



Exam
Manual

CompTIA A+

(220-701)
A+ Essentials



**Smarter
Training**

Focusing on hardware and software PC support, this LearnSmart exam manual prepares candidates who wish to pass the CompTIA A+ Essentials Certification Exam (220-701) which fills half of the requirements needed to become a certified computer technician. In addition to presenting complex topics clearly and directly, this guide includes new material related to Windows 7. Topics covered in this guide include:

- Hardware
- Troubleshooting, Repair and Maintenance
- Operating Systems and Software
- Networking

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual today!

A+ Essentials (220-701)

LearnSmart Exam Manual

Copyright © 2011 by PrepLogic, LLC.

Product ID: 012077

Production Date: September 27, 2011

All rights reserved. No part of this document shall be stored in a retrieval system or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein.

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

LearnSmart Cloud Classroom, LearnSmart Video Training, Printables, Lecture Series, Quiz Me Series, Awdeeo, PrepLogic and other PrepLogic logos are trademarks or registered trademarks of PrepLogic, LLC. All other trademarks not owned by PrepLogic that appear in the software or on the Web Site (s) are the property of their respective owners.

Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

1-800-418-6789

solutions@learnsmartsystems.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

| | |
|---|----------|
| Abstract | 7 |
| What to Know | 7 |
| Tips | 7 |
| Domain 1: Hardware | 8 |
| Storage Devices and Backup Media | 8 |
| Motherboard Components, Types, and Features | 10 |
| Power Supply Types and Characteristics | 12 |
| CPU Purpose and Characteristics | 12 |
| <i>A note on CPU speed</i> | 13 |
| Cooling Methods and Devices | 13 |
| Memory Purpose, Types, and Characteristics | 13 |
| Memory Types | 14 |
| Operational Characteristics | 15 |
| Display Devices and Characteristics | 15 |
| Input Devices | 17 |
| Adapter Cards | 17 |
| Ports and Cabling | 18 |
| Laptops and Portable Devices | 19 |
| <i>Fundamental Principles</i> | 19 |
| <i>Laptop Form Factors</i> | 19 |
| <i>Laptop Peripherals</i> | 20 |
| <i>Expansion Slots</i> | 21 |
| <i>Laptop Computer Ports</i> | 21 |
| <i>Laptop Communications</i> | 21 |
| <i>Power</i> | 22 |
| <i>LCD and Video Technologies</i> | 22 |
| <i>Input Devices</i> | 23 |
| <i>Mobile Motherboards and Processors</i> | 24 |
| <i>Power Management</i> | 24 |
| <i>Hardware Removal</i> | 25 |
| Laptop Troubleshooting and Diagnostics | 26 |
| <i>Power</i> | 26 |

| | |
|--|-----------|
| <i>LCD Issues</i> | 27 |
| <i>Pointer and Keypad Issues</i> | 27 |
| <i>Wireless Issues</i> | 27 |
| Laptop Preventative Maintenance..... | 28 |
| Printers and Scanners..... | 29 |
| <i>Fundamental Principles</i> | 29 |
| <i>Printer and Scanner Technologies</i> | 29 |
| <i>Connections and Cables</i> | 30 |
| <i>Installation, Configuration and Optimization</i> | 31 |
| Printer Troubleshooting and Diagnostics..... | 33 |
| <i>Gathering Information</i> | 33 |
| <i>Review and Analyze Data</i> | 33 |
| <i>Identifying Solutions</i> | 33 |
| Domain 2: Troubleshooting, Repair, and Maintenance..... | 34 |
| Troubleshooting Theory..... | 34 |
| Techniques and Procedures..... | 34 |
| Problems and Issues..... | 35 |
| <i>Display Issues</i> | 35 |
| <i>Storage Devices</i> | 35 |
| <i>Memory</i> | 36 |
| <i>Input Devices</i> | 36 |
| <i>Thermal Issues</i> | 37 |
| <i>Power Issues</i> | 37 |
| Preventative Maintenance..... | 37 |
| <i>Preventative Maintenance Theory</i> | 37 |
| <i>Some Additional Notes on Preventative Maintenance</i> | 38 |
| Domain 3: Operating Systems and Software..... | 39 |
| Fundamental Principles..... | 39 |
| <i>Essential Components</i> | 40 |
| <i>Operating System Interfaces</i> | 40 |
| <i>Operating System Files in Pre-Windows Vista Computers</i> | 48 |
| <i>Operating System Files in Windows Vista, Windows 7, and Windows Server 2008</i> | 49 |
| <i>Disks, Directories and Files</i> | 49 |

| | |
|---|-----------|
| Installation, Configuration and Upgrade | 51 |
| <i>Installation on a Clean Machine</i> | 52 |
| <i>Performing Upgrades</i> | 52 |
| <i>Loading Device Drivers</i> | 53 |
| <i>Installing Drivers on a Windows 7 Computer</i> | 53 |
| <i>Installing Drivers on a Windows Vista Computer</i> | 53 |
| <i>Installing Drivers on a Windows XP Computer</i> | 54 |
| <i>Operating System Optimization</i> | 56 |
| Diagnostic and Troubleshooting Procedures | 60 |
| <i>Boot Methods and Sequences</i> | 60 |
| <i>Diagnostic Techniques</i> | 61 |
| <i>Common Operational Issues</i> | 62 |
| <i>Common Error Messages and Codes</i> | 64 |
| <i>Diagnostic Tools and Utilities</i> | 65 |
| <i>Preventative Maintenance</i> | 67 |
| Software and Windows Updates | 69 |
| <i>Scheduled Backups and Restores</i> | 70 |
| <i>Restore Points</i> | 70 |
| Domain 4: Networking | 71 |
| Fundamental Principles | 71 |
| <i>Basic Concepts</i> | 72 |
| <i>Network Cables</i> | 76 |
| <i>Networking Technologies</i> | 77 |
| Network Installation and Configuration | 79 |
| Diagnostics and Troubleshooting | 81 |
| Domain 5: Security | 81 |
| Fundamental Principles | 81 |
| <i>Hardware and Software Security</i> | 81 |
| <i>Wireless Security</i> | 83 |
| <i>Data and Physical Security</i> | 84 |
| Security Installation and Configuration | 84 |
| Security Troubleshooting and Diagnostics | 85 |
| Preventative Maintenance | 85 |

| | |
|---|-----------|
| Domain 6: Operational Procedure | 87 |
| Safety Issues | 87 |
| <i>Potential Safety Hazards</i> | 87 |
| <i>Material Safety Data Sheets (MSDS) and Documentation</i> | 87 |
| <i>Repair Tools</i> | 87 |
| <i>Accidents</i> | 88 |
| Safety Procedures | 88 |
| <i>ESD Precautions and Procedures</i> | 88 |
| <i>Safe Work Environment</i> | 89 |
| <i>Equipment Handling</i> | 89 |
| Disposal Procedures | 89 |
| Communication and Professionalism | 89 |
| <i>Communication</i> | 90 |
| <i>Professional Behavior</i> | 90 |
| <i>Behavior</i> | 90 |
| <i>Property</i> | 91 |
| Practice Questions | 92 |
| Answers & Explanations | 98 |

Abstract

This manual is intended to help a candidate prepare for, and pass, the A+ Essentials Certification Exam (number 220-701). Passing this multiple-choice exam fulfills half (50 percent) of the requirements to become a certified computer technician, with a focus on hardware and software PC support. As of June of 2011, this manual has been updated to include material related to the Windows 7 upgrade.

The other half is fulfilled by passing the CompTIA A+ Practical Application (220-702) exam.

What to Know

The A+ Essentials Exam (220-701) is intended to demonstrate the technician's ability to provide PC support and a general understanding of how PCs operate. The exam covers hardware components, laptop support, operating system concepts, printers and scanners, networks, basic computer and network security, environmental issues and proper communication and professionalism. It is important for someone preparing for this exam to be aware of the objectives for the exam, as well as an understanding of the basics of troubleshooting and computer components.

According to CompTIA, "The CompTIA A+ 220-701 examination measures necessary competencies for an entry-level IT professional with the equivalent knowledge of at least 500 hours of hands-on experience in the lab or field."

Following is a table that lists the A+ Essentials content domains and their associated examination percentages:

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

To learn more information about the A+ exams, including how to register, fees, etc., please visit the CompTIA Web site.

Tips

This manual is not intended to be an all-inclusive reference for technicians. Rather, this could be considered the "Cliff's Notes" to a very broad and inclusive area of study. It is advised that a technician with little-to-no experience in the field, preparing for this exam, purchase an A+ Reference Manual. The manual should be used for quick reference and study. Also, it is recommended that the technician also purchase the study exam questions that serve as a companion to this manual.

Domain 1: Hardware

Storage Devices and Backup Media

A *storage device* is, broadly defined, any component your computer uses to permanently store information. This is done in a variety of ways by a variety of different components, but generally speaking, storage devices are split into two categories: **fixed** and **removable**.

- A **hard disk drive** (HDD) is a fixed, non-volatile storage device that stores information on the magnetic surface of hard disk platters.
 - ▶ Hard disks are measured in terms of capacity (typically in GB) and in speed (revolutions per minute, or RPMs).
 - ▶ Today, a typical workstation's hard drive might have between 40 and 200 GB of storage space rotating at 7,200 to 10,000 RPMs.
 - ▶ Hard disks are usually connected to the computer by one of several different connections:
 - **ATA** – Standard on most desktop computers; IDE and EIDE; cable is a flat, wide ribbon.
 - **Serial ATA** – Provides for faster communication speeds between hard drive and motherboard; it is *not* backward compatible with the ATA form factor.
 - **SCSI** – Interface allowing the connection of several devices in a chain.
 - For more information about connection types, refer to the **Motherboard Components** discussion below.
 - ▶ **RAID** (Redundant Array of Independent Disks) is a system utilizing multiple hard disks in tandem to share data across the drives. It helps provide data security and recoverability, protecting against hard drive failure.
- A **floppy disk drive** (FDD) is **removable** storage utilizing a thin, flexible magnetic storage medium, encased in a plastic shell to read and write data.
 - ▶ While over time drive capacities have changed, today's standard floppy disk drive size is 1.44 MB.
 - ▶ Floppy disk drives are quickly going out of standard use, due to the higher capacity, and much cheaper, writeable compact disks.
- The **CD** and **DVD-R** (or RW, for rewriteable) is removable storage that takes advantage of the higher capacity of optical disks to store information. Optical drives are, typically, IDE or SCSI devices.
 - ▶ CD-R (and DVD-R) drives utilize a red-light laser to "burn" data onto blank optical discs.
 - ▶ CD and DVD-R media come in several different types:
 - **CD-R** – Write-Once discs, with a standard size of 700MBs;
 - **CD-RW** – Rewriteable discs, with a standard size of 700MBs;

- **DVD-R** – Also write-once discs, DVDs have a standard capacity of 4.7 GB. This format includes the **DVD-RW**, the rewriteable form;
- **DVD+R** – Simply another write-once format, not currently approved by the DVD Forum. It also has a rewriteable form, **DVD+RW**, and a double layer disc with a capacity of almost 8.55 GBs, referred to as **DVD+RW DL**.
- **Blu-Ray** – Sony-proprietary optical disc storage medium. Can store high-definition video and audio at a capacity of 50 GB per disc (dual layer).
- ▶ Drive speeds are as varied as media types and are issued as multiples of the original read speed of the device. CD-ROMs start at 150Kbps, and DVD-ROMs start at 1352.54Kbps. Thus, a 52x CD-ROM reads at 7800Kbps, and a 16x DVD-ROM reads at 21,640Kbps.
- Other removable storage options include:
 - ▶ **Tape Drives** - Sequential-access data media composed of a strip of magnetic or punched tape. Usually used for archival storage due to the long shelf-life of the medium.
 - ▶ **Solid State Drives** - Such as thumb, flash and SD drives. Volatile storage (like RAM) utilized for extremely quick access speeds. These are usually used in small, hand-held devices.
 - ▶ **USB** - A serial connection used to link, typically, external devices to the computer. These can be hard drives and optical drives, and are utilized for a variety of reasons but are usually used to take advantage of the ease of operability and installation. USB external devices are plug-and-play.

Here are some important things to remember when installing, configuring or upgrading storage devices:

- If the drive is PATA, ensure that the jumper cables are properly set for the device to be master or slave and are connected to the correct connection.
- Ensure the drive is connected to power.
- Be mindful of the **file system**.
 - ▶ File system is usually decided during the initial formatting.
 - ▶ Windows 95, 98 and Me use the **FAT32** file system.
 - ▶ Windows NT, 2000, 2003 Server, XP and Vista utilize the **NTFS** file system.
 - ▶ NTFS has extra functionality for improved performance, reliability and disk space utilization.
- Imaging software, such as Norton Ghost, can be used to easily capture and restore hard drive files, settings and operating systems.

Motherboard Components, Types, and Features

Motherboards (or mainboards) are one of the most important components in a computer. They provide the backbone of communication between all devices installed on a computer, and as such, it is important to understand how the various components on a motherboard function.

- The **form factor** of a motherboard refers to several characteristics of a motherboard, including its size and format (which in turn relates to the size and format of the computer case), as well as the particular interfaces that allow communication with other devices.
 - ▶ **ATX** - (Advanced Technology Extended) is the industry standard motherboard form factor.
 - ▶ **BTX** - a newer version of ATX, focusing on a lower profile and providing better thermal regulation. BTX is currently being used in Gateway and Dell computers.
 - ▶ **Micro ATX** and **NLX** - simply smaller versions of the ATX built for smaller, workstation oriented computers.
- **Components**
 - ▶ Most motherboards include a variety of integrated input/output components. These are usually sound, video, parallel and serial ports, and USB connections. Some motherboards also provide integrated modems, network interface cards and IEEE 1394 (or firewire) connections.
 - ▶ **Memory slots** refer to the available slots for RAM modules, and come, typically, in two styles:
 - **RIMM** – This is the industry standard for RDRAM memory. Possesses a 32-bit bus length.
 - **DIMM** – Dual In-line Memory Module. This doubles the bus length to 64-bits, providing higher bandwidth for access speeds.
 - ▶ **Processor Sockets** refer to the socket type for the processor chip. ATX motherboards can potentially come with one of several different socket types:
 - **Socket 478** – Used for Intel’s Pentium 4 and Celeron chips. Supports high bus speeds, DDR, RD, and SD RAM.
 - **Socket A** – Used for AMD’s line of processors. While this is still in wide use, it has been ultimately replaced by the **Socket 939** for high-end AMD processors, and the **Socket 754** for budget processors.
 - ▶ **External Cache Memory** refers to small amounts of volatile memory located near the CPU to provide faster access times to memory modules, by duplicating frequently used locations in the RAM modules.
 - ▶ **Bus Architecture** refers to the connection medium through which peripheral cards connect to the motherboard.
 - ▶ Peripheral cards connect to the computer bus through a variety of **bus slots**:
 - **PCI** – Most commonly used bus slot; most expansion cards utilize the PCI bus (with the exception of graphics cards).

- **AGP** – PCI-derived standard with higher bus speeds utilized for 3D graphics rendering.
- **PCIe** – *PCI Express* slot developed more recently which utilizes a much faster serial communications protocol.
- ▶ **EIDE (or PATA) and SATA** are standards for connecting storage media to the motherboard.
 - **EIDE** - utilizes a parallel connection and a shared bus consisting of a master device and a slave device.
 - **SATA** - theoretically, faster. However, its largest benefits over EIDE are smaller power and interface cables and the ability to hotplug SATA devices. This is due, in part, to the dedicated cable and host controller for the serial device. A dedicated host controller means that the information passed along the bus can be more quickly assimilated or disassembled, resulting in faster speeds.
- ▶ **SCSI** (Small Computer System Interface) - commonly used to connect hard, optical, and tape drives; however, these can be expanded to connect a wide range of devices, including scanners and printers. There are several SCSI standards. Generally speaking, SCSI provides a higher range of data management and protection capabilities than the ATA standard. Refer to *Figure 1, SCSI Types* for a listing of SCSI standards and their associated speeds.

| SCSI Type | Bus Speed | Bus Width | Transfer Rate | Max Number of Devices |
|--------------------|-----------|-----------|---------------|-----------------------|
| Regular SCSI-1 | 5 MHz | 8 bit | 5 Mbps | 8 |
| Wide SCSI-2 | 5 MHz | 16 bit | 10 Mbps | 16 |
| Fast SCSI-2 | 10 MHz | 8 bit | 10 Mbps | 8 |
| Fast Wide SCSI-2 | 10 MHz | 16 bit | 20 Mbps | 16 |
| Ultra SCSI-3 | 20 MHz | 8 bit | 20 Mbps | 8 |
| Ultra Wide SCSI-3 | 20 MHz | 16 bit | 40 Mbps | 16 |
| Ultra 2 SCSI-3 | 40 MHz | 8 bit | 40 Mbps | 8 |
| Ultra2 Wide SCSI-3 | 40 MHz | 16 bit | 80 Mbps | 16 |
| Ultra3 SCSI-3 | 40 MHz | 16 bit | 160 Mbps | 16 |
| Ultra4 SCSI-3 | 80 MHz | 16 bit | 320 Mbps | 16 |

Figure 1: SCSI Types and Stats

- ▶ **Chipset** - refers to the specialized motherboard chips handling communications between outlying devices and the processor. These come in two classes:
 1. **Northbridge** – located closest to the processor, which handles communication between RAM and AGP and PCI-E slots.
 2. **Southbridge** – located furthest from the processor, handling slower devices, such as PCI, IDE, USB, etc.
- ▶ **Basic Input/Output System (BIOS)** - hard-wired software code the computer uses to prepare the machine for control by the operating system.
 - BIOS utilizes a version of non-volatile memory to store these settings, referred to as **CMOS**, and connected to a small battery.
- ▶ In this context, **Firmware** refers to the actual software hard-coded on the BIOS, which can be updated via a process referred to as “flashing.”

Power Supply Types and Characteristics

A power supply's main purpose is to both **convert** AC power, typically between 120 and 240 volts (V), into useable power and to **convey** that useable power adequately throughout all of a computer's various components.

- Though power supplies come in a wide variety of form factors for different uses, most conform to the ATX standard.
- Power supplies are rated based on their maximum output power, measured in watts (W); most fall between 200 W and 500 W.
- Output leads, from the unit, supply power to the various devices.

CPU Purpose and Characteristics

If one can visualize the motherboard as the backbone of a computer system, then it is appropriate to imagine the processor as the brain of a computer system. The central processing unit (CPU) performs all data processing and instruction interpretation that is vital to the operation of a computer.

- Virtually all personal computers utilize one of two brands of processor chips:
 - ▶ **AMD and Intel.**
 - ▶ In reality, there is very little difference between the two chips, aside from basic architecture and pin structure and the general acknowledgement that Intel processors run slightly cooler than AMD processors.
 - ▶ Processor choice should ultimately be made based on price and features.
- CPUs can potentially support a number of various chip technologies, described below:
 - ▶ **Hyper-threading** - the utilization of otherwise idle execution units to improve the over-all reaction and response time of the CPU.
 - ▶ **Dual core** - refers to a single processor which possesses two independent microprocessors.
 - ▶ **Quad core** - refers to a single processor die that possesses four independent microprocessors.
 - A great benefit of multi-core CPUs is that you get twice (or four times) the processing power in a single CPU socket on a motherboard. Hence, a motherboard with two CPU sockets can effectively be an 8-CPU machine with two quad-core CPUs installed.
 - ▶ **Throttling** - also known as clamping, cuts the amount of CPU time used on applications which stall the computer.
 - ▶ **Micro Code (MMX)** - a CPU instruction set, designed by Intel, which allows for the CPU to "package" larger instructions into smaller pieces, or microprograms.
 - ▶ **Overclocking** - the process of overriding a CPU's designed clock speed in favor of faster clock speeds, which in turn provides better performance.

- ▶ **Cache** - a designated set of smaller, faster memory units, utilized by the CPU, to perform frequently utilized instructions faster.
- ▶ **Voltage regulator Module (VRM)** - the device which provides the proper amount of power to a CPU.
- ▶ Most processors today come in a **32-bit** format, with **64-bit** processors slowly finding use in academic and corporate institutions. The essential difference between the two formats lies in their ability to handle mathematical calculations. 64-bit processors can simply handle larger numbers and can be more efficient with smaller numbers.

A note on CPU speed

The speed of a CPU is a somewhat amorphous subject. The clock speed, expressed in terms of cycles per second, or *hertz*, is an expression of how fast a CPU performs its most basic functions. Of course, most processors run in excess of a billion cycles per second, or in GHz. At these speeds, the clock speed is really only helpful in comparing processors in the same family (i.e. between two Pentium 4 chips, or two Athlons). Other factors also contribute to a CPU's overall speed and performance, such as the kind and quantity of cache memory or the size of the data bus. A software benchmark test is the only real reliable way to compare the speeds of processor chips.

Cooling Methods and Devices

Every component of a computer produces heat as a by-product of electrical conductivity. Heat will permanently damage internal components, especially the processor. Therefore, special considerations should be made to ensure the computer operates at an optimal temperature. Below are some characteristics of cooling systems, found in personal computers:

- **Fans** - mounted above the CPU and on the case, direct heat away from the processor and then out of the case.
- **Heat sinks** - objects, usually made of copper or aluminum, which absorb and dissipate heat produced by internal components. Paired with CPU and case fans, a heat sink can maintain a larger temperature gradient, replacing warmed air quickly and efficiently.
- **Thermal compound** - A ceramic, silicone or metal compound which increases the thermal conductivity of both the CPU and the heatsink.
- **Liquid cooling systems** - complex apparatus that continually cycle water over CPU units, carrying heat away to radiators, which in turn cool the water and pass it back over the CPU. These systems, at their most basic, will consist of the tubing, a pump and a radiator.

Memory Purpose, Types, and Characteristics

RAM, or system memory, is volatile storage space the computer uses to load active programs. Since RAM is accessed randomly, rather than sequentially, programs loaded into memory can be loaded quickly and used more efficiently. Since proper RAM choice and installation is vital to proper PC operation, it is important for technicians to understand the difference between various types of RAM and the technologies they use. Refer to the following table for a list of memory types and their pin sizes.

| RAM Type | Pin Size |
|----------|--------------|
| DRAM | 72-pin SIMM |
| SDRAM | 168-pin DIMM |
| DDR | 184-pin DIMM |
| DDR-2 | 240-pin DIMM |
| RAMBUS | 184-pin RIMM |

Figure 2: RAM types and pin sizes

You'll also need to know something about the available speeds of RAM. The chart below explains the various RAM standards and speeds specified by CompTIA's official objectives:

| Standard Name | Module Name | Memory Clock | Peak Transfer Rate |
|---------------|----------------------|--------------|--------------------|
| PC100 | PC100 | 100 MHz | 640 MB/s |
| PC133 | PC133 | 133 MHz | 1064 MB/s |
| DDR-333 | PC2700 | 166 MHz | 2700 MB/s |
| DDR-400 | PC3200 | 200 MHz | 3200 MB/s |
| DDR2-667 | PC2-5300 PC2-5400 | 166 MHz | 5333 MB/s |
| DDR-1600 | PC3-12800 | 200 MHz | 12800 MB/s |

Memory Types

- **SRAM** – Static memory that retains information as long as power is applied to it; this is used almost exclusively in CMOS applications.
- **DRAM** – Dynamic memory that requires refreshing in order to retain information; this is the most common type of RAM, and all other types of system memory RAM are based on this concept.
- **SDRAM** – DRAM which synchronizes with clock signals from the system bus and processor, making it more efficient.
- **Double Data Rate (DDR)** – SDRAM which transfers information twice on the same clock signal, effectively doubling its bandwidth. **DDR-2** works on the same principle and has some improvements to further increase bandwidth and transfer speed.
- **RAMBUS** – Another double data rate DRAM designed specifically by the Rambus Corporation, this type of RAM operates slightly faster than previous DRAM formats. It is also very expensive, produces much more heat and has a slower latency time.
- **Dual-Channel Memory** – This type of memory is enhanced, on motherboards which support it, with two 64-bit data channels, resulting in an incredible 128-bit bandwidth. This type of memory must be installed in matched sets. Motherboards supporting this type of memory will have color-coded memory slots.

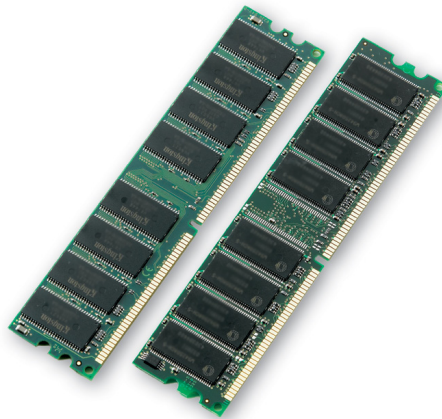


Figure 3: RAM modules

Operational Characteristics

- **Memory chips** - the individual memory chips on the RAM module and come 8, 16, 32 or 64-bit in size. Generally speaking, higher quality RAM modules use larger and fewer memory chips.
- **Parity** - a simple form of error checking that attaches a bit to transferred data. Parity is not error correcting, so data deemed corrupt by the parity bit is discarded and must be retransmitted.
- **ECC** - uses slightly more information to not only detect errors, but correct them at the point of transmission. Because the instructions are more complex, ECC RAM can be somewhat slower than non-ECC RAM and will also be more expensive, due to the complexity of construction.
- Sometimes RAM modules come rated as either **single- or double-sided**. Contrary to popular opinion, this has nothing to do with the placement of the memory chips. Rather, it has to do with how much of the RAM module is given over to transmission space. A single-sided RAM appears to the motherboard as one 64-bit area, regardless of how many chips are actually on the module. A double-sided RAM appears as two 64-bit areas.

Display Devices and Characteristics

Attached to some video output, display devices produce the visual images of computer operation. They currently come in two classes:

- **Cathode Ray Tube (CRT)** - large monitors resembling television sets. They will have a longer shelf life than LCD monitors but lower resolutions and a larger footprint.
- **Liquid Crystal Display (LCD)** - produce higher quality images and are extremely small in comparison to CRT monitors but have a much shorter shelf life.
- **Connection Types:**
 - **VGA** - the standard, analog display connection type. They are 15-pin D-connectors and are used exclusively by CRT monitors.
 - **Digital Visual Interface (DVI)** - a connection standard used exclusively by LCD monitors and projectors, providing higher resolutions.

- ▶ **High Definition Multimedia Interface (HDMI)** - an uncompressed digital audio and video connection used in high-end DVD players and Hi-Def televisions.
- ▶ **S-Video** - another analog connection standard which transmits video data on two separate channels: brightness and color.
- ▶ **Component Video** (or RGB) - separates video channels into discrete Red, Green and Blue transmissions. This is being superseded by DVI and HDMI interfaces.



Figure 4: Video connector form factors

- Important display settings to remember:
 - ▶ **Vertical hold** - maintains the vertical stability of the display.
 - ▶ **Refresh rate** - the number of times per second a display is illuminated, measured in *hertz*.
 - ▶ **Resolution** - the number of pixels a screen displays. The higher the resolution, the more detail can be seen, up to the monitor's maximum resolution.

Keep the following in mind when installing, configuring or upgrading display devices:

- Make sure the video card is properly installed and all drivers are updated prior to attaching the new display device.
- If the display device requires special connections (i.e. DVI or HDMI), make sure these are available on the video card.
- Attach the device to the video card and power source, and allow the computer to recognize the new display device.
- If drivers were provided with the display device, install them.

Input Devices

Any device used to provide human interaction with a computer is an input device. The most simple and common, of course, are the **mouse** and **keyboard**. Below are some non-standard input devices:

- **Web and digital cameras** - used to provide video-conferencing abilities and the digital storage of photographs.
- **MIDI** - used to input synthesized instruments for audio production.
- **Microphones** - capture voice input for anything from VoIP broadcasts to speech-to-text input.
- **Biometrics** - devices, such as retinal and fingerprint scanners, provide extra measures of security from unauthorized use.
- **Touch screens** - allow users to input commands by literally touching the screen through pressure, electro, acoustic or photo-sensitive materials.

Adapter Cards

Adapter or expansion cards allow the user to create extra functionality and inputs for a computer. Below are some examples of common adapter cards.

- **Video cards** - add an extra processor and RAM devoted to processing video information. They come in three types, related to the type of motherboard slot types: **PCI**, **PCIe** and **AGP**.
- **Multimedia cards** come in a wide variety of uses and standards.
 - ▶ **Sound cards** - add some extra sound functionality, above and beyond basic sound production, such as surround-sound capabilities, digital audio processing, etc.
 - ▶ **TV Tuner Cards** - act like a cable box for your computer, accepting input from coaxial cable or antenna, to produce television signals on screen.
- **Input/Output** cards add extra ports and connections, either internally or externally. **SCSI**, **USB**, **FireWire** and **Serial I/O** cards are among the most common.
- **Communications** adapter cards, such as network identification cards (NICs) and modems, allow the computer to transmit and receive data from other computers and networks.

Ports and Cabling

Inevitably, in servicing personal computers, a technician will have to deal with a wide variety of ports and cables.



Figure 5: I/O port form factors

| Port | Description | |
|------------|--|--|
| USB | Provides hot-swapping of a wide variety of connected peripherals. Comes in two speeds: 1.1 and 2. Version 2 has a higher transfer speed. | |
| Parallel | Sends every bit in a value set simultaneously; being phased out by USB, though still sometimes used for printer connections. | |
| Serial | Sends bits in a value set in series down the cable; also being phased out by faster standards; used for mice, keyboards, terminals and modems. | |
| FireWire | The IEEE 1394 connection offers high-speed communications and is used for anything from digital camcorders to data storage devices. | |
| RJ45 | The CAT-5 cable connection for Ethernet. | |
| RJ11 | The cable connection for telephone lines used in modem communications. | |
| Mini-DIN | Represents a range of connections, all identified by the number of pins the connection uses; the most common type is Mini-DIN 6, or PS/2 used in mice and keyboards. | |
| Centronics | A parallel connection that can transmit 8 bits simultaneously. Also being phased out by USB, and is indistinguishable from a regular parallel connector. | |
| Multimedia | Another broad range of connections: | |
| | 1/8" – Headphone, microphone, speaker jack. | SPDIF – carries compressed digital audio to and from the sound card and optical drive. |

Figure 6: I/O ports and descriptions

Laptops and Portable Devices

Fundamental Principles

Before learning laptop-specific components and functions, it is important to understand the various overall types and uses of laptops. In general, laptops come in four styles or types:

- **Ultraportables** - the smallest and one of the more expensive models, utilizing power-saving components and weighing less than a few pounds. These are used almost exclusively by the business traveler set.
- **Thin-and-Lights** - somewhat larger than the above, sporting a larger screen and more functionality than ultraportable laptops.
- **Medium-Sized** - the most common. They will weigh 6.5 to 7lbs and usually have somewhat larger screens and a longer battery life.
- **Desktop Replacements** - the largest of the four types. These are designed to be relatively stationary, due to their large size, which, in turn, provides space for more powerful components and the largest screens. Desktop replacement laptops usually have a short battery life.

Laptop Form Factors

Unlike desktop computers, laptops have no industry-wide standard form factor. Manufacturers utilize their own motherboard designs, which, in turn, make laptops both difficult and expensive to upgrade. However, hard drives and memory in laptops are easily user-upgradeable and, therefore, do possess a form factor:

- **Hard Drives**
 - ▶ 2.5" Form Factor.
 - ▶ Some are hot swappable (accessed by a screwed-in panel on the underside of the machine).
 - ▶ Most range from 40-80GB, with some reaching 100GB.
 - ▶ Speeds typically around 54-7200 RPMs, but expect to see 10,000 RPM notebook hard drives in the next few years.
- **Memory**
 - ▶ Small Outline Dual Inline Memory Module (SO-DIMM) - comes in three versions (refer to *Figure 7*, below):
 - 100 pins (32 bit)
 - 144 pins (64 bit)
 - 200 pins (64 bit)
 - ▶ Note that these modules can also be found in high-end office printers and routers or other networking hardware.

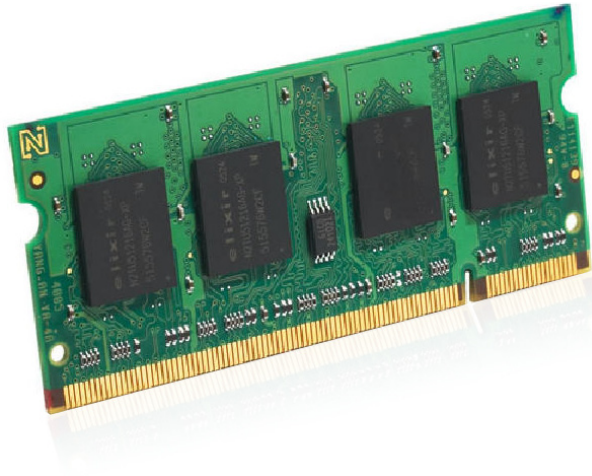


Figure 7: Laptop SODIMM memory module

Laptop Peripherals

Due to their small size and relatively limited upgradeability, several different peripheral devices have evolved in order to improve and increase the productivity and usability of laptops. These are discussed below:

- **Docking station** - a device which allows the user to accomplish two goals:
 - ▶ Use the laptop as a desktop computer: docking stations are usually attached to monitors, keyboards, mice and other desktop computer peripherals.
 - ▶ Recharge the battery: most docking stations, if nothing else, provide this most basic functionality.
- **Port replicator** - a device which provides extra communications ports to the laptop. These will typically be serial, parallel, extra USB and/or KVM connections. While functionally similar to a docking station, port replicators do not recharge batteries and will be much smaller.
- **Media bays** - allows for the connection of one or more external media devices. These can be either fixed or removable, with most media bays focusing on providing CD and DVD-R capability.
- It should be noted that the majority of these devices are being outmoded, in favor of laptops that already possess the functionality of the above devices. For instance, dual-purpose optical drives, some of which can read, write and rewrite on every available medium, have made media bays obsolete.

Expansion Slots

Laptops, in general, are not designed to be opened and upgraded like PCs. However, without some form of upgradeability, these expensive machines would quickly become obsolete. For this purpose, most laptops have some form of expansion slot, similar to the PC's PCI and AGP slots, for expanded functionality.

- **PCMCIA I** – This was the first type of expansion card for a laptop. It was used solely for SRAM and flash memory upgrades.
- **PCMCIA II** – Developed later, type II cards introduced I/O support on top of flash memory functions.
- **PCMCIA III** – Provided for further expansion of functionality, and fully focused on I/O functions.
- **CardBus** – First introduced in 1995, CardBus expansions were a massive improvement over the previous PCMCIA devices. CardBus essentially provided a 32-bit, 33MHz PCI bus for expanded functionality, as well as bus mastering abilities previously only available in PCs.
- **ExpressCard** – These are the newest expansion slot cards. ExpressCards have a direct connection to the motherboard via a PCI-E or USB 2.0 connection that allows them to take advantage of a much improved data throughput speed (500 Mbps). ExpressCards also have a lower power requirement.
- **Mini PCI** – Developed almost exclusively for integrated communications peripherals (such as modems and network cards), Mini PCI operates just like the PCI 2.2 standard, developed for standard PCs. Laptops typically possess only one of these slots.

Laptop Computer Ports

Like desktop PCs, laptops will also have a wide variety of communications ports, connecting a wide variety of devices and peripherals. This can include **serial**, **parallel**, **USB** and **FireWire**, though most laptops will have a much larger emphasis on USB connections. For a discussion on these various ports, refer to **Domain 1, Ports and Cabling**.

Laptop Communications

In deference to their portable nature, many communications technologies have been developed for laptops and other portable devices. Below is a brief discussion on the various types and purposes of portable communications technologies.

- **Ethernet** – As with desktop PCs, Ethernet is the standard wired network utilizing CAT-5 cable and speeds between 10 and 1000 Mbps. Most modern laptops have Ethernet capability built in. Older laptops required a CardBus or PC Card to provide Ethernet capabilities. The CAT-5 cable plugged into a device called a “dongle,” (*Figure 8*, below) which, in turn, connected with the small edge connector of the PC Card.



Figure 8: PC card dongle

- **Wireless Wide Area Network (WWLAN)** – This is sometimes referred to as a Cellular LAN, as it uses a cellular network to provide connectivity with an internet service provider, similar to the way dial-up networking works in PCs. Most cell phone services offer this technology.
- **Bluetooth** – This radio standard was designed primarily as a low-power alternative to Wi-Fi connections. The tradeoff for lower power consumption, of course, is range and strength of signal. Bluetooth is most commonly seen in cell phone technology (such as headsets), though mice, keyboards, microphones and headphones are common laptop Bluetooth devices.
- **Infrared** – Like Bluetooth, infrared communications are only viable in short range. Infrared peripherals can include mice and keyboards, as well as provide a method of data transmission between PDAs and other computing devices.

Power

One of the chief concerns of laptop users is power. Laptops are designed to be run without wires, promoting a mobile working environment. Therefore, it is important for a technician to understand different power technologies and devices offered by laptop technology.

- **Batteries** – Laptops will use one of three different types of rechargeable battery:
 - **Nickel Metal Hydride (NiMH)** – The first laptop battery, with a fast recharge rate and a relatively short lifespan.
 - **Lithium Ion (Li-Ion)** – Newer and most common rechargeable battery, it has a longer battery life and a better energy-to-weight ratio.
 - **Lithium Polymer (Li-Poly)** – Newest rechargeable battery, it doesn't require a metal cell casing, allowing for a lighter battery that can be manufactured into virtually any shape. It has broad applications in small devices as Li-Poly batteries can be made extremely thin.

LCD and Video Technologies

LCD technology was, originally, what set laptops apart from desktop computers and made them portable. They utilize any number of color pixels, consisting of a layer of liquid crystals, arrayed in front of a light source or a reflector. LCD screens are thinner, working without the bulky cathode ray tube that provides display on CRT monitors.

- Early LCD screens utilized **passive-matrix addressing**, where every row or column of pixels was connected to one electrical circuit. Without the benefit of a constant electrical charge, pixels in passive-matrix addressing must retain their state between refreshes.
- Newer, high-resolution LCD screens use **active-matrix addressing**. In active-matrix addressing, a thin layer of transistors is added to color filters, allowing each pixel to be connected to its own transistor, which, in turn, allows the display to access one pixel at a time, increasing both the sharpness and brightness of the display. Refer to *Figure 9*, below, for a list of the various video technologies available to active-matrix displays.

| Technology | Abbr. | Resolution | Pixels |
|--|-------|------------|-----------|
| Extended Graphics Array | XGA | 1024x768 | 786,432 |
| Super Extended Graphics Array | SXGA+ | 1400x1050 | 1,470,000 |
| Ultra Extended Graphics Array | UXGA | 1600x1200 | 1,920,000 |
| Widescreen Ultra Extended Graphics Array | WUXGA | 1920x1200 | 2,304,000 |

Figure 9: Video technology standards

- When choosing between LCD screens, in addition to resolution and video technology, there are two other important terms to know and understand:
 - **Contrast Ratio** - the ratio of the luminosity between the lightest and darkest color the screen can produce. *Static* contrast ratio is the ratio at any given instant, while *dynamic* contrast ratio is the ratio over time.
 - **Native Resolution** - the fixed resolution of any LCD device. CRT monitors can produce a variety of resolutions, LCD screens possess a fixed raster and must therefore use interpolation (which causes quality loss) to display images in anything *other* than their native resolution.

Input Devices

Laptops and portable devices take advantage of a wide variety of human input devices. Due in part to their portability, input devices for laptops, PDAs, smart phones, etc. tend to focus on producing enhanced functionality while keeping the footprint of the system small. Below is a discussion of the more common laptop input devices:

- **Fn Key** - the ubiquitous laptop input device. The key allows access to **Num Pad** functions and some laptop specific commands, such as display controls, volume, hibernate, etc. See *Figure 10*, below.



Figure 10: Laptop keyboard

- Laptops support a wide variety of **Pointing Devices**:
 - **Point Stick** (IBM's TrackPoint™) – A rubberized cap which responds to applied force. Located, usually, between the B,G and H keys.
 - **Touch Pad** – Another very common pointing device, which uses sensors to detect the moving capacitance of a user's finger. Modern touch pads have a variety of "hot spots" serving purposes such as scroll bar control and zooming.
 - **Stylus** (or digitizer) – Simply an inkless pen used to interact with touch screens to protect the screen from the natural oils of the finger and provide a finer degree of control.

Mobile Motherboards and Processors

Besides simply being smaller in form factor, laptop motherboards have other very important differences distinguishing them from desktop motherboards. For instance, a laptop motherboard will typically only have one internal expansion card slot, if it has any at all. Most expansions that might connect to expansion slots on a desktop motherboard will, instead, be integrated into the laptop motherboard or expanded with PCMCIA, CardBus or ExpressCards (see above section, **Expansion Slots**).

That being said, there are three features of laptop motherboards and processors that are perhaps the most distinctive:

- **CPU Throttling** – While this feature is merely optional in desktop PCs, it is essential in laptop and mobile PCs. CPU time and energy also means CPU heat. Since mobile devices are significantly smaller than desktop computers, CPU heat is more damaging. Innate CPU throttling allows the mobile device to cut down on the amount of time, energy and heat expended in computer operations.
- **Power Management** – As noted in the **Power** section above, one of the chief concerns of laptop use is the proper management of power usage. Laptop motherboards, therefore, have extra CMOS features which help better manage power. These settings can be adjusted by navigating to **Start > Control Panel > Power Options**. Below are screen captures of each tab and an explanation of the features available.
- **Wi-Fi** – A laptop's chief concern is mobility. Therefore, integrated Wi-Fi capabilities are becoming increasingly common in newer laptops and mobile devices. Without the use of an expansion card, integrated Wi-Fi allows laptop computers to connect to Wi-Fi "hotspots" or wireless zones of connectivity.

Power Management

As previously stated in the above sections, power management is one of the chief concerns of any mobile device. Specifically, this is the management of battery power. This section details how a user can configure and optimize laptop usage of power.


- **ACPI** – Advanced Configuration and Power Interface (ACPI) is an open industry standard for power management which superseded Advanced Power Management. Most notably, ACPI took power management out of BIOS and gave that ability to the OS. See the above section, **Mobile Motherboards**, for a point-by-point and visual breakdown of OS elements of power management. ACPI defines seven states for mobile computers:
 - **G0 Working** – This is the natural state for the computer. Everything is on.
 - **G1 Sleeping** – This state is further divided into four different sleeping states:
 - **S1 Suspend** – Power hungry sleep mode where processor and RAM caches are flushed, but power is maintained. Devices which are not required to have power will be powered down. This state is slowly going out of common use.
 - **S2 Suspend** – Same as above, but the CPU is powered down. This is almost completely out of standard use.
 - **S3 Standby** – All information about the system (CPU state, open documents, etc.) is cached to RAM, and everything else is powered down.

- **S3 Hibernate** – Most powerful sleep feature. The current state of operation is cached to a folder on the root disk drive, including the contents of RAM modules. All power to the system is then cut off.
- ▶ **G2 Soft Off** – This is simply a power down initiated by the operating system. Power is still running to the system, so that it can be quickly booted.
- ▶ **G3 Hard or Mechanical Off** – This is what happens when the power button is pressed for the required five seconds, and it is a complete power down.

Hardware Removal

This section will give step-by-step instructions on the removal of hardware from laptops, beginning with hot-swappable devices and moving towards more difficult and labor-intensive devices.

Hot-Swappable Devices

1. In the task bar, at the lower right-hand corner of the screen, is a small icon denoting hot-swappable devices. **Double-click** this icon .
2. The **Safely Remove Hardware** dialog appears; choose the device you wish to disconnect and click **Stop**.

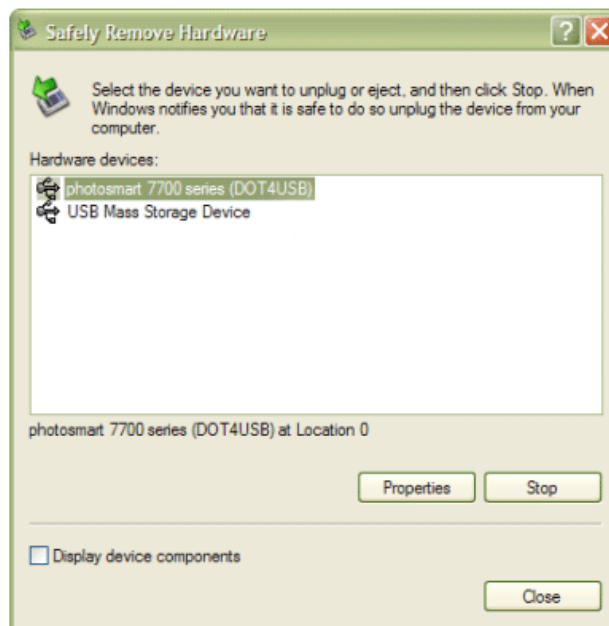


Figure 11: Safely Remove Hardware dialog

3. A **ToolTip** informing that the device has been stopped and can be safely removed will appear over the icon in the task bar. Remove the device.

Peripherals

- Peripherals, like external mice, USB and FireWire drives, port replicators, media bays and docking stations, may simply be disconnected from the laptop and removed.
- With docking stations, port replicators and media bays, it is helpful to power down the device first, and then remove the peripheral.

Internal Devices

- **Power down the device!** Always power down, unplug and remove the battery from the device before doing *any* internal servicing.
- Hard drives and memory will be located underneath the keyboard and can be accessed with a Phillips head screw driver.

Laptop Troubleshooting and Diagnostics

The following section will break the laptop down into its component parts and discuss how to go about diagnosing and troubleshooting these individual components.

Power

- **Verify AC Power**
 - ▶ Note the LEDs on the front of the laptop.
 - ▶ When you plug the adapter in, does the amber light over the battery icon light up? If not, you may have a bad AC adapter, a bad battery, or a dead wall socket.
 - ▶ Replace the AC adapter with a known good AC adapter.
 - ▶ If this doesn't resolve the problem, refer to **Verify DC power**, below.
- **Verify DC Power**
 - ▶ DC power is the power coming from the battery, and batteries can lose their charge after repeated use over a long period of time.
 - ▶ Batteries can be checked for lost charges, though the apparatus is usually prohibitively expensive; try the retailer of the battery.
 - ▶ Replace the battery with a known good battery. If this doesn't resolve the issue, the charging apparatus may be malfunctioning.
- **Unnecessary Peripherals**
 - ▶ Because laptops are so power conscious, extra peripherals may be drawing too much power and can cause a variety of errors, hangs, etc.
 - ▶ Remove unnecessary peripherals, one by one, to determine which peripheral is causing the errors or operating system hangs.

LCD Issues

- Laptops have extra features on the keyboard that control various aspects of the LCD screen for power conservation.
- A blank LCD screen may not be malfunctioning.
- Check the LCD cutoff switch, activated by pressing the **Fn** key and one of the Function keys.
- Refer to the laptop's manual for the LCD cutoff-switch combination.
- If it is activated, the computer may be on, while the LCD will be shut off.
- Brightness, contrast and backlighting may also be affected by accidental Fn key activation.
- Check each of these, in turn, to ensure that the LCD has not been over adjusted.
- If none of the above bring video back to the LCD screen, then the screen may be malfunctioning.
- Try connecting an external CRT monitor, if this is available, to the laptop.
- Display can be switched between CRT and LCD with Fn key depressions. Again, refer to the laptop's manual.

Pointer and Keypad Issues

- **Digitizer, Stylus and Pointer Issues**
 - ▶ Laptop pointer pads can be quickly overcome by oils, liquids and foods. Always ensure the pad is clean before use.
 - ▶ PDA digitizers can easily become misaligned. The PDA will have a resynchronization application; use this to realign the stylus with the digitizer.
- **Keypad Issues**
 - ▶ The user should understand that the laptop's keypad does not work like a PC's keypad.
 - ▶ The Fn key can become locked, and regular letter keys will act like keypad keys.
 - ▶ As with all keyboards, food and liquids will damage or destroy the keyboard and keypad, and eventually the laptop.

Wireless Issues

- If wireless capability is dependent on an expansion card, ensure the card is properly seated in the slot and that up-to-date drivers are installed.
- Make sure the antennas are attached – broken antennas will have to be repaired by a factory-trained service technician.
- Ensure the laptop is within range of a wireless access point. Without this access, the laptop will not connect to the network.

Laptop Preventative Maintenance

The concepts of preventative maintenance are important for every expensive piece of computer equipment, for obvious reasons. However, it is extremely important that these are practiced for laptops, due to their particular nature. As all or most laptop components are integrated into the motherboard, and therefore the entire machine, if one part goes bad, then the entire laptop goes bad. Pay close attention to the following concepts.

- **Cooling Devices**
 - ▶ Cooling devices can be a very expensive investment for laptops.
 - ▶ They typically consist of a platter, on which the laptop sits, containing fans and extra ventilation to carry heat away from the laptop.
 - ▶ Laptops have a tendency to overheat quickly, especially around the battery.
 - ▶ If the operating environment tends to be hot, a cooling device is a worthwhile investment.

- **Cleaning Materials**
 - ▶ As with desktops, laptops are especially vulnerable to dust collection.
 - ▶ Once a month, clean the keyboard and inside the laptop with a canister of compressed air.
 - ▶ LCD screens should be wiped off regularly with either a damp cloth or some LCD-specific cleaning material. **Never use Windex or other glass cleaners for this purpose.**

- **Operating Environment**
 - ▶ Optimally, all computer devices should be used in a “clean” environment: one free of dust and with sufficient climate control.
 - ▶ This can’t always be the case, so ensure that laptop ventilation is clear and temperatures remain within operating norms.

- **Storage, Transportation and Shipping**
 - ▶ While not in use, laptops should be kept in a hardened case, at best, or shut down with the screen closed, at least.
 - ▶ Always use a hardened case when transporting the laptop to and from operating environments, and keep peripherals and detachable devices in provided pockets and pouches.
 - ▶ When shipping a laptop, get an appropriate-sized box and use packing materials such as Styrofoam, air pockets, etc.
 - ▶ **Always buy shipping insurance!** A \$75 - \$200 investment is much less than the cost of the laptop itself.

Printers and Scanners

Fundamental Principles

The following section details the fundamental principles of printer and scanner operation, installation, and troubleshooting.

Printer and Scanner Technologies

As with computers, there are several different types of printers. That being said, most printers share certain components. For instance, some printers utilize **memory modules** to handle printer queues. Printer **drivers** allow the computer to communicate with the printer. **Firmware** is the hard-coded operating environment printers use internally for printing, queue management and other features. Keeping a printer's firmware up-to-date is a very important part of printer maintenance. Printer-specific consumables are discussed below.

- **Laser Printers**
 - ▶ Extremely fast, usually very expensive printers.
 - ▶ Utilize electrically-sensitive **toner** and photosensitive **print drums** to quickly imprint an entire page at one time.

- **Inkjet Printers**
 - ▶ Slower than laser printers and significantly less expensive.
 - ▶ Inkjets have print heads attached to nozzles that draw from liquid **ink cartridges** of various colors.
 - ▶ Most inkjets have one cartridge for color ink (containing cyan, yellow and magenta inks) and one for black.
 - ▶ Some specialty inkjet printers have different configurations.

- **Impact Printers**
 - ▶ Also called *dot matrix printers*.
 - ▶ Use a **solenoid** covered print head to strike a **print ribbon** covered in ink onto paper.
 - ▶ Dot matrix printers are not in wide use anymore – they are difficult and expensive to maintain and can typically only print text and very primitive graphics.

- **Solid Ink**
 - ▶ Uses wax-like sticks of CMYK ink, melted and fed into a piezoelectric print head.
 - ▶ The print head sprays melted ink onto a metal drum that “rolls” the image onto paper.
 - ▶ As expensive as laser printers but good for printing on non-porous materials.

- **Thermal Printer**
 - ▶ Consists of four key components:
 - The **thermal head**, for heat generation and actual printing;
 - The **platen**, which is a rubber roller that feeds the paper;
 - The **spring**, which presses the head against the paper;
 - And **controller boards**, which control the printer mechanism.
 - ▶ Thermo-sensitive paper passes through the platen and under the thermal head.
 - ▶ Heat from the head generates black (and red in two-color direct thermal printers) on the paper where it touches.

Connections and Cables

- **Parallel**
 - ▶ Utilize a male DB-25 pin connector on the computer and a male 36-pin Centronics cable at the printer end.
 - ▶ Most cables will be no more than ten feet, to reduce electronic interference along the cable.
 - ▶ The cable itself is a flat ribbon cable, allowing the transmission of up to 8 bits simultaneously.
- **Serial**
 - ▶ Uses either a 9-pin or 25-pin connector and a cylindrical cable much less susceptible to interference.
 - ▶ Can be up to 25 feet long.
 - ▶ Transfers one bit at a time across the cable.
- **SCSI**
 - ▶ SCSI is a serial communications standard that, in and of itself, has undergone *many* revisions and changes. For more information about specific SCSI standards, please see the **SCSI** section in **Domain 1**.
 - ▶ Generally, a SCSI printer cable will appear like the parallel cable, above.
 - ▶ Faster than either parallel or serial, SCSI allows users to attach many devices in one long "SCSI chain."
- **USB**
 - ▶ Printers and scanners using USB are the most common in-home use.
 - ▶ USB presents faster transfer speeds than serial or parallel.
 - ▶ USB devices are hot-pluggable.

- **FireWire/IEEE 1394**
 - ▶ Another new connection protocol replacing serial and parallel connections.
 - ▶ A faster version of serial that transmits between 50 and 400 Mbps.
 - ▶ Also hot-pluggable, like USB.

- **Network**
 - ▶ Networked printers are common in office environments.
 - ▶ Allows several users to share one printer as a network resource, like storage devices.
 - ▶ Networked printers can connect via either their own native NIC or through a print server, both using Cat-5 cables.
 - ▶ All networked printers utilize either TCP/IP or Telnet to transfer information.

- **Wireless**
 - ▶ Several wireless standards have also been developed for printers.
 - ▶ Bluetooth uses short-range radio transmissions to transmit data.
 - ▶ 802.11 is the same standard as wireless Ethernet and will “act” like a networked printer.
 - ▶ Infrared uses line-of-sight, reflective or scatter infrared technologies to transmit data; technology works similar to television remote controls.

Installation, Configuration and Optimization

Modern printers have a great deal of options available to users for various purposes. It is important for a technician to understand these options and when they are appropriate. Review and consider the following steps for installing, configuring and optimizing printers:

1) Power and Connect

- Connect printer to power adapter and adapter to wall outlet.
- Connect the proper input/output to printer and computer.
 - ▶ If the printer is connected locally, distinguish between the above discussed connection types (USB, FireWire, Serial, etc.).
 - ▶ If the printer is connected via a network port, ensure that Cat-5 is connected to print server or printer NIC.

2) Install, Update and Calibrate

- Computer should either automatically install necessary drivers or prompt for a driver disk. Provide the driver disk if required.
- Refer to the printer manufacturer's website for any driver or firmware updates.
- Calibrate the printer device by following the onscreen instructions mandated by the printer software.

3) Configure Options and Default Settings

- Navigate to: **Start > Control Panel > Printers and Scanners.**
- **Right click** the appropriate printer and click **Properties.**
- Evaluate how the printer will be used and adjust settings accordingly.
 - Duplex and two-sided printing.
 - Color and gray-scaled printing.
 - Paper types, sizes and orientation.
 - Printer tray switching to optimize paper output efficiently.
- Configure **Spool Settings.**
 - Navigate to Start.
- Take note of media inputs, such as SmartCards, Flash Media, etc. if available.

4) Print a Test Page

- Navigate to: **Start > Control Panel > Printers and Scanners.**
- **Right click** the appropriate printer, and click **Properties.**
- Click **Print A Test Page.**
- Printing a test page will ensure that all of the above steps have been completed successfully.
- Modern printers can automatically detect problems with calibration and color printing with a test page.

Printer Troubleshooting and Diagnostics

Invariably, printers will encounter problems and require troubleshooting and diagnostics. Often, technicians may find themselves working with printers more than computers, as printers have many moving and replaceable parts. The following section discusses the best practices for diagnosing and troubleshooting printer and scanner problems.

Gathering Information

- **Identify the symptom.** Determine whether or not the problem is physical (i.e., paper jams, empty ink cartridges, etc.) or software related (i.e., out of date or corrupted drivers, printer spool errors, etc.).
- **Review error codes.** Depending on the nature of the problem, the computer or the device may generate an error code. These are non-standardized, so refer to the device's manual for specific error code meanings. An event log can reveal any computer-related software errors, and refer to any reports filed by the user.
- **Print or Scan Test Page.** Specific information about device calibration can be gained from a test page. Alternatively, if the test page doesn't print, the problem is likely with the computer.
- **Use Diagnostic Utilities.**

Review and Analyze Data

- **Establish Probable Cause.** Use common sense to determine what could be causing the symptoms identified above. For instance, on an ink jet printer, spotty production is probably low or empty ink cartridges. Blank pages from a laser printer more than likely denote an empty toner cartridge.
- **Review Service Documentation.** Manuals can be the best source of information for problem solving. Device-specific error codes are usually found in manuals.
- **Define and Isolate Problem.** Use Internet resources such as knowledge bases and tech support forums to further isolate the problem. Verify that the problem is software related or hardware related, that proper connectivity is established and that physical impedances, such as paper jams, are cleared.

Identifying Solutions

- **Define the Specific Cause** and apply any necessary fixes, such as driver or firmware updates.
- **Replace Consumables**, if necessary. Refer to the printer's manual for instructions on how to replace ink and toner cartridges.
- **Verify Functionality** with a test page/scan. It's important to also get the user to accept that the problem is fixed, and the device is operational as per the user's expectations.

Domain 2: Troubleshooting, Repair, and Maintenance

Troubleshooting Theory

A computer technician is very much like a detective. Root causes of computer problems tend to be difficult to discern at first glance. Therefore, it is important for technicians to understand the basics of troubleshooting theory when diagnosing a problem:

1. **Make Backups.** It is extremely important to always backup important work and create operating system restore points, preferably on removable media, before doing any troubleshooting.
2. **Take a systematic approach.** Most problems will not be easy to define outright. Attack problems logically and divide the problem into smaller parts for analysis. Sometimes, it's easier to treat the symptoms before treating the disease.
3. **Never make assumptions.** Reconnecting a PC to a network may not be as simple as replacing a bad NIC; lagging computer speed may not necessarily be caused by a fragmented hard drive. Verify even the most obvious problems.
4. **Research.** Much of a technician's time is spent searching the Internet. That's ok! The Internet is an excellent source of information, and the problem may have already been solved by a technician.
5. **Make priorities.** Research and solve the largest problems first. Problems which reduce productivity the most will generally be the problems that get top priority.
6. **Document everything.** Keeping a well stocked service journal serves two important purposes. First, the journal will serve as a "trail of breadcrumbs," allowing the technician to backtrack through steps if something goes wrong in the troubleshooting process. Second, if the technician (or other technicians, if this is an online journal) encounters the problem again, it can be easily solved with documented steps.

Techniques and Procedures

In general, troubleshooting a problem comes down to five basic steps: **Identify, Analyze, Test, Evaluate,** and **Document.**

- **Identify.** Question the user thoroughly regarding the problem. Ask: What changes have you made to the computer recently? Have you added new hardware or software? What were you doing when the error occurred?
- **Analyze.** Rely on experience, observation and information gleaned from the user to analyze the problem. Consider potential causes, and determine, ultimately, whether the problem is hardware or software in nature.
- **Test.** Based on the analysis, test related components and software. Check driver installs, connections to power and motherboard, software configurations, jumper settings, etc.
- **Evaluate.** Carefully examine the results of testing. Consult user manuals, the Internet or even technical support lines if necessary.
- **Document.** Write down actions and the results of those actions. If the problem was solved, post the troubleshooting techniques used on the Internet, where other technicians can access them.

Problems and Issues

The following sections will discuss some common problems with computer devices and components, the probable causes of these problems, and some suggestions on how they might be solved.

Display Issues

- Check both the power and connection cabling, and ensure that everything is fully plugged in to the appropriate outlet/connection.
- Make sure the video card is properly seated in the appropriate slot and that the correct drivers are installed.
- If the motherboard uses integrated video and the monitor is attached to an expansion video card, the integrated video may need to be disabled in BIOS.
- Does the computer produce beep codes on boot? Refer to the following table for some common BIOS beep codes related to video errors.

| Beep Code | Meaning |
|---|-------------------------------|
| <i>AMI BIOS</i> | |
| 8 Beeps | Video Memory Error |
| <i>Award BIOS</i> | |
| 1 Long, 2 Short | Video Adapter Failure |
| 1 Long, 3 Short | Video Memory Failure |
| <i>Phoenix BIOS (dashes indicate a pause)</i> | |
| 3 – 3 – 4 | Video Memory Failure |
| 3 – 4 – 1 | Video Initialization Failure |
| 9 – 2 – 1 | Video Adapter Incompatibility |

Figure 12: Motherboard beep codes

- If the computer doesn't recognize the monitor, make sure the proper drivers are installed.
- If the picture is unclear or unstable, try adjusting brightness, contrast and vertical hold to maintain an accurate picture.

Storage Devices

- Run scandisk and defragment on hard disks. A deep scan with scandisk can indicate any physical failures with a hard disk. Defragmenting can improve access speeds.
- Listen to the sound of the drive – clicking, buzzing or excess vibrations indicate some sort of physical failure with the drive.
- Ensure that internal storage devices are connected to the power supply and the appropriate motherboard connection (IDE, SATA, SCSI, etc.).

- Ensure that external storage devices have power and are connected to the proper connection (USB, FireWire, etc.).
- And, of course, make sure any necessary drivers are installed and the storage devices have been updated with the latest firmware.

Memory

- The symptoms of memory problems can be extremely varied. If bad memory is suspected, a hardware or software memory tester can accurately diagnose it.
- Older RAM modules will require installed modules to be in matched sets. If this is true for the computer, ensure that the modules are the same speed and size, and are installed in the correct slot.
- Make sure modules are properly seated.
- Listen for BIOS Beep Codes. Below, The following table lists some BIOS beep codes for memory failures.

| Beep Code | Meaning |
|---|-------------------------|
| <i>AMI BIOS</i> | |
| 1 Beep | Memory Refresh Failure |
| 2 Beeps | Memory Parity Error |
| 3 Beeps | Base 64k Memory Failure |
| <i>Award BIOS</i> | |
| Endlessly Repeating Beeps | Memory Error |
| <i>Phoenix BIOS (dashes indicate a pause)</i> | |
| 1 – 3 – 1 | Memory Refresh Failure |
| 1 – 3 – 2 | Base 64k Memory Failure |
| 1 – 4 – 2 | Parity Error |
| 4 – 3 – 1 | RAM Test Failure |

Figure 13: More motherboard beep codes

Input Devices

- Make sure keyboard and mouse ports are firmly connected and to the proper connection, (i.e. USB, PS/2).
- A mechanical mouse may act erratically if the trackball or its sensors are dirty.
 - ▶ Unscrew the small panel on the underside of the mouse, by twisting it in the direction of the arrows.
 - ▶ Remove the trackball from its seating and clean with a damp paper cloth.
 - ▶ Clean the sensors off with a Q-Tip - lightly wet with alcohol.

- Optical and laser mice will also act erratically if the sensor glass is not clean. Wipe *gently* with a Q-Tip to clean.
- If the mouse continues to act erratically, the problem may be with the driver. Uninstall and reinstall the driver.
- Food, debris and liquids will cause a keyboard to misbehave. Keep food and drink away from the keyboard, if possible. Use compressed air to blow out a dirty keyboard.
- As with mice, if cleaning the keyboard doesn't solve the problem, try uninstalling and reinstalling the drivers.

Thermal Issues

- Computers, ideally, operate at the coolest possible temperatures. Therefore, it is important to ensure that the system is not overheating.
- Heat issues can cause the computer to act unpredictably.
- Make sure case and CPU fans are operational and spinning at their designed RPMs.
- Ensure that ventilation is clear inside of the computer.
- If the above fails to rectify the problem, try installing more fans, if there is space, or upgrading to a liquid cooling system if the problem becomes terminal.

Power Issues

- If the computer begins to reboot over and over again, the computer may be drawing too much power.
- First, start disconnecting unnecessary peripherals, such as non-boot hard disks, extra optical drives, USB and Sound Card expansions.
- If the computer stops rebooting endlessly, then the computer is overdrawing power.
- The power supply may be going bad. If this is the case, replace the unit.
- If the power supply is a known good device, the peripherals in the system are simply more than that wattage power supply can take. Consider upgrading to a higher wattage supply.

Preventative Maintenance

Preventative Maintenance Theory

Computers, being as complex as they are and constantly exposed to forces such as heat and electricity which degrade their effectiveness, require preventative maintenance. Preventative maintenance is, simply, the practice of maintaining a computer *before a problem starts*.

- **Visual and Auditory Inspections.** Examine airflow out of the computer and clean dust when necessary. Wipe the monitor screen down with an appropriate cleaning solution. Make sure a running system *sounds* like it is supposed to.
- **Driver and Firmware Updates.** Most software, Windows included, can be set up to perform driver updates automatically. Check with the websites of component manufacturers for firmware updates.
- **Schedule Preventative Maintenance.** Windows can be scheduled to perform common tasks, such as scandisk, disk defragmentation, software updates and restore points.

- **Use Appropriate Tools and Materials.** Refer to user manuals for the best way to clean monitors, keyboards, etc. A can of compressed air is the best tool for cleaning dust from computer components. Repair tools should consist of a Philips head screwdriver, a parts retriever (sometimes referred to as a “nose picker”), an anti-static wrist strap and, in some cases, soldering tools.
- **Ensure a Proper Environment.** Check fan outputs and ensure the computer is in a place receiving proper ventilation. Make sure the temperature stays relatively even and that any sensitive electrical equipment is nowhere near liquids or flammables. Keep cables and cords properly managed and away from high-traffic areas.

Some Additional Notes on Preventative Maintenance

Wireless mice and keyboards are becoming much more common in personal computing environments, and battery replacements for these devices will need to be made relatively often. They will, generally, come in two forms:

- **900MHz** – Similar to the technology used in cordless phones.
 - ▶ A signal receiver, connected by USB, receives input from the device itself.
 - ▶ More affordable than Bluetooth, but typically prone to electronic noise and interference.
 - ▶ These can also interfere with wireless networks, since wireless networks work off of the same technology.
- **Bluetooth** – Short-range, low-power radio communications.
 - ▶ More expensive than 900MHz devices and not necessarily widely in use yet.
 - ▶ Bluetooth suffers less from electronic interference than 900MHz and does not interfere with wireless networks.



Figure 14: Bluetooth headset

Consult user manuals for these devices for recommendations on the best type of battery for that device. Rechargeable batteries are usually the best option. Also, keep liquids and food away from keyboards and mice. Food particles tend to get stuck under and between keys and liquids can short out a keyboard entirely.

Domain 3: Operating Systems and Software

Unless otherwise noted, this section will deal almost exclusively with Windows 2000, Windows XP Professional, XP Home, XP Media Center Edition, Windows Vista Home, Home Premium, Business, and Ultimate, and Windows 7 Home Premium, Professional and Ultimate.

Fundamental Principles

The primary purposes of any operating system are to manage hardware usage, software applications and all of the related files and file structures associated with operating a computer. That being said, there are currently three different operating systems which have preeminence over the operating system market:

- **Apple Macintosh OS X** - now in version 10.6 (Snow Leopard), is the premier Macintosh OS. The system is based on FreeBSD UNIX and is generally considered more secure than previous Mac OS versions.
- **Microsoft Windows** - the most popular operating system, and will likely be encountered the most by technicians. Depending on the application, Windows currently has several concurrent versions:
 - ▶ **Windows XP Home** – Stripped down version of Windows marketed to home users.
 - ▶ **Windows XP Professional** – A more secure and robust version of Windows marketed to businesses.
 - ▶ **Windows 2000 and 2003 Server** – Both operating systems are in wide use today, though 2003 Server is intended as a replacement. Operating System supports extra features for server management and implementation.
 - ▶ **Windows XP Media Center** – Another home-PC version of Windows with a modified graphic user interface built for viewing on televisions, accessing surround sound systems, etc.
 - ▶ **Windows Vista** – The operating system that was released after Windows XP, targeted for home, home office, and business users. Vista had a shaky rollout that failed in large part due to poor synchronization between Microsoft and third-party device driver manufacturers. However, after initial problems subsided and Windows Service Pack 1 was released, Vista was regarded as a very secure system and was more widely accepted. The security was provided in large part to the User Account Control (UAC) module in which even administrators operated under standard user account permissions. Many users never moved from Windows XP to Vista though, although they are readily and quickly moving to Windows 7.
 - ▶ **Windows 7** – The newest operating system available from Microsoft, targeted at both home and business users, and offering several unique editions. It is, by far, the most popular edition of Windows ever offered by Microsoft. It is commonly regarded as secure, easy to use, and easy to incorporate into homes and businesses and their existing infrastructures. Windows 7 still incorporates UAC, but also offers key performance improvements such as better memory use, new search features, and better sleep and resume features; improved device management including a new Device Stage feature where users can manage all of their devices in a single place; and the Action Center, which offers solutions unique to the computer that include updated drivers, bug fixes, and troubleshooting options.

- **Linux** – another Unix-based operating system, though more heavily so than Mac OS X. Linux is unique in this group, as it is distributed freely, albeit without support. Linux's **General Public License (GPL)** allows the software kernel to be freely distributed to software developers. As a result, there are a wide variety of Linux **distributions**, or Linux OS packages.

Essential Components

- **File System** - the operating system's way of managing stored files in an organized, accessible way. As there are many different operating systems, and many different methods for storage, there are also many different file systems:
 - ▶ **Windows** - uses FAT32 and NTFS exclusively.
 - ▶ **Macintosh** - uses HFS and HFS+.
 - ▶ **Linux** - uses EXT, XFS and several other systems developed by small, independent developers.
- **Registry** - a database of configuration settings used by Windows operating systems which keeps track of every hardware, software and core system setting and option. The Registry is broken into 5 components:
 - ▶ **HKEY_CLASSES_ROOT** - Stores information about registered applications, file extension associations and OLE object class IDs.
 - ▶ **HKEY_CURRENT_USER** - Stores the settings specific to the logged-on user.
 - ▶ **HKEY_LOCAL_MACHINE** - Stores the general settings of all a computer's users.
 - ▶ **HKEY_USERS** - Stores the settings and information for each individual user on the machine; used in concert with HKEY_CURRENT_USER, to load individualized settings.
 - ▶ **HKEY_CURRENT_CONFIG** - Stores information gathered during system runtime; not permanently stored.
- **Virtual Memory** - a section of a hard disk given over for the operating system to use as it would RAM modules. This memory is slower than system RAM but allows the operating system to perform application tasks quicker, leaving computation and processing tasks to the system RAM. Windows Vista and Windows 7 offer **ReadyBoost**, a feature that enables you to add virtual memory to a machine by connecting and configuring a compatible USB flash drive or memory card.

Operating System Interfaces

Windows is, by nature, a graphical user interface. Therefore, Windows has several interfaces used to access, configure and change operating system parameters. These are discussed, in detail, below:

- **Windows Explorer (Explorer)**
 - ▶ Every window opened in the Windows environment is, essentially, a Windows Explorer screen.

- ▶ The Explorer displays the current folder or path that is being viewed, all files within that path, and a list of accessible drives, folders and subfolders.
- ▶ Here are two examples of Explorer windows, the first from Windows XP, the second from Windows 7. What you see here will depend on how the user has configured his or her computer.

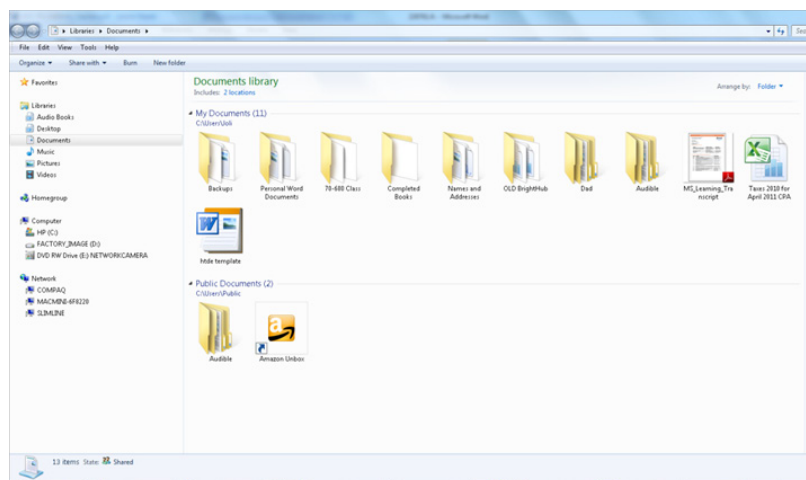
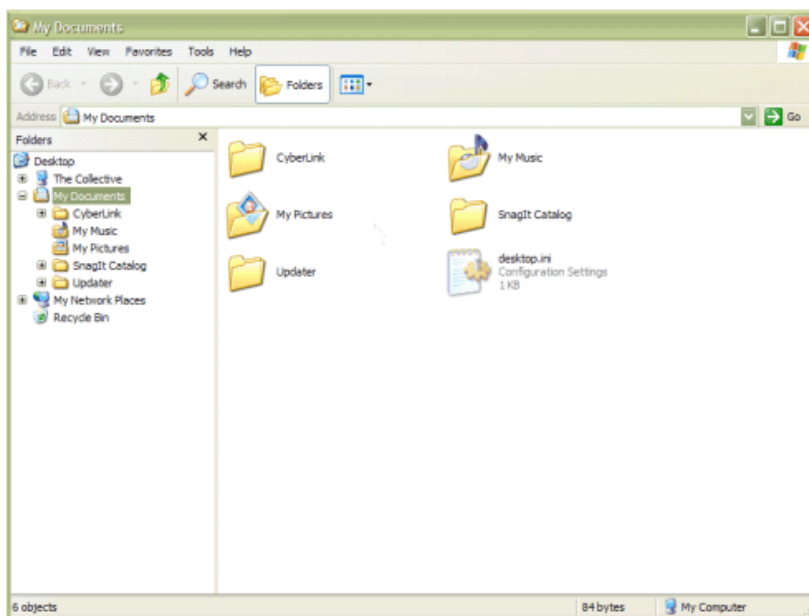


Figure 15: Windows Explorer

- **My Computer**

- ▶ This is simply a different Explorer screen which shows some different information.
- ▶ All of the main operating system functions, such as available drives, control panel, network connections and the recycle bin can be accessed from here.
- ▶ The first image shows the **My Computer** window on a Windows XP computer. The second shows the Computer window on a Windows 7 computer. What you see here will depend on how the computer is configured and the data stored on it.

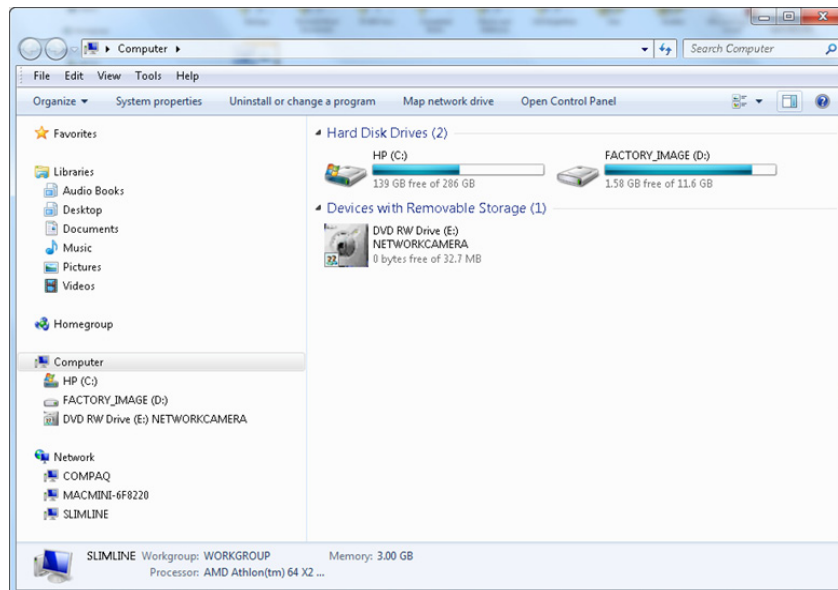
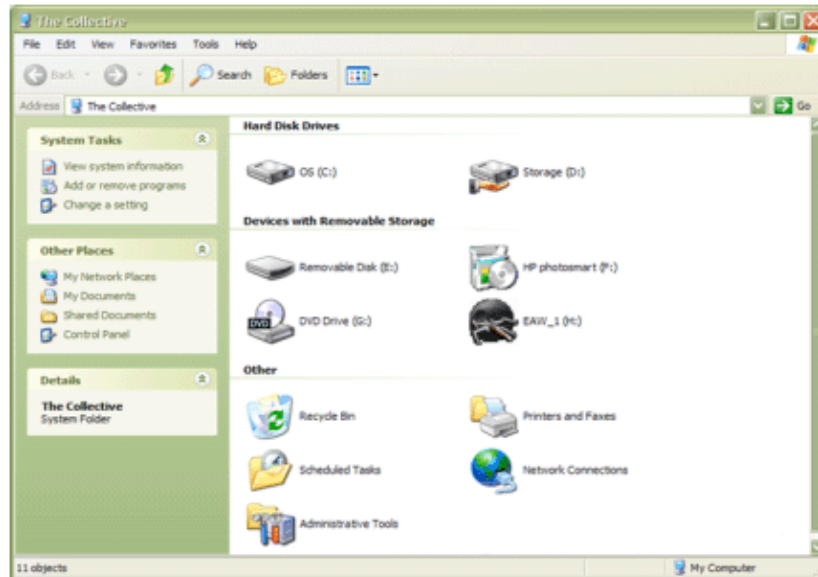


Figure 16: Windows XP and Windows 7

- **Control Panel**

- ▶ This interface allows the user to control basic system settings, such as hardware addition and removal, the uninstallation of programs, the management of user accounts; it offers easy access to network settings, homegroup, and sharing options; and enables a user to configure security settings, personalize the computer's appearance and personalization, and find and fix problems, among other things.
- ▶ Windows XP supports two versions: an **XP View**, and the **Classic View**.
- ▶ **XP View** is stripped down in an effort to prevent unwary users of accidentally reducing system productivity.
- ▶ **Classic View** appears much like the Explorer window, with icons leading to various system settings.

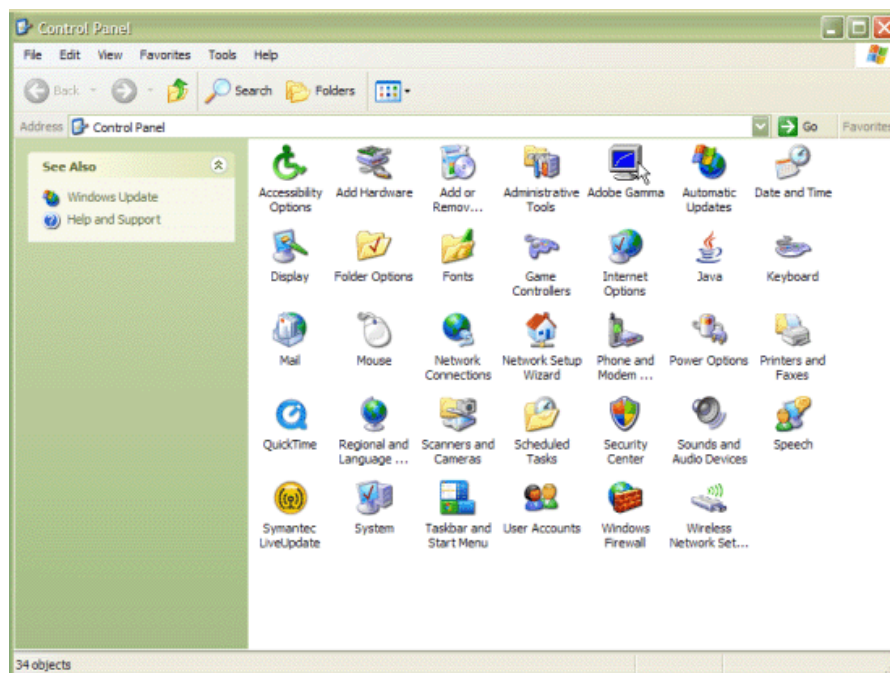


Figure 17: Control Panel

- ▶ Windows 7 supports two views: A **Category view** and an **Icons view** (Large or Small). When you click any option, a new window opens with configuration tools.



Figure 18

- **Command Prompt**

- ▶ In Windows XP, the command prompt is a re-creation of the DOS interface and can be accessed by navigating to **Start > Run**, and typing **cmd** in the prompt.
- ▶ This textual interface is useful for running troubleshooting and diagnostic commands for a variety of operating system functions.
- ▶ In Windows Vista and Windows 7, you can access a command prompt by typing **cmd** in the **Start Search** box. Many tasks require you to run the command prompt as an administrator though. To do this, right-click **cmd** and click **Run as Administrator**, shown here. You can then use the command prompt to perform DOS-like commands.

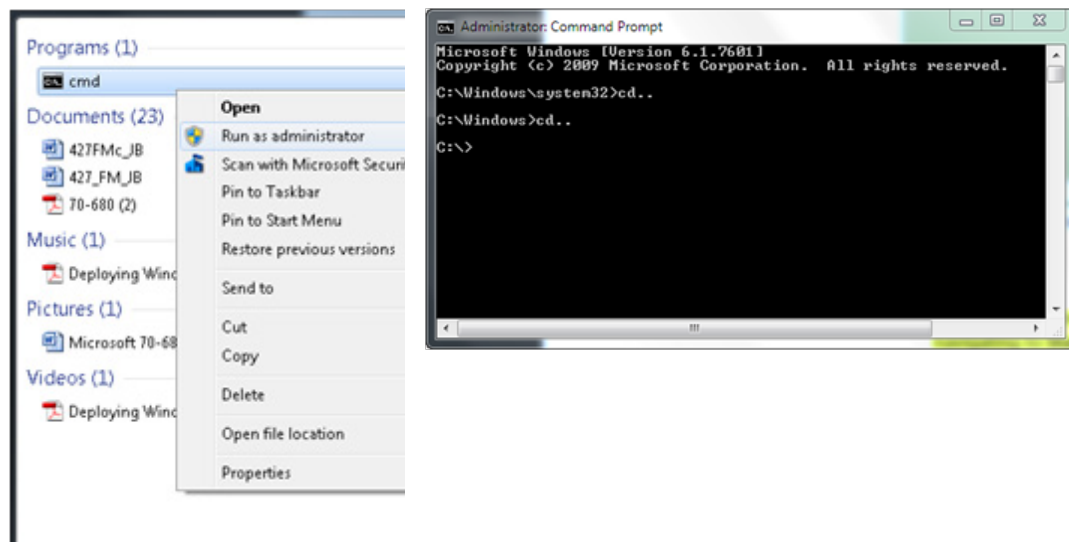


Figure 19

- **My Network Places and Network**

- ▶ **My Network Places** is used to access network resources allowed to the machine in Windows XP.
- ▶ Any shared drives, folders or printers, along with whatever computers that share your network, can be viewed and accessed here. In Windows Vista and Windows 7, **Network** is used to access available network resources, specifically computers on the network and shared media devices. Here you can see a sample Windows 7 Network window. (Open any computer listed to see the resources connected to it, including printers and other hardware.)

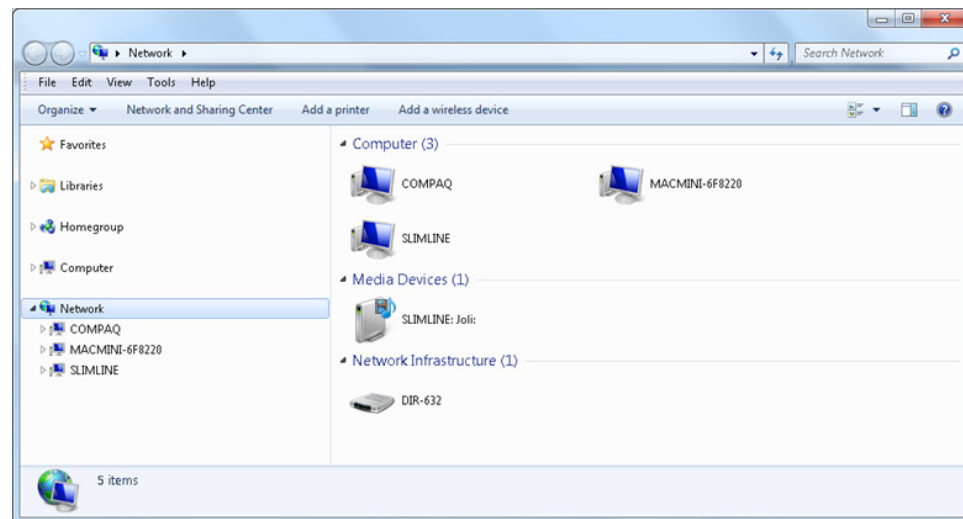


Figure 20: Control Panel

- **The Windows XP Taskbar**

- ▶ The taskbar, located at the bottom of the screen, is a representation of all the programs running in memory.
- ▶ The blocks running along the center of the screen are *active* programs, meaning that they are in use.
- ▶ The small icons to the right are those programs running *passively*, or in the background.
- ▶ Right clicking the small icons will give context menus, dependant on the running programs.



Figure 21: The Windows XP Taskbar

- **Windows Vista and Windows 7 Taskbars**

- ▶ Shows active, running programs in the middle of the **Taskbar** that were started by the user.
- ▶ Shows passive, running programs, required by the operating system, network, or configured by the user to run in the background all the time.
- ▶ Enables you to drag an item to the **Taskbar** to “pin” it there for easy access.



Figure 22: The Windows 7 Taskbar

- **Windows XP Start Menu**

- ▶ The **start menu** is the most ubiquitous feature of a Windows operating system.
- ▶ It provides access to every program installed on the machine, all of the above described interfaces, as well as personal and recently accessed documents and programs.



Figure 23: The Windows XP Luna Start menu

- **Windows Vista and Windows 7 Start Menu**

- ▶ Offers easy access to programs you use often, and enables you to drill into the **All Programs** menu to locate others.
- ▶ Offers a **Start Search** menu to easily find programs, documents, pictures, media, and other data.
- ▶ Offers easy access to **Sleep, Shut Down**, and similar commands.
- ▶ Is configurable and enables users to “pin” items, decide what to show and what not to, and more. What you see here depends on the user and computer.

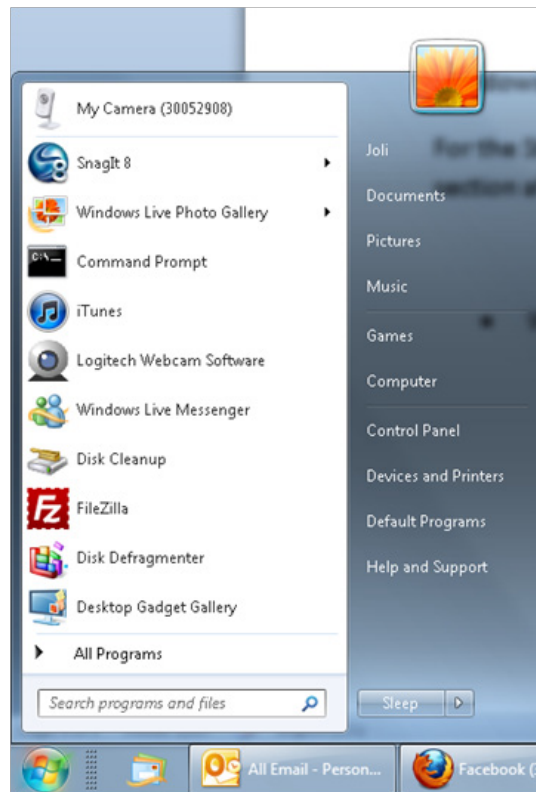


Figure 24: The Windows 7 Start menu

- **User Account Control (UAC)** - a security infrastructure introduced in Windows Vista and carried into Windows 7. Its chief advance over security in earlier Windows editions is that application software is limited to standard user privileges until an administrator explicitly authorizes the action.

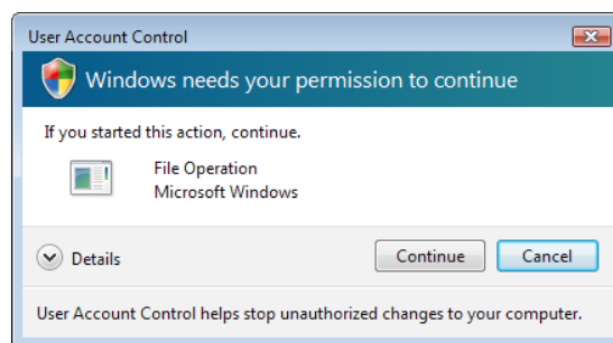


Figure 25: User Account Control in Windows Vista

- **Windows Aero Theme** - a graphically intensive user interface in most editions of Windows Vista and Windows 7. Although the Aero user interface is considered to be more interactive and aesthetically pleasing than the Luna interface that was used in Windows XP, the Aero user interface takes its toll in CPU and memory resources.

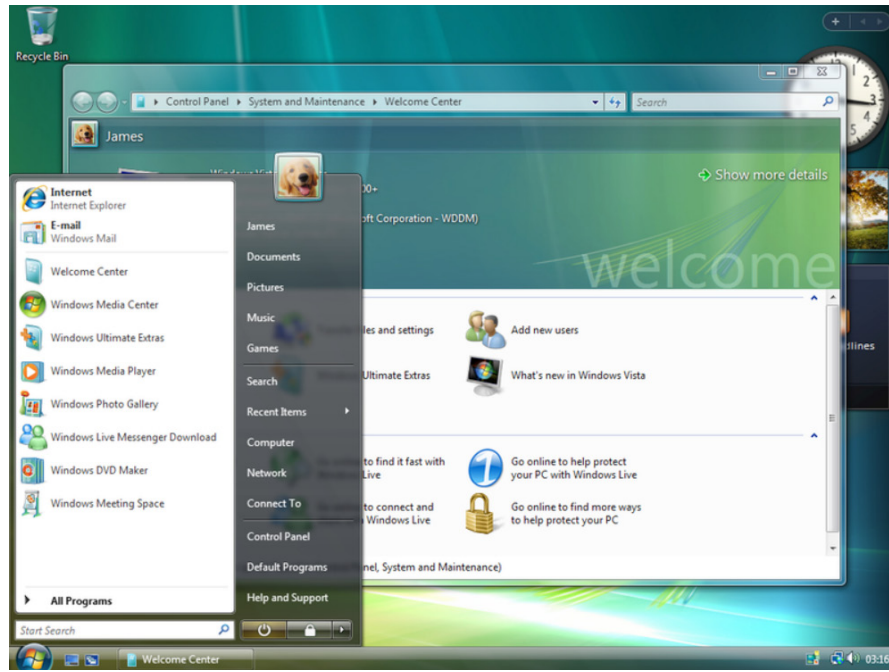


Figure 26: Aero Theme in Windows Vista

Operating System Files in Pre-Windows Vista Computers

The following section details essential operating system files, their characteristics, locations and purposes.

- **NTLDR**, or *NT Loader* - the basic system file used for the loading of the Windows NT kernel on NT-based operating systems. It is located in the %systemroot% folder and relies on both BOOT.INI and NTDETECT.COM (described below), to load the operating system.
- **BOOT.INI** - the configuration file used by NTLDR to load the operating system. It will also be located in the %systemroot% folder.
- **NTDETECT.COM** - used to detect and load the various hardware devices necessary for operating system function. It utilizes *Hardware Profiles* stored in the HKLM\HARDWARE\DESCRIPTION registry key and supports multiple profiles for machines that change hardware settings and layouts often.
- **NTBOOTDD.SYS** - an alternate loader file, used when the main disk is SCSI-based rather than IDE-based, and cannot be handled by the computer's BIOS firmware.
- **Registry data files** - discussed in more detail above, in the **Essential Components** section, are located in the %SystemRoot%\System32\Config\ folder.

Operating System Files in Windows Vista, Windows 7, and Windows Server 2008

When the computer is powered on, either the **BIOS** or the **EFI** is loaded. With BIOS, the **Master Boot Record** of the boot disk is accessed, followed by the boot sector of the appropriate hard disk partition. This boot sector then loads the rest of the boot blocks. The files that play a part in this process include:

- **Windows Boot Manager (BOOTMGR)** - reads the boot configuration data and displays an operating system menu (if applicable). In some respects, it can be compared to NTLDR in prior versions of Windows NT.
- **Boot Configuration Data (BCD)** – replaces the old boot.ini files that was used by NTLDR. It is used by the new **Windows Boot Manager**.
- **Winload.exe** - load the operating system kernel (ntoskrnl.exe) and required boot-related device drivers. This is also equivalent to the operating system loader function of NTLDR in prior versions of Windows NT.

In Windows 7 you can manage hard disks in the **Disk Management** window, available from **Administrative Tools**.

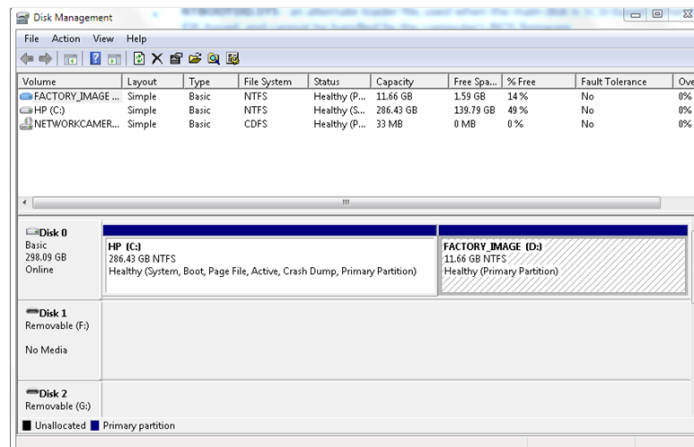


Figure 27: Disk Management

Disks, Directories and Files

- **Disks** – In general, this term refers to the hard disks used for storage on a computer. Available hard disks can be viewed either from **Windows Explorer** or the **My Computer** window. **Partitions** are logical separations on a hard disk. They are categorized as followed:
 - ▶ **Active** partitions are those partitions which can be actively booted to.
 - ▶ The **primary** partition is the partition on which the main operating system is stored, and *must* be assigned drive letter C: on Windows-based machines.
 - ▶ **Extended** partitions are those which carry any other disk space not assigned as primary.
 - ▶ **Logical** partitions are extra partitions made from the extended partition.

- **File Systems** – As previously discussed, a file system is the method by which the operating system manages and organizes files and data. The chief purpose of the system is to enable a level of file security and ease-of-access.
 - ▶ **FAT32**
 - A relatively uncomplicated file system which is still used in Home user editions of Windows XP.
 - Lack of complexity allows FAT32 to share data with disparate operating systems, making it an ideal file system for dual boot computers.
 - Unfortunately, FAT32 is limited by its maximum single file size of 4 GB and a maximum drive size of 32 GB.
 - ▶ **NTFS**
 - Long-running file system used by NT-based Windows operating systems.
 - Supports much larger drives and file sizes, as well as a host of security features, such as innate file encryption.
 - Utilizes hidden and inaccessible **metadata** files, which store all the information about every file on the system.
- **Directory Structures** – A directory is simply an organizational tool that is much like a hanging file folder in a file cabinet, only much more complicated. Directories on a computer can hold both files and other directories.
 - ▶ A directory, all of its subdirectories, and all of the files in these directories, is referred to as a **tree**.
 - ▶ In general, create a folder by **right clicking** on an empty space, choosing **New...** and selecting **Folder**.
 - ▶ Move and copy folders by dragging and dropping and using the copy/paste option, respectively.
 - ▶ The console can still be used to manage folders. Refer to the chart, *Figure 28* for a list of console directory management commands and their command-line switches:

| Command | Usage | Switches |
|---------|---|--|
| dir | Used to view files and subfolders in a folder | /w – Displays files in “wide” format. /a – Displays files with attributes listed. |
| cd | Used to change active directories | N/A |
| md | Used to make folders | N/A |
| copy | Copies files and directories | /V – Verifies written files. /Y – Prompts the user for overwrites. |
| rd | Removes and deletes folders. | /S – Removes the entire directory tree. |

Figure 28: Common Windows console commands

- **Files** – Files are the actual data stored on a computer, used either directly by the user, such as with a text file, or by an application, as with a jpeg picture file.
 - ▶ Files are created by the various applications used on a computer. For instance, this document is a file that was created by Microsoft Word.
 - ▶ Files are usually denoted by a unique name and an identifying **extension**.
 - The extension allows both the user and the operating system to recognize the file by type.
 - The operating system then creates **associations** between the extension and the appropriate application.
 - This allows the user to double click a required file and have the associated application open and display its contents.
 - ▶ Files are also given various **attributes**, which are special markers of identification for various operating system uses. The following is a list of the basic file attributes and their uses:
 - **Hidden** – File is normally hidden from the user but can be accessed, changed or deleted.
 - **Read-Only** – The file can only be accessed, not changed or deleted.
 - **Archive Ready** – The file is ready to be archived.
 - **Indexed** – Windows Indexing Service will index this file.
 - **Compressed** – File is compressed to save disk space.
 - **Encrypted** – File is encrypted to secure the contents of the data.
 - **System** – A special designation for Windows NT system files, which cannot be accessed, seen, changed or deleted. This is for system-stability issues.
 - ▶ **Permissions** allow a network administrator to rate files in terms of which types of users can access the files and what can be done to the files. For instance, files can be reserved for only the system administrator, for the “power users” or for everyone on the network.

Installation, Configuration and Upgrade

As Windows operating systems continue to develop, it will be necessary to know how to upgrade from one Windows installation to the next. It's important to understand your upgrade “paths” before attempting to install an operating system. Although you can upgrade from Windows XP to Windows Vista, and opt to keep all files and settings (and not format the hard drive), this is not possible when moving from Windows XP to Windows 7. There is no direct upgrade path. Windows offers several options for making the transition though, including the Windows Easy Transfer Wizard.

Installation on a Clean Machine

A clean install is an operating system installation on a disk without a previous operating system installation. There are several key concepts to consider when performing a clean Windows install:

- **Check Hardware Compatibility.** System requirements for the operating system will be printed on the software box, usually on the back or bottom panel. Installing the operating system on a computer that does not meet minimum system requirements will result in poor performance. You can also check compatibility from the installation media.
- **Choose an Installation Method.** More often than not, this will be from some sort of removal media, such as a DVD or CD-ROM. In larger businesses, installation may occur over the network. In this case, the computer will need network access to a shared distribution of Windows. After attaching to the network resource, installation proceeds as per the steps below.
- **Configure OS options.** Choose whether to perform the installation unattended (default options are chosen and the installation can proceed without human intervention), or attended, where options are chosen manually. Choose the appropriate file system for the installation. It is recommended to use NTFS on Windows XP Pro installs. Finally, determine how the network will be configured: is this a client or server computer? Will it need access to shared resources, or will it share resources?
- **Prepare disks for install.** Format the target disk or partition, and install the chosen file system. Start the installation itself, and follow the onscreen instructions. The first half of the installation will be a text-only interface, covering hard disk setup and file-system choice. Following this, setup will restart the machine and enter a GUI setup screen, where network options will be configured, device drivers installed and services initialized.
- **Configure and install necessary device drivers.** Not all hardware devices will have their drivers installed. Check the **Device Manager** for any device driver problems, and install drivers for devices where necessary.
- **Verify Installation.** Check to ensure installation proceeded correctly. Test applications, network configuration, etc. to ensure that everything is working properly.

Performing Upgrades

- Check to see if an upgrade path is possible. As noted, you can't perform an upgrade from Windows XP to Windows 7 (unless you upgrade Windows XP to Vista, and then Vista to Windows 7). Likewise, you can't perform cross-architecture upgrades, meaning, you can't upgrade a 64-bit Vista OS to a 32-bit Windows 7 OS. For more information, perform a search for Windows 7 Upgrade Paths.
- Consider using **Windows Easy Transfer** if the user wants to perform an upgrade but can't. Allow a lot of time for this though, and clean the machine of unwanted data prior to starting to shorten the process and avoid bogging down the newly upgraded machine.
- As with a clean installation, **check hardware compatibility**. Also, ensure that previously installed third-party software applications are compatible with the upgrade and that the computer's current network configuration is also compatible. You can check compatibility from the installation media.
- Before any upgrade, backup important data, preferably on removable media. Load the upgrade CD into the drive, and follow the onscreen instructions. When installation is complete, perform the same verification check described in the section for a clean install, above.
- If prompted to go online to check for updates during the installation process, do.

Loading Device Drivers

With newer operating systems, specifically Windows 7, Windows Vista, and Windows 2008 Server, driver installation will almost always be seamless. Windows comes with a very large driver library, and almost all hardware is recognized and drivers installed, with no additional input from you or the user. However, in some instances drivers won't be found, and in these cases, you'll have to look for and install them manually.

Installing Drivers on a Windows 7 Computer

- Windows 7 comes with a feature called **The Action Center**. You can access it in various ways, but the easiest is to click the flag icon on the **Taskbar**, in the Notification area and click **Open Action Center**.



- Once in the Action Center, note if there are any drivers or driver updates available. If so, install them. You can also click Windows Program Compatibility Troubleshooter, to configure older programs to run in a compatibility mode, if applicable.

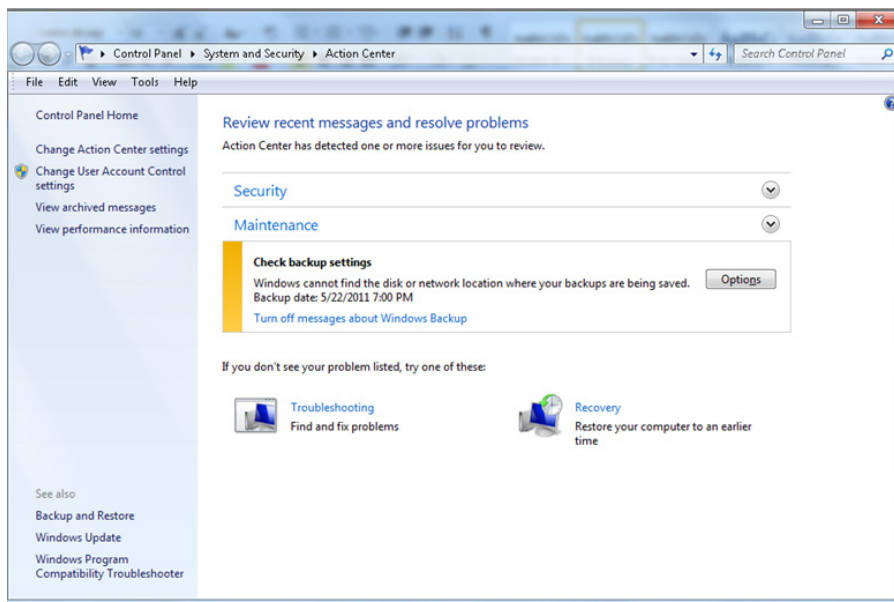


Figure 29

- If this doesn't work, open **Control Panel** and under Hardware and Sound in **Category view**, click **Add** a device. Work through the wizard to add the device to the computer, and install its driver.

Installing Drivers on a Windows Vista Computer

- To install new hardware on a Windows Vista machine, click Start, click Control Panel, and click Hardware and Sound. You'll see various options to add printers, sound devices, and other hardware. Work through the wizards as applicable. What you'll see here depends on the device you want to add.

Installing Drivers on a Windows XP Computer

If you must install drivers manually on a Windows XP machine because the hardware is old and no driver is automatically installed:

- First and foremost, ensure that the user account has permission to actually perform the task. If not, contact the system administrator to gain this permission.
- Check the device manager for the specific driver issue. Is the hardware being recognized by the computer? If so, then it may be possible to perform an automated driver install. Navigate to **Start > Control Panel > Add Hardware**. The **Add Hardware Wizard** appears.



Figure 30: Add Hardware Wizard

- Click **Next**. Windows will search for the hardware to be added. If the system does recognize the hardware and possesses the driver files, it will automatically install the necessary files, and the hardware will be ready for use.
- If Windows does not recognize the hardware, the following screen appears. It will be necessary to perform a manual driver install.

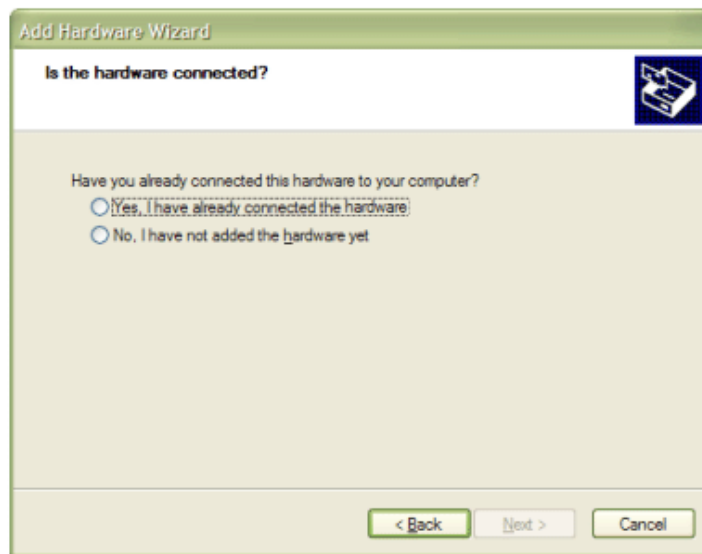


Figure 31: Add Hardware Wizard

- Mark that the hardware is connected and click **Next**. The next screen presents the user with a list of possible devices. Scroll to the bottom, and choose “Add a new hardware device.”
- From here, the user can choose to have the system search through available resources for the driver for the device. If Windows can find the files, either on its own system, or on the Internet, it will automatically install the files, and the hardware will be ready for use.
- If the user chooses to manually search for and install the file, the following screen, *Figure 32*, comes up, prompting the user to choose a device from the list:

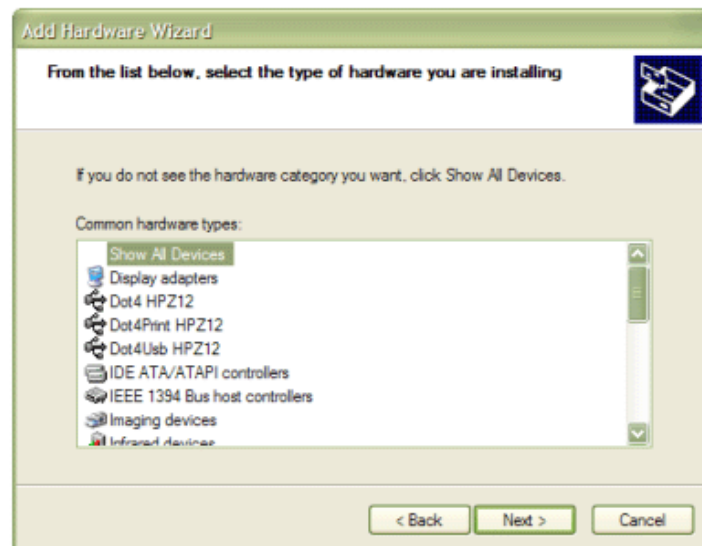


Figure 32: Add Hardware Wizard

- Select the appropriate category, or if the category desired is not listed, choose “Show all devices.” Click **Next**.
- Choose the appropriate device from the list, and then, click **Next**. At this point, the user will need to either provide a driver diskette, or manually point Windows to a drive path or file location for the specific device.
- After the driver is installed, verify functionality, by viewing the **Device Manager**, for any driver conflicts. Ensure the device itself is also in proper working order.

Operating System Optimization

Windows includes several features which help to optimize the operating system’s performance. These features are discussed below:

- **Virtual Memory** - the term used for a special file on the hard drive, called a **swap** or **paging** file, which the CPU uses to offload main memory information.
 - Virtual memory can be lowered or increased, according to preference, though the rule is that the page file should be about 2.5 times system RAM. Follow the steps below to change paging file size:
 1. Right click **My Computer** and choose **Properties**.
 2. Click the Advanced tab.

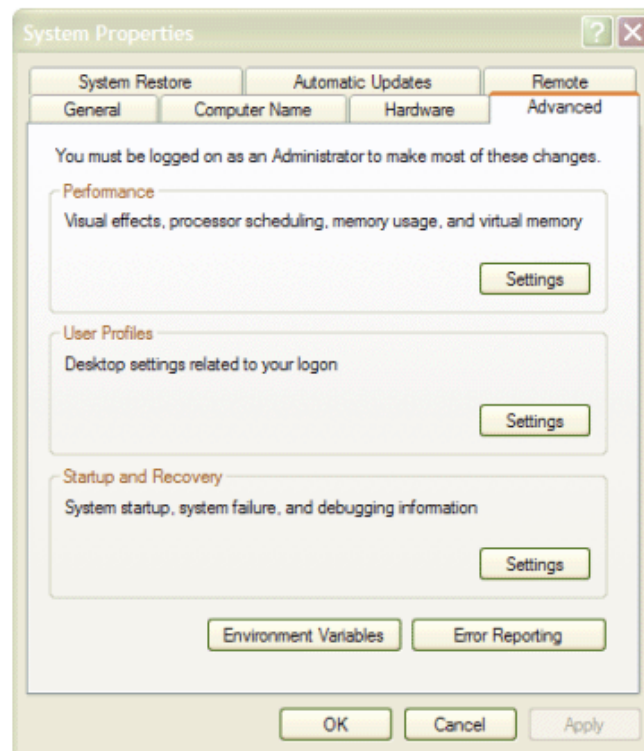


Figure 33: Accessing virtual memory and performance options

3. In the first box, Performance, choose **Settings**, and then, click the **Advanced** tab (Figure 34).

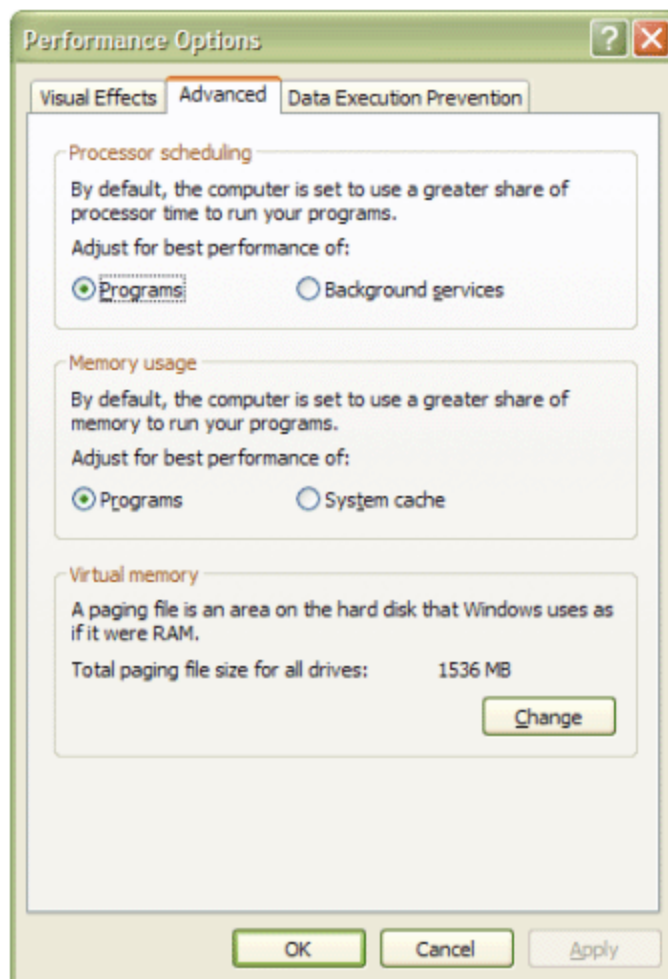


Figure 34: Customizing virtual memory and performance options

4. In the last box, **Virtual Memory**, click the **Change** button (Figure 35).

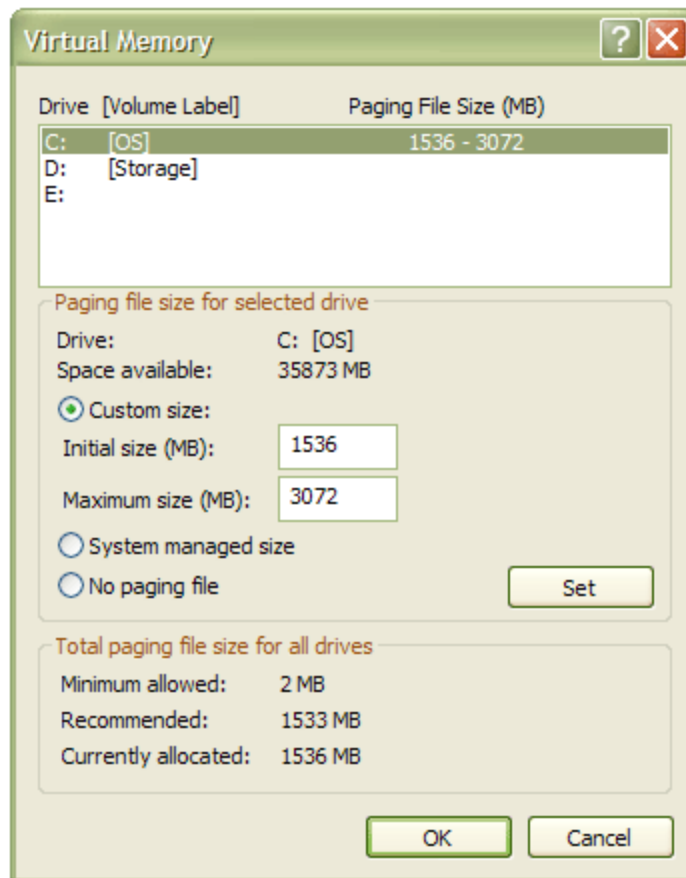


Figure 35: Virtual Memory dialog box

5. From here, change virtual memory settings according to preference.
 - User can choose which disk to save the page file.
 - User can choose between a system-managed page file and a custom-sized page file. Again, page file should be no more than 2.5 times system RAM.
6. In Windows 7, click Start, right click Computer, and click Properties. Then, click Advanced System Settings to access this screen.

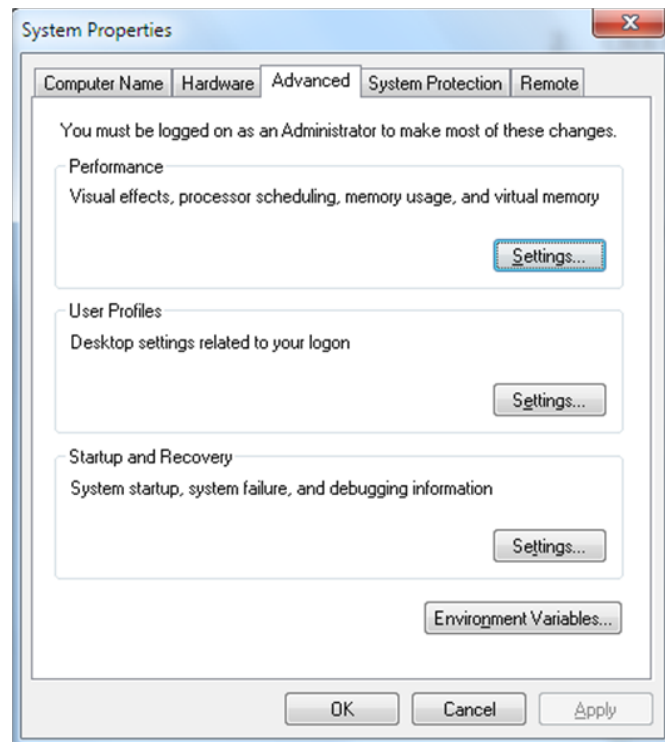


Figure 36

- **Hard Drives** - can be optimized by keeping fragmentation in check.
 - The Windows defragmenter can be run whenever the user deems necessary.
 - It is appropriate to run the defragmenter at least once a week, on heavily used computers.
 - This feature can be setup to perform automatically by navigating to **Start > Accessories > System Tools > Scheduled Tasks**. Schedule tasks by day and time. Defragmentation should be done during a computer's usual downtime.

- **Temporary files** - should be cleaned often, as well.
 - Often temporary install files, cookies and cached web pages can take up large amounts of space, quickly.
 - To manage the amount of disk space devoted to internet temporary files, refer to the configuration options for the specific browser.
 - Additionally, there are many third party drive cleaners which quickly and easily clear a system of temporary files.

- Unused **services** should be terminated, and the associated software should be uninstalled. Services can be terminated by accessing the task manager through **CTRL+ALT+DEL**. Click the **Processes** tab, and select the appropriate service; then, click **Terminate**.
- Some applications, when installed, are configured to run on startup. This can create unreasonably-long boot times. Check that only the most essential programs, such as virus protection and firewalls, are loaded at startup. Any other software can be loaded manually or, if used often, can be added to the quick launch bar, between the Start button and the task bar.

Diagnostic and Troubleshooting Procedures

Boot Methods and Sequences

In order to properly troubleshoot computer problems, Windows has several boot methods that provide different configurations.

- **Safe Mode** - a stripped Windows boot that only has the most necessary drivers and services loaded for Windows operating. This is useful to determine if the problem is hardware or software in nature. Safe mode itself has several options:
 - ▶ **Safe Mode with Command Prompt.** This option boots safe mode but uses the command console, instead of the GUI.
 - ▶ **Safe Mode with Networking.** This allows the user to access network resources for troubleshooting, such as uncorrupted restore files or Internet access for research.
 - ▶ **Last Known Good Configuration.** This option boots into Windows normally, but with the last known hardware configuration that worked with Windows. This is useful for determining if recently added or changed hardware devices are causing malfunctions.
- **Recovery Console** - allows system administrators to perform a limited range of repair tasks using a text interface similar to the command console. The recovery console can be accessed by booting from the Windows (2000 or XP) CD-ROM and choosing the recovery console option, **R**, when prompted. The Recovery Console can be accessed on a Windows 7 computer by pressing **F8** during boot up, and clicking **Repair** your computer. From within the console, administrators can:
 - ▶ create and remove directories, and copy, erase, display, and rename files;
 - ▶ enable and disable services;
 - ▶ format volumes;
 - ▶ expand files from the compressed format in which they are stored on the installation CD-ROM, and
 - ▶ perform a full CHKDSK scan to repair corrupted disks and files, especially if the computer cannot be started properly.
- **Restore points** - provide points in the past, usually defined automatically by Windows when new software is installed or changes to the operating system are made.
 - ▶ These restore points can provide a fall-back point, if the system becomes radically corrupted.
 - ▶ To access the restore point wizard, navigate to Window XP computer, **Start > Help and Support > System Restore.**
 - ▶ On a Windows Vista or Windows 7 PC, if the computer is bootable, click **Start**, and in the **Start Search** window, type **System Restore**. If the computer cannot be booted, choose **System Restore** from the Recovery Console.

- ▶ The user can either define a new restore point, or restore the system to a previous point.
- ▶ The system restoration calendar shows when restore points were created.
- ▶ Choose an appropriate point, and click **Restore**.
- ▶ The system will then reboot and will have reverted to its state *that day*.
- ▶ Only software and hardware configurations will have changed; stored files are not added or deleted.
- **Automated System Recovery (ASR)** - is a utility that actually performs two functions: backup and recovery.
 - ▶ The backup utility is located in Windows Backup, accessed through **Start > Accessories > System Tools > Backup**.
 - ▶ The wizard will back up the system state, services, all operating-system associated disks, restore information and the backup file itself.
 - ▶ ASR backups can be scheduled by clicking the **Schedule Jobs** tab in the **Advanced View** of Windows Backup and should be made regularly.
 - ▶ Access ASR recovery by pressing **F2** during startup. ASR startup will appear similar to Windows Installation. ASR information is located, and Windows restores the system using this backup information.
- **Emergency Repair Disks** - are used to check for disk integrity errors and can be used to repair a corrupted operating environment or boot sector. To create emergency repair disks, follow the following steps:
 - ▶ Navigate to **Start > Programs > Accessories > System Tools > Backup**.
 - ▶ Open the **Tools** menu and choose **Create Emergency Repair Disks**.

Diagnostic Techniques

These techniques are helpful when determining what the problem is, where it is originating from and how the problem can be fixed.

- **Identify the problem.** Question the user thoroughly about recent changes made to the computer, including any hardware or software that was recently installed or changes made to the operating system. Ask what the user was doing or using when the problem first occurred.
- **Analyze the problem.** Narrow down a list of possible causes of the problem, based on experience, training and observation. Determine if, ultimately, the problem is hardware or software in nature.
- **Test components.** Test affected hardware components by unplugging or otherwise disabling supposedly malfunctioning hardware. If the problem disappears, then the device is likely the issue. Examine software configurations for any conflicts or problems that may be arising from software installations or uses. Inspect the Device Manager for any device driver conflicts, and consult vendor documentation if necessary.

- **Evaluate the results.** Research the problem thoroughly in manuals, on the Internet and through technical support lines if necessary. Using the evaluation, correct the problem by applying information gained during research.
- **Document the results.** As discussed previously in this manual, a well-stocked service journal can help solve similar problems in the future.

Common Operational Issues

The following section covers ubiquitous Windows problems and errors and possible solutions to these problems.

- Perhaps the most recognizable and infamous Windows issue is the **stop error**, sometimes referred to as the Blue Screen of Death.
 - This usually indicates that either the Windows kernel or an application accessing the Windows kernel attempted an illegal operation.
 - This could, potentially, represent any number of problems. Follow the troubleshooting steps above.
 - Ensure that Windows is updated with the latest service packs and security updates and that all software and hardware is updated with the latest patches and firmware updates.

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2, 0x00000001, 0xFBFE7617, 0x00000000)

*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
```

Figure 37: The STOP error, AKA the “Blue Screen of Death”

- **System lockups** - these occur when Windows runs out of available resources to perform operations. No programs will respond to user input.
 - Sometimes, the user can access the task manager (**CTRL+ALT+DEL**) and terminate programs sapping computer resources. If this occurs often, it may be helpful to enable CPU throttling.

- ▶ If the system does not respond to the task manager, it will be necessary to manually restart the machine.
- ▶ Either upgrading the system's memory or reducing the number of active programs will, usually, solve this problem.
- **Input/Output Errors** - caused by improper driver installs. Download and install the correct and most up-to-date driver for the input/output device.
- **Corrupted Application Installs** - these happen either through a corruption of the Windows installer or because the installation medium itself is corrupted.
 - ▶ In the first case, download and reinstall the latest version of Windows installer.
 - ▶ In the second case, first uninstall the program. If the installation medium *is* corrupted, a new disk or download may need to be acquired. Otherwise, simply try reinstalling the software.
- **Application Fails to Load**
 - ▶ This can be caused by a wide variety of problems, ranging from low system resources to software incompatibility.
 - ▶ Ensure that the computer meets the minimum operating requirements of the application.
 - ▶ Also, make sure that the user has the proper permissions to install, run and access the application.
 - ▶ If all else fails, uninstall and reinstall the application – the original installation may have become corrupted.
- **Windows Specific Printing Errors**
 - ▶ In the case of a **stalled printer spool**, try stopping and restarting the service.
 - Navigate to **Start > Control Panel > Administrative Tools > Computer Management**.
 - In the console tree, click **Services**.
 - Find the **Print Spooler**, click **Stop** to cease the service, and then **Start** to restart it.
 - The print spooler may also stall if the disk on which it resides is low on free space. Try clearing out some unused files.
 - ▶ If the printer prints nonsensical characters, grid lines over the text or the program in which the user is trying to print crashes on a print request, the problem may be with the **printer driver**. Ensure an appropriate and up-to-date driver is installed.

Common Error Messages and Codes

- **Boot Errors** (Invalid boot disk, boot disk inaccessible, missing NTLDR).
 - ▶ All of the above errors indicate that the boot.ini file necessary for Windows load is either missing or corrupted.
 - ▶ In either case, it will be necessary to create a new boot.ini from the ASR. Follow the instructions listed in the above section on ASR to access the console.
 - ▶ The command **bootcfg /rebuild** will search available resources and re-create a fresh boot.ini.

- **Startup Messages** (Device/service failed to start, device/program in registry not found).
 - ▶ In the event of a startup error message, the message itself will be recorded in the **Event Viewer**.
 - ▶ Navigate to **Start > Accessories > System Tools > Event Viewer**.
 - ▶ Record the specific error message, and use Microsoft's Knowledge Base to troubleshoot the problem.

- **Registry Errors**
 - ▶ Registry errors can come in a wide variety, as Windows is constantly accessing and updating the database.
 - ▶ **Regedit.exe** and **regedt32.exe** access and edit the registry.
 - ▶ Refer to Windows Knowledge Base before performing any registry edits.
 - ▶ There are also a good number of third party programs that will scan the registry for errors and automatically fix them.

- **Windows Reporting**
 - ▶ Windows XP supports an automatic error reporting software.
 - ▶ If an error occurs and Windows detects it, the information will be sent to Microsoft over an available internet connection.
 - ▶ Navigate to **Start > Control Panel > System**. Click the **Advanced** tab and choose **Error Reporting**.
 - ▶ From here, the user can administer the type of error reporting that the system takes part in.

Diagnostic Tools and Utilities

- **Disk Management Utilities**
 - ▶ **DEFRAG** – Utility used to recover from drive fragmentation.
 - Drive fragmentation occurs over time and with usage, as files are written and deleted from the hard drive, fragments of files become strewn across the disk, lowering access speeds and reducing overall efficiency.
 - Defrag can be performed through the command console by typing defrag and the drive the technician wants defragmented.
 - Windows has a graphical defrag. Navigate to **Start > Accessories > System Tools > Disk Defragmenter**.
 - All of the command line options available to this utility are included within the graphical interface of Disk Defragmenter.
 - ▶ **NTBACKUP** – Once a command line utility, NTBACKUP has been completely absorbed into the Windows GUI. Please refer to the section on **Automated System Recovery (ASR)** above.
 - ▶ **CHKDSK** – a utility that verifies a disk's integrity by sifting through drive sectors searching for bad or corrupted sectors.
 - As with defrag, chkdsk can be run very easily from the Windows Shell.
 - Open **My Computer**; **right-click** on the appropriate drive and choose **Properties**.
 - Under the **Tools** tab, choose "**Check Now...**," and a small window appears. Click **Start**, and the computer will begin the check.

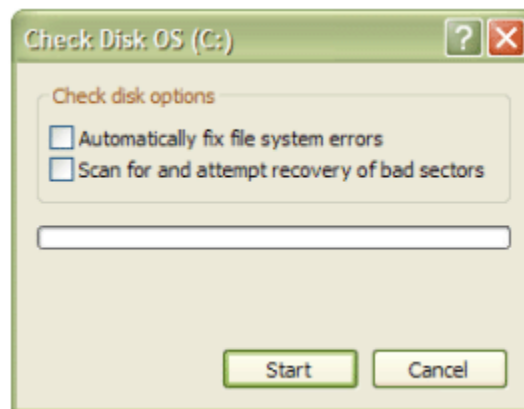


Figure 38: Windows Check Disk utility

- Should Windows detect some hard disk problem during boot, the user will be presented with a blue screen, and Windows will begin running the chkdsk routine.
- It is strongly encouraged to allow the system to complete the check.

- ▶ **FORMAT** – Utility used to erase all data on a partition and/or change the file system format of that disk.
 - Format can be used both in the GUI and in the console.
 - The GUI method is helpful for disks that are not bootable or are not carrying the operating system.
 - **Right click** on the drive which is to be formatted.
 - Click **Format**.

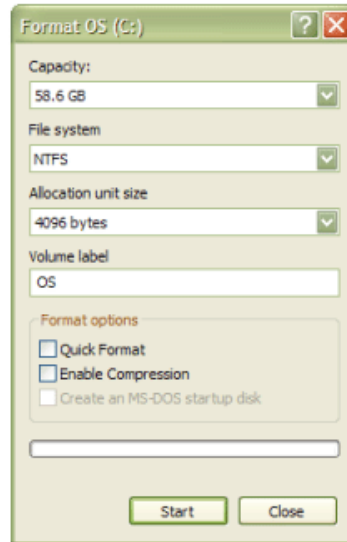


Figure 39: Formatting a disk

- Choose the appropriate file system, and label the disk. It is not recommended to change any of the other options.
- The console method is helpful for recovering a disk for operating system installs.
- Refer to the chart for usage and a list of format subcommands.

| Usage: FORMAT <i>volume</i> /FS: <i>filesystem</i> /N: <i>label</i> /Q | |
|---|---|
| Subcommand | Effect |
| /FS: <i>filesystem</i> | Defines the file system for the format. Acceptable variables are: FAT, FAT32, NTFS. |
| /N: <i>label</i> | Specifies the volume label. Example: /N:Storage. |
| /Q | Formats the disk in quick mode, rather than checking the disk for integrity issues. |

Figure 40: FORMAT command syntax

- **System Management Tools**

- ▶ **Device Manager** – A helpful application for viewing installed hardware device drivers and checking for device driver problems, such as conflicts or missing drivers.
 - The device manager can be accessed by navigating to **Start > Control Panel > System**. Click the **Hardware** tab and then the **Device Manager** button.

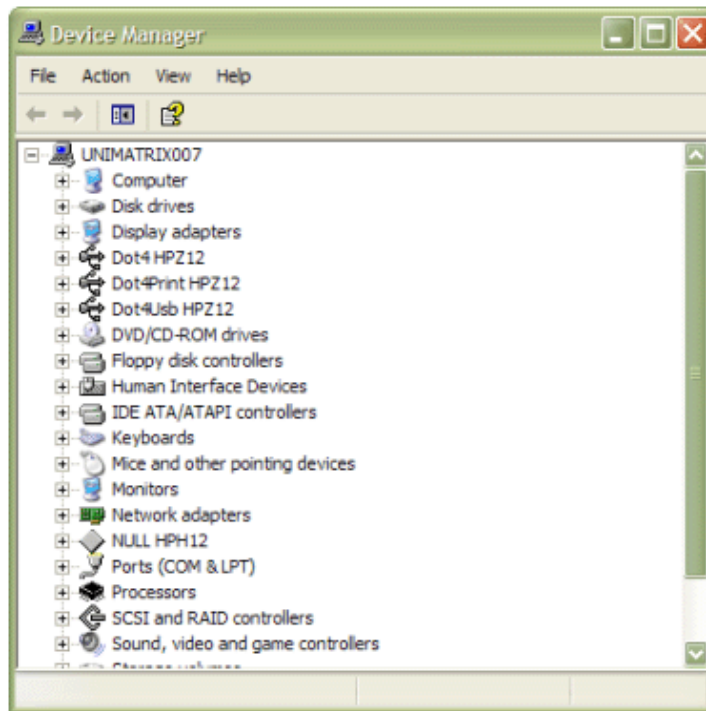


Figure 41: Windows Device Manager

- A missing, corrupted or otherwise malfunctioning driver will show next to the device in question as a small yellow exclamation mark.
- Follow the instructions listed in the **Loading a Device Driver** section, above.
- ▶ **Task Manager** – Another helpful application, which can be used to terminate resource-sapping programs, monitor network traffic, start and stop running processes or manage logged in users.
 - Can be accessed by pressing **CTRL+ALT+DEL** or **CTRL+ALT+ESC**.
 - Alternatively, right clicking the task bar and selecting **Task Manager** will also load the task manager.
 - To terminate a running program, select it, and press **End Task**.
 - To terminate a process, click the **Processes** tab, choose the appropriate process and click **End Process**.

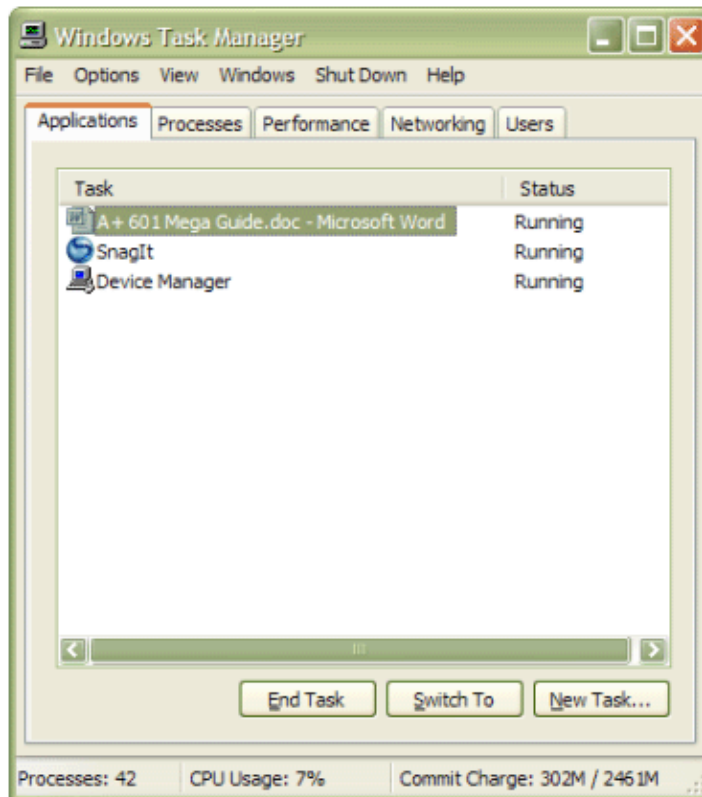


Figure 42: Windows Task Manager

- ▶ **MSCONFIG.EXE** – This helpful graphical utility allows the user to edit system configuration information.

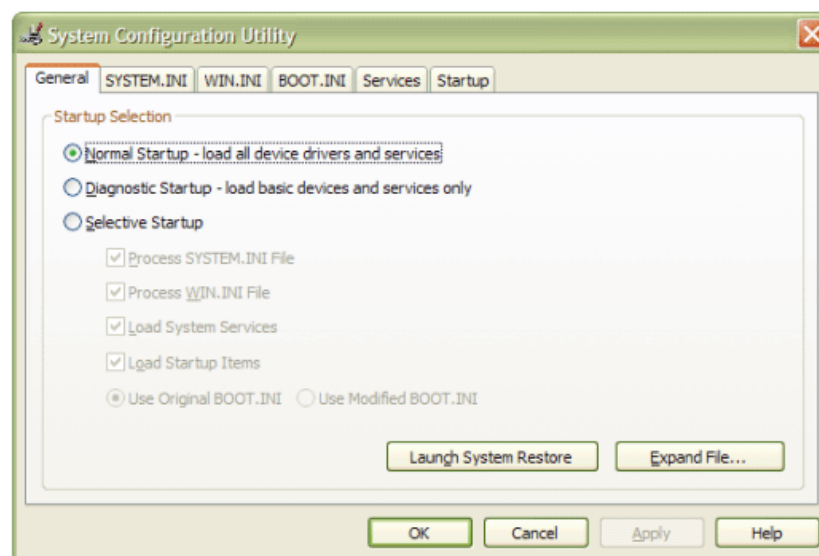


Figure 43: System Configuration Utility (MSConfig.exe)

- **Diagnostic Startup** - similar to Safe Mode, in that only the drivers and services needed to run Windows will load.
 - **Selective Startup** - allows the user to choose which system file is processed during boot. This is helpful when a corrupted system file is suspected.
 - **Services and Startup Tabs** - allows the user to choose which services and applications load on startup.
- **File Management Tools**
 - **Windows Explorer** – As previously discussed, Explorer is the basic way to navigate through Windows' files and folders. From Explorer, the user can create, delete, move or copy folders and files.
 - **Attrib.exe** – Attrib.exe is a console command that allows the user to add file attributes. Alternatively, file attributes can be added to a file by right clicking it and choosing **Properties**, then selecting the appropriate attribute from the list at the bottom of the window.

Preventative Maintenance Software and Windows Updates

Most software packages today will be automatically setup to download updates for themselves. Refer to vendor-specific documentation for options and configuration of this feature on third-party software.

Windows can be scheduled to search, download, and install regular updates. It is vitally important to ensure that Windows is updated with the latest service packs and security updates.

To schedule Windows Updates:

- Navigate to Start > Help and Support > Windows Update.
- On the right hand corner of the screen is a small box. Click Pick a time to install updates.
- Choose a day and time for Windows to look for, download and install updates.

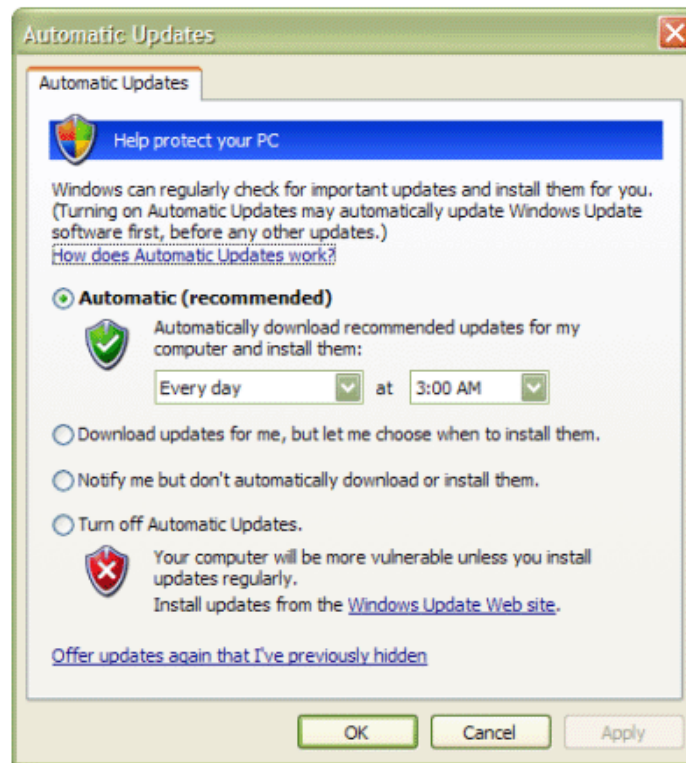


Figure 44: Configuring Automatic Updates

Scheduled Backups and Restores

As with Windows updates, backups and restores can be scheduled through **Windows Backup**.

- Navigate to **Start > Accessories > System Tools > Backup**.
- Click the **Schedule Jobs** tab. The user is presented with a calendar. Double clicking the desired day will bring up the Backup Wizard.
- Follow the on-screen instructions, just as if creating a backup *now*. The backup will be carried out on the proscribed day.

Restore Points

In addition to creating restore points automatically when changes are made to the operating environment, the user can manually create a restore point.

In Windows XP:

- Navigate to **Start > Help and Support > System Restore**.
- When prompted, choose **Create a restore point**.
- The user is prompted to name the restore point.
- Click **Create**, and the restore point is created.

In Windows Vista or Windows 7:

- Click **Start**, and in the Start Search window type **Create a Restore Point**.
- Click **Create a Restore Point** in the results.
- Choose the desired drive to create the restore point for.
- Click **Create**.

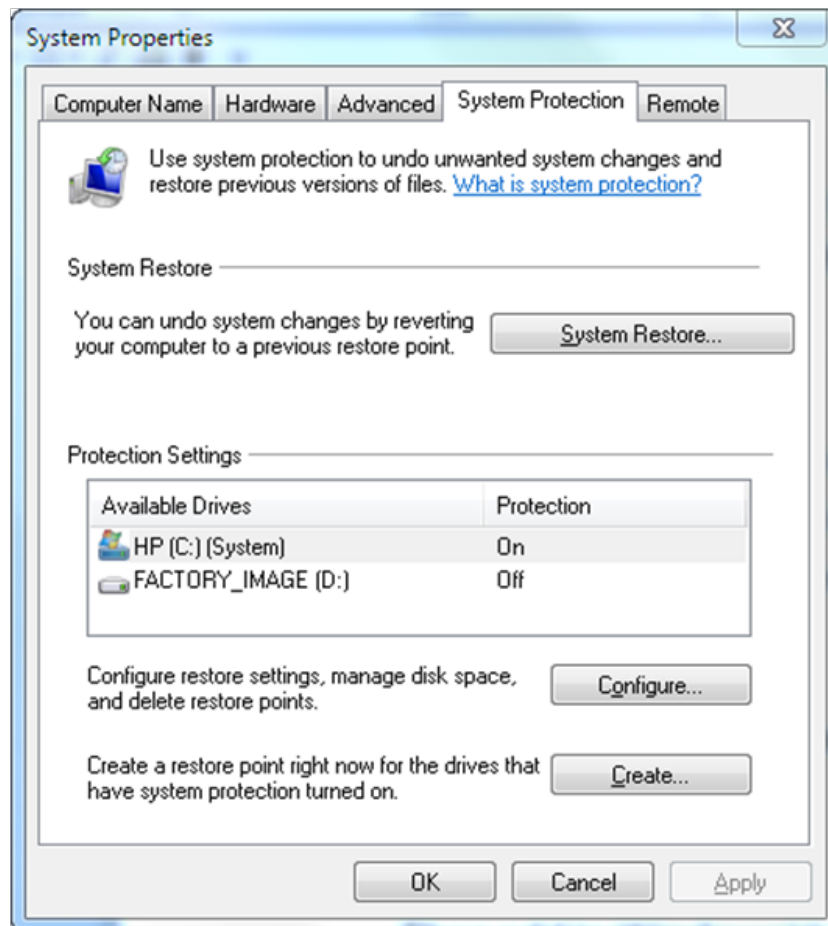


Figure 45

Domain 4: Networking Fundamental Principles

Networking is the practice of connecting two or more computers into a group, for the purposes of resource sharing. The networks themselves come in all shapes and sizes. The Internet is one massive network, made up of hundreds of millions of computers, connecting in a variety of ways, over a variety of mediums. Because this can be rather complex and sense networking (*especially* the Internet) is such an indelible aspect of computing, it is important for the A+ Certified Technician to know and understand these concepts.

Basic Concepts

Addressing

Every computer accessing the Internet (and the same holds true for every computer on a network) must possess a unique **Internet Protocol (IP) Address** with which it can be identified over the network. This address is very much like a street address. As with many computer standards, the IP address has undergone several revisions since its inception. This manual will cover the latest two:

- **IPv4** – Supports 32-bit (or 4 byte) addresses. This is the dominant standard today, and appears in the familiar xxx.xxx.xxx.xxx (called **dotted-decimal**) format.
- **IPv6** – This standard is still in development, but due to the severe shortage of addresses available to IPv4 (2^{32}), IPv6 will inevitably become dominant once development is finished. IPv6 addresses are 128 bits wide, which increases the number of available addresses to about 3×10^{38} . Rather than the dot-decimal format, IPv6 will use eight groups of four hexadecimal digits: 2001:0db8:85a3:08d3:1319:8a2e:0370:7334.

Because none of these formats are especially meaningful to human operators, especially in the case of IPv6, IP addresses resolve into **host names** (or domain names). For instance, google.com is the hostname for the IP address 64.233.167.99. The process of resolving hostnames into IP addresses and back again is left to a **Domain Naming Service (DNS)**. A more in-depth discussion of the **IP** protocol is included in the section **Protocols**, below.

Bandwidth

Bandwidth, in terms of networking, is simply the throughput speed of data over a particular connection. In dial-up networking, this term is synonymous with **baud**. An in-depth description of each type of connection technology and their specific bandwidths is included in the section, **Networking Technologies**, below.

Protocols

Protocols are the life-blood of any network system. Much like device drivers, they provide the means of translating the raw information sent over data lines across the network, into a language understandable to the computer and, eventually, to the user. As with most computer components, protocols are subject to a standard. The **OSI Stack** is the standard by which protocols are created, and it defines a seven-layer stack that describes the process of information translation from hardware to software:

1. **Physical Layer** – This is where all the electrical and physical specifications are contained; it defines cable specifications. Networking *hardware* operates at this level.
2. **Data Link Layer** – Provides error correction over Layer 1, as well as the means by which data is transferred between network entities.
3. **Networking Layer** – Provides the means by which data is transferred from a source to a destination, as well as routing procedures.
4. **Transport Layer** – Provides for the transparent transfer of data between end users.
5. **Session Layer** – Initializes, maintains and terminates the dialogue (or session) between local and remote computers.
6. **Presentation Layer** – Transforms data into something recognizable by the application.
7. **Application Layer** – Provides the means by which users access the information that has thusly traveled through all of the previous layers. This is where HTTP, SMTP, FTP, etc. operate.

In order to be successful on your CompTIA A+ and especially your Network+ exams, you must commit the Open Systems Interconnection (OSI) reference model to memory and fully understand how it works. The following table, presents the model another way:

| OSI Model | | | |
|---------------------|-----------|-----------------|---|
| | Data unit | Layer | Function |
| Host Layers | Data | 7. Application | Network process to application |
| | | 6. Presentation | Data representation and encryption |
| | Segment | 5. Session | Interhost communication |
| | | 4. Transport | End- to- end connections and reliability |
| Media Layers | Packet | 3. Network | Path determination and logical addressing |
| | Frame | 2. Data Link | Physical addressing |
| | Bit | 1. Physical | Media, signal and binary transmission |

Figure 46: OSI Reference Model

The most common protocol, **TCP/IP** (Transmission Control Protocol/ Internet Protocol; the name is derived from the two most important protocols within the suite) is actually a suite, or stack, of protocols that cover the layers of the OSI stack. Refer to *Figure 47*, below, for an explanation of how the TCP/IP stack compares with the OSI stack.

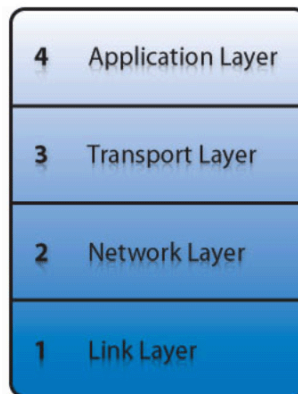


Figure 47: TCP/IP Reference Model

The earliest versions of the internet protocol, developed by the Department of Defense, had a very small amount of available addresses. In order to address this, ARPANET created the practice of subnetworking IP networks. A **subnet** is, simply, a division of a larger network. In the addressing scheme created by the DOD for the quickly expanding ARPANET, this was called a **classful subnet**, as it relied on various classes to separate addresses into three different sized networks.

Other Protocols within the TCP/IP Stack:

- **IPX/SPX** – Short for Internet Packet Exchange/ Sequenced Packet Exchange, both protocols are used almost exclusively by Novell networks and in local area networking. IPX operates at the network layer and is a packet protocol used for connectionless communications. SPX is a transport layer protocol used primarily by client/server applications.
- **NWLink** – A protocol very similar to IPX/SPX, used in Microsoft NT networks for resolving NetBIOS names.
- **NetBIOS** – Short for Network Basic Input/Output System, NetBIOS is a session-layer protocol that allows applications, on separate computers, to communicate over a LAN. It provides name resolution and registration, session services for connection-oriented communication and packet distribution.
- **NetBEUI** – An extension of NetBIOS (Network BIOS Extended User Interface), NetBEUI is a non-routable protocol operating at the network and transport layers and is responsible for implementing the services provided by NetBIOS.

Duplex

A duplex communication is one which can send and receive. A television is not a duplex device, whereas a telephone or your computer's Network Interface Card are duplex devices. All duplex devices are split into two types:

- **Half-Duplex** - devices can only send or receive at one time. A walkie-talkie would be a half-duplex device. Older computer modems could only either transmit or receive, but never both at the same time.
- **Full-Duplex** - devices that can transfer information and send information at the same time, down the same medium. This literally describes every form of computer communications used commonly today.

Cabling

As with any sort of communications, – be it between devices or between computers – some sort of cabling will be involved (except in the case of Wireless Networking, which will be discussed in the section, **Networking Technologies**, below). This section describes some of the common cable types found in computer networking:

- **Twisted Pair** (*Figure 48, below*) - a copper cabling standard used for Ethernet connections. Pairs of copper wire are twisted according to a **twist rate** (twists per meter), which is defined by the specific cable specification (described below). These twists reduce electromagnetic interference, which, in turn, reduces crosstalk. This is because the direction of the current generated by electromagnetic interference is reversed at every twist, so that twists eventually cancel each other out.

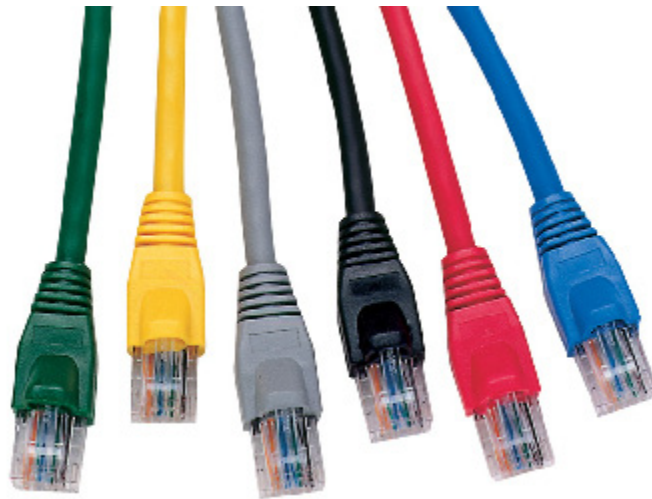


Figure 48: RJ-45 plug

- **Coaxial Cable** - used primarily for carrying broadband signals, which is done over a solid copper wire, surrounded by a spacing insulation layer, which is further surrounded by a conductive sheath. The whole cable is then surrounded with the familiar black or white plastic sheath. The coaxial connection is the thin, short and rigid line surrounded by a screw-in mechanism.
- **Fiber Optic Cable** - cable utilizes light to carry signals across great distances. The medium for this transmission is a vacuum-sealed tube, or "fiber," of glass less than 10 micrometers in diameter. Fiber optics can carry information over much larger distances than electrical cabling and can do it much faster, with an upper capacity, theoretically, somewhere in the 100s of terabits per second.
- **RS-232** - was one of the first cabling standards, developed in 1969 for use in communications transmissions between a typewriter and a modem. Later they were used in serial communications, on personal computers. Today, RS-232 cabling is used almost exclusively in point-of-sale devices and in connecting legacy peripherals, in industrial equipment and in serial console devices. In personal computing, this has been *completely* superseded by USB.

Network Models

Originally, the network model was an abstract way of representing objects and their relationships to each other, which became the basic theory behind databases. With the evolution of the Internet (which, in its own way, can be seen simply as a set of objects with relationships to each other), the network model has expanded to describe the way computers interact with one another on the network. There are two basic models for this interaction:





- **The Client/Server Model** - the most widely used network model, and most easily recognizable. At work, an employee will log onto their computer, which, along with all of the other computers in that workgroup, is *managed* by a central server. An internet service provider is a collection of servers that a computer either dials into, or logs onto over a broadband connection.
- **The Peer-to-Peer (P2P) Model** relies on the bandwidth of all the participants of the network, rather than a few servers. All the computers on a P2P model are called *nodes*, which "share" content such as music, video or telephony traffic and act as both client and server.

Network Cables

As discussed briefly in the section above, it is important to understand the various differences between network cables, especially in a wired network environment. This section offers some additional information on network cables, including types of twisted pair and the differences between types of fiber optic cabling.

- **Plenum / PVC** – Plenum cabling is simply cabling that is present in the spaces used for the circulation of heating or air conditioning systems and is heavily regulated by fire codes. This space is typically between a structural ceiling and a suspending ceiling, or underneath a raised floor.
- **UTP** – Unshielded Twisted Pair cabling is the ubiquitous networking cable that most technicians will see connecting computers to Ethernets. Twists in the cable reduce electromagnetic interference and crosstalk in the cable. UTP comes in 3 types:
 - ▶ **CAT-3** – Category 3 UTP, which is now obsolete (though the only cable type recognized by the international standards committee which regulates network cable types), was capable of a throughput of up to 10 Mbps.
 - ▶ **CAT-5** – Category 5 and its later enhancement, Cat-5e, provided speeds of up to 100 Mbps. The enhanced version was made to be compatible with Gigabit Ethernet and reduce far-end crosstalk.
 - ▶ **CAT-6** – Category 6 is the newest standard for Gigabit Ethernet and is capable of speeds up to 10 Gbps.
- **STP** – Shielded Twisted Pair cabling adds a metal shield to each pair of twisted copper wires. This adds another level of electromagnetic interference protection and was originally developed for IBM's Token Ring network.
- **Fiber Optics** - comes in two different types, determined largely by the way light propagates across the cable:
 - ▶ **Single-mode** - utilize only the lowest order wavelength to transmit light. This type is best for transmitting over long distances (up to 60 km) with extremely high data rates, because more information can be passed along the wire per unit time.
 - ▶ **Multi-mode** - slower than single-mode and only works over short distances but is also less expensive than single-mode fiber. Multi-mode fiber is also larger; it's almost ten times the diameter of single-mode fiber.

Refer to the following chart for the various connections used by network cables:

| Name | Appearance | Cable Type |
|--------------------|--|-----------------------------|
| RJ-45 |  | Category 3-7 network cables |
| RJ-11 |  | Phone line cables |
| USB |  | USB Cord |
| IEEE 1394/FireWire |  | FireWire serial cable |

Networking Technologies

Originally, the only method computers used to communicate with each other was either through a serial (null modem) connection or by dialing in to each other. Today, computers can communicate with each other utilizing a wide variety of technologies, discussed below:

- **Area Networks** - networks which cover a number of computers within a self-contained network.
 - **Local Area Networks (LAN)** are a set of computers, connected within a short geographical range, usually within one building. Most LANs use Ethernet for connection, wireless or wired.
 - **Wide Area Networks (WANs)** utilize the same technology but over long distances. An internet service provider is a kind of WAN.
- **Integrated Services Digital Network (ISDN)** - a high-speed (when compared with analog, dial-up networking) internet connection that uses circuit switching to transmit both data and voice, over existing copper telephone lines. There are two ISDN implementations:
 - ▶ **Basic Rate Interface (BRI)** - consists of two bearer channels (at 64 Kbps) and a delta channel at (16 Kbps).
 - ▶ **Primary Rate Interface (PRI)** - utilizes a large number of bearer channels and a higher-rate delta channel (at 64 Kbps). The speed of PRI depends on the number of bearer channels, which is then determined by the country of use. Speeds can range anywhere from an aggregate 1.5 Mbps to 2 Mbps.

- **Broadband** - define several networking technologies but generally are any technology utilizing cables to transmit a large amount of data. Broadband can be a loaded and relative term. However, for the purposes of this study manual, broadband communications come in three types:
 - ▶ **Digital Subscriber Lines (DSL)** - utilize existing telephone lines to transmit broadband information, sending data on one wire and voice communications on a separate wire. Capable of speeds between 128Kbps to 2.4Mbps.
 - ▶ **Cable** - utilizes existing coaxial cable, used to send cable television, for communications. These are capable of speeds between 3Mbps to 15Mbps.
 - ▶ **Satellite** - uses a receiving dish to collect data communications from orbiting satellites. This technology is used in areas where terrestrial internet service is unavailable (i.e., rural areas). It comes in three types:
 - **One-way multicast** - can only receive, as with television;
 - **One-way multicast with terrestrial return** - uses a dial-up modem to transmit, and
 - **Two-way satellite** - can transmit and receive.
- **Dial-up** - utilizes phone lines and a dial-up modem to access the Internet. Most dial-up modems operate at 56Kbps and are internal devices, much like a NIC.
- **Wireless (802.11)** - use radio transmissions to transmit data. Refer to the chart, *Figure 49*, below:

| Protocol | Frequency | Bandwidth |
|----------|-----------|-----------------------------------|
| 802.11 | 2.4GHz | 1, 2 Mbps |
| 802.11a | 5GHz | 6, 9, 12, 18, 24, 36, 48, 54 Mbps |
| 802.11b | 2.4GHz | 5.5, 11 Mbps |
| 802.11g | 2.4GHz | 6, 9, 12, 18, 24, 36, 48, 54 Mbps |
| 802.11n | 2.4GHz | 540 Mbps |

Figure 49: Wireless networking standards

- **Infrared** - used exclusively for short-range communication, utilizing the same technology remote controls used for data exchange.
- **Bluetooth** - uses radio communication technologies over short range for devices and is designed for low-power consumption. It has a variety of uses, including input/output devices (keyboards, mice and printers) as well as in networks requiring low bandwidth and in confined spaces. Bluetooth is currently in revision 2.0.
- **Cellular Modems** - used exclusively in laptops and require a PC card and a cellular service which supports data transmission.
- **Voice over IP (VoIP)** - is a method of voice communications using the Internet Protocol and a specially-equipped phone. It is distinguishable from regular voice communications in that there are no "area boundaries" or long distance phone calls.

Network Installation and Configuration

The following section details the installation and configuration of Network Interface Cards (NIC) and the connection to both a wired and wireless network.

- **Hardware**
 - ▶ After powering down the computer, retire the unit to a clear area to work.
 - ▶ Use best practices for hardware installation, including being careful to prevent ESD discharge by wearing an ESD bracelet or ankle strap.
 - ▶ Insert the NIC into a free PCI slot, by applying firm pressure to the card, but avoid directly touching the circuitry on the board; then, screw the card down to the chassis.
 - ▶ Replace the computer, and power up.
 - ▶ PCI cards are PnP compatible; so, upon power up, the PC will recognize the new card and attempt to install drivers. If a driver disk is supplied with the NIC, insert this now, and install the software.
 - ▶ The installation procedure will be exactly the same for a wireless NIC.

- **Obtaining Network Connection (Wired)**
 - ▶ Once the software is installed, navigate to **Start > Control Panel > Network Connections**. **Double-click** the appropriate network connection in Windows XP. In Windows Vista or Windows 7, click the Network icon on the Taskbar (in the Notification area), and click Open Network and Sharing Center. Click the local area connection.

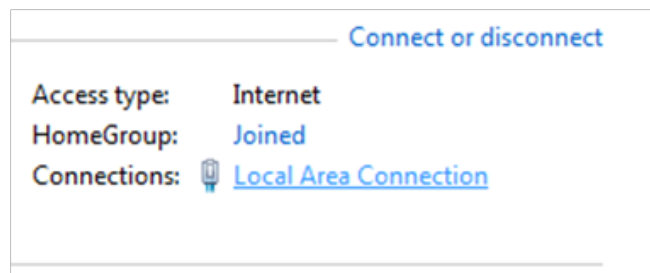


Figure 50: Windows 7, click **Local Area Connection**. In Vista (not shown) click **Show Details**.

- ▶ In Windows XP, the local connection is shown. In Windows Vista or Windows 7, click **Details** to see similar information.

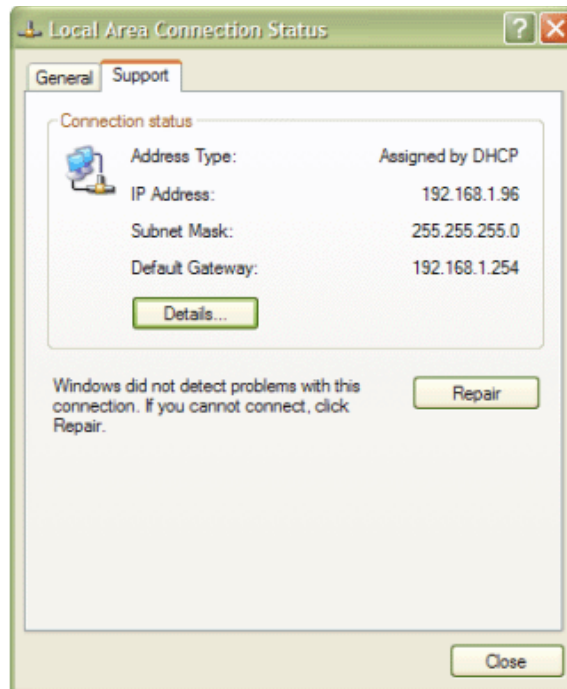


Figure 51: LAN Status dialog in Windows XP

- ▶ In most network connections, this information will already be filled out. If so, then the computer is connected to the wired network. If not, clicking **Repair** will release the current state, and then, renew the network connection, reconnecting with the proper network and supplying the IP address necessary for Internet communications.
- **Obtaining a Network Connection (Wireless)**
 - ▶ Obtaining a wireless network connection requires a little more work.
 - ▶ Once the network card is installed, an icon in the system tray will demonstrate that the card is searching for a network. Right-click this icon and choose **View Available Wireless Networks**. This command is virtually the same in all OSes. Look for the network icon in the Taskbar's Notification Center to see what options are available to you.
 - ▶ A list of wireless networks within range of the card will appear. Select the appropriate network, and click **Connect**.
 - ▶ A series of options will be presented. If the wireless network is secure, it will require a 128-bit encryption key. Enter this in the provided space, and click **Connect**.
 - ▶ If the key is correct and the computer is allowed access to the network, the connection routine will run and a tool-tip will appear above the wireless networking icon, in the system tray, indicating that connection has been established, the quality of the connection and its speed.

Diagnostics and Troubleshooting

Most problems that occur with wireless connections have to do with either not being close enough to the wireless access point or not having the wireless features of the computer or mobile device enabled. Check these things first. If problems still persist, review the various indicators available to you. Various **status indicators** on the NIC provide information useful for diagnosing and troubleshooting wired and wireless network connections.

- The **connection** light is perhaps the most important. A solid green connection indicates that the connection is idle, but a link is established and good. An amber light usually indicates a “limited or no connectivity” status, which means that one or more services necessary for Internet connectivity is not working properly. If the light is off, then there is no connection.
- The **activity** light indicates the level of activity and will blink according to the level of traffic.
- The **speed** indicator shows at what speed the network is running at, in terms of 10, 100 or 1000 Mbps.
- In **wireless** cards, an LED will show whether or not the card has a link to the wireless network. Within the operating system, this indicator will be represented by a one-word description of the strength of signal (poor, good, excellent, etc.).

Domain 5: Security

Rapid and unchecked advances in computer communications technologies have led, inexorably, to massive gaps in necessary protection for the sensitive information users keep on their computers. Literally millions of dollars a year is lost to data theft and security breaches, while tens of millions of dollars are spent to stop such occurrences. That being said, it is extremely important for an A+ Certified Technician to understand the concepts and theories behind network and computer security.

Fundamental Principles

The following section details the basic concepts of computer security. It is often overlooked that computer security is a multifaceted discipline, with factors covering a wide range of topics, including hardware, software, physical security and issues of social engineering. These topics are covered below.

Hardware and Software Security

Issues relating to hardware and software are, perhaps, the most important concerns for a computer technician. This is where the actual data is kept, and, as such, it is important to understand how to protect this sensitive information from leaking to uninvited parties.

- Computer equipment, especially storage devices, quickly become obsolete, broken or are replaced. Replaced equipment should be fully **deconstructed**, following manufacture guidelines.
- In many cases, this equipment can be **recycled** and reused for other purposes. For instance, older, legacy storage devices can be turned into SAN or NAS devices. Before the equipment is to be reused, ensure that any and all sensitive information is completely removed before recycling it for other uses.
- **Biometrics** is the practice of assigning security protocols to certain unique characteristics of a human being. These include fingerprint and handprint scanners, retina scanners, voice-print identification, etc.
- **Smart Cards** are similar to biometrics in that authentication requires some physical input. However, instead of a fingerprint or a voice-print, the user must insert an electric key-fob, card or chip, hard-coded with the user's identification information.

- **Authentication technology** is a blanket term for all of the methods by which a computer connects the identification of the user with access.
 - ▶ The most basic technology is the **user name/password**. Each user is given a unique, identifying name, which is public, and a chosen, private password. Together, these two pieces of information authenticate the user to the system and provide access.
 - ▶ Similar to the above technology, **biometrics** simply replaces the password with the required input. A user inputs a username and then scans their fingerprint, retina or voice on the associated hardware and is granted access.
 - ▶ As with biometrics, **smart cards** are hard coded with password information, and their presence in the system is physically required before access is granted.
- The Internet is full of **malicious software**, software which seeks to infect, rob, access without authentication or otherwise adversely affect a computer or network system:
 - ▶ **Viruses** - designed to not only propagate themselves within a system, as the name implies, but usually to sap system resources or corrupt system files and spread themselves to other systems. They require the execution of the program which they infect to become active.
 - ▶ **Trojans** - a type of virus used to gain access to a computer by pretending to be a benign piece of software.
 - ▶ **Worms** - another type of virus that is self-contained and self-replicating, but is not reliant on an outside program. In other words, a worm does not require human action or the execution of the program it has infected in order to become active. Worms sap bandwidth in order to propagate to other systems.
 - ▶ **Spam** - unsolicited advertisement that comes in the form of banner advertisements, pop-up ads or e-mail.
 - ▶ **Adware** - very much a virus that performs the same duty as spam: it installs itself on a computer system and then feeds the user advertisements over the Internet, usually as pop-up ads.
 - ▶ **Spyware** - similar to adware, in that it is a program and is used for advertisement. In addition, spyware tracks a user's web use and history to "tailor" the advertisements.
 - ▶ **Greyware** - a blanket term covering both adware and spyware, and is generally defined as any program that is annoying. In addition to ad- and spyware, greyware can be dialing programs, joke programs, hacking software and remote access software.
- **Software Firewalls** - programs which operate between the network and the computer (logically, not literally) to block unwanted network access and use. A set of **rules** is used to determine what sorts of access is malicious and what is benign. These rules can be manipulated by the user to achieve the appropriate level of security for a specific computing environment.
- **File system security** - another important security consideration. The FAT 32 (used in earlier versions of Windows and the Windows XP Home edition) file system is inherently less secure than NTFS (used in versions Windows NT and Windows XP Pro and 2003 Server) thanks, in part, to an embedded and transparent file encryption system.

Wireless Security

Because wireless networks are, essentially, transmitted freely over the airwaves, it is extremely easy to utilize this broadcast for malicious use. Therefore, careful attention should be paid to the security of any wireless network.

- Wireless networks utilize unique **encryption keys**, which provide a measure of security over computers attempting to access the wireless network. If the computer doesn't possess the key, it will be denied access. The encryption comes in two formats:
 - ▶ **Wireless Equivalent Privacy (WEP)** – basic security standard included in the 802.11 standard; possesses a 128-bit encryption, entered as a string of 26 hexadecimal characters. Limited key size expresses some security concerns.
 - ▶ **Wi-Fi Protected Access (WPA)** – the other standard, developed in response to the weaknesses of WEP. Utilizes longer keys and error-checking suites to maintain a higher level security. WPA technologies have been continually improved on each year, and new security options are available. You may see WPA 2, WPA-PSK, and other options. Wireless security is a very broad field, and changes often, so make sure to review the new technologies often to stay on top of the changes. All WPA requires a passcode though, so you'll still have to configure the various WPA technologies in the same manner.
- **Wireless access points** - provide areas of connectivity, require special security considerations, as they innately "trust" every device attempting connection.
 - ▶ **Enable MAC Address Filtering** - this feature will limit access to specific MAC addresses, allowing only certain users to gain access.
 - ▶ **Change the SSID** - the wireless network's SSID - should be changed from its default, and its broadcast over the network should be turned off. This is a weak form of security and should never be used by itself.
 - ▶ **Use a static IP address** - instead of allowing the **DHCP** to obtain an address, setting a static IP is another way of adding cheap and easy security to a wireless network, as it will reduce the number of sniffable packets being sent from a machine.
 - ▶ **Change Passwords often** - also **usernames** should be unique.
 - ▶ **Update the network hardware firmware** - take advantage of the latest security updates for devices on networks.
 - ▶ **Use a firewall** should be used on any wireless network to prevent access into the computer itself.



Figure 52: Residential wireless access point (WAP)

Data and Physical Security

In any secure environment, it is very important to have a **basic local security policy** mandating levels of access. These policies, on Windows computers, allow administrators to define users by their “rights” on the system and then assign resources to groups of users based on these rights.

- Whenever possible, the strongest **encryption technologies** should be used. Each type of encryption technology is defined by the **algorithm** it uses to encrypt and decrypt data.
 - **Symmetric key algorithms** - use a private key of variable bit length (higher being stronger) that is secret and has been set up and shared between the user and the system, prior to access. The sender and receiver use the same key for encryption and decryption. Examples include: the **Data Encryption Standard (DES)** and the **Advanced Encryption Standard (AES)**.
 - **Asymmetric key algorithms** - use a public key that is published for all parties that will access the system and allows all parties to encrypt data. The receiver has a secret key that is not shared and enables only the receiver to decrypt data. Examples include **RSA**.
- **Keep backups secure** - preferably behind firewalls or stored by a third party. Access to backups should also be kept limited and secure, ideally accessed by the few people who store and restore backed-up information.
- **Maintain data migration security** - or the movement of massive amounts of information from one system to another should be done in a closed environment, to prevent sensitive information from leaking out.
- **Make sure data is completely removed** - when removing unneeded (but still sensitive) data, it is important to ensure that the data is actually gone. That is, no remnants remain on the system which could be used or accessed maliciously.
- **Enforce password management** - passwords should be heavily enforced. Passwords should be changed often and kept as strong as possible, preferably as random strings of letters and numbers.
- **Lock down unattended computer systems** - laptops should be put in cases and locked with a key, and desktops should have the operating system lock engaged, by pressing **Ctrl+Alt+Del** and clicking the **Lock Workstation** button.
- **Incidence reporting** - another important aspect of computer security. Incident reports, if properly kept, enable a computer security team to properly defend against future attacks and update the system as needed.
- **Social engineering** - the process of duping users into voluntarily giving out authentication information. Inform computer users of these types of attempts, and make sure users know not to ever give out password information.

Security Installation and Configuration

The following section details the practical aspects of setting up security on network systems.

- It is possible to add a level of physical security to computer systems by creating a **boot password** in the BIOS. The user will be prompted for a password on boot, and the computer will not complete the process without the correct password. Refer to the BIOS-specific manual for this process.

- Install **smart card readers** at workstations.
 - Smart card readers are, typically, USB devices, which support hot-plugging.
 - Simply plug in the device and provide installation software, if required.
 - Once installed, navigate to **Start > Control Panel > Network Connections**, and access the properties of the appropriate network connection.
 - Click the **Authentication** tab and ensure that the IEEE 802.1x authentication box is checked and “**Smart Card or other Certificate**” option is selected.
 - Server-side software will provide the means of managing Smart Card passwords.
- Install the Windows Malicious Software Removal Tool to ensure the system is safe from adware, spyware or greyware. Additionally, there are several third party tools that work just as well, if not better.
- Windows XP SP2 also includes Windows Defender, an antispymware application. This should also be supplemented with third party virus protection software, such as Norton AntiVirus, is one is not installed on the computer already.
- **Backup procedures** and **data migration** should always take place in a closed, cut-off environment to prevent any data leakage. Once the processes are done, the systems can be brought back to the network. Access to backups should be strictly regulated as well.
- When data is deleted, make sure to empty the **Recycle Bin** as well. This is still not, necessarily, permanent. Therefore, it may be necessary to use a third party data removal program.

Security Troubleshooting and Diagnostics

- If a BIOS boot password becomes lost or forgotten, it can be recovered or bypassed.
- Device drivers can always become corrupt; therefore, if the system is experiencing problems with a **smart card reader** or a **biometrics device**, it is important to resolve the problem quickly. Try uninstalling and reinstalling the device software.
- If malware removal programs cease to be effective, ensure that virus and adware definitions are up to date. Visit the developer's website for specific update information.
- Update the **data security policy** as changes arise within personnel or resources. In a secure environment, no resource should be left undefined, and no user should be allowed administrator rights.

Preventative Maintenance

One of the most important steps to improving network security is to ensure that operating system software is as up-to-date as possible. Viruses, malware and hackers utilize security holes within the operating system itself to gain access. Set up the **Automatic Update** feature in Windows to ensure the system gets the latest service packs and security hotfixes:

- Navigate to **Start > Help and Support > Windows Update**. In Windows Vista and Windows 7, click **Start**, and in the **Start Search** window, type **Windows Update** and select it in the results.

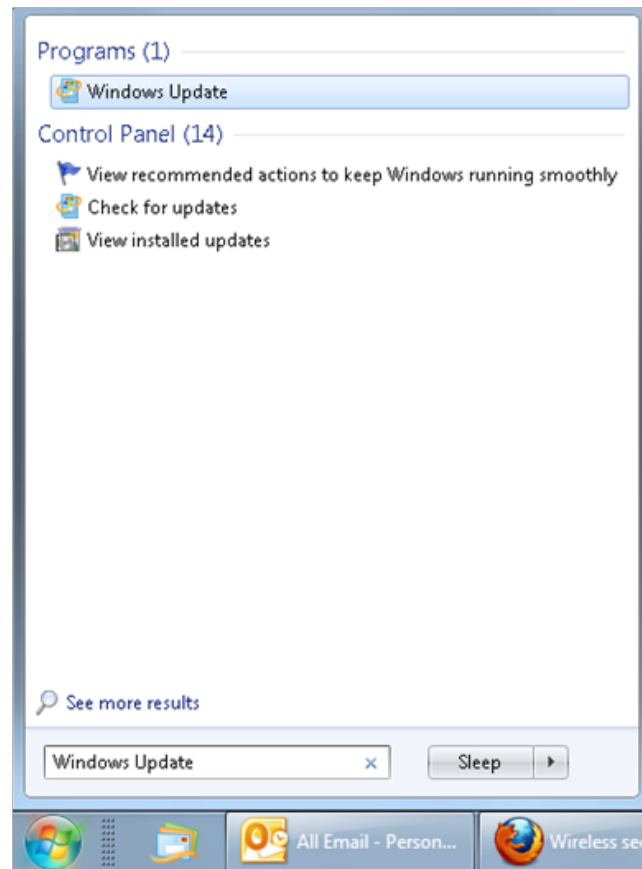


Figure 53

- Ensure that the shield in the upper right hand corner of the dialogue is green and says "Automatic Updates turned ON."
- Click "**Pick a time to install updates**" to setup the time of day Windows will check for updates.

It is also useful to inform and educate all users on a network system of the dangers of malicious software and how to prevent propagation; for instance, opening emails and attachments from unverified sources, navigating to websites which utilize pop-up ads and ad- or spyware, etc. A strong security policy is only as strong as the least-informed person on the network. So long as members of a network remain *aware* of the dangers and how those dangers are given access to the system, then the system will remain secure.

Domain 6: Operational Procedure

While the inert grey boxes that make up a computer and monitor may not necessarily seem all that threatening, it is important to take into account various safety issues when it comes to computer technical work and the environment in which this work takes place. The following section details these ideas.

Safety Issues

Potential Safety Hazards

- Cords present the most ever-present safety hazard, causing falls and creating the danger of damaging equipment and personnel. Ensure that cabling is properly managed and kept away from general traffic.
- Most computer components, even when disconnected from a power source, carry electrical charges, especially monitors. Ensure that the technician is properly grounded and is using best practices when it comes to electrical discharge. **All powered devices should be powered down before any work is done.**
- Old batteries, whether they are from self-powered peripherals or uninterruptible power supplies (UPS) can pose a danger from leaking acid and even explosion. Follow the safety guidelines provided by the manufacturer.

Material Safety Data Sheets (MSDS) and Documentation

- Always properly document every piece of equipment that comes into the technician's care. Ensuring that materials are properly documented will ensure that hazardous materials or flammable materials are properly taken care of or disposed of.
- MSDS allows employees to have on-hand documentation for the safe handling of hazardous substances. They contain information regarding toxicity, physical tolerances, first aid, health effects, electrical information, etc. Always make sure these documents are in an easily accessible place.
- Before sitting for your exam be sure to familiarize yourself with MSDS documents. You can view them online.

Repair Tools

- Appropriate repair tools should be used at all times.
- ESD bracelets or ankle straps should be used when working with equipment that carries electrical charges.
- Magnetic tools should be kept away from sensitive drive mechanics and especially from hard disks and tape drives, where magnetism can harm stored data.
- Most tool kits provide a device for the retrieval of dropped items. This tool is sometimes colloquially called a "nose-picker." Always use the retrieval tool, and never use bare hands.



Figure 54: PC technician's tool kit

Accidents

- Every accident, no matter how minor, should always be reported to superiors and **well documented**.
- Contact with toxic chemicals should be treated according to proper first aid: wash the affected area thoroughly. If the chemical should get in the eyes, flush with a lab-station eye cleaner. If the chemical is accidentally ingested, note the name of the chemical and call a Poison Control Center **immediately**.
- Electrical accidents, even minor ones, may require hospitalization. Disconnect the power from the source of the accident, preferably by throwing a breaker. **Never try to physically remove a person from electrocution**, no matter how properly grounded.
- Physical accidents should also be treated very carefully. Never try to move someone who has suffered a physical injury, as this may exacerbate the problem. If the victim cannot move, call for medical assistance immediately.

Safety Procedures

ESD Precautions and Procedures

- Always wear some sort of ESD prevention device when working inside of a computer.
- A wrist strap, grounded to the CPU chassis via an alligator clip, is perhaps the most common.
- Some work environments have special anti-static mats or conductive flooring in conjunction with ankle straps to reduce this possibility.
- Work environments where there is a danger of ESD should be kept as clean as possible, with little to no humidity.
- Another method of ESD prevention is the placement of ion generators, which inject ions into the air stream to reduce, or even neutralize, the charge carried by humans and surfaces.

Safe Work Environment

- Keep the environment clean, especially of liquids. Even a slip and fall can be dangerous around heavy and often sharp-edged computer equipment.
- Walkways should be clear and well lit.

Equipment Handling

- One of the oldest rules regarding workplace safety still applies: any heavy thing that can be lifted by one person can be lifted safely and more easily by two people.
- Especially when carrying heavy equipment, always be very aware of surroundings and other co-workers.
- When available, use dollies, hand trucks, carts, etc.

Disposal Procedures

Computer components can't simply be thrown in the garbage. Most components are, at best, sharp or otherwise dangerous to handle, and at worst, toxic to people and the environment. Therefore, it is important to practice safe disposal procedures, especially when dealing with batteries, display devices and chemical solvents and cans.

- **Batteries** - most cities now have recycling centers which accept used and old batteries. Where available, recycle at designated centers. There are also plenty of battery reclamation organizations.
- **Display Devices** - as with batteries, display devices have many toxic materials and disposal concerns. Of course, display devices, before disposal, should be cleared of any retaining electrical charge. Afterwards, they should be committed to a local electrical reclamation center. Unfortunately, there is no standard method for disposing of electrical devices, as the concept is still considered largely controversial.
- **Chemical solvents and cans** - As with batteries and display devices, chemical solvents are usually subject to federal regulation, as far as the method of disposal, and each state is different in its guidelines. In general, however, chemical solvents should be stored in a cool, dry place until they can be reclaimed. Refer to the specific state's guidelines for hazardous waste removal before making any decisions.

Communication and Professionalism

Ultimately, being a computer technician is about dealing with *people*, not with *machines*. A technician's expertise allows them to serve as a liaison between the sometimes difficult-to-understand world of computing and the people who use computers. Also, computers are the third most expensive item people buy, after houses and cars. People can and will be very protective of their computers for that very reason. That being said, it is important for a technician to practice good communication and professionalism when working with people and their computers.

Communication

The majority of a technician's time will be spent listening to the user; therefore, good communication skills are extremely important to properly diagnosing and fixing computers.

- **Use clear and concise statements** when speaking with the customer. Explaining computer problems in terms that the lay-user will understand is very important to proper client relationships. Keep comments short and to the point, and leave any preconceived opinions at the door.
- **Avoid interrupting** the customer when they are describing the problem. Remember, the customer will not have any technical experience with computers. They will describe their problem in terms of how they use the computer. Allow the customer to make complete statements.
- **Clarify customer statements** by asking pertinent questions regarding the computer. For instance, ask "What were you doing when the problem first occurred?" or "Have you installed new software or hardware recently?" Without a clear context for the problem, it will be impossible to diagnose it.
- **Avoid using jargon**, abbreviations and acronyms. This is, arguably, the most important and difficult skill to master. Speaking in jargon and with copious abbreviations and acronyms will alienate the user immediately, and appear condescending. Imagine going over to a foreign friend's house for dinner, and the entire time the family speaks in another language. It is rude, and in the business world, it is extremely unprofessional.
- **Listen to customers.** Computer problems can be extremely disruptive to anyone, and especially disruptive to people who use their computers for work. Listening carefully to the customer and his/her problem will put the customer at ease and will make diagnosing the problem much easier.

Professional Behavior

Proper communication with customers and coworkers is certainly a very important aspect of professionalism. However, there are several behavioral concerns important to professionalism as well.

Behavior

- **Maintain a proper attitude and tone.** This is *extremely* important, especially in the world of computers. Too often, computer technicians are seen as reclusively anti-social at worst, arrogantly self-assured at best. Maintaining a professional attitude and tone of voice will put the customer at ease and will help to keep the flow of communication moving freely between technician and customer.
- **Avoid arguing with customers.** Don't get defensive! It's easy to interpret the frustration a customer is feeling over computer problems with frustration towards the technician. The customer is just having a bad day, so keep a level tone of voice. You don't have to *agree* with the customer, but you do have to *respect* the customer's opinions. If they ask you to try something or to give a piece of input that you know won't work or is unimportant, follow up on it anyway.
- **Do not minimize the customer's problem.** This happens, regrettably, a good deal in business environments where there is a separate team of computer technicians. While a technician may have infinitely more computer experience than the user, that customer does *his/her* job much better than the technician. Be respectful of what, to the customer, is a *very big deal*.
- **Avoid being judgmental.** The best example of how *not* to be a computer technician is the insulting and annoying computer tech on Saturday Night Live's "Nick Burns" sketch. The character is insulting, rude and constantly minimizes the customer's problems and abilities with a computer. Again, whereas the technician may be experienced and trained at handling computers, the customer is skilled and trained at his/her job.

- **Avoid distractions and interruptions.** The cell phone is almost required equipment for every professional. That being said, the technician should take pains to ensure that cell phones, beepers, blackberries, etc. don't disturb conversation between the technician and a customer. Whatever problem the user is having is much more important than any phone call. If the phone call is business or service related, politely ask the customer's permission to be excused, answer the phone and inform the caller that a customer is currently being served and will be called back.

Property

Working in any company as a computer technician, it is likely that the technician will be given tools and equipment to better handle the work load. This can include laptops, cell phones, walkie-talkies, desktop computers, printers, etc. It is important to treat all of these items with the same respect that someone would treat his/her own personal belongings. Don't make personal phone calls, waste hours on the Internet, install games or other unapproved software on computers; keep screensavers and wallpapers appropriate for a business and professional atmosphere, etc.

Practice Questions

Chapter 1

1. Your customer is interested in purchasing an external hard drive to expand her notebook's storage capacity. She is very concerned about the portability of the drive, as she tries to travel light. Which of the following drive features should you pay special attention to when recommending an appropriate drive? Select the best answer.
 - A. Capacity.
 - B. Support for both USB 2.0 and FireWire connectors.
 - C. Bus-powered.
 - D. Compatibility with both Windows and Macintosh operating systems.
2. You are upgrading the Operating System on a desktop PC and discover you need to upgrade the RAM to support it. The motherboard documentation indicates that it uses SDRAM DIMMs. What additional information must you consider before placing your order for the additional RAM? Select TWO correct answers.
 - A. Must the memory be in pairs?
 - B. Do the memory slots have 240, 184 or 168 Pins?
 - C. Does the memory bus use 2.5v or 4.3v?
 - D. How many memory slots are available?
3. You are a computer service technician for a cellular phone company. The company has many remote unmanned cell phone tower sites, each of which contains a typical desktop computer to control operations of the cellular equipment at the site. Your boss asks you to assure that the computer in each cell tower site can remain running during power outages lasting up to 45 minutes, without incurring unnecessary cost. You have determined that the computer will present a 250VA load on the UPS. How can you determine what size of Uninterruptible Power Supply to provision at each site? Select the best answer.
 - A. Use the following formula, Where S is the VA rating of a proposed UPS, and R is the resulting run time of the UPS running your equipment: $(S / 250) \times 1.5 \times 10 = R$.
 - B. Use the following formula, Where S is the VA rating of a proposed UPS, and R is the resulting run time of the UPS running your equipment: $(S \times 250) / (1.5 \times 10) = R$.
 - C. Use the following formula, Where S is the VA rating of a proposed UPS, and R is the resulting run time of the UPS running your equipment: $(S / 250) \times 2.5 \times 10 = R$.
 - D. Use the following formula, Where S is the VA rating of a proposed UPS, and R is the resulting run time of the UPS running your equipment: $(S / 10) \times 1.5 \times 250 = R$.

4. You have a laptop computer which works fine when plugged in to a power supply. However, when the laptop is running off battery power, the unit runs for less than one hour. You check the documentation that came with the unit and find that the existing battery is capable of supplying power for up to three hours. What is the best way to get more life from the battery? Select the best answer.
- A. Replace the existing battery with one that can run longer.
 - B. Only run one application at a time when you are running on battery power.
 - C. When running the laptop on battery power first disable all unnecessary devices in the CMOS settings.
 - D. Configure the Power Option properties in the operating system for portable/laptop.

Chapter 2

1. Which of the following would you advise a laptop owner about regarding the rechargeable battery? Choose all that apply.
- A. Periodically check with the laptop or battery manufacturer to check for recall notices.
 - B. Periodically check the battery and look for any swelling or discoloration.
 - C. Storing the laptop in a hot car for an extended period of time is OK.
 - D. You can always replace one type of rechargeable battery with another.
2. A Human Resources staff member sends an urgent request for assistance. He indicates that he accidentally printed a document containing employee salaries and social security numbers to the wrong printer. Instead of printing to the HR printer, he mistakenly chose the PR printer, which is located in the Public Relations department in a different building on the campus. You check the print queues and find that the document is no longer there. How should you handle this situation? Select the best answer.
- A. Immediately send an email to the PR users group, asking if someone could retrieve and secure the document until you arrive, then go and get the document and bring it to HR. Then educate the user on how to set the HR printer as his default printer.
 - B. Immediately send a colleague to retrieve the document from the printer and return it to HR while you instruct the user on how to set his default printer to the HR printer.
 - C. Immediately contact the Director of Public Relations and the Senior Information Security Officer and inform them of the security breach. Ask the Director of Public Relations to retrieve and secure the document and await further instructions from the Security Officer. Then, inform the user on how to set their default printer to the HR printer.
 - D. Calmly reassure the user that you can help him solve his problem. Tell the user where the PR printer is so he can retrieve the document before anyone sees it. Then, inform the user how to set his default printer to the HR printer.

3. A user says she was unable to locate a file in the Sales folder on her Windows XP machine. She thinks the file may have been marked as hidden. The user asks what command she could use from the command line to see all the files in the folder, including those that have been hidden. What command should you tell the user to use? Select the best answer.
- A. `dir c:\Sales.`
 - B. `LS c:\Sales.`
 - C. `dir c:\Sales /p.`
 - D. `dir c:\Sales /a.`

Chapter 3

1. A user would like to increase the size of displayed fonts on visited Web pages and change how some of the colors appear. What would you tell them or what steps would you take to adjust this for them? Select the best answer.
- A. They cannot change how Web pages appear. It is controlled by the Web page developer.
 - B. Change the Accessibility options in their browser to ignore font colors and sizes specified on Web pages.
 - C. Use the Accessibility Options dialog box in Control Panel to make the requested changes.
 - D. Use the Fonts dialog box in Control Panel to make the requested changes.
 - E. Use the Settings tab in the Display dialog box in Control Panel to make the requested changes.
2. A user would like to dual boot between Mac OS X and Windows XP. Is this possible and why or why not? Select the best answer.
- A. No, these are completely different operating systems for completely different computer systems.
 - B. Yes, you can dual-boot Mac OS X with Windows XP regardless of the CPU so long as you have Boot Camp installed.
 - C. Yes, you can dual-boot Mac OS X with Windows XP if the CPU is made by Intel so long as you have Boot Camp installed.
 - D. Yes, you can dual-boot Mac OS X with Windows XP if the CPU is made by Motorola or IBM so long as you have Boot Camp installed.
3. A user has asked you to help her decrease the amount of time it takes her machine to boot. She observes that unless she manually chooses an option, the computer stays on the Multi-boot list of operating systems for an extended period of time before proceeding with the default selection. She would like to know where she can change the amount of time it waits before proceeding. In which TWO places could she change this setting? Select TWO answers.
- A. In the Startup Options applet in Control Panel.
 - B. In the Startup and Recovery Settings page under the Advanced tab of the System Properties.
 - C. In the `C:\NTLDR.inf` file.
 - D. In the `C:\boot.ini` file.

4. Listed below is a set of permissions available for a file stored on a Windows Server 2003 computer. Which permission is missing? Select the best answer.
- Modify
 - Read & Execute
 - Read
 - Write
- A. Supervisor.
- B. Execute.
- C. List contents.
- D. Full Control.
5. After installing a new device driver, a Windows 7 computer cannot successfully boot. It hangs at a gray screen, and the Welcome Screen never appears. You reboot and press F8 to access your recovery options. Which two options provide a viable solution (or access to a viable solution)?
- A. Choose Repair my computer. From there, choose System Restore.
- B. Choose Last Known Good.
- C. Choose Repair my computer. From there, choose Device Driver Rollback.
- D. Choose Automatically Fix Errors.
6. You have a brand new laptop computer with Windows 7 Ultimate installed. Which of the following would be appropriate security practices for you to follow when using this computer? Choose THREE.
- A. Always log on with a user account that has administrative privileges.
- B. Always log on with a user account that has limited user rights.
- C. Ensure that the option "Allow users to connect remotely to this computer" is enabled.
- D. Ensure that the file system is configured for NTFS.
- E. Disable the Guest account.
- F. Assign a complex password to the Guest account.

Chapter 4

1. A company has consulted with you to specify a network protocol for them to use. The company is a small business that has about 50 network devices (Windows), and plans to NOT exceed 100 any time soon. The network is one network, and is not split in any way. They want to be able to have the fastest possible network. Which protocol would you suggest for their PC network? Select the best answer.
- A. TCP/IP.
- B. NetBEUI.
- C. IPX/SPX.
- D. AppleTalk.

2. Which subnet mask would you use for a standard class B IP address? Select the best answer.
 - A. 255.0.0.0.
 - B. 255.255.0.0.
 - C. 255.255.255.0.
 - D. 255.255.255.255.

3. A user is unable to access the company intranet site by name, but is able to access web sites on the Internet by name. The user is able to access the intranet site using its IP address. Which of the following is most likely to be the problem? Select the best answer.
 - A. The user's DNS settings include only an external DNS server.
 - B. The user does not have WINS configured properly.
 - C. The user's Internet Explorer is not configured to bypass the Proxy Server for local addresses.
 - D. The company firewall is blocking access to the intranet server.

4. You need to know the current global wired adapter configuration for a given Windows 7 workstation. Which command would you issue to identify this configuration? Select the best answer.
 - A. Open a command prompt with administrator rights and issue netsh lan show interfaces.
 - B. Open a command prompt with administrator rights and issue netsh lan show profiles.
 - C. Open a command prompt with administrator rights and issue netsh lan show settings.
 - D. Open a command prompt with administrator rights and issue netsh lan show tracing.

5. A portion of Windows 7 core functionality permits support administration to resolve problems quickly via remote control and view over a networked desktop. What is at your disposal for this task? Select the best answer.
 - A. Use User Assistance.
 - B. Use Remote Assistance.
 - C. Use Windows NetBIOS.
 - D. Use Windows Remote Procedure Call.

Chapter 5

1. While working with a user, you notice she has written her password on a sticky note pressed against the display. Which of the following techniques will help prevent this security concern presenting itself in the future? Select the best answer.
 - A. Shortening the number of days before passwords expire.
 - B. Using server controls to enforce complex passwords, such as the use of special characters and minimum length.
 - C. Educate the user on the company's Information Security policy.
 - D. Educate the user on ways of concealing the written password more effectively, such as under the keyboard or on the bottom of the mouse pad.

2. The Windows Sidebar application takes up a good deal of space on small displays. Affected users usually disable it every time they log in, but want a more permanent solution. How do you prevent it from appearing after a restart? Select the best answer.
 - A. Right-click on the desktop and choose Personalize, and modify the display settings.
 - B. Right-click on Windows Sidebar or its icon and choose Close Sidebar.
 - C. Right-click on Windows Sidebar or its icon, choose Properties and uncheck the option Start Sidebar when Windows starts.
 - D. Right-click on Windows Sidebar or its icon, choose Properties and check the option Start Sidebar when Windows starts.

3. Many applications designed for Windows XP will work on Vista and others may run poorly or not at all. One end-user reports such issues with an existing business program. How can you configure his computer to run this application correctly? Select the best answer.
 - A. Start the Microsoft Application Compatibility toolkit.
 - B. Start the Program Compatibility Wizard.
 - C. Disable Windows Error Reporting for this application.
 - D. Disable Problem Reports and Solutions for this application.

Chapter 6

1. You are part of a network security team at the company where you work. What items would you include in a security event response plan? Choose all that apply.
 - A. In the event of a virus attack, unplug all computers from the network.
 - B. Train users to immediately shut down their machines in the event of a suspected virus attack.
 - C. Use a mock virus attack to test the response plan.
 - D. Include a follow-up process for after the security incident is resolved.
 - E. Include a follow-up process for after the security incident is discovered.

2. Which of the following statements are true about smart cards? Choose all that apply.
 - A. A smart card uses a magnetic stripe to store information.
 - B. Smart cards utilize a serial interface and receive power from the card reader.
 - C. Smart cards are very durable.
 - D. All smart cards include a set of contact points for connection to the card reader.
 - E. Smart cards can be used as credit cards, electronic cash, secure identification and secure computer access.

3. A user calls and asks for help in maintaining the operating efficiency of their hard drive. Which THREE tools of the following six listed would you suggest your user schedule to run automatically? Choose the best THREE answers.
- A. Have the user schedule the automatic synchronization of commonly visited websites.
 - B. Have the user schedule regular scan disk operations.
 - C. Have the user schedule regular defragment operations.
 - D. Have the user schedule automatic virus definition updates.
 - E. Have the user schedule automatic Windows updates.
 - F. Have the user schedule Outlook to automatically archive old emails.
4. When is it acceptable to refer a customer to your superior? Choose the best answer.
- A. It is never appropriate to send a customer to a superior; all problems should be handled by you and you alone.
 - B. If you cannot solve a problem, after exhausting all options, then you should transfer a customer to your superior.
 - C. When the customer has become abusive, insulting or otherwise incapable of being dealt with.
 - D. Any security-related problem should be directed to your superior.

Answers & Explanations

Chapter 1

1. ANSWER: C

Explanation A. Incorrect. While certainly a factor, the user's priority is portability, not capacity.

Explanation B. Incorrect. While this may be an important fact to take note of, portability is the highest priority.

Explanation C. Correct. Drives that are bus-powered tend to be designed specifically for notebook use. They do not require an extra power adapter to lug around and are often built in a smaller form factor for easier portability.

Explanation D. Incorrect. Other than OS support for a particular bus type such as Firewire, USB, or SCSI, There are no compatibility issues between operating systems and hard drives.

2. ANSWERS: B, D

Explanation A. Incorrect. SIMM and Rambus modules are always installed in pairs. DIMMS can be installed individually.

Explanation B. Correct. 240-pin DIMM modules are used for DDR2 SDRAM, 184-pin DIMM modules are used for DDR SDRAM, and 168-pin DIMM modules for EDO SDRAM.

Explanation C. Incorrect. DDR SDRAM memory modules do operate at 2.5v, but no DIMM modules operate at 4.3v.

Explanation D. Correct. It is common for manufacturers to fill all the memory slots with smaller capacity memory modules. This may alter your upgrade plan, as you will need to replace existing modules instead of merely adding additional ones.

3. ANSWER: A

Explanation A. Correct. First we divide the VA rating of the proposed UPS, for example 750VA, by the load it will be running (in this case 250VA). Then we take that ratio and multiply it by a variable multiplier. If the ratio was less than three, the multiplier is 1.3. If it was three or more, the multiplier is 1.5. Then we multiply that figure by the advertised run time of the proposed UPS (when running at its maximum load). This is typically about ten minutes. The resulting number is the estimated run time of the proposed UPS when running your equipment. So: $750/250=3$ Therefore, $3 \times 1.5 \times 10=45$ minutes.

Explanation B. Incorrect - The correct formula is $(S / 250) \times 1.5 \times 10 = R$ First we divide the VA rating of the proposed UPS, for example 750VA, by the load it will be running (in this case 250VA). Then we take that ratio and multiply it by a variable multiplier. If the ratio was less than three, the multiplier is 1.3. If it was three or more, the multiplier is 1.5. Then we multiply that figure by the advertised run time of the proposed UPS (when running at its maximum load). This is typically about ten minutes. The resulting number is the estimated run time of the proposed UPS when running your equipment. So: $750/250=3$ Therefore, $3 \times 1.5 \times 10=45$ minutes.

Explanation C. Incorrect - The correct formula is $(S / 250) \times 1.5 \times 10 = R$ First we divide the VA rating of the proposed UPS, for example 750VA, by the load it will be running (in this case 250VA). Then we take that ratio and multiply it by a variable multiplier. If the ratio was less than three, the multiplier is 1.3. If it was three or more, the multiplier is 1.5. Then we multiply that figure by the advertised run time of the proposed UPS (when running at its maximum load). This is typically about ten minutes. The resulting number is the estimated run time of the proposed UPS when running your equipment. So: $750/250=3$ Therefore, $3 \times 1.5 \times 10=45$ minutes.

Explanation D. Incorrect - The correct formula is $(S / 250) \times 1.5 \times 10 = R$ First we divide the VA rating of the proposed UPS, for example 750VA, by the load it will be running (in this case 250VA). Then we take that ratio and multiply it by a variable multiplier. If the ratio was less than three, the multiplier is 1.3. If it was three or more, the multiplier is 1.5. Then we multiply that figure by the advertised run time of the proposed UPS (when running at its maximum load). This is typically about ten minutes. The resulting number is the estimated run time of the proposed UPS when running your equipment. So: $750/250=3$ Therefore, $3 \times 1.5 \times 10=45$ minutes.

4. ANSWER: D

Explanation A. Incorrect. While this might resolve the problem, it is not the most cost effective way to do so. There are easier ways to resolve this problem without spending money.

Explanation B. Incorrect. Limiting the number of concurrently running applications will not enable the battery to last longer.

Explanation C. Incorrect. While this might help it is not the best solution to this problem. You would need to remember to run the CMOS setup each time you switch how you are using the laptop.

Explanation D. Correct. By using the Power Option properties in the operating system to power down the hard drive and other components when not in use you can extend the life of the battery.

Chapter 2

1. ANSWERS: A, B

Explanation A. Correct. Problems may occur in the manufacturing of the rechargeable battery that could possibly cause the battery to catch fire during use. It is important to check for recall notices.

Explanation B. Correct. Swelling or discoloration may be an indication of a serious problem with the battery. It should immediately be removed from the laptop and the manufacturer contacted.

Explanation C. Incorrect. Laptop batteries should not be exposed to high temperatures because they can easily rupture, ignite, or explode under those conditions.

Explanation D. Incorrect. NiCad, NiMH and Li-ion are all fundamentally different from one another and cannot be substituted unless the device has been pre-configured from the factory to accept more than one type of rechargeable battery. You should refer to the owner's manual to find out which rechargeable battery types a particular device supports.

2. ANSWER: C

Explanation A. Incorrect - This approach will result in the sensitive data being handled (and probably photocopied) by too many unauthorized staff members including yourself, in clear violation of any reasonable security policy.

Explanation B. Incorrect - Time is of the essence in this situation. The paper will probably be discovered by another staff member before your colleague can retrieve it. This approach will result in the sensitive data being handled (and probably photocopied) by too many unauthorized staff members including your colleague, in clear violation of any reasonable security policy.

Explanation C. Correct - In a scenario like this, the security breach takes priority over the user's issue and must be handled first. In most organizations, the computer support technician or field service technician would not be authorized to handle the situation directly. Therefore, informing appropriate management of the issue and taking reasonable immediate steps to mitigate further risk and exposure of the data is the best course of action. Additionally, you might consider suggesting that the printers be Troubleshooting, Repair and Maintenance 30 renamed to avoid similar mistakes in the future.

Explanation D. Incorrect - If he had printed a grocery list, then this approach would be appropriate. However, the information he printed constitutes a security breach if discovered by staff members who are not authorized to view such information. It must be handled in the same way as any other security breach in accordance with company policy. There is little point in reassuring the user that everything will be OK, as this wouldn't be entirely honest. You could reassure them that you will do everything you can to minimize the impact of their mistake and inform them as to what the process is in handling an issue like this.

3. ANSWER: D

Explanation A. Incorrect. This command will display the contents of the directory, but not show hidden or system folders, thus the file would not be visible.

Explanation B. Incorrect. LS is a UNIX command, not an MS-DOS command.

Explanation C. Incorrect. The /p switch causes dir to pause after each screen of output.

Explanation D. Correct. The /a switch causes dir to display all files, even those that are marked Hidden or System files.

Chapter 3

1. ANSWER: B

Explanation A. Incorrect. While there are many things that a Web page developer can do to control how their Web page is displayed, Internet Explorer and other browsers allow you to configure options that ignore both selected colors, font styles and font sizes that have been specified for a Web page.

Explanation B. Correct. Internet Explorer and other browsers allow you to configure options that ignore selected colors, font styles and font sizes that have been specified for a Web page.

Explanation C. Incorrect. The Accessibility Options dialog box in Control Panel does not specifically affect how Web pages are displayed. Accessibility Options controls such things as keyboard and mouse behavior, display options for system sounds, display options to make information easier to read, and other settings for special needs individuals.

Explanation D. Incorrect. The Fonts dialog box in Control Panel shows you what fonts are installed on your computer, enables you to install new fonts and print a sample of an installed font. It does not affect how Web pages are displayed.

Explanation E. Incorrect. While you can use this dialog box to increase or decrease the size of objects and text on your screen, it will affect all screen displays not just Web pages.

2. ANSWER: C

Explanation A. Incorrect. Apple's Boot Camp software allows an Intel-powered Macintosh to dual boot between Mac OS X and Windows XP.

Explanation B. Incorrect. With Boot Camp software from Apple you can dual boot with Windows XP only if the CPU is Intel.

Explanation C. Correct. Boot Camp lets you install Windows XP without moving your Mac data. Boot Camp will burn a CD of all the required drivers for Windows so you don't have to get them yourself. Once you've completed Boot Camp, simply hold down the option (alt) key at startup to choose between Mac OS X and Windows. Operating System and Software 32 Here are the requirements:

- Mac OS X
- The latest Firmware updates
- An Intel-based Mac
- Microsoft Windows XP, Service Pack 2, Home or Professional

Explanation D. Incorrect. No, you can only dual-boot Mac OS X with Windows XP if the CPU is made by Intel and you have Boot Camp installed.

3. ANSWERS: B, D

Explanation A. Incorrect. There is no Startup Options applet in Control Panel.

Explanation B. Correct. The Startup and Recovery Settings page includes an option to change the amount of time the system waits for user input while displaying the List of Operating systems. Setting this to 5 seconds is usually sufficient.

Explanation C. Incorrect. There is no such file.

Explanation D. Correct. The boot.ini file, which is a hidden system file, contains the configuration information. Although typically modified through the Startup and Recovery Settings page, it can be modified manually.

4. ANSWER: D

Explanation A. Incorrect. The Supervisor permission is associated with permissions on a Novell network.

Explanation B. Incorrect. The Execute permission is associated with the permissions on either a Novell Network or a Unix/Linux based network.

Explanation C. Incorrect. List contents is a permission found on a folder rather than on a file.

Explanation D. Correct. The full control permission grants the user or group full control over a file, if the user or group has not been denied permission at any upper level of the file system.

5. ANSWER: C

Explanation A. Incorrect. System Restore is an option from the Recovery Console, available by clicking Repair my computer. Use System Restore to choose a time before the problematic driver installation.

Explanation B. Incorrect. When a computer won't boot, choosing Last Known Good often works by letting Windows boot with the last configuration that worked.

Explanation C. Correct. A missing NTLDR error message means that the hard drive normally accessed for booting is not available or has some corruption. It may become "not available" if there is media placed in devices that could be used for booting, ie a floppy drive.

Explanation D. Incorrect. The usual cause of an NTLDR error message is an unbootable media in the floppy drive or in the CD/DVD drive.

6. ANSWERS: B, D, F

Explanation A. Incorrect. Although very convenient, you should only use an account with administrative rights when absolutely necessary. The best practice is to log on as an account with limited rights and use the `Run As` command option when you need to perform actions requiring administrative rights.

Explanation B. Correct. Logging on as a user with only limited rights is an excellent way to protect the computer. If you were to download a web site or open an e-mail attachment that contains malicious code, the infected code will have only limited rights to execute.

Explanation C. Incorrect. This option should be enabled only when absolutely necessary. If a hacker were to use this feature to connect to your computer, he would have full access to the system, just as if he were sitting in front of it.

Explanation D. Correct. The NTFS file system includes many important security features, such as folder and file level security and folder and file level encryption. With NTFS you can control which users and groups can read, write, modify, read and execute, or list folder contents. You can use NTFS to prevent all users, except for your user account, from viewing or changing your private information.

Explanation E. Incorrect. By default, the Guest account is disabled.

Explanation F. Correct. Although the Guest account is disabled by default, you should assign a complex password to the Guest account to prevent malicious code from activating the account and using it to gain access to the computer.

Chapter 4

1. ANSWER: B

Explanation A. Incorrect - The TCP/IP protocol has a lot of overhead and can be slow compared to other protocols.

Explanation B. Correct - NetBEUI is a very fast protocol with little overhead for use on small non-split networks or non-routed ones.

Explanation C. Incorrect - IPX/SPX is a protocol that has high overhead and therefore can be slow.

Explanation D. Incorrect - AppleTalk is a proprietary network protocol for use with Apple computers not Windows-based computers.

2. ANSWER: B

Explanation A. Incorrect. This is the standard subnet for a class A address.

Explanation B. Correct. This is the standard subnet for a class B address.

Explanation C. Incorrect. This is the standard subnet for a class C address.

Explanation D. Incorrect. This is not a subnet address. This address is used for a network broadcast.

3. ANSWER: A

Explanation A. Correct. Companies typically use an internal DNS server to resolve names of hosts on the internal network, and an upstream external DNS server (typically run by an Internet Service Provider) to resolve names on the Internet.

Explanation B. Incorrect. While WINS can be used by Windows machines to resolve the NetBIOS names of other hosts in a workgroup or domain, this aging functionality exists only for backward compatibility and is not likely to be used in most environments Networking 36 today.

Explanation C. Incorrect. If this setting were configured incorrectly, the user would not be able access the site by IP address. Also, Proxy server settings typically would not affect name resolution.

Explanation D. Incorrect. This is unlikely because the user can access the site by IP address.

4. ANSWER: C

Explanation A. Incorrect. This action will display a list of current and available wired interfaces.

Explanation B. Incorrect. This action will display a list of locally configured wired profiles.

Explanation C. Correct. This action will display the current global settings for the local area network.

Explanation D. Incorrect. This action will indicate whether wired tracing is enabled or disabled.

5. ANSWER: B

Explanation A. Incorrect. This is the Windows Vista version of the local help file, used to provide better search capabilities customized by local IT departments.

Explanation B. Correct. This application improves the economy of servicing Windows computers in remote or physically inaccessible locations.

Explanation C. Incorrect. This is a low-level network software interface that allows applications on different computers to communicate over a local connection.

Explanation D. Incorrect. This method of communication and control between remote computers does not directly lend administrative capability to Windows desktops.

Chapter 5

1. ANSWER: C

Explanation A. Incorrect. This will not change the fact that the user keeps her password in plain sight, just how often she writes a new one down.

Explanation B. Incorrect. Forcing the user to use a more complex password will end up with a result of simply having a different password on the sticky.

Explanation C. Correct. An Information Security policy will document proper password policy and the details of its enforcement. This policy should give clear instruction to users about the ramifications of keeping any written documentation of passwords, including the sticky not on the monitor.

Explanation D. Incorrect. There is no safe method of writing down a password to help in remembering it later. Once its written down, its just waiting to be discovered by someone who intends to use it for malicious purposes. Most attackers know every trick in the book when it comes to hiding a written password.

2. ANSWER: C

Explanation A. Incorrect. Each display has a maximum viewable resolution, but its configuration will not necessarily produce optimal desktop usability.

Explanation B. Incorrect. This will close the Windows Sidebar only to have it reappear in the next restart or log-in.

Explanation C. Correct. This will prevent the Sidebar application from reappearing after restarts.

Explanation D. Incorrect. This will enable the Sidebar application to reappear at each log-in.

3. ANSWER: B

Explanation A. Incorrect. This is a lifecycle management toolkit designed to identify compatibility issues for existing Windows applications; it is not included with Vista.

Explanation B. Correct. This operates the application in a compatibility mode by simulating an earlier version of Windows.

Explanation C. Incorrect. This feature is a set of feedback technologies designed to trap software crashes and optionally report failure conditions back to Microsoft.

Explanation D. Incorrect. This application feature identifies many software problems with probable causes and likely solutions, but does not fix hardware issues.

Chapter 6**1. ANSWERS: A, C, D**

Explanation A. Correct. By isolating the computers from the network you can help prevent the spread of the virus until it can be removed from the infected machine(s).

Explanation B. Incorrect. It would be better to train the users to unplug their network connection and notify their supervisor in the event of a suspected virus attack.

Explanation C. Correct. It is important to test a plan to see if it is effective. You may find that containment steps need to be adjusted or users need more training for the plan to be effective in the event of a real incident.

Explanation D. Correct. Follow-up is an important step in a security incident response plan. By reviewing what happened and why you can prevent similar future incidents.

Explanation E. Incorrect. Adding a process at this point would only succeed in slowing down the recovery process.

2. ANSWERS: B, E

Explanation A. Incorrect. Smart cards do not utilize magnetic stripes. Instead they are embedded with either a microprocessor and a memory chip or just a pre-programmed memory chip.

Explanation B. Correct. Smart cards do utilize a serial interface and they do receive power from the card reader. It's a very convenient feature.

Explanation C. Incorrect. Unfortunately, because the chip utilized by the smart card is embedded into a plastic card generally about the size of a credit card it is very vulnerable to bending and breaking.

Explanation D. Incorrect. There are two types of smart cards: those with contacts and those without contacts. Contactless smart cards utilize Radio Frequency Identification (RFID) for data transmission.

Explanation E. Correct. Smart cards have many uses. They are widely utilized in Europe. In the United States they are generally used to provide access to secure buildings or computer systems.

3. ANSWERS: B, C, F

Explanation A. Incorrect. This particular option is really only useful for computers that have intermittent connections to the Internet and has nothing to do with the operating efficiency of a hard disk drive. In fact, considering the user's concern, you should advise your customer NOT to enable synchronization.

Explanation B. Correct. Scan Disk can be used to check a hard drive for physical and logical errors in its structure. Windows can be set up to automatically perform this function. It is advised to configure Scan Disk to run while the computer is not in regular use.

Explanation C. Correct. Defragmentation, paired with Scan Disk, can go a long way toward preventing many of the common access speed problems associated with high-traffic computers. As with Scan Disk, Defrag should be scheduled during a computer's downtime.

Explanation D. Incorrect. While this is always a good thing to do, it has nothing to do with maintaining a hard drive's operational efficiency.

Explanation E. Incorrect. This is an excellent preventative maintenance action, but it has little to do with maintaining a hard disk.

Explanation F. Correct. Email inboxes can get cluttered quickly, and without the archiving option through Microsoft Outlook, they can eat away at both hard disk space and access times. Scheduling regular archive activities can help maintain the operating efficiency of hard disk drives.

4. ANSWER: C

Explanation A. Incorrect. There are some instances when you will not be able to handle a customer, especially one that has become irate or irritable as a result of a particularly difficult computer issue.

Explanation B. Incorrect. Really, you should be able to handle most computer issues on your own. However, in the case that an issue cannot be resolved over the phone, you should refer the customer to a desktop or on-site support team, not your manager.

Explanation C. Correct. Computer issues can be extremely disruptive to someone's day, and they tend to make end-users especially irate because they don't understand the equipment well enough to understand the problem. While you should be able to handle irate or angry customers, you should never take abuse or insults from a client. Your manager or superior will be trained to handle difficult customers like these.

Explanation D. Incorrect. Security related issues should actually be transferred to an Information Security department, if your company has one. If your company does not have an InfoSec department, then it's likely you support security-related issues, also!