

Central Sierra Regional Occupation Program

Course Outline

Computer and Data Networking Technology

Introduction

The CompTIA A+ and N+ certification examinations measures necessary competencies for an entry-level IT professional. In order to receive the CompTIA A+ certification a student must pass two exams. The first exam is CompTIA A+ Essentials, exam number 220-701, and the second exam is the CompTIA A+ Practical Applications, exam number 220-702.

The CompTIA N+ certification requires the successful completion of the Network+ 2009 exam.

Successful students will have the knowledge required to understand the fundamentals of computer technology, networking, and security, and will have the skills required to identify hardware, peripheral, networking, and security components. Successful students will understand the basic functionality of the PC operating system and basic troubleshooting methodology, practice proper safety procedures, and will effectively interact with customers and peers.

The CompTIA A+ exams are based on the following objectives:

Objective	Percentage of Examination
1.0 Hardware	27%
2.0 Troubleshooting, Repair &	20%
3.0 Operating System and Software	20%
4.0 Networking	15%
5.0 Security	8%
6.0 Operational Procedure	10%
Total	100%

The CompTIA N+ exam is based on the following objectives:

Objective	Percentage of Examination
1.0 Network Technologies	20%
2.0 Network Media and	20%
3.0 Network Devices	17%
4.0 Network Management	20%
5.0 Network Tools	12%
6.0 Network Security	11%
Total	100%

1.0 Hardware

1.1 *Categorize storage devices and backup media*

- FDD
- HDD
 - Solid state vs. magnetic
- Optical drives
 - CD / DVD / RW / Blu-Ray
- Removable storage
 - Tape drive
 - Solid state (e.g., thumb drive, flash, SD cards, USB) External
 - CD-RW and hard drive
 - Hot swappable devices and non-hot swappable devices

1.2 *Explain motherboard components, types and features*

- Form Factor ATX / BTX,
micro ATX
NLX
- I/O interfaces Sound
Video USB 1.1 and 2.0
Serial
IEEE 1394 / Fire Wire
Parallel
NIC
Modem
PS/2
- Memory slots RIMM
DIMM SODIMM
SIMM
- Processor sockets
- Bus architecture
- Bus slots
 - PCI
 - AGP PCIe AMR CNR
- PATA
 - IDE EIDE
- SATA, eSATA
- RAID (levels 0, 1, 5)
- Chipsets
- BIOS / CMOS / Firmware
 - POST
 - CMOS battery
- Riser card / daughterboard

1.3 *Classify power supplies types and characteristics*

- AC adapter
- ATX proprietary
- Voltage, wattage and capacity
- Voltage selector switch
- Pins (20,24)

1.4 Explain the purpose and characteristics of CPUs and their features

- Identify CPU types AMD
 - Intel
- Hyper threading
- Multi core
 - Dual core Triple core
 - Quad core
- On-chip cache
 - L1
 - L2
- Speed (real vs. actual)
- 32 bit vs. 64 bit

1.5 Explain cooling methods and devices

- Heat sinks
- CPU and case fans
- Liquid cooling systems
- Thermal compound

1.6 Compare and contrast memory types, characteristics and their purpose

- Types
 - DRAM
 - SRAM
 - SDRAM
 - DDR / DDR2 / DDR3
 - RAMBUS
- Parity vs. Non-parity
- ECC vs. non-ECC
- Single sided vs. double sided
- Single channel vs. dual channel
- Speed
 - PC100
 - PC133
 - PC2700
 - PC3200
 - DDR3-1600 DDR2-667

1.7 Distinguish between the different display devices and their characteristics

- Projectors, CRT and LCD
- LCD technologies
 - Resolution (e.g., XGA, SXGA+, UXGA, WUXGA)
 - Contrast ratio
- Connector types VGA
 - HDMI
 - S-Video
 - Component / RGBDVI pin compatibility
- Settings
 - Refresh rate
 - Resolution
 - Multi-monitor
 - Degauss

1.8 Install and configure peripherals and input devices

- Mouse
- Keyboard
- Bar code reader
- Multimedia (e.g., web and digital cameras, MIDI, microphones)
- Biometric devices
- Touch screen
- KVM switch

1.9 Summarize the function and types of adapter cards

- Video
 - PCI
 - PCIe
 - AGP
- Multimedia
 - Sound card
 - TV tuner cards
 - Capture cards
- I/O
 - SCSI
 - Serial
 - USB
 - Parallel
- Communications NIC
 - Modem

1.10 Install, configure and optimize laptop components and features

- Expansion devices PCMCIA cards
 - PCI Express cards
 - Docking station
- Communication connections
 - Bluetooth Infrared
 - Cellular WAN
 - Ethernet Modem
- Power and electrical input devices
 - Auto-switching
 - Fixed input power supplies
 - Batteries
- Input devices
 - Stylus / digitizer
 - Function keys
 - Point devices (e.g. touch pad, point stick / track point)

1.11 Install and configure printers

- Differentiate between printer types
 - Laser Inkjet
 - Thermal
 - Impact
- Local vs. network printers
- Printer drivers (compatibility)
- Consumables

2.0 Troubleshooting, Repair and Maintenance

2.1 *Given a scenario, explain the troubleshooting theory*

- Identify the problem
 - Question the user and identify user changes to computer and perform backups before making changes
- Establish a theory of probable cause (question the obvious)
- Test the theory to determine cause
 - Once theory is confirmed determine next steps to resolve problem. If theory is not confirmed re-establish new theory or escalate.
- Establish a plan of action to resolve the problem and implement the solution
- Verify full system functionality and if applicable implement preventative measures
- Document findings, actions and outcomes

2.2 *Given a scenario, explain and interpret common hardware and operating system symptoms and their causes*

- OS related symptoms
 - Bluescreen
 - System lock-up
 - Input/output device
 - Application install
 - Start or load
 - Windows specific printing problems
 - Print spool stalled
 - Incorrect / incompatible driver
- Hardware related symptoms
 - Excessive heat
 - Noise
 - Odors
 - Status light indicators
 - Alerts
 - Visible damage (e.g. cable, plastic)
- Use documentation and resources
 - User / installation manuals
 - Internet / web based
 - Training materials

2.3 *Given a scenario, determine the troubleshooting methods and tools for printer*

- Manage print jobs
 - Print spooler
 - Printer properties and settings
 - Print a test page

2.4 *Given a scenario, explain and interpret common laptop issues and determine the appropriate basic troubleshooting method*

- Issues
 - Power conditions
 - Video
 - Keyboard
 - Pointer
 - Stylus
 - Wireless card issues
- Methods
 - Verify power (e.g. LEDs, swap AC adapter) Remove unneeded peripherals
 - Plug in external monitor

Toggle Fn keys or hardware switches Check
LCD cutoff switch
Verify backlight functionality and pixilation
Check switch for built-in WIFI antennas or external antennas

2.5 Given a scenario, integrate common preventative maintenance techniques

- Physical inspection
- Updates
 - Driver
 - Firmware OS
 - Security
- Scheduling preventative maintenance
 - Defrag
 - Scandisk Check disk
 - Startup programs
- Use of appropriate repair tools and cleaning materials
 - Compressed air
 - Lint free cloth
 - Computer vacuum and compressors
- Power devices
 - Appropriate source such as power strip, surge protector or UPS
- Ensuring proper environment
- Backup procedure

3.0 Operating Systems and Software – Operating systems include Microsoft Windows 2000, Windows XP, XP MediaCenter, Windows Vista, and Windows 7

3.1 Compare and contrast the different Windows Operating Systems and their features

- Windows 2000, Windows XP 32bit vs. 64bit, Windows Vista 32 bit vs. 64 bit
Side bar, Aero, UAC, minimum system requirements, system limits
Windows 2000 and newer – upgrade paths and requirements
Terminology (32 bit vs. 64 bit – x86 vs. x64)
Application compatibility, installed program locations (32bit vs. 64bit),
Windows compatibility mode
User interface, start bar layout

3.2 Given a scenario, demonstrate proper use of user interfaces

- Windows Explorer
- My Computer
- Control Panel
- Command prompt utilities
 - telnet
 - ping
 - ipconfig
- Run line utilities
 - msconfig msinfo32
 - Dxdiag
 - Cmd
 - REGEDIT
- My Network Places
- Task bar / systray
- Administrative tools o Performance monitor, Event Viewer, Services, Computer Management
- MMC
- Task Manager
- Start Menu

3.3 Summarize the following security features

- Wireless encryption WEPx and WPAx
Client configuration (SSID)
- Malicious software protection
 - Viruses
 - Trojans
 - Worms
 - Spam
 - Spyware Adware
- BIOS Security
 - Drives
 - Passwords
 - Intrusion detection
 - TPM
- Password management / password complexity
- Locking workstation Hardware
Operating system

3.4 Explain the process and steps to install and configure the Windows OS

- File systems
 - FAT32 vs. NTFS
- Directory structures
- Create folders
- Navigate directory structures
- Files
 - Creation Extensions
 - Attributes Permissions
- Verification of hardware compatibility and minimum requirements
- Installation methods
 - Boot media such as CD, floppy or USB
 - Network installation
 - Install from image
 - Recover CD
 - Factory recovery partition
- Operating system installation options
 - File system type
 - Network configuration
 - Repair install
- Disk preparation order Format
 - drive Partition
 - Start installation
- Device Manager Verify
 - Install and update devices drivers
 - Driver signing
- User data migration – User State Migration Tool (USMT)
- Virtual memory
- Configure power management
 - Suspend
 - Wake on LAN
 - Sleep timers
 - Hibernate
 - Standby
- Demonstrate safe removal of peripherals

3.5 Explain the basics of boot sequences, methods and startup utilities

- Disk boot order / device priority
 - Types of boot devices (disk, network, USB, other)
- Boot options
 - Safe mode
 - Boot to restore point
 - Recovery options
 - Automated System Recovery (ASR)
 - Emergency Repair Disk (ERD)
 - Recovery console

4.0 Network Technologies

4.1 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

4.2 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

4.3 Identify the following address formats

- IPv6
- IPv4
- MAC addressing

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

Addressing Technologies

- Subnetting
- Classful vs. classless (CIDR, Super-netting)
- NAT
- PAT
- SNAT
- Public vs. private
- DHCP (static, dynamic API PA)

Addressing schemes

- Unicast
- Multicast
- Broadcast

4.5 Identify common IPv4 and IPv6 routing protocols

OSPF

- IS-IS
- RIP
- RIPv2
- BGP
- EIGRP

4.6 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)

4.7 Compare the characteristics of wireless communication standards

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

4.8 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

4.9 Identify common connector types

- RJ-11
- RJ-45
- BNC
- SC
- ST
- LC
- RS-232

4.10 Identify common physical network topologies

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

4.11 Given a scenario, differentiate and implement appropriate wiring standards

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

4.12 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

4.13 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

4.14 Explain common logical network topologies and their characteristics

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

4.15 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

4.16 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

4.17 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

4.18 Explain the advanced features of a switch

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

4.19 Implement a basic wireless network

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

4.20 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

4.21 Identify types of configuration management documentation

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

- Regulations

4.22 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

4.23 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

4.24 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

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

- Traceroute
- Ipconfig
- Ping
- Arp
- Nslookup
- Hostname
- Dig
- Mtr
- Route
- Netstat

4.26 Explain the purpose of network scanners

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

4.27 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

4.28 Explain the function of hardware and software security devices

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

4.29 Explain common features of a firewall

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

4.30 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
 - PPPoE
 - PPP

4.31 Explain methods of user authentication

- PKI
- Kerberos
- Network access control
- 802.1

4.32 Explain the basic principles of security concepts and technologies

- Encryption technologies
- Data wiping / hard drive destruction / hard drive recycling
- Software firewall
 - Port security
 - Exceptions
- Authentication technologies
 - User name
 - Password
 - Biometrics
 - Smart cards
- Basics of data sensitivity and data security
 - Compliance
 - Classifications
 - Social engineering

5.0 Operational Procedure

5.1 *Outline the purpose of appropriate safety and environmental procedures and given a scenario apply them*

- ESD
- EMI
 - Network interference
 - Magnets
- RFI
 - Cordless phone interference
 - Microwaves
- Electrical safety
 - CRT
 - Power supply
 - Inverter
 - Laser printers
 - Matching power requirements of equipment with power distribution and UPSs
- Material Safety Data Sheets (MSDS)
- Cable management
 - Avoiding trip hazards
- Physical safety
 - Heavy devices
 - Hot components
- Environmental – consider proper disposal procedures

5.2 *Given a scenario, demonstrate the appropriate use of communication skills and professionalism in the workplace*

- Use proper language – avoid jargon, acronyms, slang
- Maintain a positive attitude
- Listen and do not interrupt a customer
- Be culturally sensitive
- Be on time
 - If late contact the customer
- Avoid distractions
 - Personal calls
 - Talking to co-workers while interacting with customers
 - Personal interruptions
- Dealing with a difficult customer or situation
 - Avoid arguing with customers and/or being defensive Do not minimize customers' problems
 - Avoid being judgmental
 - Clarify customer statements
 - Ask open-ended questions to narrow the scope of the problem
 - Restate the issue or question to verify understanding
- Set and meet expectations / timeline and communicate status with the customer.
 - Offer different repair / replacement options if applicable
 - Provide proper documentation on the services provided
 - Follow up with customer / user at a later date to verify satisfaction
- Deal appropriately with customers confidential materials