsement(s)	
Endorsement 1	Network+, or
Endorsement 2	Microsoft Certified Professional (MCP), or
Endorsement 3	Cisco Certified Networking Associate (CCNA), or
Endorsement 4	Certified Novell Administrator (CNA)

STRAND 1

Networking Concepts

Standard 1

Compare the layers of the OSI and TCP/IP models. OSI model:

- OSI model:
  - Physical
  - Data link
  - Network
  - Transport
  - Session
  - Presentation
  - Application
- TCP/IP model
  - Network Interface Layer
  - Internet Layer
  - Transport Layer
  - Application Layer

Standard 2

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

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

Standard 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
- Multicast vs. unicast vs. broadcast
- APIPA

Standard 4

Explain the purpose and properties of routing and switching.

- RIP
- Static
- Routing metrics (Hop counts, bandwidth, Latency)
- Next hop
- Broadcast domain vs. collision domain

Standard 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

Standard 6

Explain the function of common networking protocols.

- TCP
- FTP
- UDP
- TCP/IP suite
- DHCP
- TFTP
- DNS
- HTTPS

- HTTP
- ARP
- SSH
- POP3
- NTP
- IMAP4
- Telnet
- SMTP
- SNMP2/3
- ICMP

Standard 7

Summarize DNS concepts and its components.

- DNS Servers
- New 1.8 Trouble Shooting Methodology

STRAND 2

Network Installation and Configuration

Standard 1

Given a scenario, install and configure routers and switches.

- Routing tables
- NAT
- PAT
- Interface configurations (Full duplex, Half duplex, Port speeds, IP addressing, MAC filtering)
- PoE

Standard 2

Given a scenario, install and configure a wireless network.

- WAP placement
- Channels
- Wireless standards
- SSID (enable/disable)
- Compatibility (802.11 a/b/g/n)

Standard 3

Explain the purpose and properties of DHCP.

- Static vs. dynamic IP addressing
- Reservations
- Scopes
- Leases

Standard 4

Given a scenario, troubleshoot common wireless problems.

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

Standard 5

Given a scenario, troubleshoot common router, switch and general network 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

Standard 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

Standard 7

IP Configuration

- IP Configuration
- Subnetting
- Classless Subnetting

STRAND 3

Network Media and Topologies

Standard 1

Categorize standard media types and associated properties.

- Fiber
  - Multimode
  - Singlemode
- Copper
  - UTP
  - STP
  - CAT3
  - CAT5
  - CAT5e
  - CAT6
  - CAT6a
  - Crossover
  - T1 Crossover
  - Straight-through
- Plenum vs. non-plenum
- Distance limitations and speed limitations
- Broadband over powerline

Standard 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)

Standard 3

Compare and contrast different wireless standards.

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

- MIMO
- Channel bonding

Standard 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

Standard 5

Describe different network topologies.

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

- Client-server
- Hybrid

Standard 6

Cable problems:

- Bad connectors
- Bad wiring
- Open, short
- Split cables
- DB loss
- TXRX reversed
- Cable placement
- EMI/Interference
- Distance

Standard 7

Compare and contrast different LAN technologies.

- Type
  - Ethernet
  - 10BaseT
  - 100BaseT
  - 1000BaseT
  - 100BaseTX
  - 100BaseFX
  - 1000BaseX
  - 10GBaseSR
  - 10GBaseLR
  - 10GBaseER
  - 10GBaseSW
  - 10GBaseLW
  - 10GBaseEW
  - 10GBaseT
- Properties
  - CSMA/CD
  - CSMA/CA
  - Broadcast
  - Collision
  - Bonding
  - Speed
  - Distance

Standard 8

Identify components of wiring distribution.

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

STRAND 4

Network Management

Standard 1

Explain the purpose and features of various network appliances.

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

Standard 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

Standard 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

Standard 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

Standard 5

Describe the purpose of configuration management documentation.

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

Standard 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
  - oHigh bandwidth applications (VoIP, video applications, unified communications)
  - Uptime

STRAND 5

Network Security

Standard 1

Given a scenario, implement appropriate wireless security measures.

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

Standard 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
  - PPoE
  - PPP
  - ICA
  - SSH

Standard 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
- Secure passwords

Standard 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

Standard 5

Given a scenario, install and configure a basic firewall.

- Types
  - Software and hardware firewalls
- Port security
- Firewall rules
  - Block/Allow
  - Implicit deny
  - ACL
- NAT/PAT
- DMZ

Standard 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

Skill Certificate Test Points by Strand

Example table below. Refer to instructions for specifics.

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