CompTIA® A+

Quick Reference

(220-701, 220-702)

Ben Conry

PEARSON

www.pearsoncertification.com

Contents at a Glance

shortcut

Your Short Cut to Knowledge

CompTIA A+ Quick Reference (220-701, 220-702)

Ben Conry

Visit us on the Web: www.pearsoncertification.com

Pearson Education, Inc.
Rights and Contracts Department
One Lake Street
Upper Saddle River, NJ 07458
United States of America
Fax: (201) 236-3290

ISBN-13: 978-0-7897-4327-5
ISBN-10: 0-7897-4327-2

First release, October, 2010

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Executive Editor
Mary Beth Ray

Technical Reviewer
Ken Quamme

Managing Editor
Patrick Kanouse

Project Editor
Jennifer Gallant

Copy Editor
Sheri Cain

Publishing Coordinator
Vanessa Evans

Compositor
Bronkella Publishing LLC

Table of Contents

Introduction

This quick reference guide is a late-stage exam prep resource designed to be used as review shortly before your scheduled CompTIA A+ exam (2009 objectives). It is not intended to be a comprehensive curriculum. If you are using this resource, you should have already learned the material through a class or formal study method. This CompTIA A+ Quick Reference provides brief, straight forward, explanations on major topics of the two CompTIA A+ exams—the 220-701 Essentials Exam and the 220-702 Practical Applications Exam.

About the Author

Benjamin P. Conry graduated from Oberlin College in 1995 with a Bachelor's degree in Music Education with an emphasis in composition. He earned a Master's degree in Instructional Technology from Johns Hopkins University in 2002. Currently, he holds CCNA, CCAI, and A+ certifications and is the lead instructor for Information Technology Essentials, PC Hardware and Software in Baltimore County Public Schools. Ben Conry consistently takes disadvantaged and minority students and sees them through their A+ and CCNA certifications and into college and careers. He has received awards and citations for his commitment to educational excellence and for preparing students for college and the workforce. Ben Conry lives with his wife and two children in Lutherville, Maryland.

About the Technical Reviewer

Ken Quamme, CCNA, CCAI, A+, is an assistant professor at Williston State College, Williston, North Dakota, where he teaches the CCNA curricula, IT Essentials I, Security, Server Administration, Linux, Cisco wireless, and IP telephony. Ken has served as vocational director and chief information officer for Williston State College. Ken resides in Williston, North Dakota, with his wife, Julie, and their children, Christopher, Jaci, and Logan.

1

Hardware

Hardware is one of six domains in the CompTIA A+ Exams. It is a major piece of both exams. Hardware accounts for 27 percent of the 220-701 Essentials Exam and 38 percent of the 220-702 Practical Applications Exam.

CPUs

The Central Processing Unit (CPU) is the main processing unit of the personal computer (PC). It has an integral relationship with the motherboard and the system memory. These three devices control the data-processing aspect of the PC. Drives handle data storage, and input/output (I/O) interfaces allow human interaction, communication with peripherals, and network communication.

RISC Versus CISC

Most general purpose PCs use a complex instruction set chip (CISC). Many dedicated computers used in data collection, sensors, routers, and graphics processors are reduced instruction set chips (RISC). These two types of processors can complete the same tasks, but if the computer is processing the same kind of data all the time, it is often more efficient to reduce the amount of possible instructions the CPU can execute. This makes the decision-making process simple and quick.

32-Bit Versus 64-Bit CPUs

32-bit processors are slowly being replaced by 64-bit processors as an increasing number of applications and operating systems (OS) support them. You should use a 64-bit OS and applications on a 64-bit CPU to get the full benefit of increased performance. Most 64-bit applications are backward compatible and will work on 32-bit CPUs.

Clock Rate

The actual speed of the CPU is governed by a BIOS setting called the clock rate. CPUs run in a range of speeds, not just one specific speed. Increasing the speed is called over clocking. It improves performance, but it comes at a cost. The faster the CPU runs, the hotter it gets. If it gets too hot, the BIOS shuts down the CPU. If the temperature thermocouple is not correctly reading the CPU heat, the CPU can actually melt or catch fire. More sophisticated motherboards throttle down the CPU speed in the event it gets too hot to prevent entirely shutting down the computer.

Cores and Cache

CPUs traditionally contain only one core. Some server and workstation motherboards can support multiple CPUs (multiprocessor). More commonly, you can find PCs with one CPU that includes two or four cores (dual or quad core, respectively) Multicore is not the same as multiprocessor. Multiple cores allow the PC to simultaneously process multiple tasks (threads).

Multicore CPUs still share a common front side bus, which can cause traffic bottlenecks as competing cores communicate on the main system bus. In contrast, each core has its own internal bus that allows independent access RAM.

Shared cache is another good reason for multiple cores. Cache is a temporary storage for the core so that it can "remember" the most recent processes. It is like looking up a topic in this quick reference guide as opposed to a giant 1,400 page A+ exam-preparation book.

There are three levels of cache:

- Level one cache is located on the CPU.
- Level two cache is located on the motherboard.
- Level three cache is located on removable chips on the motherboard.

CPU Interfaces and Socket Types

The motherboard supports the CPU in several ways:

- Chipsets help direct and process data and commands for the CPU.
- Sockets allow the CPU to connect to the computer.
- The motherboard provides power to the CPU.
- It measures the temperature and controls fans to cool the CPU.
- The motherboard shuts down the PC if the CPU is too hot to prevent damage.

Intel and Advanced Micro Devices (AMD) have many models and qualities of CPUs. Each model is designed to fit into a specific socket on the motherboard. Many pins connect the CPU to the motherboard. Bending (or breaking) even one pin renders the CPU inoperable. A Zero Insertion Force (ZIF) physical interface lets you set the CPU into the array, and then you actuate a lever to make actual contact. It is imperative to orient the CPU correctly. Usually, there is an obvious guide or indication, like a missing corner pin on the CPU, that aligns to a missing hole in the ZIF. Pin Grid Array (PGA) and Line Grid Array (LGA) describe the pin arrangement of the CPU interface with the motherboard. Tables 1-1 and 1-2 list processors and their associated sockets.

Table 1-1 AMD Sockets and CPUs

Socket	Supported CPUs
Socket 462 and Socket A	Athlon, XP, XP-M, and MP
	Duron
	Sempron
Socket 754	Athlon 64
	Sempron
	Turion 64
Socket 940	Opteron
	Athlon 64 FX
Socket 939	Athlon 64, FX, and X2
	Opteron
Socket S1	Turion 64 X2
Socket AM2	Athalon X2
	Athlon 64, FX, LE, and X2
	Phenom, X3, and X4
	Sempron and LE
	Opteron and SE
Socket AM2+	Athlon X2 BE
	Athlon 64, FX, LE, and X2
	Phenom, X3, and X4
	Phenom II X2, X3, and X4
	Sempron and Sempron LE
	Opteron and Opteron SE
Socket AM3	Athlon II X2 and X4
	Phenom and Phenom FX
	Phenom II X3 and X4
	Sempron
Socket 563	AMD Athlon XP-M

Table 1-2 Intel Sockets and CPUs

Socket	Supported CPUs
Socket 370	Pentium III
	Celeron
Socket 478 and Socket N	Pentium 4, 4 EE, and M
	Celeron
Socket 495	Celeron
PAC418	Itanium
Socket 603	Xeon
PAC611	Itanium 2
Socket 604	Xeon
Socket 479	Pentium M
	Celeron M
	Core Solo and Core Duo
LGA 775 and Socket T	Pentium 4, D, and XE
	Celeron and Celeron D
	Core 2 Duo and Core 2 Extreme
Socket M	Core Solo and Core Duo
	Core 2 Duo
	Dual-Core Xeon
LGA 771 and Socket 771	Xeon
Socket P	Core 2
Socket 441	Atom
Socket B	Core i7

System Memory

There are two major types of memory: dynamic and static. Dynamic Random Access Memory (DRAM) loses information in the absence of power. Static RAM (SRAM) retains its data like a hard drive regardless of power state. In general, DRAM is used as system memory, and SRAM is used for cache and storage devices.

SDRAM is neither a contradiction in terms nor a type of hybrid RAM. It actually stands for Synchronous Dynamic RAM. Synchronous means that the data transfer is timed to the system clock. For many years, 168 pin SDRAM was the standard system memory. It has largely been replaced with Double Data Rate (DDR), DDR2, and DDR3. All these types of RAM use a com-

mon Dual Inline Memory Module (DIMM) form factor, but they all have unique form factors and are, therefore, not interchangeable.

Like most things on a PC, RAM is measured in speed. The motherboard must support the speed of the RAM, or the increased performance promised by the fast RAM will not be realized; or worse, the PC might not even Power On Self Test (POST).

Other Types of RAM

RAMBUS Inline Memory Module (RIMM) uses a proprietary 184-pin or 232-pin slot called a RIMM. This RAM, often called RDRAM, is found in some game console systems and a limited number of PCs. On such systems, empty RIMM slots must be filled with Continuity RIMM (CRIMM) modules.

Older Single Inline Memory Modules (SIMM) have 30 or 72 contacts on only one side. SIMMs must be installed in identical pairs.

Laptops use a small form factor called Small Outline DIMM (SODIMM). Many netbooks, Ultra Mobile PC (UMPC), and portable devices, such as cell phones and PDAs, use a MicroDIMM form factor. Figure 1-1 compares the relative size and form factors found in RAM.

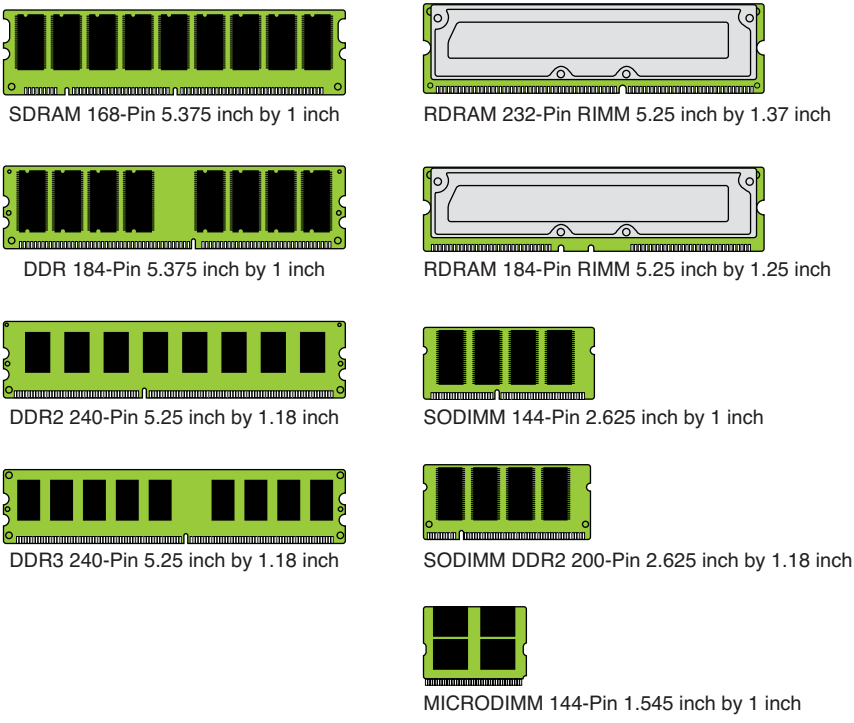


Figure 1-1 RAM Comparison

VRAM and Virtual RAM

VRAM is video RAM for the use of the Graphic Processing Unit (GPU). VRAM does not stand for Virtual RAM. Virtual RAM is space on the HD that the RAM uses as an overflow area and as a backup copy of the contents in case of power failure.

Parity and ECC

Parity is a method of verifying data integrity. It is used when the reliability of the data is more important than the speed at which it is written or read. Parity adds a bit to each byte so that every byte is an even number. When the data is read or received, the bytes should still be even. If not, the data is corrupt. Parity is used in some network communications, hard drives, and RAM. Error correction code (ECC) detects and fixes corrupt data in RAM. Both Parity and ECC decrease efficiency, but increase reliability.

Motherboards

A motherboard connects everything. It facilitates interoperability among the trinity (CPU, RAM, and motherboard). It communicates with storage devices through SATA and PATA headers. It also allows for expansion through the use of adapter cards. Motherboards usually have integrated I/O ports to support common peripherals.

BIOS

The BIOS is stored on the CMOS chip that is on the motherboard. The BIOS handles fundamental system configuration. The CMOS chip is actually a combination of NVRAM and volatile RAM. The NVRAM allows the BIOS to be updated (flashed). If the BIOS cannot recognize a new device, updating the BIOS is a solution. A small battery maintains a charge so the settings are not lost in the RAM when the PC is off. If the date and time reset when the computer restarts, replace the battery. The BIOS allows you to do the following:

- Enable/disable integrated devices
- Order the boot sequence
- Manage drive controllers
- Adjust battery and power supply settings

Form Factors

There are a few basic form factors for motherboards. ATX is the basis of all modern motherboards. BTX is slightly bigger and is used primarily by manufacturers. ATX is often the choice of custom-built computers. There are countless motherboard sizes and capabilities. Table 1-3 outlines the common form factors.

Table 1-3 Motherboard Form Factors

Form Factor	Dimensions in Millimeters	Details and Descriptions
ATX	305×244	The basic motherboard.
BTX	325×266	Most PC manufacturers use proprietary versions of the BTX.
Micro ATX	244×244	A smaller square version ATX motherboard with fewer expansion slots.
ITX	215×191	Designed to be small and used with completely integrated devices.
NLX	254×228	Integrated AGP, NIC, and USB support.
LPX	330×229	Expansion cards run parallel to motherboard and can, therefore, fit in to a smaller case.

Expansion Cards and Slots

Expansion cards allow the motherboard to connect and control countless devices to the PC via proxies called adapter cards. Adapter cards also share some of the processing responsibility, which lightens the load on the CPU. Table 1-4 describes the standard expansion slots.

Table 1-4 Expansion Slots

Adapter Card/ Bus Name	Bus Width	Details and Descriptions
PCIe	x1	Full duplex lets data be sent and received simultaneously.
	x4	Measured in throughput as a multiple of 250 MBps.
	x8	For example, a x4 PCIe slot and card can transfer data at 1000 MBps.
	x16	(250 MBps x 4 = 1000 MBps)
PCI	64	Current standard, 32 bit and 64 bit, shorter than ISA.
	32	Usually white.
		32 bit have two inline slots; 64 bit have three.
AGP	32	Dedicated graphics card slot, 32 bit, shorter than PCI.
		Brown.
EISA	32	Old technology, slot 8 and 16 bit versions (32 bit EISA).
ISA	16	Black.
	8	Common in older PCs.

Figure 1-2 shows the relative size and form factors of the common expansion slots. You should be able to identify these during your CompTIA A+ Exams.

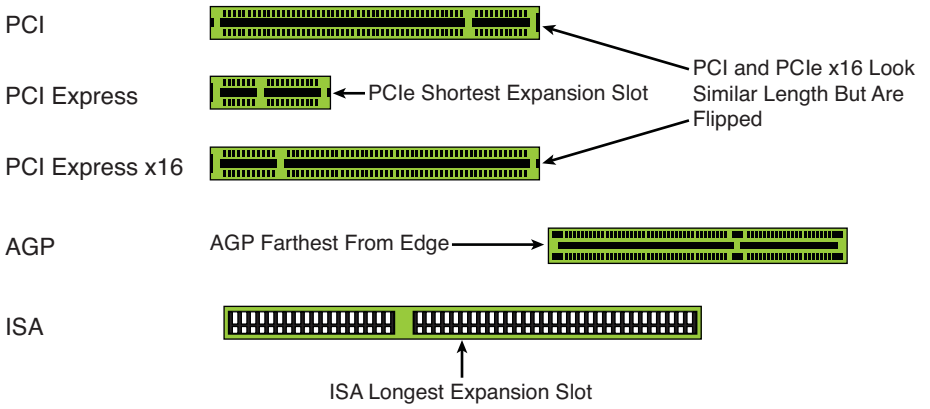


Figure 1-2 Expansion Slot Comparison

Adapter Cards

The expansion slots support adapter cards. Some cards control internal devices, such as hard drives, and most communicate with external devices, such as monitors, printers, network equipment, and so on. Table 1-5 focuses on the most common adapter cards.

Adapter cards have two connections: One connects to the expansion slot, and the other connects to devices. This usually involves a port or plug. Table 1-5 contains the standard ports.

Table 1-5 Adapter Cards

Adapter	Expansion Buses	Ports and Plugs	Details and Descriptions
NIC	PCI, PCIe, or USB	RJ45	Connects the PC to a network.
Wireless NIC	PCI, PCIe, or USB	2.4 GHz Antenna	Connects a PC to a wireless network.
Video Adapter	PCIe, AGP, or PCI	VGA, DVI, HDMI, Component Video, S-video	Translates data into video signal for the monitor.
USB	PCI	USB	Is an adapter in this case. Like an SCSI, it forwards data onto another kind of bus. It often provides both internal and external USB ports.
IEEE 1394 (FireWire)	PCI or PCIe	FireWire	Is similar to USB, but it is almost twice as fast. Commonly used to transfer video or other data intensive applications.

Table 1-5 Adapter Cards *continued*

Adapter	Expansion Buses	Ports and Plugs	Details and Descriptions
Sound/Audio Adapter	PCI or PCIe	Mini DIN (TSR 3.5)	Translates data into audio signal for speakers.
SCSI Adapter	PCI or PCIe	Internal SCSI header and often an external SCSI port	Is an additional bus link, like a transfer station. It forwards data to and form the PC to SCSI HDDs and devices.
RAID Adapter	PCI or PCIe	Multiple hard drive connections SATA, PATA, or SCSI	Controls the spreading of data across multiple HDDs. Commonly used for SCSI but can also be used for SATA.
eSATA	PCIe, PCI	eSATA	Connects external SATA drives to the PC.
Modem	PCI or USB	RJ11	Is like a combination NIC and sound adapter. It connects the PC to an audio/telephone based network.
IEEE 1284 (Parallel Port)	PCI	DB25	Connects peripheral parallel devices mainly printers to the PC. The distinctive cable has a 25-pin D plug on the computer end and a 36-pin Centronics port on the other. Moves data along multiple channels simultaneously (parallel).
Serial Port	PCI	DA15	Connects peripheral parallel devices to the PC. Not commonly used today. Moves data along one channel, bit by bit (serial).

Daughter Boards and Riser Boards

Daughter boards and riser boards are essentially the same device. These smaller boards plug into the motherboard that expand the number of expansion slots, ports, or, in some cases, add devices. If the board is used solely to add extra PCI slots or turn the angle of adapter cards to fit into smaller cases, it is a riser. The two exceptions are Audio Modem Riser (AMR) and Communications Network Risers (CNR). They are an evolutionary missing link between true integrated devices and full-fledged expansion cards.

Storage Devices

There are many types of storage media: magnetic disk, tape, laser, and solid state flash. There are internal drives and external storage devices. Internal hard drives mount in 3.5 inch or 2.5 inch

bays. Optical drives mount in 5.25 inch bays. External drives connect through many kinds of readers and ports. USB, FireWire, and eSATA are common. Card readers and optical drives support flash memory cards and optical discs.

Dynamic and Solid State Drives

Dynamic state drives (DSD) use armatures that move read/write heads over spinning magnetic platters. The disk is organized into tracks (rings) and sectors (radial lines).

Solid state drives (SSD) contain chips that contain NVRAM. This is often called flash memory. The name came from flashing the CMOS Chip's NVRAM to update the BIOS. Solid state HDs, flash, NVRAM, Thumb drives, Jump drives, and USB drives are essentially the same type of device.

Optical Drives CD/DVD/RW/Blu-Ray

Optical disks organize data in a long outward spiral. Optical drives use a laser to shine on the surface of the spinning disk. The laser reflects off the surface and hits a sensor or hits a bump and bounces somewhere else. From the sensor's perspective, it "sees" a binary pattern. Table 1-6 compares the different kinds of optical drives.

Table 1-6 Optical Drives

CD Family	DVD Family	Details and Descriptions
CD-ROM	DVD-ROM	Can only read premade disks.
CD-R	DVD+/-R	(Recordable) Write a disk once and it is read only after that.
CD-RW	DVD+/-RW	(Rewritable) Read and write a disk repeatedly.
(CDRAM is not an optical drive)	DVD-RAM	("Endlessly" rewritable) Used primarily as surveillance camera footage.

Installing SATA, PATA, and SCSI Drives

Serial ATA drives are fast becoming the industry standard. They are hot swappable, and the header must be enabled in the BIOS. eSATA is simply an extension cord that puts a SATA header on the outside of the case for external SATA HDs. To install a SATA drive, simply plug it into a SATA or eSATA header and make sure that header is enabled in the BIOS.

Parallel ATA (PATA) is more complicated. The BIOS manages PATA configurations. There are typically two PATA channels: primary and secondary. Each channel can contain two drives: master and slave. The master/slave or cable select (CS) settings must also be set by jumpers on the drives. The cable select allows the drive at the far end of the cable to be master. Note that, in some cases,

in both 80 and 40 pin PATA environments, the CS simply does not work. Simply set the jumpers to reflect the master on the end and slave in the middle. If you still have no luck, consider an HDD failure or PATA controller failure. Put together, any given PATA drive (HDD or optical) has one of the assignments shown in Table 1-7.

Table 1-7 Typical PATA Settings

PATA Designation	Number	Typical Assignment	Jumper Setting	BIOS Setting
Primary Master	0	Main Hard Drive	Master	Auto Detect
Primary Slave	1	(Available)	N/A	None
Secondary Master	2	Main Optical Drive	Master	Auto Detect
Secondary Slave	3	(Available)	N/A	None

SCSI is actually a small network of devices controlled by an SCSI controller. The controller is a card that plugs into a PCI or PCI-e slot and has one of many different kinds of SCSI style ports on the outside and several internal ribbon cable connections. One way to spot an SCSI cable is its width. It will always be the widest (most pins) in the PC, markedly more than PATA 40, FDD 34, and SATA 7. (SATA sometimes has 15 pins if it provides its own power.) Another way SCSI cables differ from other cables is that they have nine connectors to support the card and eight devices. An SCSI array requires unique IDs, created using a binary code: 3 bits for SCSI1 and 4 bits for Wide SCSI. This code is set by jumper, dip switch, push button switch, or can be configured with a separate SCSI BIOS. SCSI arrays also need a common medium (SCSI cable), termination at each, and a controller card.

Just like on a network, every device needs a unique ID number. SCSI "chains" need terminators at each end to absorb the signal. In place of terminators, it is common to install a termination enabled device at each end to serve as both HDD and terminator.

RAID

Redundant Array of Inexpensive (or Independent) Disks (RAID) has several defined levels, but the most common are 0, 1, and 5. RAID 0 writes the data across two drives. This increases speed, but does not provide any protection. Striping is the technique used to write the data across multiple disks. Raid 1 (mirroring) simply copies one HDD to the other.

In RAID 5, there are at least three HDDs. RAID 5 also strips the data so that it has some benefit of increased performance and spreads out the data in case of failure. RAID 5 is the most common implementation. Hybrids such as RAID 1+0 and 0+1 exist, and they require at least four disks, because they are either two striped disks that are mirrors to two others, 0+1, or they are two mirrored disks striped to two others, 1+0.

Table 1-8 compares SATA, PATA, and SCSI drives.

Table 1-8 Drive Interfaces

Interface	Drives per Channel	Number of Pins	Hot Swappable	Descriptions and Details
PATA, ATA, IDE, EIDE	2	40 80	No	Old standard. Two drives per channel. Jumpers assign master and slave drives.
SCSI	8 or 16	50 68 80	Yes	Typically found on servers. Drives are arranged along a bus-like cable with terminators on both ends. Jumpers or dip switches assign drive numbers in binary.
SATA	1	7 or 15	Yes	Small cable improves air cooling. Faster than PATA. One drive per channel. No jumpers, no master, and no slave.
FDD	1	34	No	Only for the FDD. Pin 1 is usually oriented closest to the power connector, but look for the red stripe. Some old FDD cables support multiple FDDs. They have a twist in the middle of the ribbon connectors.

Media Cards

There is a wide variety of SSD storage cards used primarily in phones, cameras and other portable devices. PCs use card readers to interface with this type of storage media. The secure digital card (SDcard) is a common media card. One particular note about SDcards is they have a switch that makes the card read/write or read-only. Floppy disks also have this feature. SDcards are small and hold a considerable amount of data that is comparable to small HDs.

Other Storage Devices

Floppy Disk Drives (FDD) mount to a 3.5-inch bay and read a removable media, such as the SDcard. Unlike the small hi-capacity SDcard, the floppy disk is about 3 inches square and holds only 1.44 MB.

USB flash drives are essentially a smaller (both in size and capacity) external SSD that connects through a USB port. These are easily lost and should not be used to store secure information.

Network attached storage (NAS) is an HD with a NIC interface. It often uses a web interface and controls user access. These devices are a small office, home office (SOHO) version of proper file servers found in corporate environments. A mapped drive is an icon that is a shortcut to an NAS or file server.

Cooling

There are several methods of removing heat from a PC. The most common solution is a heat fan that blows air over a heat sink that is held firmly to the CPU. Heat sinks use parallel fins to increase the surface area like motorcycle and lawn mower engines. Many GPUs have their own cooling fan and heat sink assembly.

A thermal compound is used between the heat sink and the CPU. Note: The thermal compound is poisonous and toxic to humans. Use care when applying or removing thermal compound. Dust collects on the heat sink, which decreases its efficiency. Use compressed air or a PC vacuum to remove dust.

In some exotic and gaming PCs, liquid cooling systems transfer heat from the CPU to a radiator using water and antifreeze. These work in much the same way as an automobile's cooling system. They are somewhat less reliable, but they provide excellent heat exchange.

Power Supplies

Safety first: Do not open a power supply. It contains capacitors that hold a dangerous charge, even while unplugged. It is a field replaceable unit (FRU). In other words, if it is broken, simply replace the entire power supply. Before sending it to a recycling facility, the capacitors should be discharged by touching and connecting the phase with the ground plug and then the neutral to the ground plug with an insulated screwdriver or pliers.

Most power supplies follow a standard form factor. The myriad form factors of computers warrants an equally diverse number of power supply form factors.

Power supplies are measured in watts. The watts output should exceed the PCs power demand. There are four kinds of power connections from the power supply top to the PC. Berg and Molex are the standard small and large (respectively) connections for drives and other devices. The motherboard has a 20-pin connector and most have an additional 4-pin connector.

Power fluctuations are devastating to a PC. Table 1-9 describes five power fluctuations.

Table 1-9 Power Fluctuations

Power Condition	Description
Blackout	Power failure
Brownout	Too little voltage
Sag	Very brief time (milliseconds) of too little voltage
Surge	Too much voltage
Spike	Very brief time (milliseconds) of too much voltage

Table 1-10 describes solutions to the previous power issues.

Table 1-10 Power Protection Devices

Power Protection Device	Description
Surge Protector	Multiple plugs. Protects against too much voltage. Note: Power strips and standard multiplugs do not offer such protection.
Line Conditioner	Cleans and smoothes the AC power signal.
Standby Power Supply (SPS)	Backup power supply (usually a battery).
Uninterruptible Power Supply (UPS)	A UPS is usually a battery backup to the computer that is recharged by the wall outlet. UPSs are measured by the volt-amp (VA) rating.

Monitors and Display Metrics

Contrast ratio is the comparison of the brightest to the darkest color a monitor can create. The higher the ratio, the more brightness variation exists in the monitor.

Video cards have a basic resolution, usually 640x480 or 800x600, with 256 colors. If the PC boots to this reduced resolution and limited color scheme, it needs a better video driver. Table 1-11 shows the resolutions you need to know for the A+ exam.

Table 1-11 Monitor Resolutions

Name	X Pixels Wide	Y Pixels Tall
VGA	640	480
SVGA	800	600
XGA	1024	768
XGA+	1152	864
SXGA	1280	1024
SXGA+	1400	1050
UXGA	1600	1200
QXGA	2048	1536

These are examples of 4:3 aspect ratios. Many new computers and laptops use a 16:9 aspect ratio (HDTV/widescreen). After the correct drivers are installed, an LCD screen really should be run in its native mode.

CRT

Warning: Do not open CRTs. They are field replaceable units (FRU). In other words, replace CRT. Do not fix them. They contain capacitors that can shock you long after they are unplugged. Before sending CRTs to a recycler for disposal, the capacitors should be discharged by touching and connecting the phase with the ground plug and then the neutral to the ground plug with an insulated screwdriver or pliers.

A Cathode Ray Tube (CRT) monitor has many manual adjustments that should all be set to "middle" level. A beam sweeps sideways lines down the entire length of the screen 60–100 times a second. The width and height of the picture is controlled by controls Vertical and Horizontal, respectively. Contrast and brightness should also be set for a middle setting. Contrast controls the ratio of the brightest and darkest light. Brightness controls the overall intensity of the display. They are physically measured diagonally. A 17-inch display means it is 17 inches of viewable display measured from diagonal corners. Interlacing draws the odd numbered rows of each frame, and then one-sixtieth of a second later, fills the space with the even numbered rows.

LCD

Liquid Crystal Display (LCD) is quickly replacing large, heavy CRT monitors. LCD monitors are illuminated several different ways: a flat florescent tube, a panel of LEDs, or in the case of LCD projectors, a bright bulb. LED backlighting offers more clarity, thinner, and is more rugged than the florescent.

Passive matrix LCD monitors have chips that control the vertical and horizontal sets of wires. When a pixel is charged by both chips, it turns on. Active matrix monitors act like one big integrated circuit with the crystals for transistors.

Other Display Devices

The two principal measures of projectors are resolution and lumens. A lumen is a measure of brightness. There are two competing display technologies that make projectors and, by extension, rear projection TVs/monitors work. LCD is a small high-definition LCD screen with a light shone through it, like a stained glass window. Digital Light Processing (DLP) uses an array of mirrors that reflected light either onto the screen or away, in much the same way optical drives read their media.

It is not uncommon to have multiple monitors on one PC. The most common case of this is a laptop paired with a projector. Function keys toggle among settings that mirror the display, extend the display from the main screen onto the projector, or run the projector exclusively and shut off the main screen. Workstation and gaming PCs commonly have two or more monitors usually set up as a continuation from one to the next. The display settings in the Control Panel provide more control and support for multiple monitors.

I/O Devices

Most input/output (I/O) devices connect to a PC via a USB port. Even wireless devices ultimately terminate at the PC through a USB port. All I/O devices require drivers. Drivers are instructions to

teach the OS how to use and communicate with a new piece of hardware. They are normally stored on CDs that come with the device, but they can also be downloaded from the manufacturer's website. Often, drivers are included in the OS for commonly used devices, such as mice, keyboards, USB storage, and many printers.

Mice and Keyboards

Optical mice use an LED to illuminate the area directly beneath the mouse and a motion-sensing technology to determine the direction and speed of that surface as the mouse moves. Ball mice use a ball that roles on two rollers mounted perpendicular to each other. One measures movement along the Y axis and the other on the X axis.

Speakers and Microphones

The audio port uses a "headphone jack." The formal name for this port is a mini DIN Tip Sleeve Ring (TSR) 3.5 millimeter jack. This makes the audio port compatible with standard stereo equipment. A higher quality audio connection splits the signal into component signals. Dolby 5.1 uses five and often seven ports each to a dedicated speaker. These are analog signals, which means that the sound card is responsible for digital-to-audio conversion (DAC). Sony/Phillips Digital Interface Format (SPDIF) sends a digital signal over a fiber-optic line to the speakers where it is decoded and converted to an analog signal and, ultimately, an audible sound.

Microphones are essentially speakers in reverse. The diaphragm moves in response to sound waves. That signal is converted into a digital signal inside the sound card. Note: The pink is a microphone port, the blue color is a line in like a stereo or iPod, and the green color is audio out for speakers and headphones. These are de facto standards and are, therefore, not consistent among all manufactures.

Video Input Devices

Still image, video, and webcams work on the same basic principal. A charged coupled device (CCD) or complementary metal-oxide semiconductor (CMOS) converts a visual input into a binary stream through an analog-to-digital conversion (ADC). A significant difference is the way in which the camera transfers that image to the PC.

With standalone video cameras (camcorders and digital cameras), video and pictures are often stored as files that are transferred to the PC, such as a USB flash drive through a USB, FireWire port, or Bluetooth connection. In streaming video environments (security cameras, TV, and movie production), the ADC can take place in the camera and stream a digital signal through a USB or FireWire port.

In many situations, the camera does not stream a digital signal. Instead, it sends an analog signal through RCA, S-video, network interfaces, or proprietary ports. In this case, the ADC takes place in a video capture card.

Once on the PC, the video must either be stored or viewed in real-time or both. Applications such as video-editing software manipulate the raw video, much like a word processor can open, edit, and save a document.

Other I/O Devices

Some devices require additional applications to work properly. Biometric devices combine an input device with an application that compares a unique pattern retina, fingerprint, palm print, and so on, to a password. That password is then used to gain access to the OS or file. Touch screens are an input device that maps the coordinates of the touch location to an application that translates that into executable commands or files. Barcode readers shine a laser on a black-and-white barcode. The laser reflects the pattern to a sensor and reads the code. That code is compared to a database and the associated item or file is accessed.

Laptop Hardware

There are a few types of laptops, each with a different philosophy. A general laptop (notebook) is a portable, battery-powered desktop. A netbook is a barebones, tough, lightweight notebook that is cheap, but has limited capabilities. An ultra mobile personal computer (UMPC) is powerful, small, and very expensive compared to traditional laptops and netbooks.

Laptop Form Factors

Most components in a laptop are specially designed to reduce weight, space, heat, and power consumption. As a result, many have unique form factors. Small Outline Dual Inline Memory Module (SODIMM) and MicroDIMM are RAM form factors used in laptops and mobile devices (smart phones), respectively. Laptop hard drives measure 2.5 inches and can either be dynamic (platters, read/write heads) or solid state (flash). Optical drives are often removable or purely external and connect through a USB port.

ACPI Power Management

Advanced Configuration Power Interface (ACPI) is found in the power management applet in the Control Panel. On a historical note: Advanced Power Management (APM) is the predecessor of ACPI and was supported in 9x, 2K, XP. Vista and Windows 7 do not support APM. ACPI is not exclusively a laptop technology, but it is designed to maximize battery life. ACPI must first be enabled in the BIOS, like an integrated device. There are six power states, as shown in Table 1-12.

Table 1-12 ACPI Power States

State	CPU	RAM	Description
S0	On	On	PC is fully on.
S1	On	On	Power saving mode.
S2	Off	On	More power saving.
S3	Off	Slow	Standby mode.
S4	Off	Off	Hibernate mode.
S5	Off	Off	PC is fully off.

Batteries

Batteries are a major issue with all portable devices. Physical dimensions and connections vary widely based on the manufacturer. In addition to laptop batteries' proprietary nature (noninterchangeable), they are also measured by the number of cells and Amps per hour (Ah). A cell is the actual electrochemical unit. Ah is a rough estimate of how many amps are delivered over time.

Over time, the electrochemical reaction happens faster and leads to the battery forming a "memory." Periodically, technicians "exercise" some batteries to combat memory problems. To exercise a lead-acid, alkaline, and Ni-Cad, drain the electricity completely and then charge it slightly above normal several times in a row. Ni-Mh, Li-Ion, and Li-Po naturally do not have memory problems. All batteries from giant UPS to BIOS must be disposed of according to local government regulations. Table 1-13 describes the characteristics of different battery types.

Table 1-13 Batteries

Battery	Characteristics	Usage
Ni-Cd	Heavy, long life, bad memory.	Power tools, cordless phones, camera flash, motorized toys. Anything that draws a big load and does not live long outside the charger.
Ni-MH	Moderate weight, moderate life expectancy.	Cell phones, GPS systems, digital cameras, flashlights. Most things that are meant to be carried around for a while but don't have a large electrical load.
Li-Ion	Light, long lasting. It will catch fire if overcharged or too much draw.	Cell phones, laptops, and medical devices like pacemakers and monitors.
Li-Po	Quick recharge, small, light, expensive, medium lasting, medium life span.	PDA, laptops, MP3 players, gaming devices, radio controlled toys.

Laptop I/O Devices

Laptops and portable devices have many unusual I/O methods. Touch pads and touch screens are essentially the same device. A touch screen is clear and sits in front of a monitor. A digitizer is a higher resolution touch screen. Often, it uses a stylus, which is a sharp stick that allows users to contact the screen with precision. This should not be confused with a point stick, which is a pointing device that functions like a small "joystick" game controller in the middle of the keyboard that moves the arrow on the screen. Function keys control many aspects, such as switching between external monitor modes, ten-key pads, and screen settings.

Laptop Expansion

Mini-PCI expansion allows for some additional functionality of laptops. Personal Computer Memory Card International Association (PCMCIA) cards can be used if the laptop is designed for them. Express cards look and act much like PCMCIA cards, but they are slightly narrower. Table 1-14 compares the laptop expansion buses.

Table 1-14 Laptop Expansion Buses

Bus Type	Thickness	Usage and Description
PCMCIA Type I	3.3 mm	SRAM Flash (like a USB flash drive).
PCMCIA Type II	5 mm	Standard PCMCIA, used for Modem, NIC, WiFi.
PCMCIA Type III	10.5 mm	Double thick primarily used as an HDD.
Express Card /34	5 mm	The name notates the length in mm. 34 mm.
Express Card /54	5 mm	Usually used for card readers and sometimes the cutest little HDD ever made (stick with solid state flash drives).

Printers

There are many kinds of printers. The A+ exam focuses on a few common ones: laser, inkjet, impact (dot-matrix), solid ink, thermal, and dye-sublimation. The following is a list of common printer measurements:

- **Pages per minute (PPM):** Measures printer speed.
- **Characters per second (CPS):** Measures printer speed in impact (dot-matrix) printers.
- **Dots per inch (DPI):** Measures quality (resolution).
- **Mean time between failures (MTBF):** Measures reliability.
- **Cost per page (CPP)**: Measures the price of each printed page. A proper measurement of CPP takes into consideration the cost of ink, paper, electricity, and scheduled printer maintenance.

Laser

Laser printers are good balance between cost and quality. They are quiet, reliable, and produce high quality printouts. Laser printers are not cheap, and toner can be pricy. Except for the initial costs, the actual CPP is low. Table 1-15 outlines the six steps of the laser-printing process with a helpful mnemonic.

Table 1-15 Laser Printing Process

Step	Details of Each Step	Mnemonic
1. Cleaning	The drum is cleaned by a wiper or in some cases an electrical charge can drop excess toner from the drum.	**C**alifornia
2. Conditioning	Puts uniform charge of -600 VDC. This phase is also called charging.	**C**ows
3. Writing	Laser traces the image on the charged drum and changes the voltage to -100 VDC in those areas the laser touched.	**W**on't

Table 1-15 Laser Printing Process *continued*

Step	Details of Each Step	Mnemonic
4. Developing	Negatively charged toner is applied to the drum and sticks to the areas with altered voltage.	**D**ance
5. Transferring	The secondary corona wire charges the paper. The toner is statically attracted to the paper.	**T**he
6. Fusing	Rollers melt the toner and embed it into the paper.	**F**andango

Another mnemonic that is used to remember the Laser Printing Process: Cool Cowboys Will Drive Their Fords.

Inkjet

Inkjet printers include either thermal or piezoelectric nozzles. Thermal nozzles boil the ink and jets of steamed ink shoot onto the paper. Piezoelectric nozzles energize crystals that vibrate and control ink flow.

Impact Printers

A dot matrix printer uses a group of pins that strike a ribbon against the paper. When the pins are used in combination, they create shapes of letters. Daisy wheel printers have a wheel of letter symbols and numbers that rotate into position, and then the solenoid hits the letter into the ribbon and onto the paper. Impact printers are measured in CPS, not PPM. Near letter quality (NLQ) is the best quality a dot matrix printer can have. Impact printers are used on carbon copy paper because the impact travels through to the carbon copies beneath the original paper.

Solid Ink

Solid ink printers use a combination of laser and inkjet technologies. The solid ink is melted and sprayed (written) to a drum that is transferred onto the paper. These printers are used for posters and other large format, high quality photos.

Dye Sublimation

Dye sublimation is a process that prints the page four times each with a different color of ink. This produces long lasting, high quality images.

Thermal

Thermal printers are used most often on point-of-sale systems, thermal printers print receipts, and other inexpensive continuous feed outputs, such as those produced by EKGs, label makers, and old fax machines. The paper is stored on rolls and is treated so that heat darkens it.

Printer Connections

Regardless of the physical connection, the drivers must be installed on the PC from which the print job is sent. Drivers can be found on the installation CD or on the manufacturer's website. Printer drivers and printer firmware can be updated based on the manufacturer's recommendation. The three primary methods to connect to a printer are

- Directly connected to a PC via USB, parallel, FireWire, or infrared (IR).
- Directly connected to a remote networked PC that acts as a print server for the network.
- A networked printer that has a NIC and is a fully capable network device.

USB is the most common method to connect a printer because of the autoconfiguring nature of the USB interface. The entire process is /Parallel (ECC and ECP)/ IrDa.

Local Versus Network Printer

TCP/IP printers are controlled by a print server. Print jobs are sent to the print server, which are forwarded to the printer. A formal print server is a standalone PC with a locally connected printer. Many print servers are integrated into the printer, which eliminates the need for the additional computer and simplifies user management. Print jobs are directed to either uniform (or universal) naming convention (UNC) or an IP addresses. A UNC is always formatted with backslashes, such as \\hostname\sharedfolder\sharedresource.

Printer Maintenance

To improve longevity and reliability, it is important to keep printers clean, supplied, and updated. Note: Always turn off and unplug the printer before cleaning it. Table 1-16 outlines printer maintenance.

Table 1-16 Printer Maintenance

Maintenance	Details	Mnemonic
Clean	Use a vacuum on loose toner and dust.	**C**lients
	Use damp cloth for general cleaning.	
	Follow the manufacturers recommendation for cleaning the rollers and other parts.	
Supply	Paper.	**S**eldom
	Ink/toner (all colors).	
Calibrate	Run printer self checks to align print heads and clean nozzles.	**C**learly
Update	Drivers.	**U**nderstand
	Firmware.	

This page intentionally left blank

2

Troubleshooting

Troubleshooting repair and maintenance is the reason technicians exist. Although it does not appear on the 220-702 CompTIA A+ Exam, it makes up 20 percent of the 220-701 CompTIA A+ Exam. Just because it is not formally tested on the second exam, it is still very much a part of a technician's thinking and methodology.

Troubleshooting Process

Troubleshooting can take place face-to-face, over the phone, via chat, text, e-mail, avatar, or, in the case of a bench tech, without any customer interaction. A good PC technician is well versed in all these methods and *always* maintains a positive and productive attitude, regardless of the customer's mood or personality.

Gather Data From the Customer

Find out the following:

- Customer's name and contact info
- Style, brand, and model of malfunctioning device
- OS (including the service pack in use), antivirus (AV), and method of networking and Internet access

Start the troubleshooting process with open-ended questions, such as, "How may I help you?" Narrow the focus of your questions to isolate the fault; for example, "Does this happen every time it boots or only sometimes?" or "Does the light blink when the cable is connected?"

Verify the Obvious Issues

In the early questioning phase, eliminate the obvious problems first. Usually, you can eliminate broad areas that work fine and do not need further scrutiny. For example, to rule out basic connectivity issues, you might ask, "Let's just double-check the cables to make sure they are securely connected. Do any feel loose?"

Try Quick Solutions First

Briefly assume that the problem is simple to fix or is a simple user error. Polite, on-the-spot user training might solve the problem. "Laptops often have a switch that enables the wireless network card. Let's start there," or "It's funny, but some printers are actually brand conscious about paper. Why don't we try a brand new pack of paper to see if yours is 'paper picky?'"

Gather Data from the Computer

Check for damaged cables, devices plugged in incorrectly, bent pins, noises, blue-screens-of-death, burning smells, and so on. Watch the computer boot, note any error messages, and reproduce the problem.

Evaluate the Problem and Implement the Solution

Make an educated guess, make a plan of action to prove or disprove your theory, and test it. (Before doing anything to the computer, perform a backup.) Document your work. Verify full system functionality and implement preventative measures. Be sure to reset any printer counters and chassis intrusion settings.

Close with the Customer

Explain what you found, what you did, and how you did it to the customer in language free of acronyms and computer jargon. Make sure that this is documented to create a trail as to what was done. This helps in troubleshooting later on with the same customer. Be sure to thank them for their time and business.

Tools

The following are common tools found in technicians' tool kits:

- Standard flathead (minus) screwdriver
- Phillips-head (plus) screwdriver
- 5-in-1 screwdriver
- Tweezers/hemostat
- Part retriever (long, flexible, three-prong grabber)
- Needle-nosed pliers
- Torx screwdriver (star-shaped screwhead)
- Digital multimeter
- Vacuum with HEPA filter
- Rubbing alcohol that is greater than 70 percent isopropyl

- Cotton swabs
- LCD cleaning solution or wipes (Never use a paper towel on a soft LCD screen. It will scratch it.)
- Mild detergent solution or wipes (for the outside of the case)
- Glass cleaner (for CRT monitor screens, your safety glasses, and your hands after you've picked up toner).
- Paper towels (only for general cleanup, not for inside the PC)
- Soft, lint-free cloth
- Compressed air (Always use right side up.)
- Antistatic wrist strap to prevent electrostatic discharge (ESD)
- Grounded mat to work on
- Antistatic bags to ship and store components
- Specialized testers, such as cable testers, loopback plugs, and POST cards
- RJ-11, RJ-13, and RJ-45 crimping tool (RJ-11 for phone, RJ-13 for modular phone, like in an office, and RJ-45 for network cables)

Multimeters and Electricity

The following is a list of straightforward statements that you should commit to memory regarding multimeters and electricity for the A+ exam:

- Power (the ability to do something) is measured in watts (W).
- Voltage is electrical potential (pressure) on the circuit.
- Amps are the current (flow) of electrons.
- Resistance slows the current and gives off heat. (That is why computers are hot.)
- P = IE, meaning power (P) is equal to amps (I) multiplied by volts (E).
- V = IR, meaning voltage (V) equals amps (I) multiplied by resistance (R).
- Alternating Current (AC) goes long distance and cycles 115 volts at 60 Hertz; 250 volts at 50 Hertz in Europe. (Other combinations exist elsewhere.)
- The power outlet in a wall is measured in AC.
- Direct Current (DC) maintains a constant voltage.
- Inside the PC, electricity is measured in DC.
- Resistors are measured in ohms.
- Capacitors are measured in Farads.

- Continuity sends the signal through one lead, and the other lead listens for it. When it hears the signal, it beeps, which verifies that they share a common connection. Don't send current through sensitive electronics. It is mainly used for wire identification.
- A good fuse reads few, if any, ohms.
- A bad fuse reads infinite ohms (because the wire inside is broken).
- A good speaker reads 8 ohms (although, sometimes, they are supposed to read 4 ohms).
- A bad speaker reads any other amount of ohms, usually 0 ohms (shorted out) or infinite ohms (separated).
- A simple circuit includes a power supply, a load, and connections between them in a circle (hence, the word *circuit*).

Troubleshooting Hardware

Troubleshooting hardware is a major part of the PC technician's job. Unlike operating systems with countless settings and controls, hardware is much more straight-forward. Use a strict fault isolation technique. Make only one change at a time so you can be sure of the problem. Document your work.

BIOS Settings

There are many settings in the BIOS that can cause problems. Here are some basic settings that should be set in the BIOS:

- Remove any BIOS passwords by parking the jumper (placed on only one pin) on the motherboard and restarting the PC.
- Make sure that the integrated devices are enabled.
- Set the boot sequence to select a media that has a master boot record.

Device Management

If the device cannot be "seen" by the operating system (OS) and you visually confirm that it is present, look in the BIOS and see if it is disabled.

Another scenario is the OS knows that the device is present, but cannot access or use it. Check for a missing driver in the device manager. The device manager flags troublesome devices with a yellow exclamation point or question mark. Devices can also be disabled or enabled in the device manager.

Controller Cards and Media Readers

SDcards (and FDDs) have switches that convert from read/write read only. Always use the Safely Remove Hardware procedure to unmount the removable media before unplugging it.

Barebones and Known-Good Techniques

One method of troubleshooting is to strip the PC to the fundamentals: motherboard, processor, and RAM. If it boots properly, add the HDD and reboot. If it boots properly, add an optical drive and reboot. Repeat this process until the PC is reassembled. At some point, it will not reboot properly. The last thing you added is likely the fault. To be sure, use a known-good replacement instead. If it boots properly with the known-good device, you have verified that the questionable device is the fault.

POST Cards

Power-On Self Test (POST) cards plug into an expansion slot on the motherboard and "watch" the PC's POST. The POST card finds the problem and displays a code which identifies the faulty device.

Overheating

Overheating is caused by several reasons:

- Inadequate or ineffective heat removal devices, such as heat sinks.
- Dust prevents heat transfer from sinks to the air.
- Inadequate or misdirected air flow through the PC.
- The system could be over clocked.
- The thermocouple could not be connected properly and gives inaccurate reading to the BIOS.
- The fans could malfunction or simply not be powered.
- Liquid cooled systems can have leaks or air in the lines that reduce flow and heat transfer.

Power Supply Testers

While wearing your properly connected wrist strap, use a multimeter to test the DC output. Set the multimeter to read volts DC (20 V DC on older, non-autoranging multimeters). Put the common lead on the black ground wire or directly on the chassis (metal frame). The chassis is the electrical ground. Use the test lead to contact the other colors on a plug. The colors should read as shown in Table 2-1.

Table 2-1 Power Supply Voltages

Color	Voltage	Mnemonic
Yellow	12 V	**Y**ou
Red	5 V	**R**eally
Orange	3.3 V	**O**ught to
Black	0 V	**B**elieve
White	–5 V	**W**arren
Blue	–12 V	**B**uffett

Troubleshooting FireWire and USB

If given a troubleshooting scenario about a peripheral, check the following:

- Make sure that the port is enabled in the BIOS.
- Make sure that the device is enabled in the device manager.
- The peripheral gets its power either from the USB port or its own power supply. Make sure it has power and is turned on.
- Is there an application missing that controls the peripheral? For example, a video camera needs a utility or third-party application to view the video stream. The Internet requires not only the NIC to work, but also a browser to see the web content.
- Not to overlook the obvious, but make sure that the cable is securely connected to the port at both ends and that it is in the correct port. A USB plug fits surprisingly well into an NIC port.

Troubleshooting Parallel, Serial, and SCSI

Parallel, serial, and SCSI are not plug-and-play. They are older technologies and require manual setup and configuration.

A parallel printer cord has two rows of pins on the PC side and a Centronics port on the printer side. Many older parallel port printers must be "online" to print. This is a button on the printer.

SCSI cords and ports contain the most pins of any port, ranging from 50 to 80 or more. SCSI chains can have 7 (narrow or normal SCSI) to 14 (wide SCSI) drives or devices. Each device must have a unique SCSI ID set by jumper or push button. Each end of the SCSI chain must end at a drive set for termination or a specific termination plug.

Serial ports had nine pins arranged in two rows and the only male port on a PC. Serial ports use a utility, such as HyperTerminal, to communicate with or sync with devices. Note: These look similar to VGA ports. VGA is female and has three rows of five pins.

Troubleshooting LCDs

If the screen is readable but not backlit, check the monitor and power/battery settings. If those are correct, the backlight is either not receiving power from the inverter or the florescent panel is broken. In the case of LED backlit, check the inverter first.

If the screen looks like broken glass, the LCD screen is cracked. If this is the case, check to see if the backlight is also broken.

Odd flashing colors or bars indicate a driver issue or perhaps an overheating PC. A flickering screen, or one that is "tinted" a certain color, is usually a loose monitor plug.

Troubleshooting Operating Systems

Operating systems have countless settings, drivers, and sequences any of which can cause a problem. Fortunately, there are techniques and many utilities that aid your troubleshooting. A quality technician is equally proficient in troubleshooting both hardware and software.

XP/Vista Boot Sequence

The following list describes what happens when the PC is booted. It is important to know this sequence in order to troubleshoot boot problems.

1. After POST, which also checks all the embedded and integrated devices, BIOS looks for the master boot record (MBR). It is found on the first active partition. The MBR figures out which kind of file system is running and then loads NTLDR.
2. NTLDR protects the system by switching to protected mode and then starts the file system.
3. NTLDR reads BOOT.INI. This is particularly important for dual-boot PCs. Dual-boot PCs use BOOT.INI or BOOTSECT.DOS to manage which OS to boot.
4. NTLDR runs NTDETECT, which installs device drivers. NTLDR then runs NTOSKRNL.EXE and HAL.EXE. These files begin services and further separate the hardware from software, with the hardware abstraction layer (HAL).
5. NTLDR loads the HKEY_LOCAL_MACHINE\SYSTEM Registry hive that loads the device drivers.
6. NTLDR passes the torch to the NTOSKRNL.EXE, which loads WINLOGON, and the user is asked for logon credentials.

OS Tools and Utilities

The following list of OS tools and utilities are available in XP and Vista:

- Last Known Good Configuration allows the computer to “go back” to a previous configuration in the event that something changed that prevents it from booting.
- MSCONFIG/Startup allows fine control over exactly what is loaded during startup.
- System Information shows detailed information about the devices and components of the PC.
- System Restore allows you to take “snapshots” of your PC and later return to that state if something goes wrong.
- Remote Desktop Versus Remote Assistance allows users to connect to other computers through an interface that replicates what it is like to be there. Remote Assistance allows help-desk technicians to locate and fix problems in customers’ computers.
- Task Scheduler automates the timing of tasks and utilities so that they can run after hours, at start up, or shut down.

- NTBACKUP starts the Automatic System Recovery, which returns the PC to a former state, similar to System Restore.
- Event Viewer logs many things, such as start up errors, user logins, system failures, memory problems, and so on.
- Services are resources for other computers on a network, such as file sharing and remote desktop.
- Performance Monitor watches how the PC uses its resources.
- DEFRAG rearranges the files on the HDD so they are more efficient to read.
- Check Disk checks for bad sectors on an HDD.
- Regional and Language and Ease of Access settings allow technicians to customize a PC to fit the needs of customers with special language or physical needs.

CLI Syntax and Switches

Command Prompt is launched by entering CMD in the Run line or via shortcut under Accessories. Remember, a directory in a command line interface (CLI) is the same thing as a folder in a graphic user interface (GUI). Almost every command has switches that customize how the command is executed. There is usually an argument, which is the file or destination or the subject or recipient of the command. Syntax describes how to type the command.

All command-prompt statements follow the same syntax (grammar): Command (space) Argument Switch. In other words, Verb, Object, Modifier (see Table 2-2).

Table 2-2 Command Prompt Syntax

Command	Argument	/Switch
“Do this”	“To this”	“Like this”

Basic Commands

Table 2-3 shows basic navigation and file-maintenance commands. They are entered using the Command Prompt.

Table 2-3 Basic Commands

Command	Description
DIR	Shows the contents of the current directory.
CD	Changes the focus to another directory.

Table 2-3 Basic Commands *continued*

Command	Description
MD	Makes a new directory.
RD	Removes a directory.
Copy /a /v /y and	Copies files to a new location. /a copies ASCII text files. /v verifies the copy was successful. /y automatically overwrites existing duplicate files without prompting. (Remember "Y" as in "Yes, please overwrite.")
xcopy	Copies folders and their contents to a new location.
/?	Add this switch to a command and the output displays information about the command, including a brief description, syntax and switches.

Disk Management and Troubleshooting Commands

Table 2-4 shows some troubleshooting commands.

Table 2-4 Disk Management and Troubleshooting Commands

Command	Description
Chkdsk /f and /r	Checks for bad sectors on the HDD. /f attempts to fix bad sectors found on the HDD. /r attempts to recover lost data from bad sectors found on the HDD.
SFC	System File Checker scans and verifies the versions of all protected system files upon the next restart.
Format	Creates partitions on the HDD.
MSCONFIG	Launches MSCONFIG (a powerful OS configuration file).
MSINFO32	Launches MSINFO32 (info about the PC).
DXDIAG	Checks device drivers.
REGEDIT	Lets you edit your registry.

Network Troubleshooting Commands

Table 2-5 shows the commands used for network troubleshooting.

Table 2-5 Network Troubleshooting Commands

Command	Description
IPCONIFIG (all, release, renew)	Displays IP address of the PC. /all displays all the network identification information of the PC, including MAC address, gateway, and subnet mask. /release flushes the leased IP address from the NIC. /renew asks for a new IP address from the DHCP server.
PING (/t and /l)	Tests connectivity to another host on the network. /t keeps pinging until the technician enters CTRL-Break or CTRL-C to stop pinging. /l followed by the length changes the size of the ping packet.
TRACERT	Like ping, it tests connectivity, but TRACERT maps the exact route the packet took and displays the name of the routers along the way (useful when determining if the network problem is on your end or the ISP's).
NSLOOKUP	Troubleshoots DNS servers.
NET	Updates, fixes, or views network settings.
NETSTAT	Shows real-time network connection activity on all ports.
NET USE	Manages connections to shared resources.
Telnet	Connects to a remote computer via CLI.
SSH	A more secure remote computer connection than Telnet.

Disk Management

There are a few important locations (or paths) to know. System files, fonts, temporary files, logs, and anything else associated with the OS is stored in C:\Windows. C:\Program Files contains folders of most of the installed applications. Each folder is organized in the way the application creators dictate. C:\users (or documents and settings in XP) contains a folder for every user that contains user-specific information, desktop settings, documents, favorites, and so on.

Offline files and folders is an automatic way to sync "working copies" stored on portable devices with sporadic network connectivity, with original documents stored on a server.

Another method of simplifying remote storage is mapped drives. This shortcut looks and acts like just another storage volume "computer" (or My Computer in XP). Mount points do not use letter assignments and do not need to be mapped to the root of the destination volume. This allows users to store and access files seamlessly in individual and dedicated space on a remote server.

To make a new volume, the HDD must be prepared by partitioning and formatting. A physical HDD can have up to four partitions, only one of which can be active. Active means the one from which the Master Boot Record (MBR) was copied into RAM on boot. An extended partition is not the bootable, but it can contain many logical drives. A logical drive is what the user sees in "Computer" C:, D:, and so on. After the partition is created, it must be formatted. New Technology File System (NTFS) is the current standard file system for HDDs. FAT32 was used in the Windows 9x family.

In XP and Vista, Disk Manager allows more control of partitions and unallocated disk space. A RAID controller allows the technician to manage multiple drives that work together to reduce data loss. RAID should not be confused with a spanned volume, in which two or more disks appear to the user as one large logical drive.

Common OS Problems and Errors

Table 2-6 contains common OS problems and their associated symptoms.

Table 2-6 Common OS Problems and Errors

Symptom or Error Message	Problem or Solution
Device or peripheral not recognized by OS	Device malfunctioning, is not powered, not connected properly or the OS is using incorrect or corrupt drivers.
Auto-Restart / Auto-Shutdown	Heat forces the PC to shut down to protect itself (check fan). Corrupt boot file in the MBR can cause autorestarts.
Bluescreen and System Lockups	Badly written software. Reinstall offending application.
"Invalid boot disk"	The MBR of the boot media does not contain bootable files.
"Inaccessible boot drive"	The BIOS is looking for boot files to boot, but it cannot find the drive.
"Missing NTLRD"	The MBR of the boot media does not contain bootable files.
"Device (or Service) failed to start"	A device or service did not connect and start up properly during boot.
"Device (or Program) in registry not found"	The registry thinks there is a device or program that does not exist. (Install and properly uninstall the device or program.)

Troubleshooting Printers

Store paper in a cool, dry environment to reduce paper pickup problems and jams. The tires that pick up the paper wear out over time and need to be replaced. The spring that holds paper against the tire also is problematic over time. Rollers and drums are replaceable. Keep the printer clean. Use mild detergent (no ammonia) on the outside, and 70 percent isopropyl and brushes to collect toner on the inside. Use rubber conditioner on the tires.

Table 2-7 lists common printer problems and their associated symptoms.

Table 2-7 Common Printer Problems

Symptom	Problem or Solution
Printer does not print at all.	1. Make sure it has paper. 2. Make sure all doors and access panels are securely closed. 3. Check power and PC connection. 4. Make sure the printer is on. 5. Check for filled ink and toner cartridges. 6. Check the print spooler; there may be a “stuck” print job before yours. Clear the stalled spooler and print again. 7. Check the device manager to ensure that the port is working properly. 8. Check the printer applet in the Control Panel to make sure it is installed. 9. Check the application printer dialog box; you might be printing to a different printer.
Blank pages.	Out of ink or toner.
Light color or “cloudy,” text seems to “vanish” into white areas.	Low ink or toner. Remove toner and (gently) shake from side to side to redistribute the toner.
Laser printer produces “smudgy” images and text.	The fuser is not working properly.
Image is “tinted.”	One or more of the color ink or toner cartridges is low or out.
Streaks or lines on the paper.	Replace the toner cartridge.
Predictable tick marks.	Clean or replace the drum.
Prints gibberish characters.	Reinstall the drivers or clear printer queue, turn off the printer, and reboot the computer.
More than one paper enters feeder at the same time.	Humidity causes paper to “clump.” Store paper in cool dry area.
Printer will not pick up the paper.	Clean the grip wheel with some rubbing alcohol. If the wheel surface is smooth from excessive wear, replace the pickup roller.

Table 2-7 Common Printer Problems *continued*

Symptom	Problem or Solution
Paper tray does not push paper up high enough.	Check spring tension in the tray.
Alphanumeric codes.	Look at the manufacturer's documentation or website to translate the code.
Out of Memory code.	The print job is too big for the print server's memory.

Troubleshooting Laptops

Before opening laptops and portable devices, always back up the data and perform a proper shut down. If the shut down "hangs" (seems stuck and fails to turn off), push and hold the power button for five seconds to force the power off. Next, remove all unneeded peripherals (they often provide their own power sources). Finally, remove the laptop's battery. Note: A few laptops have multiple batteries. Be sure to remove all of them.

To test a battery and power transformer, use a multimeter to measure the DC power adapter's and the battery's output. Compare them to the manufacturer's documentation. To test the longevity of the battery, play a DVD or another power-hungry application to see how long the battery lasts on a full charge. If this is an unacceptably short time (30 minutes, for example), replace the battery.

Function and toggle keys alternate keyboard, video, audio, and wireless modes. This means another level of complexity when troubleshooting such areas on a laptop. For example: Is the LCD screen broken or is the video being sent exclusively to an external monitor port? Is the NIC driver not working or is the wireless NIC turned off?

Laptops commonly overheat and shut down. Use compressed air or a vacuum to remove dust and lint in the vents. Educate the user not to block vents with blankets or books. Also, check for latest BIOS updates, because that is what controls the cooling system.

Troubleshooting Networks

Always check the physical layer first. All devices get both a power and an information cable. Look for erratically blinking lights that indicate network traffic and visually inspect cables for damage. In a wireless environment, physical means in range and right frequency (or channel).

All devices on a network must have unique IP addresses and hostnames. MAC addresses are already unique. Every device on a basic LAN must have a common gateway and subnet mask. Any deviation in this is cause for connectivity issues. Note: Networks can be complicated with multiple routers and complex addressing schemes. For the A+ exam, focus on a basic stub network: one Internet connection, one router, one switch, and many PCs (see Figure 2-1). In the case of a home wireless network, the switch and router is usually the same device.

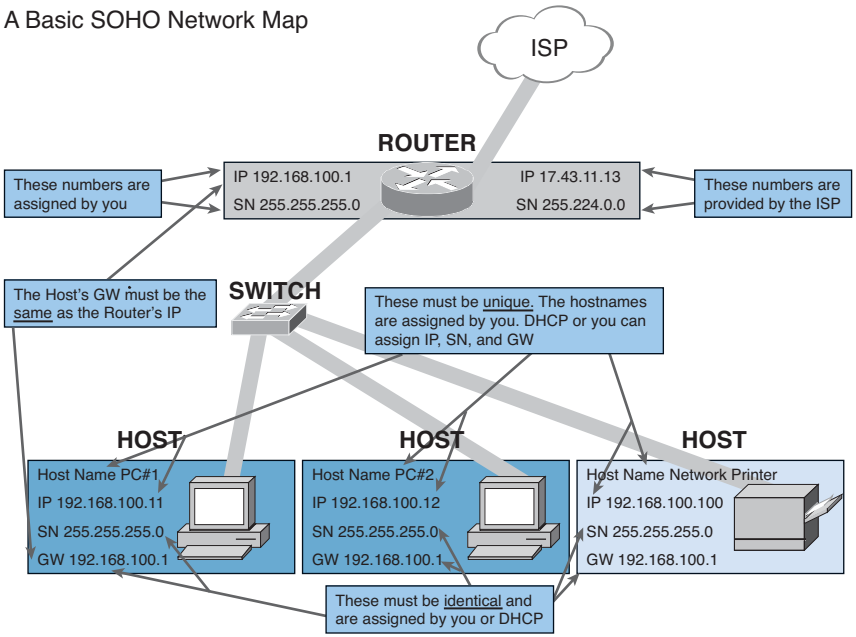


Figure 2-1 Basic Home Network

Continue moving up the OSI model, and make sure that the sessions are established correctly, especially in a dialup or ISDN environment. In the presentation layer, check for file compression, encryption, and missing plug-ins and viewers. At the application layer, a program needs to present the data to the user. Keep in mind that European versions of Windows do not include Internet Explorer. Finally, consider that the user might be the source of network issues and could use some respectful and courteous training.

Troubleshooting TCP/IP

Use **ping** to verify that the protocol stack is working properly. First, ping 127.0.0.1, which is the loopback address. Then, ping your own IP address, your gateway, and a remote site (for example, **ping 209.202.161.67** or **www.informit.com**), assuming there are no DNS issues. If there is a failure somewhere, go to that device and troubleshoot from there. In more complicated LANs or WLANs, use **tracert**. The traceroute command returns all the networking devices that are working properly. Note that some routers and firewalls drop **tracert** requests in an effort to fend off denial of service (DoS) attacks. A failed **tracert** does not necessarily indicate a network problem.

Other Network Troubleshooting Techniques

ipconfig /? shows all the arguments of the command. A particularly useful one is **ipconfig /flushdns**, which forces the resolution of Domain Name System (DNS) entries. Other less used commands are **NSLOOKUP**, which asks a DNS server what IP address is mapped to a specific friendly name; and **NETVIEW**, which shows other PCs in your workgroup.

Preventative Maintenance

Preventative maintenance is a critical part of a technician's job. There are four main areas of preventative maintenance: Backup, Update everything, Clean, and Schedule tasks (Mnemonic: BUCS). Remember it like this: Preventative maintenance saves you big "BUCS."

Backups

There are five kinds of backups (see Table 2-8). Set up a schedule and implement these backups on a regular basis.

Table 2-8 Backups

Backup	Description
Normal or full	Everything gets copied.
Copy	Makes a backup, but does not mark files with the archive bit.
Differential	Backs up anything that has changed since the last full backup. Does not change the archive bit.
Incremental	Same as differential, but it clears the archive bit.
Daily	Backs up the files that changed that day; does not change archive bit.

Updates

Software is constantly getting fixed or improved. A good technician frequently looks for and implements updates to the following:

- OS (especially service packs)
- Antivirus (update every day)
- All applications
- Drivers (only when necessary)
- Firmware (only when necessary)

Clean

Computers collect dust which can cause overheating. Peripherals suffer the wear and tear of human usage. Routine cleaning is a great preventative maintenance. It also improves customer relations.

- Keyboards (use compressed air or vacuum)
- Monitors (only soft, lint-free cloths; no paper towel on soft LCD screens)

- Case and surfaces (no ammonia-based cleaners on plastics)
- Physical inspection (for broken, loose, or missing panels, ports, or parts)

Schedule

Most preventative maintenance utilities can run automatically and in the background. This allows the computer to take care of many problems itself.

- Automatic updates (schedule big updates for nighttime or nonpeak network usage hours)
- Antivirus scan and automatic update
- On Dynamic Hard Drives (DHD) schedule: Defrag, Scandisk, Checkdisk

3

Operating Systems

The subject of operating systems (OS) is a significant area of the CompTIA A+ Exams. It makes up 20 percent of the 220-701 Essentials Exam and 37 percent of the 220-702 Practical Applications Exam. The operating system exam objectives look in depth at Windows 2000, Windows XP, and Windows Vista; it covers just the fundamentals of Linux and MacOS.

OS Concepts

The OS serves as the middleman between a user and the equipment. It handles resource management, such as hard drives, printers, I/O cards, and the user interface, such as mouse pointers, icons, and windows.

When troubleshooting an OS, first start with the hardware, and then move to BIOS, drivers, updates and service packs, and applications. Don't rule out the possibility of user error. Figure 3-1 shows the layered PC model with the interactions among the hardware, software, and the user.

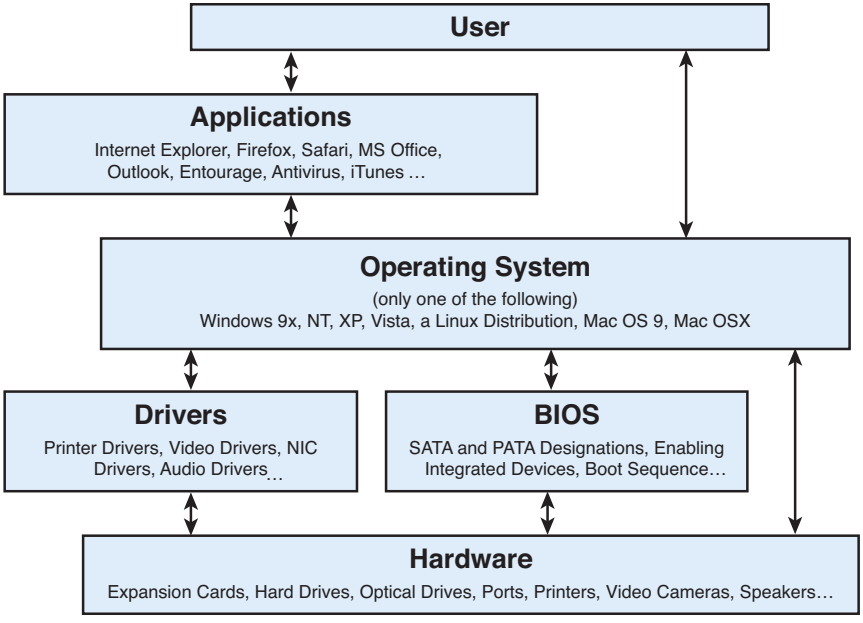


Figure 3-1 Layered PC Model

Minimum System Requirements

Table 3-1 compares the major OS's minimum requirements. These are the absolute minimum. If you want to run anything else, such as office software, antivirus, Internet apps, and so on, then at the very least, double these values when shopping low-end PCs.

The Windows Display Driver Model (WDDM) gives the OS more control of the video content. The Internet connection is used for verification of authenticity and for providing support for integrated programs, such as Instant Messaging (IM), Really Simple Syndication (RSS) feeds, widgets/dashboard, and updates and service packs.

Table 3-1 Minimum System Requirements

OS	CPU	RAM	Hard Drive	Video	Other
Microsoft Windows 2000	133 MHz	64 MB	2 GB	VGA	—
Microsoft Windows XP	233 MHz	64 MB	1.5 GB	SVGA	—
Microsoft Windows Vista	1 GHz	1 GB	40 GB	WDDM driver 128 MB graphics RAM	DVD-ROM Internet connection
Mac OS X	867 MHz	512 MB	9 GB	Only proprietary video card	DVD-ROM Internet connection
Linux RedHat 9	400 MHz	192 MB	5 GB	Practically any video card	DVD-ROM Internet connection

Network Operating Systems

Any OS can provide network services, such as sharing files or a printer. A true Network Operating System (NOS) does not focus on supporting local users or applications like Word, PowerPoint, and so on. An NOS is a simple, reliable OS that's used on servers to provide resources, such as data, files, application, access, authentication, and so on, to other PCs on a network. All these are dedicated resources to other network devices. Popular NOSs are Linux Server, OS X Server, the many Windows Servers, and Novell.

Vista: Sidebar, Aero, and Glass

Vista has several unique features. The sidebar allows users to install gadgets (like shortcuts) for searches and small apps that display real-time information, ranging from weather to system performance. A user-interface feature is called aero. To display a navigable, 3D view of the open windows, press Ctrl-Windows key-Tab. Glass is an option that makes the actual window borders semi-transparent.

UAC and the Administrator Account

The User Account Control (UAC) asks the user for permission when a program requests access or is about to run a task that might harm the PC.

In the NT/2K/XP/Vista environment, administrators can access everything. NT, 2K, and XP have hybrid users (like power users) who have some admin privileges and guests who essentially have none. For security reasons, guest accounts should always be disabled. Vista's administrator account is disabled by default, relying on the UAC to control access to administrative privileges. To force a program to run in Administrator Mode, right-click the icon and choose Administrator Mode. This requires an administrator password. Some programs only run in this mode, which prevents end users from making catastrophic changes.

Windows Compatibility Mode

XP, Vista, and Windows 7 allow any program to run as though it was in a previous version of Windows. For example, a program written for Windows 95 expects to have complete access to the computer. In an XP environment, users have different levels of permissions and access is restricted. Right-click the program icon and set it to run in 95.

Upgrade Paths

If given the choice, always back up the user data and perform a clean install. A clean install means that the drive is reformatted and the OS is installed, not upgraded. If a clean install is not an option, use an upgrade. The following statements are designed to simplify memorizing upgrade paths:

- Windows 2000 requires a clean install to go to Vista.
- Use a clean install when migrating between a home edition to a professional or enterprise edition.
- Use a clean install if you are going from a 32-bit (x86) to 64-bit (x64) OS (or reversed).
- Use a clean install when going from XP Pro or Tablet editions to Vista Home Basic or Premium.
- XP Media Center can only upgrade to Vista Home Premium and Ultimate.
- XP Home Edition can upgrade to any Vista edition, except Enterprise.
- Downgrading should always use a clean install.
- When possible, use the User State Migration Tool to expedite the coping of user data and settings.

Directory Structures

As a technician, it is important to know where files are located. There are some subtle differences in the directory structure among the different versions of Windows OSs, but the NT, 2000, XP, Vista, and Windows 7 are really similar. Figure 3-2 maps the basic directory structures.

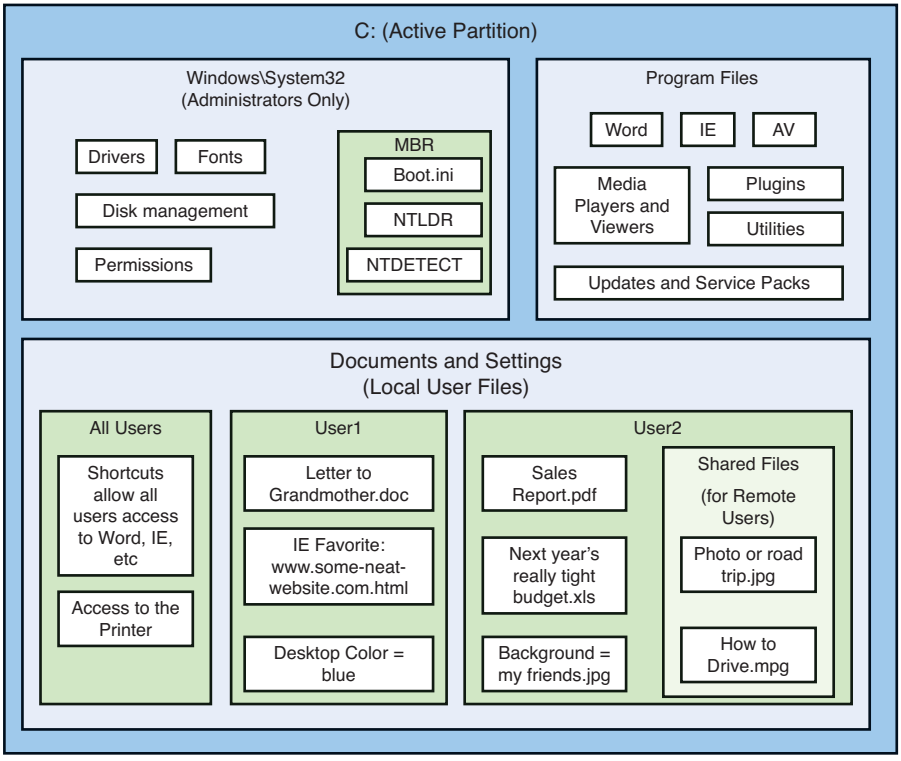


Figure 3-2 Directory Structure

The following are some key locations in Windows directory that should be committed to memory. Typically, all these directories are located on the hard drive named C:

- C:\Windows\System32 contains all the system files, including drivers, fonts, and the MBR files Boot.ini, NTDETECT.
- C:\Program files has all the third-party applications and bundled programs, such as Paint, Solitaire, Movie Maker, and so on.
- C:\Documents and Settings contains all the user information, such as desktop colors and user-created files. Items placed in the All Users account can be seen by every user regardless of permission level. In Vista, the path is C:\Users.

Registry

The Registry contains every conceivable setting in the OS. These settings are divided into several groups called hives. Table 3-2 lists the hives and describes their content.

Table 3-2 Registry Hives

Registry Hive	What It Contains
HKEY_CLASSES_ROOT	File extension mapping
HKEY_CURRENT_CONFIG	All devices in current use
HKEY_CURRENT_USER	User environment
HKEY_LOCAL_MACHINE	All devices regardless of current usage
HKEY_USERS	Settings that affect all users

File Extensions

All files have an extension, which is three to five characters and acts as a "last name." The filename associates files with the appropriate application. Sometimes, a new installation assumes certain extensions, and the user complains that his music or pictures file only opens in the new application. Go to **Control Panel, Default Programs, Associate file type or protocol with a program**. From there, you can reassociate the extension back to the original application.

Anytime you see an extension with an underscore (for example, .do_), it is a backup copy. NTOSKRNL.EX_ is a duplicate and the backup copy of NTOSKRNL.EXE. Because it is unrecognizable as a file, it is ignored. Simply editing the file extension makes the file active.

NTOSKRNL.EXE is a good example of the "8+3" or "8.3" naming convention. OSs pre95 and NT used only eight characters (dot) and three characters for the extension. This led to some creative abbreviations. New Technology Operating System Kernel (dot) Executable becomes NTOSKRNL.EXE. Today's OSs use long filenames (up to 255 characters) that support names such as Documents and Settings and have extensions like .html. Table 3-3 lists the common extensions.

Table 3-3 Common File Extensions

Extension	Description
.exe	An executable file, also called a program.
.bat	Script file.
.doc	Text document with complex formatting usually associated with MS Word.
.txt	Simple text document.
.ppt	PowerPoint file.

Table 3-3 Common File Extensions *continued*

Extension	Description
.xls	Excel spreadsheet.
.jpg	Picture.
.mpeg	Movie.
.avi	Movie.
.wav	Short audio file.
.html	Web page.
.zip	File-compression software.
.rar	Another file compression software called RAR (found in all three major OSs).
.tar	Linux version of a compressed file. A tar ball is a group of files compressed into one tar.
.mp3	Music file. Note: mp4 is a movie format. It's not, as some end users insist, an upgrade to mp3.

Plug-Ins and Players

Many troubleshooting scenarios involve an unrecognized file type. Third-party viewers, plug-ins, and players are required to access many common file types. Table 3-4 lists common file extensions and their associated third-party software.

Table 3-4 Common File Extensions That Require Third-Party Software

Extension	Third-Party Software
.pdf	Adobe Acrobat Document
.mov .qt	Quicktime movie
.ram	Real Audio music
.rm	Real Movie File
.swf	Adobe Shockwave Animation
.fla	Adobe Flash Animation
.wmv	Windows Media Viewer
.wma	Windows Media Audio

File Attributes

To change the file attributes, go to Folder options, View, right-click the file, and choose properties. Another method is found in the CLI. Using the ATTRIB command allows you to modify the attributes of a file (for example, **Attrib +R quepublishing.doc**). Any file can have any combination of the four attributes. Table 3-5 outlines the four file attributes.

Table 3-5 File Attributes

Attribute	Description	Mnemonic
Read-only	Allows anyone to read the file, but no one can change the content.	**R**
Archive	Flags the file to be backed up during system-wide backups.	**A**
System	Marks the file as a system (important) file. They should not be moved or modified.	**S**
Hidden	Hides sensitive files from the end users.	**H**

Safe Removal of Peripherals

OSs must mount external drives before they can be accessed. They also should be unmounted before removing them. This is accomplished through the Safely Remove Hardware applet, which is located on the taskbar. Select the external device and wait until it says, "OK to remove device."

Windows Interfaces

Vista and Windows 7 have several user interface improvements. Aero includes Live Thumbnails icons that look like the documents they represent, semitransparent windows called Glass Effects, and Flip 3D that allows users to scroll though the open files like a three-dimensional filing cabinet. Sidebar allows users to plug in gadgets that do a wide range of things, such as display real-time stock market prices, system monitoring, weather, and so on. Indexing settings allow the user to limit the locations and types of files for which the automatic search function looks.

Start Menu, Taskbar, and System Tray

Windows, MacOS, and Linux use similar user interfaces. A menu is simply a hierarchical organization of shortcuts. Taskbar indicates what is currently open. The system tray contains frequently used utilities and shortcuts to commonly accessed Control Panel applets, such as volume controls and networking. Icons represent individual files, folders, devices, and applications.

Windows Explorer

Windows Explorer (not to be confused with web browser, Internet Explorer) is style of window that uses multiple panes to display what is located in a specific window and a visual representation of the directory tree. This allows for quick drag-and-drop functions anywhere in the OS.

My Computer and My Network Places

My Computer is a window that displays all the storage devices that reside locally on the PC, including jump drives and external HDDs. Remote mapped drives can appear in My Computer, but they really reside on a different PC. They are identified by a network symbol as a part of the icon. My Network Places displays nearby networked devices, printers, shared files on other PCs, routers, and so on. In Vista, these terms are simplified to Computer and Network.

Task Manager

The Task Manager displays which applications are currently running and gives you the power to stop a troublesome application that is "stuck" in an effort to prevent the PC from total crash. You can launch the Task Manager by pressing Ctrl-Alt-Delete. In Vista and Windows 7, these key strokes launch a menu from which you can choose Task Manager. The Applications tab contains all currently running programs. Processes displays everything that the CPU is doing. Performance displays CPU, HDD, and RAM performance. The Networking tab monitors network activity, and the Users tab displays current user info.

Control Panel and MMC

Like My Computer, the Control Panel is a convenient interface that includes the tools and utilities used to troubleshoot and maintain the PC. A Microsoft Management Console is a customizable control panel that administrators can create to simplify locating and executing programs and tasks that they frequently use.

Remote Desktop Connection and Remote Assistance

Remote Desktop Connection (RDC) and Remote Assistance allow you to connect to a computer to configure it from anywhere. The target computer needs to be set to allow remote control. XP Home edition can serve only as a destination of a remote connection. It does not have the capability to establish this connection without using third-party software. The only difference between RDC and Remote Assistance is that the person seated at the target PC is asked to accept the connection. Do not confuse Remote Assistance with Remote Access. Remote Access assumes that no one is sitting at the target PC; it is used for long-distance maintenance.

System Performance and Optimization

Improving performance and running preventative maintenance is a big part of a technician's job. Most of the tools are located in the Control Panel. Table 3-6 lists the administrative tools and describes their use.

Table 3-6 System Performance Utilities

Tool	Description
Event Viewer	A list of activities and failures that are logged by the OS to help determine troublesome programs or processes.
Disk Management	A collection of tools used to maintain hard drives, including the ability to partition, format, and defrag them.
Device Manager	A list of all the internal and external devices and their associated drivers. An exclamation or question mark next to a device indicates a missing or corrupt driver.
Virtual Memory	Adjusts the amount of hard drive space used for swap files copied from the RAM.
ACPI Power Management	Changes power settings, such as how long before the PC enters sleep mode.
Default Programs	Associates file extensions with programs.
Performance Monitor	Monitors performance to see if the CPU or RAM is overused.

Installation and Configuration

During the installation process, the administrator is prompted with questions regarding the size and location of the partition, kind of format (NTFS versus FAT32), specific programs, and device support to include during the install. Only use FAT32 if you're connecting to Windows 9x PCs; otherwise, always use NTFS. Always check the online Hardware Compatibility List before making purchases that might prevent or cause problems during the install.

Installation Methods

There are several methods to install an OS. An install CD/DVD is the traditional method. A network install prevents the need to carry the CD/DVD from PC to PC. An unattended install uses a regular install CD/DVD and an answer file that automates the options during setup. A remote install works like an unattended install, but it uses a network source for the install files. Imaging copies an HD and stores it on a network server or on a local partition. At any time, it can be recopied and "installed" on the PC.

OS Repair and Adding Services

The install CD/DVD is a powerful troubleshooting tool. With the CD/DVD, you can repair an OS by recopying the system files to fix corrupt or add missing files. You can add services or device support that was left out during the original setup.

Startup

In Windows 2000 and earlier versions of Windows OSs, every major system change, like a new IP address, new USB device, and so on, required a restart.

The first step in the boot process is POST. The PC counts all its RAM and registers, reads and registers all the hardware addresses, and runs some diagnostic tests. Then, it asks the BIOS which boot media to use. The BIOS needs to provide a correct boot order. Typically, the OS is located on the HD. If you want to boot to the CD, you might need to promote the optical drive on the boot list. On the other hand, if the media has no boot files, it gives an error message, such as "Missing OS" or "Missing NTLDR."

The following is a list of possible boot options used for troubleshooting:

- Safe Mode loads a basic device drivers, which bypasses the potential troublesome high level or incorrect drivers.
- Last Known Good Configuration automatically reverts back to a boot with no reported errors.
- Boot to a restore point allows you to "go back in time" to a time when you made a previous restore point when everything worked properly.
- Automated System Recovery (ASR) works much like restore points, but you actually create a disk with the restore information on it. That disk is used during the restore process. Windows 2K and earlier Windows versions use a similar program called Emergency Repair Disk (ERD).
- Recovery Console can run from the HD if it was previously installed or from the OS install CD/DVD. It provides a CLI and basic commands that aid in data recovery.

4

Networking

Networking is an integral part of the technician's job. It is difficult to imagine a PC without the ability to connect to a shared printer or drive, let alone the Internet. Networking accounts for 15 percent of both the 220-701 and 220-702 CompTIA A+ Exams.

Network Basics

The seven layer OSI model reduces complexity, ensures interoperability among devices, and simplifies learning. Developed by the International Standards Organization (ISO), it is the global model used to teach and organize the countless networking protocols and devices. Table 4-1 describes the layers of the OSI model.

Table 4-1 OSI Model

Layer	Name	Mnemonic	Description
7	Application	**A**ll	The actual application used to view network data, such as IE, Chrome, Outlook, AIM, and so on.
6	Presentation	**P**eople	Data compression and encryption.
5	Session	**S**eem	Establishes, maintains, and terminates communications.
4	Transport	**T**o	Flow control, error checking, and correction.
3	Network	**N**eed	IP addresses. Routers make routing decisions in this layer.
2	Data Link	**D**ata	Media Access Control (MAC) addresses. Switches make forwarding decisions in this layer.
1	Physical	**P**rocessing	The actual wire, light impulses, or radio waves that carry the data. Repeaters retime and regenerate signals. Hubs allow ingress to the network, but do not make forwarding decisions.

Another mnemonic that is used goes from bottom up, which is many times the troubleshooting process, starting at the physical layer: Please Do Not Throw Sausage Pizza Away.

LAN, WAN, and WLAN

A network is a group of devices that share services. In a local-area network (LAN), devices are close by (within a building, campus, or house). Wide-area networks (WANs) cover a wide geographic area. WANs connect LANs to each other. Wireless LANs (WLAN) allow portable devices, such as PDAs, phones, laptops, heart monitors, alarm systems, and others, to connect to each other and to the Internet. The physical layer of a WLAN is the antennas and radio signals.

Network Devices

Routers connect networks to each other. They control the addressing scheme for attached networks and route data packets to other networks. IP addressing is used by Layer 3 devices, such as routers, to identify computers on networks. Switches connect to a router and provide both ingress to the network (many ports) and make forwarding decisions based on the location of the sending and receiving hosts. Switches use MAC addresses to make these decisions. They only forward packets to the intended host, which reduces overall network traffic. A hub looks like a switch, but it is not as sophisticated. It only provides ingress. A repeater retimes and regenerates signals that travel great distances. A host is any device on a network. Usually, the name host implies a PC, but it could be a printer, access point, or another networked device.

Bandwidth, Throughput, and Latency

Bandwidth is the amount of data that a media can transmit in ideal circumstances. Throughput is the amount of data received, minus protocol overhead and latency. Latency is the slight time lag found in most long-distance communications.

Full-Duplex and Half-Duplex

In a half-duplex environment, a sender and receiver take turns. One talks, the other listens, and then they switch roles. A full-duplex environment allows for a sender and receiver to simultaneously communicate.

Workgroups and Domains

A workgroup is a group of computers that share resources. They are managed individually and are not dependant on one another. A workgroup is considered a peer-to-peer network. Client-server networks group computers into domains with a domain controller for each. Domain controller is a server that handles user authentication, access, services. The clients are managed. Domains increase security and simplify client management by using a central controller.

TCP/IP Addressing

IP addresses are considered logical because they can be assigned to the NIC by the network administrator. MAC addresses are permanently burned into the NIC and are, therefore, considered physical. It is actually a Layer 2 technology. (Do not assume that a physical address and the physical layer are related.)

An IP address has four numbers, ranging from 0–255, separated by dots (decimals). 192.168.7.3 is an example of an IP address. The hostname is a "friendly" name that is given to a host (such as Ben-PC).

A gateway is the IP address of the router to which that PC is connected. It is the "gateway" to the rest of the World Wide Web. A subnet mask is a number that the router uses to determine what part of the address is the name of the network and what part is the name of the host.

A static IP address is manually assigned to the host by the technician or network administrator. A dynamic address is assigned to the host by a server using Dynamic Host Configuration Protocol (DHCP).

127.0.0.1 is the loopback address, which is also referred to as localhost. It is returns the packet directly back to the sending host. (Actually, the packet never really leaves the NIC.) It is used for testing.

Network Architectures

Four main transmission technologies are used in networks. Table 4-2 describes these technologies and provides some memorizing tips.

Table 4-2 Network Architectures

Architecture	Standards Organization	Memorizing Tips
Ethernet	IEEE 802.3	"Threee" sounds like "Eeeethernet."
Token Ring	IEEE 802.5	A pentagon has five sides and is in the shape of a ring.
FDDI	ANSI and ISO	Fiber-optic cable. The two double "D"s is a reminder that it is a double ring topology.
WiFi	IEEE 802.11	The 11 looks like two antennas.

Network Services

Table 4-3 lists the most common networking protocols, their ports, and gives a brief description.

Table 4-3 Ports and Protocols

POP	110	E-Mail
IMAP	143	E-mail
SMTP	25	E-mail outgoing to a server or between e-mail servers, not from sever to client
SSH and Telnet	22 or 23	CLI remote access
FTP	21	Downloading files

Table 4-3 Ports and Protocols *continued*

POP	110	E-Mail
TFPT	69	Transferring files
DNS	53	Friendly URL names
DHCP	67	Autoconfigure network settings
VOIP	Depends on ISP	Voice over IP Telephone that runs on a computer network
NAT	Varies	Maps a private IP address to a public IP address so multiple PCs can share a single IP address
Proxy	Varies	Go-between server that "hides" the sender from the receiver

Network Cables

Unshielded twisted pair (UTP) has the basic categories of Category 3 for phones and Category 5 for computer networks. UTP has a catchment area of 100 meters (328 feet), which means that the cables should not exceed this length. TIA/EIA standards allow for 90 m of horizontal run (in the walls, ceilings, and plenum). This leaves 10 m for patch cables (outside the walls). Patch cables connect devices in a room to the wall jack. Heating, venting, and air conditioning (HVAC), lights, and fans produce electromagnetic interference (EMI) that interferes with the network signal. Shielded twisted pair or fiber-optic cable should be used around these appliances to reduce the effect of EMI. Fiber-optic cables can be as long as several kilometers.

Category 6 and 6A have more twists to improve protection from crosstalk and line noise.

A straight-through patch cable directly maps the pins on both ends of the cable. Pin 1 goes to pin 1, pin 2 to pin 2, and so on. These cables are used when connecting different layered devices, a host to a switch, or a switch to a router. A crossover cable maps the sending pin to the expected receiving pin. Pin 1 maps to pin 3, pin 2 to pin 6, and so on. These are used when connecting similar devices, such as a host to a host and a switch to a switch.

ISP Connections

Internet service providers (ISP) offer high-speed Internet connections. Table 4-4 lists the most common methods in their order of importance for the A+ exam.

Table 4-4 Internet Connections

ISP Connection	Need to Know (In Order of Importance)
POTS	Plain old telephone system (or service) uses a dialup modem and is slow (56 kbps).
ADSL	Asymmetric digital subscriber line. 8.10.1 asynchronous is the most common form of DSL. It is slower upstream (toward the ISP) and much faster downstream (toward the client). Common ADSL speeds (downstream/upstream): 768 kbps/364 kbps 1.5 Mbps/384 kbps 3 Mbps/512 kbps 6 Mbps/768 kbps (Source: AT&T DSL plans) DSL requires the use of filters for the telephones so that the voice traffic and the data traffic do not interfere with each other. Designed for residential clients, small office, and home office (SOHO) environments, DSL has a quick download speed, but it is not designed to support high traffic in and out of a web server or FTP site.
Cable	Cable TV providers use coaxial cable to provide many services, including Internet access. It is very fast. However, performance varies because it is a shared medium. Everyone in a building, block, street, and so on shares the same connection. If someone uses a lot of bandwidth, others see a drop in performance.
Satellite	Satellite is 56 kbps up and 500 kbps down. It is slower than cable and ADSL, but it can provide service almost anywhere, such as on a boat, in a motor home, or rural and remote locations. Leaves and weather may adversely affect satellite Internet performance.
PRI ISDN	Primary rate ISDN is a T1 line. It has 24 64-kbps B channels, of which 23 are used together to achieve speeds of 1.544 Mbps. The D channel is used for signal timing, starting and stopping the sessions. Europe has 30 B channels and can have speeds up to 2.048 Mbps.
BRI ISDN	The basic rate interface (BRI) has three wires: two B channels that can carry 64 kbps and a D channel that can carry 16 kbps. BRI uses both B channels for data and the D channel for timing, initializing, and ending the call. This use of the B channel is similar to the session layer on the OSI model.
Cellular WAN	Cellular WAN technology is currently in its third generation (3G). The first generation (1G) was voice-only analog and only voice phone calls. 2G is digital and provides some data services, such as texting. 3G provides high-speed data and voice.

Network Security

Network security is a constantly evolving area. Here are some common devices and technologies used to improve the security of data and PCs.

Firewalls

A good security plan uses layered defenses, including hardware and software firewalls. Firewalls work in three ways:

- **Packer filtering:** The most common and straight forward. Firewalls that use packet filtering either block or allow packets by using basic criteria, source or destination IP address, ports, or protocols. The disadvantage of packet filtering is that it is not subtle. It is a reliable but inflexible gate guard. Sometimes, legitimate packets get filtered because they are different.
- **Proxy filters:** Advocates for a kinder, gentler network community allow packets of all persuasions to enter or leave and use more sophisticated rules. These proxy filters are more concerned about network intrusion rather than internal issues.
- **Stateful packet inspection:** Looks for unfamiliar packets and hides the bodies. After a rogue packet enters the target network, a hacker never hears from it again.

Hardware firewalls are expensive and difficult to set up and configure, but they don't impact the individual PC's performance. Plus, a hardware firewall can support an entire network.

HASH

SHA and MD5 are similar to checksum. They are numbers generated by the actual message using an algorithm. Checksum counts the number of bits in a message. If the receiver counts the bits and they do not equal the checksum number, something has been lost or changed. SHA and MD5 work the same way, but the algorithm is more complicated. In any case, these technologies verify that nothing was lost or altered during transmission.

Encryption

Symmetric encryption scrambles the data based on a mathematical algorithm. A key is similar to a password, but it is part of the output from that algorithm.

Asymmetric encryption requires two different keys to view the data: one for the sender (private) and the other for the receiver (public). This system authenticates both parties and requires both parties to participate in the encryption process.

VPN

Virtual Private Networking (VPN) uses a token (not to be confused with the Token Ring network topology) to encrypt a message. That message is sent through secure tunnels to the receiver that uses the token to unencrypt the message.

Telnet and SSH

Telnet and Secure Shell (SSH) are CLI-driven connections between computers. For these to work, Terminal Service must be running. Telnet and SSH sessions are initiated from the CLI. Simply type **TELNET** in the CLI, followed by the target name or IP address. Then, you log in as a local user with local password. Once in, you have the access of that user on the remote machine. Telnet is less secure because it uses plain-text passwords.

HTTPS

HTTPS is a website that establishes a connection to the host using Secure Socket Layer (SSL) or Transport Layer Security (TLS). It improves security when entering data into a website.

Wireless Networks

All WiFi standards for the A+ Exam are defined by IEEE 802.11. The four standards are a, b, g, and n. The a standards are not compatible with any of the others, and they have a small range of 150 feet. b and g are interoperable, and n works with both b and g. Table 4-5 summarizes what is different among those four versions.

Table 4-5 Wireless Comparison

802.11	Bandwidth	Frequency	Max Range
a	54 Mbps	5 GHz	150 feet (45.7 m)
b	11 Mbps	2.4 GHz	300 feet (300 m)
g	54 Mbps	2.4 GHz	300 feet (300 m)
n	540 Mbps	2.4 or 5 GHz	984 feet (250 m)

Bluetooth

Bluetooth supports file transfer and streaming signals directly from one device to another. It functions on the same 2.4 GHz frequency range as WiFi. A MAC address scheme allows one Bluetooth controller to connect with up to 8 devices.

Infrared

Infrared (IrDA) supports point to point, line of sight connection. It transmits at 16Mbps and has a range of about one meter.

Wireless Network Security

Table 4-6 shows a list of security techniques used on a wireless network.

Table 4-6 WiFi Security

Security Technique	Characteristics
Use antivirus (AV) software.	AV is the last line of defense against malicious attacks. Update the viruses daily.
Use an adware removal application.	Third-party-like software removes spyware.
Update the OS and applications.	Updates patch security holes.
Firewall.	Traffic entering a network is analyzed by the hardware-based firewall. Software firewalls shut down ports, except for the ones normally used and assigned to useful applications, like e-mail, web, and FTP.
Change the default password on the router.	Hardens the admin password and renames the user, if possible.
WEP.	Wired Equivalency Protocol (WEP) offers simple encryption and requires a key to be entered when initially connecting to a network. 64 bit is good, and 128 bit is better.
Hardened passwords.	Hardens passwords by using many characters, uppercase and lowercase letters, symbols, and numbers, and by requiring new ones frequently.
No SSID broadcast.	"Hides" your WLAN, but you must manually enter the SSID on your wireless devices.
WPA and WPA2.	WiFi Protected Access (WPA) offers better encryption than WEP, and WPA2 is the current standard.
MAC filtering.	The router only issues IP addresses to recognized MAC addresses.
Update the router's firmware.	Flashes the router like you would a PC BIOS.
LEAP or EAP-Cisco.	Lightweight Extensible Authentication Protocol (LEAP), also called EAP-Cisco.
WTLS and WAP.	Wireless Transport Layer Security (WTLS) and Wireless Applications Protocol (WAP) are used on portable devices.

5

Security

Security is an ever-growing field in the world of computer repair. A good working knowledge of attacks and defenses is a must in the IT industry. Security is one of the smaller domains in the CompTIA A+ Exams, but it still accounts for 8 percent of the 220-701 Essentials Exam and 13 percent of the 220-702 Practical Applications Exam. Figure 5-1 shows a layered defensive strategy that is designed to protect the user and data. Notice that the first line of defense is network based, the second line is on the local PC (host), and the third line of defense is the user.

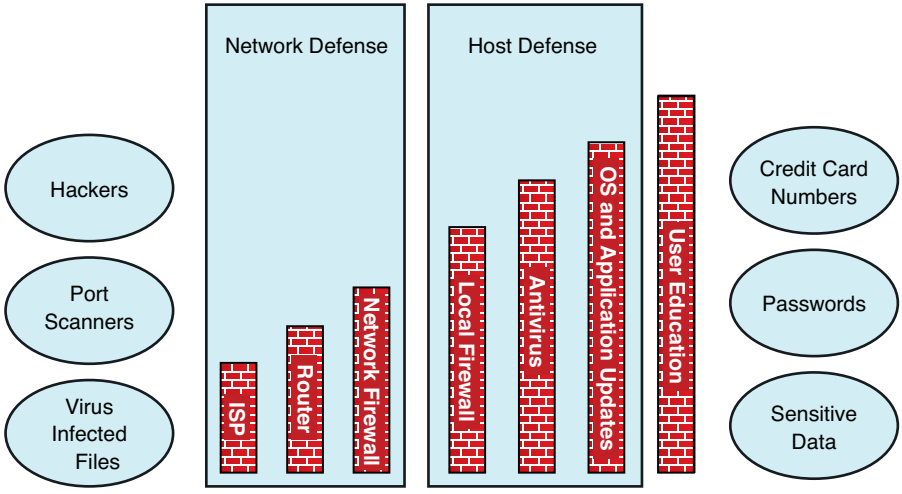


Figure 5-1 Layered Defense

Antivirus

The first step in antivirus (AV) is to detect a suspicious file or program. AV employs a scanning engine that uses one or both of the following techniques.

Heuristics analyze the behavior and activity of a file or program. If it is replicating, scanning other files, or connecting to other computers, it is flagged as a virus. Unfortunately, its hyper-vigilance tends to cause many false positives because many legit programs do exactly those behaviors. Search tools and programs that verify software keys often set off a heuristic scanning engine.

The other methods of detecting viruses are by comparing files to signatures (often called definitions) of known viruses. Much like fingerprint analysis, the AV software receives updates from a database maintained by the software manufacturer. The drawback of this method lies in its inability to quickly identify new and emerging threats. A proper AV uses a combination of both techniques.

Scan Schedules

Scan early and scan often. Scanning takes considerable system resources, so perform scheduled updates and scans during off-peak hours.

Updates (Signature and Engine)

Both the signatures and the engine need to be as updated as possible. This is best done by setting it to commence automatically during down times, such as at night and on holidays.

Quarantine

After a file or program is found to be a match either by its activity (heuristics) or via update of known virus signatures, one of three things happens to the file. If it can be cleaned (removed from the host file) it will be; if not, the file is quarantined. In other words, nothing can be written to or read from that place on the HDD.

Remediation

As a technician, to prevent reinfection, you need to determine how the computer became infected. The most common methods of catching a virus is not using AV, using an obsolete AV, and not using up-to-date virus definitions and scan engines. The following is a list of common remediation:

- Install AV software
- Update definitions
- Update patches and service packs for OS and applications
- Use virus removal features of the AV
- Identifying the source of infection

Customer Education

Customers are often the victims of computer attacks, ranging from random malware intent on causing untold damaged to selective, premeditated identity theft. It is the technician's responsibility to educate the end user of potential threats and common preventative measures without causing unnecessary alarm. The following are common sources of viruses:

- E-mail attachments from known senders (because users are more likely to open attachments from a friend)
- Free software downloads (especially free malware scans, desktop backgrounds, and screen savers)
- Peer-to-peer file-sharing services
- Copying and moving files among computers via a network or portable media

User Authentication

User authentication is the first line of defense against computer threats. The first thing hackers do is try to assume administrator privileges. If the end user gives free reign by allowing every User Account Control (UAC) request, a hacker can easily gain control of the PC.

Local Users and Groups

When a user logs on, the credentials (username and password) are compared to a local database. In large client/server networks or in environments with roaming users, authentication servers compare logon credentials to a database stored on a remote server. If the credentials are correct, the database also contains and assigns the permission level of the users. In 2000 and XP, there are various levels of increasing authority, including Guest Accounts, Users, Power Users, and Administrators. Vista and Windows 7 have moved away from many multilevel users in place of simply administrators and limited users. The UAC allows temporary admin privileges to those logged in as a limited user.

NTFS Versus Share Permissions

New Technology File System (NTFS) allows file-level security that File Allocation Table 32 (FAT32) did not. After users are created, any folder or file can have custom privileges per user. Permission propagation applies the parent folder permissions to any child object (folders, files, and apps "inside" the parent folder). Tables 5-1 and 5-2 show a list of privileges.

Table 5-1 NTFS Permissions

Privilege	Description
Read	Users can only read contents.
Write	Makes changes to a file or folder contents.
Modify	Makes the folder or file read and writeable.
Execute	Runs programs.
Full Control	Creates, modifies, and deletes files and programs.

Permissions regarding shared files and folders are a simplified version of NTFS permissions. Note that "read" in file-sharing permission also allows the user to execute programs.

Table 5-2 Share Permissions

Permission	Description
Read	Allows users to read files and execute
Change	Views, creates, changes, and deletes files
Full Control	Takes ownership of files and change permissions

Encryption

Encryption works by applying an algorithm to a key (like a password) and the data. For example, if 3 is the key, simple multiplication is the algorithm, and the data is 4, the scrabbled data would look like 12. Because the algorithms are complicated and the keys should be hardened with upper- and lowercase letters numbers and symbols, this becomes more difficult to reverse engineer to get the data (which is markedly more complex than the number 4).

When using encryption in communications, both the sender and receiver have separate keys (public and private). Both are needed to decrypt the message. If the message is intercepted or either the sending or receiving end is compromised, the data is still secure.

BitLocker and EFS

Microsoft BitLocker is an integrated encryption program available in the Ultimate and Enterprise editions of Vista and Windows 7. It requires two logical partitions: one for system files and one for sensitive files that are encrypted. The key can be manually entered or contained on a removable media, such as a USB drive.

Encrypting File System (EFS) is available on Windows 2000, XP, Vista, and Windows 7. It works much the same way as BitLocker. The main difference for the user is EFS requires the manual entry of the key. The advantage to the USB drive key is this: Whoever has control of the USB has access to the data and no one else. No one needs to know the actual key. The drawback of both of

these is, if the data on the USB or HDD is corrupt, it is extremely difficult—if not practically impossible—to access and reconstruct the data.

Drive Lock

Drive Lock works like other encryption methods, but it is hardware based. It protects the entire drive, not just selected logical partitions. It is primarily used on theft-prone, portable devices, such as USB drives, laptops, and cell phones.

BIOS Passwords

BIOS security can play a role by providing passwords to gain access to the PC and other passwords that protect the boot order and external devices. The problem with BIOS security is that, when parked, jumpers on the motherboard remove the passwords. This security method should be mainly used so end users do not accidentally reconfigure the BIOS rather than a proper security feature.

Intrusion Detection and TPM

Trusted Platform Module (TPM) stores password keys on a chip on the motherboard. This allows the computer to boot, compare keys, and grant access to drives if they match. Intrusion detection senses unauthorized changes or out-of-character requests and flags them as possible intruders.

Data Wiping, Hard Drive Destruction, and Recycling

When an HD is retired, data is often left on the drive. This can be a serious liability for a company. Some data-wiping programs write the entire drive with 0s and then write over it with 1s. This process is adequate for most erasing needs. However, high end computer forensics programs can observe how the molecules were arranged prior to the wiping and can resurrect a surprising amount of the data. If the data is very sensitive, use a Department of Defense (DoD) quality data-wiping program that repeats the 0 and 1 writing process 22 times.

Passwords: Management and Complexity

Passwords should be at least 8 characters long and include capital and lowercase letters, as well as symbols and numbers. This greatly increases the time it takes brute-force cracking programs to guess a password.

Attacks

Most computers get attacked many times a day. Fortunately, most attacks are obsolete and unsophisticated and are dispatched with simple preventive measures, such as AV and firewalls. Table 5-3 describes common computer attacks.

Table 5-3 Security Threats

Attack	Characteristics
Theft	Theft is a major problem because of the cost and portability of the equipment and software.
DoS	Denial of service (DoS) attacks a PC by flooding it with useless requests.
DDoS	Distributed denial of service (DDoS) is a DoS attack run by zombie machines to maximize the effect and make the attack difficult to trace.
Physical Damage	Nothing takes down a website faster than unplugging the server, or worse.
Trojan horse	Posing as harmless or even helpful software, a Trojan horse does nasty things behind the scenes, like remotely control the target's PC, read, modify, or delete files. These often come in the form of e-mail attachments, ActiveX, Java, or JavaScript programs.
Worm	Worms are self-replicating software that fill HDDs and modify and spread to others.
Phishing	Phishing gains information, usually via phone or website, from the target by pretending to be a technician, account representative, or another trusted person.
Social engineering	A more brazen version of phishing, where a hacker poses as a permit inspector or repair person to gain admittance to the home or business. Once inside, he has physical access to the target where he can leave any number of malware programs.
Replay attacks	Replay attacks use packet sniffers to find a packet and gather user names and passwords to use later. Packet sniffers are a cool tool for useful information, such as finding out who on your network is doing exactly what.
Spoofing	Spoofing changes the IP address, MAC, or any other identifying marker on a PC to pretend it is someone else.
DNS poisoning	DNS poisoning changes the entries in a DNS so traffic is routed to a malicious site instead of the legit target. This is especially bad if the malicious site looks and feels like the real target.
Brute force	An example of brute force is password cracking by trial and error. Programs run millions of combinations and will eventually happen upon the right combination. The more complicated the password, the longer this process takes. Before they run a proper brute-force attack, a password cracker runs a dictionary attack first. All normal words are compared to the password file, and it takes a matter of seconds to discover an unhardened password this way.

Table 5-3 Security Threats *continued*

Attack	Characteristics
Man-in-the-middle	A look-a-like website can request a username and password and then forward the user onto the correct site, acting as if the user was denied and should try again. The user tries again and is successful. In reality, the fake one forwarded the logon credentials to the hacker, who uses it to gain entry to the target's bank accounts, e-mail, or other network resource.
SYN flood	A SYN flood opens ports and requests attention, such as a DoS.

This page intentionally left blank

6

Operational Procedures

Operational procedures covers safety, environmental issues, help desk, and customer service. This section accounts for 10 percent of the CompTIA A+ 220-701 Essentials Exam, and it is not tested in the 220-702 Practical Applications Exam.

Scenario: Safety and Environmental Issues

The A+ exam is moving toward using more scenario-driven assessments. It is arguably a better way to assess applied knowledge. Safety and environmental issues are a great opportunity for exam takers to demonstrate their ability to draw on theoretical knowledge and make good choices.

ESD, EMI, and RFI

Internal devices are normally protected from electrostatic discharge (ESD), electromagnetic interference (EMI), and radio frequency interference (RFI) by the metal chassis. Outside the case, they are susceptible to those dangers. Communication cables also suffer from RFI and EMI.

ESD is the equalizing of voltages when two things touch. When your hand touches a device, a discharge of excess electrons can destroy the tiny circuits inside that device. Motherboards and RAM are particularly susceptible to this.

EMI and RFI are caused by electromagnetic fields and radio broadcasts, respectively, that interfere with the device or cable's normal function. Long straight runs of copper wire often act as antennas and pick up waves of nearby sources. Table 6-1 outlines the preventions for ESD, EMI, and RFI.

Table 6-1 ESD, EMI, and RFI

Problem	Preventions
ESD	■ Increase humidity
	■ Use antistatic wrist straps
	■ Use antistatic mats
	■ Store internal devices in antistatic bags
EMI	Increase the distance from the following:
	■ Magnets (as in speakers and fans)
	■ Motors (vacuums, blender, and fans)
	■ HVAC equipment (air conditioners and heat pumps)
	■ Unshielded electrical wires (extension cords)
	■ Lights (network cable draped over florescent light in the plenum, for example)
RFI	Terminated network cables properly (no parallel wires)
	Increase distance from the following:
	■ Cordless phones
	■ Broadcasting radios
	■ Walkie-talkies
	■ Microwave ovens

Electrical Hazards

CRTs, power supplies, LCD inverters, and laser printers all have capacitors and should be replaced, not opened. Power supplies and uninterruptible power supplies (UPS) should provide more power than the equipment requires. Failure to do so causes the power supply to dangerously overheat and, ultimately, fail.

MSDS

Material Safety Data Sheets (MSDS) need to be available if there is a fire or another emergency. They are instructions on how firefighters and hazmat crews should deal with evacuation and clean up of dangerous chemicals. These chemicals include the silver oxide that's used to increase heat transfer from the CPU to the heat sink, the phosphorus in CRT monitors, and PVC-coated cables that turn into poisonous gas in a fire, to name a few. Even innocuous things, such as bug spray, glass cleaner, and even shampoo have chemicals that can require an MSDS.

Trip Hazards

Computers and cables often accompany one another. A power cord or network cable should never be placed across a walk way. Add outlets and network drops where needed to prevent this scenario. When carrying computer equipment, unplug everything first and carry the cables separately.

Physical Safety

Computers and printers are heavy. Always lift with your legs and keep your back straight. Rotate by moving your feet, not by twisting your back. The inside of a PC or printer can be very hot and often have sharp surfaces. Let the PC cool, and then use tape to cover any sharp edges.

Computer and Battery Recycling

Computer equipment contains many recyclable metals and other chemicals. Companies will recycle computers for a fee, so you do not need to illegally dispose of them. As a PC technician, you need to know your local government guidelines regarding equipment disposal.

Scenario: Help Desk

The help desk is the place where many technicians start. Remote support has its unique challenges. You rely on the customers to see, hear, and touch the equipment. You have the added challenge that end users often do not understand much about computers. Terms like partitioning, PCMCIA, cold boot, and blue-screen-of-death are called jargon, acronyms, and slang. They are unfamiliar to customers and should be avoided. Keep in mind that you might be communicating with your customers via e-mail, chat, or avatar.

It is important to respect the customers' time and attention. Make sure that you are not interrupted or distracted by other activities during a troubleshooting phone call. They hired you to solve their problem, not play solitaire.

Difficult Customers

Difficult customers are often frustrated because they fear loss of productivity, loss of self esteem (calling someone for help), or loss of equipment, time, or money. Reassure the customer, but do not make promises. You cannot guarantee success before you know what is wrong. In a help desk phone call, you and the customer must work together. Make sure that you let the difficult customer know how vital a role he or she plays. Do not put the customer on the defensive by making condescending or accusatory remarks.

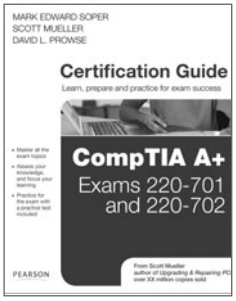
Troubleshooting Long Distance

Start with open-ended questions, such as, "Please describe what happened," or "How is your PC troubling you?" Narrow the focus of the questions to arrive at a small number of possible problems. "Does this happen all the time, or only when you use the web?" "Is it only grainy when printing in color, or any time you print?" Eventually, narrow it to isolate the fault. Make a plan to test or fix the problem and execute it. "Restart the PC and enter Safe Mode by pressing F5. Can you see all the icons now?" "Let's download Flash Player again and reinstall it. Then, we can launch the browser and see if it works." Make sure that you change only one thing at a time so you can correctly document exactly what fixed the problem. Be sure to follow up with the customer a day or two later to verify that the problem is fixed and thank him for the business.

Get prepared for the CompTIA® A+ Exams

Pearson Certification has the learning tools that you need to get ready for the CompTIA® A+ Exams. From foundational learning to late-stage review, practice, and preparation, the varied print, software, and video products from Pearson Certification can help you succeed!

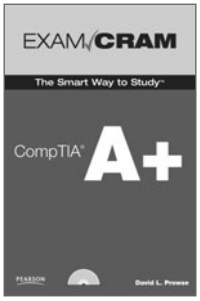
Book/CD Learning Products



CompTIA A+ Certification Guide

ISBN-13: 9780789740472
ISBN-10: 0789740478

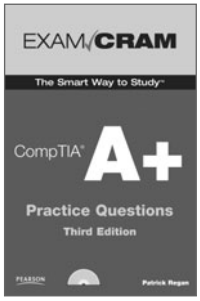
Comprehensive A+ learning from best-selling author Scott Mueller



CompTIA A+ Exam Cram, Fourth Edition

ISBN-13: 9780789742421
ISBN-10: 078974242X

The best-selling late-stage A+ study book of all time



CompTIA A+ Practice Questions, Third Edition

ISBN-13: 9780789742575
ISBN-10: 0789742578

Prepare with 850 practice questions in print and electronic test engine formats

Online Learning Services & Late-Stage Electronic Kits

CompTIA A+ Cert Prep Online, Second Edition

ISBN-13: 9780789742612
ISBN-10: 0789742616

Online service assesses knowledge, creates customized learning plans, and delivers study materials

CompTIA A+ Cert Flash Cards Online, Second Edition

ISBN-13: 9780789742636
ISBN-10: 0789742632

Online flash cards provide review, practice, and enhance memory retention

CompTIA A+ Cert Kit

ISBN-13: 9780789742438
ISBN-10: 0789742438

Expert video training and other electronic learning tools like online flash cards and exam quick references prepare you for the A+ exams!

PEARSON EXAM CRAM

For more information on this and other Pearson Certification products, visit www.pearsoncertification.com