Professor Messer's

CompTIA A+

220-902 Course Notes

http://www.ProfessorMesser.com

The 220-901 CompTIA A+ Exam

220-902 Exam Objectives

- 1.0 - Windows Operating Systems (29%)
- 2.0 - Other Operating Systems and Technologies (12%)
- 3.0 - Security (22%)
- 4.0 - Software Troubleshooting (24%)
- 5.0 - Operational Procedures (13%)

- Maximum of 90 questions
- Multiple choice and performance-based questions
- 90 minutes
- Passing score is 700 on a scale of 100-900
- Twelve months of hands-on experience recommended

Windows Vista

	Windows Vista Home Basic Minimum Requirements	Windows Vista Home Premium / Ultimate / Business / Enterprise Minimum Requirements
Processor	800 MHz	1 GHz
Memory	512 MB RAM	1 GB RAM
Hard drive size / Free space	20 GB / 15 GB	40 GB / 15 GB
Disk requirements	DVD-ROM Drive	DVD-ROM Drive
Video	32MB of graphics RAM	128MB of graphics RAM

Windows Vista Edition	Aero	Media Center	Domain Member	EFS	BitLocker	Maximum x86 RAM	Maximum x64 RAM
Home Basic	✖	✖	✖	✖	✖	4 GB	8 GB
Home Premium	✓	✓	✖	✖	✖	4 GB	16 GB
Business	✓	✖	✓	✓	✖	4 GB	128 GB
Enterprise	✓	✖	✓	✓	✓	4 GB	128 GB
Ultimate	✓	✓	✓	✓	✓	4 GB	128 GB

Windows 7

	Windows 7 Minimum Requirements (x86)	Windows 7 Minimum Requirements (x64)
Processor / CPU	1 GHz processor	
Memory	1 GB RAM	2 GB RAM
Free disk space	16 GB	20 GB
Video	DirectX 9 graphics device with WDDM 1.0 or higher driver	

Windows 7 Edition	DVD Playback	Aero	ICS	Domain Member	EFS	BitLocker	x86 RAM	x64 RAM
Starter	✖	✖	✖	✖	✖	✖	2 GB	N/A
Home Premium	✓	✓	✓	✖	✖	✖	4 GB	16 GB
Professional	✓	✓	✓	✓	✓	✖	4 GB	192 GB
Enterprise	✓	✓	✓	✓	✓	✓	4 GB	192 GB
Ultimate	✓	✓	✓	✓	✓	✓	4 GB	192 GB

Windows 8 and 8.1

	Windows 8/8.1 Minimum Requirements (x86)	Windows 8/8.1 Minimum Requirements (x64)
Processor / CPU	1 GHz processor with support for PAE, NX, and SSE2	
Memory	1 GB RAM	2 GB RAM
Free disk space	16 GB	20 GB
Video	Microsoft DirectX 9 graphics device with WDDM driver	

Windows 8/8.1 Edition	Windows Media Player	EFS	BitLocker	Domain Member	AppLocker	BranchCache	Max x86 RAM	Max x64 RAM
Core	✓	✖	✖	✖	✖	✖	4 GB	128 GB
Pro	✓	✓	✓	✓	✖	✖	4 GB	512 GB
Enterprise	✓	✓	✓	✓	✓	✓	4 GB	512 GB

Windows Features

32-bit vs. 64-bit

- Hardware drivers are specific to the OS version (32-bit / 64-bit)
- 32-bit OS cannot run 64-bit apps
- 64-bit OS can run both 32-bit and 64-bit apps

Windows Aero

- Windows Vista and Windows 7 graphical enhancements
- Requires 1 GHz processor,
- 1 GB of RAM, and
- 128 MB graphics card

UAC (User Account Control)

- Limit software access
- Requires apps to have administrator permissions
- Secure Desktop limits automated access

BitLocker

- Encrypt an entire volume
- Windows Vista and Windows 7 Ultimate and Enterprise
- Windows 8 - Pro and Enterprise

Volume Shadow Copy

- Volume Snapshot Service (VSS), Volume Shadow Copy Service
- Backup entire volumes while Windows is running
- Provides the "Previous Versions" tab

System Restore

- Creates restore points
- Go back-in-time to correct problems
- All Programs / Accessories / System Tools / System Restore

Version 0x06

Windows Features (continued)

Sidebar and Gadgets
- Windows Vista Sidebar
- Gadgets go anywhere in Windows 7
- Gadgets have been discontinued, not available in Windows 8

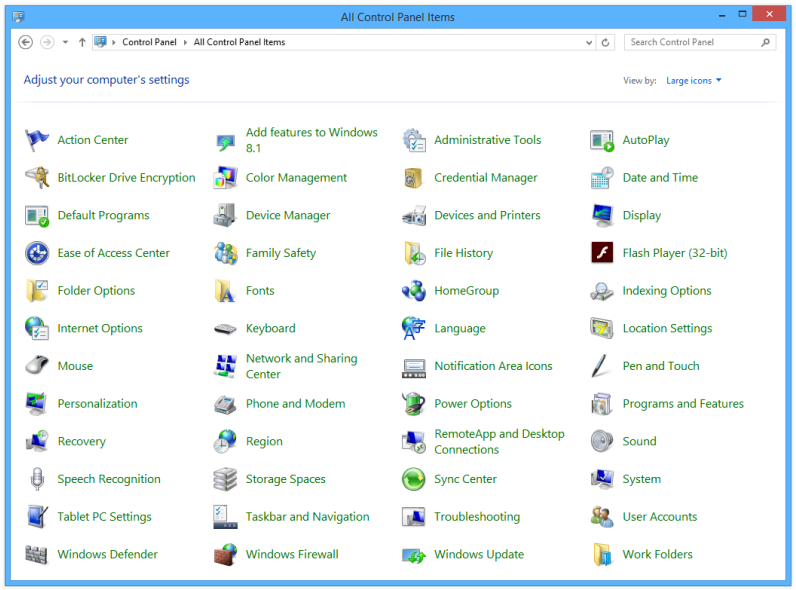
ReadyBoost
- Windows Vista, 7, and 8/8.1
- Uses USB, SD card, CompactFlash, etc.
- Cache to RAM instead of disk

Compatibility mode
- Run an application as an old OS
- Your OS emulates another OS - run your outdated applications
- Configured per-application - properties of the executable

Windows XP Mode (XPM)
- Windows Virtual PC on Windows 7
- Not supported in Windows 8/8.1
- Runs Windows XP Service Pack 3, integrates into the OS

Windows Easy Transfer
- Migrate files and settings from Windows XP, Windows Vista, Windows 7, and Windows 8/8.1
- Supports both side-by-side and wipe-and-load
- Limited functionality in Windows 8.1

Control Panel Classic View



Administrative Tools
- Control Panel / Administrative Tools
- Not exclusive to admins
- Computer Management, Services, Memory Diagnostic, etc.

Windows Defender
- Real-time anti-malware
- Included with Vista and 7 - Includes Anti-virus in Windows 8/8.1
- Updated by Microsoft Security Essentials in Windows Vista/7

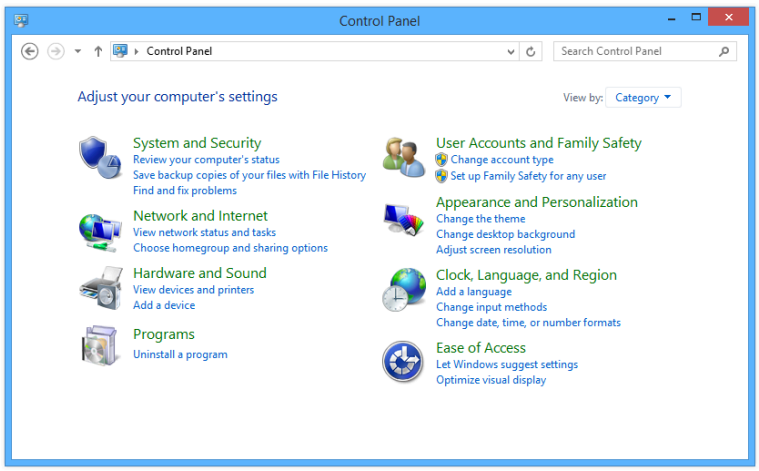
Windows Firewall
- Allow or disallow traffic - protect from attacks
- Control Panel / Windows Firewall

Security Center
- Windows Vista - "Action Center" in Windows 7 and 8/8.1
- Central security overview - Anti-virus, Anti-spyware, updates, etc.

Event Viewer
- Central event consolidation
- Application, Security, Setup, System
- Information, Warning, Error, Critical, Successful Audit, Failure Audit

Previous file versions
- Restore a previous file version - Maintained automatically by the OS
- Windows Vista and 7
  - Created by Windows Backup or as part of restore point
- Windows 8/8.1 - File History
  - Requires a separate drive for the backups

Control Panel Category View

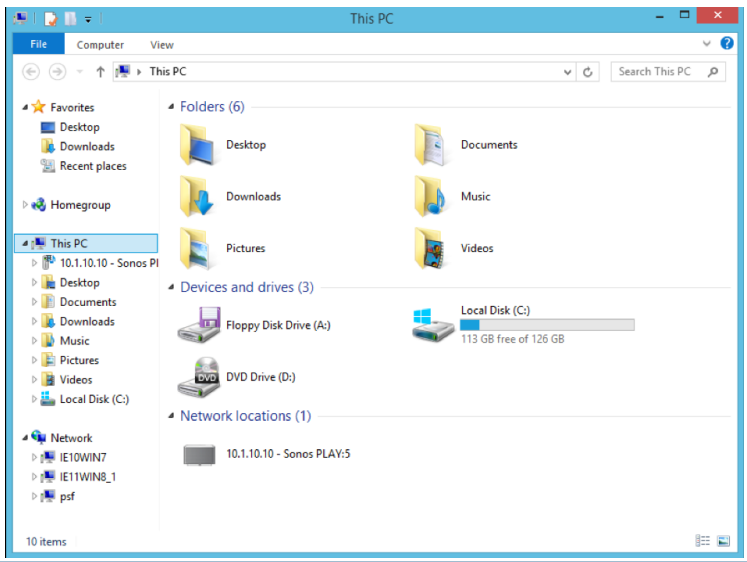


Windows File Structures and Paths

Storage Device Naming
- Every volume has a letter
- Common assignments
  - A: - Floppy drive
  - C: - Primary hard drive
  - D: - CD-ROM or DVD-ROM

Files and folders
- Folders can contain files, just like a real folder
- Folders can contain other folders, not usually like a real folder
- Folder names are separated with a backslash \
  - C:\Users\Professor\Documents\Budget.xls

Windows folders
- C:\Users - User documents
- C:\Program Files - All of the applications
- C:\Windows - The operating system



Windows 8 and 8.1 Features

Side by side apps
- Two apps on one screen
- Drag from the top edge and place on one side
- Windows + Left Arrow or Windows + Right Arrow

Modern UI
- Microsoft's common user interface
- Formerly known as the Metro UI
- A combination of typeface, graphical style, and animation

Pinning
- Put application icons on the task bar for quick and easy access
- Available in Windows 7 and Windows 8/8.1
- Right-click application and "Pin this program to taskbar"
- Or touch and hold and "Pin to taskbar" in Windows 8/8.1

Microsoft OneDrive
- Formerly known as SkyDrive or Live Folders
- Sync files in the cloud - store pictures, Office 365 documents
- Integrated with Windows 8/8.1

Windows store
- Curated list of Windows apps
- Central point for Modern UI apps
- Sales pages for independent developers

Multi-monitor taskbars
- Separate monitors can have different taskbar settings
- Define where taskbar buttons are shown
- Define how buttons are combined

Charms
- Shortcuts available at any time - Search, share, settings, etc.
- Use keyboard, mouse, or touch
  - Windows + C
  - Mouse on bottom or top right corner
  - Swipe from right edge towards the center

Start screen
- Tiled set of applications - The Modern UI
- Dynamic information without launching individual applications

PowerShell
- Command line for system administrators
- Extend command-line functions with cmdlets (command-lets)
- Automate and integrate system administration

Microsoft account sign-in
- Use a centralized Microsoft account instead of a local account
- Automate and syncrhonize many OS functions

Windows Upgrade Paths

Upgrading to Windows Vista
- Upgrade from Windows XP
- Keep Windows settings, personal files, and applications
- Must upgrade to a similar Edition

	Vista Home Basic	Vista Home Premium	Vista Business	Vista Ultimate
Windows XP Home	Upgrade	Upgrade	Upgrade	Upgrade
Windows XP Professional	Install	Install	Upgrade	Upgrade
Windows XP Media Center	Install	Upgrade	Install	Upgrade

Upgrading to Windows 7
- Upgrade from Windows Vista
- No in-place upgrade available from Windows XP to Windows 7
- Must upgrade to a similar Edition

	Windows 7 Starter	Windows 7 Home Basic	Windows 7 Home Premium	Windows 7 Professional	Windows 7 Ultimate	Windows 7 Enterprise
Windows XP - All Editions	Install	Install	Install	Install	Install	Install
Windows Vista Home Basic	Install	Upgrade	Upgrade	Install	Upgrade	Install
Windows Vista Home Premium	Install	Install	Upgrade	Install	Upgrade	Install
Windows Vista Business	Install	Install	Install	Upgrade	Upgrade	Upgrade
Windows Vista Ultimate	Install	Install	Install	Install	Upgrade	Install
Windows Vista Enterprise	Install	Install	Install	Install	Install	Upgrade

Upgrading to Windows 8
- Upgrade from Windows 7
- No in-place upgrade available from Windows XP or Windows Vista to Windows 8
- Must upgrade to a similar Edition

	Windows 8 Core	Windows 8 Pro	Windows 8 Enterprise
Windows 7 Starter	Upgrade	Upgrade	Install
Windows 7 Home Basic	Upgrade	Upgrade	Install
Windows 7 Home Premium	Upgrade	Upgrade	Install
Windows 7 Professional	Install	Upgrade	Upgrade
Windows 7 Ultimate	Install	Upgrade	Install
Windows 7 Enterprise	Install	Install	Upgrade

Windows Upgrade Paths (continued)

Upgrading to Windows 8.1
- Upgrade from Windows 7
- No in-place upgrade available from Windows XP, Windows Vista or Windows 7 to Windows 8.1
- Must upgrade to a similar Edition

	Windows 8.1 Core	Windows 8.1 Pro	Windows 8.1 Enteprise
Windows 8 Core	Upgrade	Upgrade	Install
Windows 8 Pro	Install	Upgrade	Upgrade
Windows 8 Enterprise	Install	Install	Upgrade
Windows 8.1 Core		Upgrade	Install
Windows 8.1 Pro			Upgrade

Planning a Windows Installation

Installation Sources
- Bootable USB - Computer must support booting from USB
- CD-ROM and DVD-ROM
- PXE ("Pixie")- Preboot eXecution Environment
- NetBoot - Apple technology to boot Macs from the network
- Solid state drives / hard drives - Store many OS installation files
- External / hot swappable drive - Boot from USB
- Internal hard drive - Install and boot from separate drive

Types of installations
- In-place upgrade - Maintain existing applications and data
- Clean install - Wipe the slate clean and reinstall
- Image - Deploy an clone on every computer
- Unattended installation - Answer questions in a file (unattend.xml)

Other installation types
- Repair installation - Fix problems with the OS
- Multiboot - Pick from two or more operating systems from a single installation media
- Recovery partition - Hidden partition with installation files
- Refresh / restore - Windows 8 feature to clean things up

MBR (Master Boot Record) partition style
- Maximum of four primary partitions per hard disk
- One of the primary partitions can be marked as Active
- Extended partitions increase the maximum number of partitions
- Logical partitions inside an extended partition are not bootable

GPT (GUID Partition Table) partition style
- The latest partition format standard - Requires a UEFI BIOS
- Can have up to 128 primary partitions
- No need for extended partitions or logical drives

Disk partitioning
- The first step when preparing disks
- An MBR-style hard disk can have up to four partitions
- GUID partition tables support up to 128 partitions

FAT - File Allocation Table file system
- One of the first PC-based file systems (circa 1980)
- FAT32 - Native support in Windows 2000 and newer
  - Larger (2 terabyte) volume sizes
  - Maximum file size of 4 gigabytes
- exFAT - Extended File Allocation Table
  - Microsoft flash drive file system
  - Files can be larger than 4 gigabytes

NTFS (NT File System) and CDFS (Compact Disk File System)
- NTFS is included with Windows NT, 2000, XP, Server 2003, Server 2008, Vista, 7, 8, 8.1
- Provides quotas, file compression, encryption, symbolic links, large file support, security, recoverability

CDFS (Compact Disk File System)
- Read data from a CD-ROM
- CDFS is an ISO 9660 international standard

Other file systems
- ext3 - Third extended file system - Commonly used by Linux OS
- ext4 - Fourth extended file system - An update to ext3
- NFS - Network File System
  - Access files across the network as if they were local

Basic disk storage
- Available in DOS and Windows versions
- Primary/extended partitions, logical drives
- Basic disk partitions can't span separate physical disks

Dynamic disk storage
- Span multiple disks to create a large volume
- Split data across physical disks (striping)
- Duplicate data across physical disks (mirroring)

Quick format vs. full Format
- Quick format in Windows Vista, 7, and 8/8.1
- Quick format creates a new file table - Data is not erased
- Full format fully erases data from the drive - Checks sectors

Other installation considerations
- Load alternate third party drivers when necessary
- Decide on Workgroup vs. Domain setup - Home vs. business
- Time/date/region/language settings
- Driver installation, software and windows updates
- Install a factory recovery partition

OS Command Line Tools

diskpart – Disk Partitioner
- Replaces the Pre-Windows-XP FDISK command

format - Format a disk
- Prepare a disk for use by the operating system

chkdsk - Check Disk
- `chkdsk /f` - Fixes logical errors on the disk
- `chkdsk /r` - Locates bad sectors, recovers information

md, cd, rd
- `md` - Make directory
- `cd` - Change directory
- `rd` - Remove directory

dir - Directory listing
- List files and directories

del - Delete
- Remove a file from a directory or disk
- `del names`

copy - Duplicate files
- `copy /v` - Verifies that new files are written correctly
- `copy /y` - Suppresses overwrite prompts

xcopy - Extended copy
- Copies multiple files and directory trees
- `xcopy source [destination]`

robocopy - Robust copy
- Functionally replaces xcopy
- Designed to handle NTFS file system details

tasklist - Task List
- Displays a list of currently running processes
- Local or remote device

taskkill - Task Kill
- Terminate tasks by process id (PID) or image name

sfc - System File Checker
- `sfc /scannow` - Run the check
- Scan integrity of all protected system files

shutdown
- Shutdown a computer

extract - Remove files from a Windows cabinet file
- `/d` - Display files in a cabinet
- > `extract /d <cabinetname>`
- `/a` - Extract a file
- > `extract /a <cabinetname> filename`

gpupdate - Force a Group Policy update
- `gpupdate /target:{computer|user} /force`

gpresult - Verify policy settings for a computer or user
- `gpresult /user [domain/]user`

The Windows Recovery Environment Command Prompt

Starting the Console
- Windows Vista - System Recovery Options / Command Prompt
- Windows 7 - System Recovery Options / Command Prompt
- Windows 8/8.1 - Troubleshoot / Advanced Options / Command Prompt

Fixing the Master Boot Record (MBR)
- Fix the Master Boot Record on a physical drive
- `BOOTREC /FixMbr`

Fixing the Volume Boot Record
- Writes a new boot sector
- `BOOTREC /FixBoot`

Rebuilding the Boot Configuration Data
- Creates a new Boot Configuration Data store
- `BOOTREC /RebuildBcd`

Windows Administrative Tools

Computer Management
- A pre-built Microsoft Management Console

Device Manager
- View the status of all device drivers
- Enable and disable hardware devices

Users and Groups
- Manage access to the operating system
- Administrators and Guest users

Local Security Policy
- Administration of security rules
- Password policy, account lockout policy, etc.

Performance Monitor
- Gather long-term statistics
- Set alerts, store statistics

Windows Services
- Manage background processes
- Start, stop, manage automatic start
- Start with services.msc

Task Scheduler
- Schedule an application or batch file

Component Services
- Device COM+ Management, Event Viewer, Services

ODBC Data Sources
- Administer ODBC drivers and connectivity

Print Management
- Manage printers from one central console

Memory Diagnostics
- Perform a hardware check of your RAM
- Included with Windows Vista and 7

Windows Firewall with Advanced Security

Windows Firewall
- Integrated into the operating system
- Control Panel / Windows Firewall

Windows Firewall with Advanced Security
- Click “Advanced settings”

Advanced Security features
- Inbound rules
- Outbound rules
- Connection security rules
- Granular - Program, port, predefined services, custom
- Custom - Program, protocol/port, scope, action, profile

Using Windows System Configuration (msconfig)

System Configuration
- Manage boot processes, startup, services, etc.
- Control Panel / Administrative Tools - `msconfig.exe`

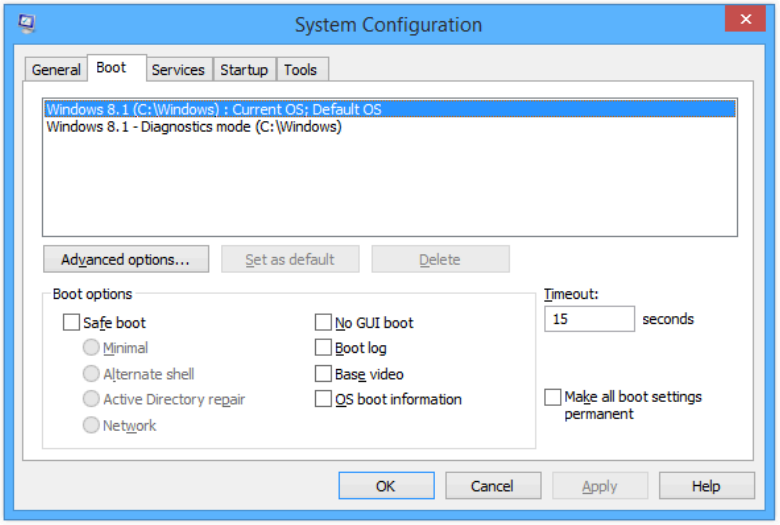
General tab
- Control the startup process - Normal, Diagnostic, Selective

Boot tab
- Control the boot location
- Advanced options - Number of processors, maximum memory, etc.
- Boot options - Safe boot, GUI, create a log file, base video

Services tab
- Enable and disable Windows services
- Determine what starts during boot

Startup tab
- Manage which programs start with a Windows login
- Has moved to the Task Manager in Windows 8/8.1

Tools tab
- Easy access to popular administrative tools
- UAC settings, System Information, Computer Management, etc.



Using Windows Task Manager

Task Manager
- Ctrl-Alt-Del, select Task manager
- Right mouse click the taskbar and select Task Manager
- Ctrl-Shift-Esc

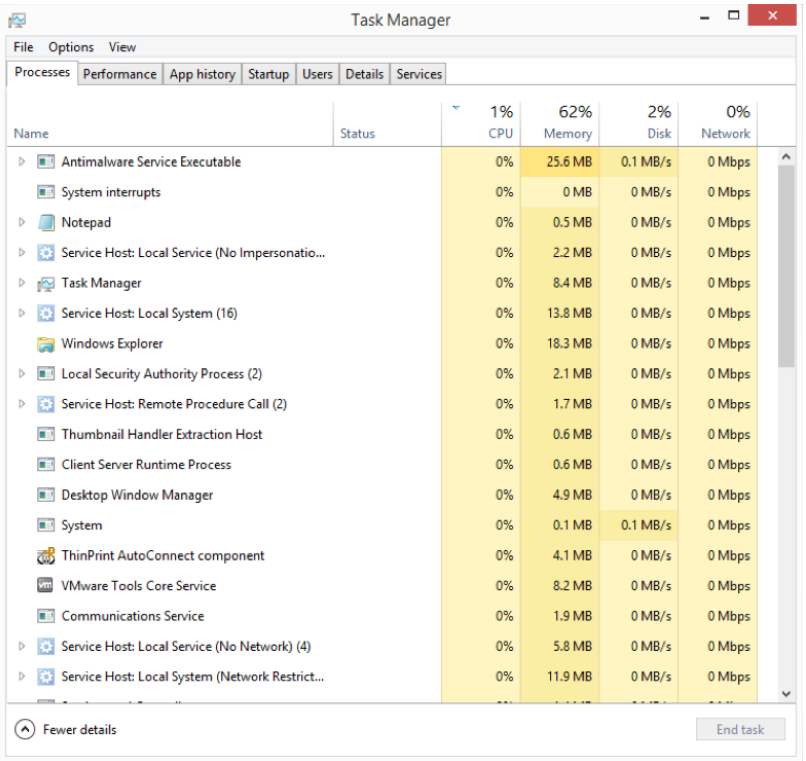
Applications tab
- Lists user-interactive applications in use
- Administratively control apps - End task, start new task
- Combined with the Processes tab in Windows 8/8.1

Processes tab
- View all running processes - Interactive and system tray apps
- View services and processes from other accounts
- Windows 8/8.1 combines all apps, processes, and services into a single tab

Performance tab
- View CPU, memory, etc.
- Real-time and historical statistical views
- Windows 8/8.1 includes CPU, memory, disk, Bluetooth, and network in the Performance tab

Networking tab
- Network performance
- Separate tab in Windows 7
- Integrated into the Performance tab in Windows 8/8.1

Users tab
- Who is connected? What are they doing?
- Windows 7 - User list, disconnect, logoff, send message
- Windows 8 - Separate processes, performance statistics



Using Windows Disk Management

Disk Management
- Computer Management - Storage / Disk Management

Disk status
- Healthy - The volume is working normally
- Healthy (At Risk) - The volume has experienced I/O errors
- Initializing - Normal startup message
- Failed - Cannot be started automatically - Damaged disk
- Failed redundancy - A drive has failed in a RAID 1 or RAID 5 array
- Resynching - Mirrored (RAID 1) volume is synching data
- Regenerating - RAID 5 volume is recreating the data

Storage Spaces
- Storage for data centers, cloud infrastructures
- Multiple tiers, administrative control
- Storage pool - A group of storage drives
  - Combine different storage devices into a single pool
- Storage space
  - Allocate virtual disks from available space in the pool
  - Includes options for mirroring and parity
  - Hot spare availability

Windows Migration Tools

Disk Windows Upgrade Advisor
- Check your system for upgrade compatibility to Windows 7
- Called "Upgrade Assistant" in Windows 8/8.1

Migration methods
- Side-by-side - Move information from one PC to the other
- Wipe-and-load - Export data, nuke and install, and import
- Windows 8/8.1 relies on syncing to the OneDrive cloud

Windows Easy Transfer
- Migrate from Windows XP, Windows Vista, Windows 7, or Windows 8/8.1
- Not always a direct path between versions
  - You can Easy Transfer from Windows XP to 8, but not from Windows XP to 8.1
- Accounts, documents, application settings, videos, pictures, etc.
  - Does not transfer applications
- Supports both side-by-side and wipe-and-load

User State Migration Tool
- Migrate between Windows versions from the command line
- Source: Windows XP, Windows Vista, Windows 7, Windows 8/8.1
- Destination: Windows Vista, Windows 7, and Windows 8/8.1
- Included with the Windows Automated Installation Kit (AIK)
- Very scalable - Built for large enterprises
- `ScanState` - Compiles and stores the migration data
- `LoadState` - Loads profile onto the destination computer

The Windows Control Panel

Internet Options
- Windows browser and proxy configuration

Display
- Resolution options, text size

User Accounts
- Local user account names and types

Folder Options
- Manage Windows Explorer options

System
- Computer information - Including version and edition
- Performance - Virtual memory settings
- Remote settings - Remote Assistance and Remote Desktop
- System protection - System Restore,select drives

Windows Firewall
- Control network access, protect from attacks

Power Options
- Manage power use, especially on laptops
- Display, storage devices, hibernation options

Programs and features
- Install and Uninstall applications and Windows features

HomeGroup
- Easily share information in Windows 7 / Windows 8 (no Vista)

Devices and Printers
- Everything on the network - Desktops, laptops, printers, etc.

Sound
- Set levels for output and input

Troubleshooting
- Automate some of the most common fixes

Network and Sharing Center
- All network adapters and adapter configurations

Device Manager
- Manage devices - Add, remove, disable and troubleshoot

Windows System Utilities

`regedit` - Registry editor
- Large master database
- Used by the kernel, drivers, services
- Can be used to backup and restore parts of the registry (hives)

`services.msc` - Windows Services
- Control Panel / Administrative Tools / Services
- Control background applications
- Services can reveal dependencies between applications

`mmc` - Microsoft Management Console
- Build your own management framework
- Choose from a list of snap-ins
- The mmc framework is used by many built-in tools

`mstsc` - Microsoft Terminal Services Client
- Remote Desktop Connection
- Access a desktop on another computer
- Commonly used to manage "headless" servers

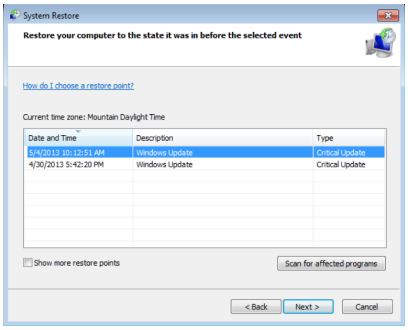
`notepad` - Windows text editor and viewer
- View and edit text files
- Included with all Windows versions

`explorer`
- Windows Explorer - File management
- View, copy, launch files

`msinfo32` - Windows System Information
- Hardware resources - Memory, DMA, IRQs
- Components - Multimedia, input, network
- Software environment - Drivers, print jobs

`dxdiag` - DirectX Diagnostic Tools
- Manage your DirectX installation
- Multimedia API
- Generic diagnostic tool for audio and video

`defrag` - Disk defragmentation
- Moves file fragments so they are contiguous
- Not necessary for solid state drives
- Graphical version in the drive properties



System Restore
- Creates frequent restore points
- F8 - Advanced Boot Options - Repair
- Vista: All Programs / Accessories / System Tools / System Restore
- Windows 7/8/8.1: Control Panel / Recovery

Windows Update
- Keep your OS up to date - Security patches, bug fixes
- Automatic installation - Updates are always installed
- Download but wait for install - You control the time
- Check but don't download - Save bandwidth
- Never check - Don't do this

Windows HomeGroup, Workgroups, and Domains

Windows Workgroups
- Logical groups of network devices
- Each device is a standalone system, everyone is a peer
- Single subnet

Windows HomeGroup
- Share files, photos, video, etc. between all devices
- Works on a single private network only

Windows Domain
- Business network
- Centralized authentication and device access
- Supports thousands of devices across multiple networks

Configuring Windows Firewall

Enabling and disabling Windows Firewall
- Your firewall should always be enabled (unless troubleshooting)
- Temporarily disable from the main screen
- Different settings for each network type - Public / Private

Windows Firewall configuration
- Block all incoming connections - Ignores your exception list
- Modify notification - App blocking

Creating a firewall exception
- Allow an app or feature through Windows Firewall
- Port number - Block or allow
- Predefined exceptions - List of common exceptions
- Custom rule - Every firewall option

Windows IP Address Configuration

How Windows gets an IP address
- DHCP (Dynamic Host Configuration Protocol)
  - Automatic IP addressing - This is the default
- APIPA (Automatic Private IP Addressing)
  - There's no static address or DHCP server
  - Communicate on the local network - No Internet connectivity
  - Assigns 169.254.1.0 to 169.254.254.255 - link local address
- Static address
  - Assign all IP address parameters manually
  - You need to know very specific details

TCP/IP host addresses
- IP Address – Unique identifier
- Subnet mask – Identifies the subnet
- Gateway – The route off the subnet to the rest of the world
- DNS – Domain Name Services - Converts names to IP addresses
- DHCP – Dynamic Host Configuration Protocol
- Loopback address - 127.0.0.1 - It's always there!

Windows Network Connections

Network setup
- Control Panel - Network and Sharing Center
- Set up a new connection or network

VPN connections
- Built-in VPN client - Included with Windows
- Integrate a smart card - Multi-factor authentication
- Connect from the network status icon

Dialup connections
- Modem connection over standard phone lines
- Configuration - Authentication and phone number
- Connect / Disconnect from the network status icon

Wireless connections
- Network name - SSID (Service Set Identification)
- Security type - Encryption method
- Encryption type - TKIP, AES
- Security key - WPA2-Personal or WPA2-Enterprise

Wired connections
- Ethernet cable - Direct connection
- Fastest connection is the default - Ethernet, Wireless, WWAN
- Alternate configurations - Use when DHCP isn't available

WWAN connections
- Wireless Wide Area Network - Built-in mobile technology
- Hardware adapter - Antenna connections
- Requires third-party software - Each provider is different

Windows Network Connections

Speed and Duplex
- Auto-negotiation isn't always foolproof
- Both sides of the link must match

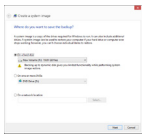
Wake on LAN
- Computer sleeps until needed
- Designed for late-night updates

Quality of Service (QoS)
- Prioritize network traffic
- Applications, VoIP, video
- Infrastructure must support QoS
- DSCP (Differentiated Services Code Points)
- Manage through Local Computer Policy

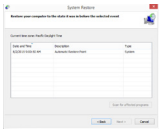
BIOS settings
- Enable/disable network adapters

Windows Preventive Maintenance Tools

Windows Backup
- Backup and restore individual files
- Windows Vista
  - Control Panel / Backup and Restore Center
- Windows 7
  - Control Panel / Backup and Restore



Recovery image
- Use images for system recovery
- Windows Vista / 7
  - Control Panel / Backup and Restore Center
- Windows 8 / 8.1
  - Control Panel / File History / System Image Backup



System Restore
- Creates frequent restore points
- F8 - Advanced Boot Options - Repair
- Windows Vista/7/8/8.1: Control Panel / System /
- Advanced System Settings / System Protection tab
- Doesn't guarantee recovery from malware

Disk maintenance utilities
- Drive properties - Tools tab
- Error-checking - Check Disk
- Defragmentation - Make files contiguous
- Backup - Available in Windows Vista and 7

Windows Preventive Maintenance Best Practices

Scheduled backups
- Regularly scheduled backups - Hourly, daily, weekly
- Determine what to backup - All files, changed files, image all
- Onsite and offsite - Or in the cloud with OneDrive

Scheduled disk maintenance
- Avoid hardware failure - Look for warning signs
- S.M.A.R.T. - Self-Monitoring, Analysis, and Reporting Technology
- Logical and physical disk check - Error-checking (chkdsk)

Scheduled defragmentation
- Moves file fragments so they are contiguous
- Graphical version in the drive properties, command line: defrag
- Control Panel / Administrative Tools / Task Scheduler

Windows updates
- Keep the operating system updated
- Security patches, new features, driver updates
- Download and install, download only, notify only, or disable

Patch management
- A well-documented process
- Not every update can be a good thing
- Many different patches
  - Operating system, applications, device drivers
- The process - Testing, scheduling, implementing, fallback

Driver/firmware updates
- Some drivers are updated more often than others
- Many drivers updated through Windows Update
- Use Device Manager to manage updates

Antivirus updates
- The bad guys are good at this - Keep your signatures updated!
- Daily schedule or hourly checks - May already be automatic
- Updates are usually managed in the antivirus user interface
- Large organizations will update from a central internal server

Best Practices for Mac OS

Scheduled backups
- Time Machine - Included with Mac OS X
- Hourly, daily, and weekly backups
- Starts deleting oldest information when disk is full

Scheduled disk maintenance
- Disk Utility - Built-in disk maintenance
- Rarely needed - No ongoing maintenance required
- Run “Verify disk” - Every few months

System updates / App store
- Centralized updates for both OS and apps
- App Store application - choose the “Updates” option
- Automatic updates or manual install
- Patch management - Install and view previous updates

Driver/firmware updates
- Almost invisible in Mac OS X - Designed to be that way
- System Information utility - Shows a detailed hardware list
- View only - No changes to settings by design

Anti-virus/Anti-malware updates
- OS X does not include anti-virus or anti-malware
- There are many 3rd-party options from the usual companies
- Automate your signature updates - New updates every hour / day

Best Practices for Linux

Scheduled backups
- tar - Tape Archive
- rsync - Sync files between storage devices

Scheduled disk maintenance
- Check file system - File systems can’t be mounted
  - Done automatically every X number of reboots
  - Force after reboot by adding a file to the root
  - `sudo touch /forcefsck`
- Clean up log space in `/var/log`

System updates
- Command line tools - apt-get, yum
- Graphical update managers - Software updater
- Patch management - Updates can be scheduled
- Software center - The Linux “App Store”

Driver/firmware updates
- Many drivers are in the kernel - updated when the kernel updates
- Drivers are managed with software updates or at the command line

Anti-virus/Anti-malware updates
- Relatively few viruses and malware for Linux
- ClamAV - Open source antivirus engine
- Same best practice as any other OS
- Always update signature database
- Always provide on-demand scanning

Mac OS Tools

Time Machine backups
- Automatic and easy to use - Familiar Finder UI
- Dates along the right side - Files in the middle
- Mac OS takes snapshots if the Time Machine storage isn’t available
- You can restore from the snapshot

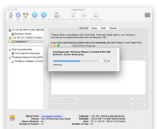
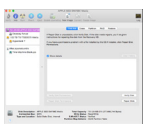
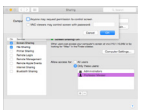


Image recovery
- Build a disk image in Disk Utility
- Creates an Apple Disk Image (.dmg) file
- Mount on any Mac OS X system
- Appears as a normal file system
- Use the restore feature in Disk utility

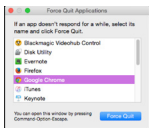


Disk Utility
- Manage disks and images
- Verify and repair file systems, erase disks, modify partition details, manage RAID arrays, etc.
- Create, convert, and resize images

Terminal
- Command line access to the operating system
- Manage the OS without a graphical interface
- Run scripts, manage files
- Configure OS and application settings



Screen sharing
- Integrated into the operating system
- Can also be viewed with VNC
- Available devices appear in the Finder



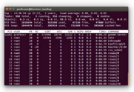
Force Quit
- Stop an application from executing
- Command-Option-Esc - List application to quit
- Hold the option key when right-clicking the app icon in the dock - Choose Force Quit

Linux Tools

Backups
- May be built-in to the Linux distribution
- Backup and restore with scheduling
- Command-line options - `rsync`

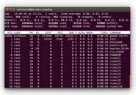
Image recovery
- Not as many options as Windows
- dd is built-in to Linux (and very powerful)
- Other 3rd-party utilities - can image drives
  - GNU Parted, Clonezilla

Disk maintenance
- Linux doesn't require a lot of maintenance
- Clean up log space - All logs are stored in /var/log
- File system check - done automatically every X number of reboots



Terminal
- Command line access to the Linux OS
- Run scripts, manage files
- Configure OS and application settings

Screen sharing
- Many options, like most of Linux
- May be included with your distribution
- UltraVNC, Remmina



Closing programs
- Use terminal - sudo for proper permissions
- `sudo killall firefox`
- Graphical kill - `kill <pid>`

Mac OS Features

Mission Control and Spaces
- Quickly view everything that's running
- Spaces - Multiple desktops
- Add Spaces inside of Mission Control

Keychain
- Password management - Passwords, notes, certificates, etc.
- Integrated into the OS - Keychain Access
- Passwords and Secure Notes are encrypted with 3DES
- Login password is the key

Spotlight
- Find files, apps, images, etc. - Similar to Windows search
- Magnifying glass in upper right or press Command-Space
- Type anything in, see what you find
- Define search categories in System Preferences / Spotlight

iCloud
- Integrates Apple technologies - Mac OS, iOS
- Share across systems - Calendars, documents, contacts, etc.
- Backup iOS devices - Never lose data again
- Store files in an iCloud drive - Similar to Google Drive, Dropbox

Gestures
- Extend the capabilities of your trackpad
- Use one, two, three fingers - Swipe, pinch, click
- Customization - Enable/disable

Gestures
- Extend the capabilities of your trackpad
- Use one, two, three fingers - Swipe, pinch, click
- Customization - Enable/disable

Finder
- The central OS file manager - Compare with Windows Explorer
- File management - Launch, delete, rename, etc.
- Integrated access to other devices - File servers, remote storage

Remote Disk
- Use an optical drive from another computer
  - Will not work with audio CDs or video DVDs
- Set up sharing in System Preferences - Appears in the Finder
- Utility available for Windows - Share a Windows CD or DVD drive

Dock
- Fast access to apps - Quickly launch programs
- View running applications - Dot underneath the icon
- Keep folders in the dock - Easy access to files
- Move to different sides of the screen - Auto-hide or display

Boot Camp
- Dual-boot into Windows on Mac hardware - Not virtualization
- Requires Apple device drivers - Windows natively on Intel CPU
- Everything is managed through the Boot Camp Assistant

Client-side Virtualization

Virtualization
- One computer, many operating systems
- Separate OS, independent CPU, memory, network, etc.

The hypervisor
- Virtual Machine Manager
- Manages the virtual platform and guest operating systems

Resource requirements
- CPU Processor Support - Intel: VT, AMD: AMD-V
- Memory - Above and beyond host OS requirements
- Disk space - Each guest OS has it's own image
- Network - Configurable on each guest OS

Emulation vs. Virtualization
- Virtualization is a native operating system
- Emulation is one device running processes designed for completely different architecture

Hypervisor security
- Hypervisor is a sweet spot for the bad guys
- VM escaping
  - Malware recognizes it's on a virtual machine
  - Malware compromises the hypervisor
  - Malware jumps from one guest OS to another

Guest operating system security
- Use traditional security controls - Host-based firewall, anti-virus
- Watch out for rogue virtual machines (VMs)

Network requirements
- Most client-side virtual machine managers have their own virtual (internal) networks
- Shared address - VM and host shares the same IP address
- Bridged address - The VM is a device on the physical network
- Private address - The VM does not communicate to the outside

Basic Linux Commands

ls – List directory contents
- Lists files, directories
- For long output, pipe through more: `> ls -l | more` (use q or Ctrl-c to exit)

grep - Find text in a file
- `grep PATTERN [FILE]`
- `> grep failed auth.log`

cd - Change current directory
- Nearly identical to Windows command line
- Forward slashes instead of backward
- `cd <directory>`
- `> cd /var/log`

shutdown - Shut the system down
- `sudo shutdown 2`
  - Shuts down and turns off the computer in two minutes
- `sudo shutdown -r 2`
  - Shuts down and reboots in two minutes
- Ctrl-C to cancel

pwd - Print Working Directory
- Displays the current working directory path
- Useful when changing directories often

passwd - Change a user account password
- `passwd [username]`

mv - Move (rename) a file
- `mv SOURCE DEST`
- `> mv first.txt second.txt`

cp - Copy a file
- `cp SOURCE DEST`
- `> cp first.txt second.txt`

rm - Remove files or directories
- Does not remove directories by default
- Directories must be empty or must be removed with `-r`

mkdir - Make a directory
- `mkdir DIRECTORY`
- `> mkdir notes`

chmod - Change mode of a file system object
- r=read, w=write, x=execute
- Can also use octal notation
- Set for the file owner (u), the group(g), others(o), or all(a)
- `chmod mode FILE`
- `> chmod 744 script.sh`

chown - Change file owner and group
- `sudo chown [OWNER:GROUP] file`
- `> sudo chown professor script.sh`

iwconfig - View or change wireless network configuration
- Requires some knowledge of the wireless network
- `iwconfig eth0 essid studio-wireless`

ifconfig - View or configure a interface and IP configuration
- `ifconfig eth0`

ps – View the current processes
- Similar to the Windows Task Manager
- View user processes - `ps`
- View all processes - `ps -e | more`

su - Become super user
- You continue to be that user until you exit

sudo - Execute a command as the super user
- Only that command executes as the super user

apt-get - Advanced Packaging Tool
- Handles the management of application packages
- `> sudo apt-get install wireshark`

vi - Visual mode editor
- Full screen editing with copy, paste, and more
- `vi FILE`
- `> vi script.sh`
- Insert text - `i <text>`
- Exit insert mode with `Esc`
- Save (write) the file and quit vi - `:wq`

dd - Convert and copy a file
- Backup and restore an entire partition
- `> dd if=<src file name> of=<target file name> [Options]`
- Creating a disk image
- `> dd if=/dev/sda of=/tmp/sda-image.img`
- Restoring from an image
- `> dd if=/tmp/sda-image.img of=/dev/sda`

Basic Cloud Concepts

Software as a service (SaaS)
- On-demand software - No local installation
- Central management of data and applications
- Google Mail

Infrastructure as a service (IaaS)
- Sometimes called Hardware as a Service (HaaS)
- You're still responsible for the management and security
- Your data is out there, but more within your control
- Web server providers

Platform as a service (PaaS)
- No servers, no software, no maintenance team, no HVAC
- Someone else handles the platform, you handle the product
- You don't have direct control of data, people, or infrastructure
- Salesforce.com

Cloud deployment models
- Private - Your own virtualized local data center
- Public - Available to everyone over the Internet
- Hybrid - A mix of public and private
- Community - Several organizations

Cloud computing characteristics
- Rapid elasticity - Scale up and scale down as needed
- Seamless to everyone
- On-demand self-service
- The cloud enables instant resource provisioning
- Resource pooling - All of the computing power in one place
  - One large resource instead of many small resources
- Measured service
  - Costs and utilization are closely tracked

Network Services

Web server
- Respond to browser requests - Standard HTML/HTML5 protocols
- Web pages are stored on the server, downloaded to the browser
- Static pages or built dynamically in real-time

File server
- Centralized storage of documents, spreadsheets, videos, etc.
- Standard system of file management
- SMB (Server Message Block), Apple Filing Protocol (AFP), etc.
- The front-end hides the protocol - Copy, delete, rename, etc.

Print server
- Connect a printer to the network
- May be software in a computer, may be built-in to the printer
- Uses standard printing protocols - SMB (Server Message Block), IPP (Internet Printing Protocol), LPD (Line Printer Daemon)

DHCP server - Dynamic Host Configuration Protocol
- Automatic IP address configuration
- Available on most home routers
- Enterprise DHCP will be redundant

DNS server - Domain Name System
- Convert names to IP addresses, and vice versa
- Distributed naming system
- Usually managed by the ISP or enterprise IT department

Proxy server
- An intermediate server
  - Client makes the request to the proxy
  - The proxy performs the actual request
  - The proxy provides results back to the client
- Access control, caching, URL filtering, content scanning

Mail server
- Store your incoming mail, send your outgoing mail
- Usually managed by the ISP or the enterprise IT department
- Usually one of the most important services

Authentication server
- Login authentication to resources, extremely important service
- Almost always an enterprise service
- Usually a set of redundant servers that's always available

IDS and IPS
- Network-based Intrusion Detection System / Intrusion Prevention System
- Intrusions - Exploits against operating systems, applications, etc.
- Buffer overflows, cross-site scripting, other vulnerabilities
- Detection – Alarm or alert
- Prevention – Stop it before it gets into the network

All-in-one security appliance
- Unified Threat Management (UTM) / Web security gateway
- URL filter / Content inspection, malware inspection, spam filter, CSU/DSU, router, switch, firewall, IDS/IPS, bandwidth shaper, VPN endpoint

Legacy and embedded systems
- Embedded systems - Purpose-built device
- Not usual to have direct access to the operating system
- Alarm system, door security, network switch

Mobile Operating System Features

Apple iOS
- Apple iPhone and Apple iPad OS - Based on Unix
- Closed-source - No access to source code
- Exclusive to Apple products
- iOS apps are developed with iOS SDK on Mac OS X
- Apps must be approved by Apple before release

Google Android
- Open Handset Alliance - Open-source OS, based on Linux
- Supported on many different manufacturer's devices
- Apps are developed on Windows / Mac OS X / Linux
- Apps available from Google Play
- Apps also available from third-party sites

Windows Mobile
- Windows Phone - Microsoft operating system
- Closed-source - Based on the Windows NT kernel
- The Windows Store - Curated by Microsoft
- Sideloading is supported and also available on Windows 8 Enterprise that has joined a domain

Device displays
- Older resistive touchscreens required periodic calibration
- Modern capacitive touchscreens do not require calibration
- Accelerometer - Motion sensor, detects orientation
- Gyroscope - Detects pitch, roll, and yaw

Global Positioning System (GPS)
- Created by the U.S. Department of Defense
- Precise navigation - Need to see at least 4 satellites
- Determines location based on timing differences
- Mobile device location services and geotracking

WiFi calling
- Make phone calls over a WiFi connection
- Voice over IP technology Integrated into the phone OS
- Carrier must support this feature
- Useful when outside of your calling area or in a bad signal area
- Call local numbers from anywhere

Virtual assistant
- Talk to your phone and get assistance - No typing, no buttons
- iOS - Hold home button or say "Hey, Siri…"
- Android - Hold home button or say "Ok Google…"
- Windows Mobile - Hold the search button or say "Hey, Cortana…"

Production and development models
- iOS - Apps are developed on Mac OS X with iOS SDK, Xcode
- Android - Apps are developed on Windows / Mac OS X / Linux with the Android SDK, Android Studio
- Windows Mobile - Apps are developed on Windows 8.1 / 10 in Visual Studio

Wireless Emergency Alerts
- United States alerting system
- Alerts from the President, imminent threats to safety of life, AMBER alerts (child abduction)
- Similar to text messages
- Works across all mobile operating systems

Mobile payment service
- SMS-based transactional payments - Pay with a text message
- Direct Mobile Billing - Charge your mobile account
- Mobile web payments (WAP) - Pay from your browser or app
- NFC (Near Field Communication) - Pay with your physical phone

Mobile Device Connectivity

Your phone is a radio
- Baseband radio processor - A network interface for your radio
- Has it's own proprietary firmware and memory
- Real-time operating system - Everything happens very quickly
- The firmware can be updated over the air (OTA)

PRL updates - Preferred Roaming List
- CDMA networks (i.e., Verizon, Sprint)
- Contains radio bands, sub-bands, and service provider IDs
- Allows your phone to connect to the right tower
- Can be updated over the air (OTA)

PRI updates - Product Release Instructions
- Radio settings - ID numbers, network codes, country codes, etc.
- Also updated over the air

IMEI - International Mobile Station Equipment Identity
- Identifies a physical mobile device
- Every phone has a different IMEI
- Can be used to allow or disallow access

IMSI - International Mobile Subscriber Identity
- Identifies the user of a mobile network
- Can be provisioned in the SIM card
- Swap the SIM to move between phones

Wireless networks
- Enable and disable cellular and WiFi independently
- iOS - Settings / Cellular
- Android - Settings / Wireless & network settings
- Windows Mobile - Settings / WiFi

Bluetooth
- Short-range personal area network (PAN) - About 10 meters
- Connect different devices - Mouse, keyboard, headset, computer, automobile, speakers

Bluetooth pairing process
- Enable Bluetooth on both devices
- Set devices to discoverable mode - May require key sequence
- Select discovered device - Many devices may appear!
- Enter or confirm PIN - Should be the same on both devices
- Test connectivity - Devices should now communicate

Tethering
- Turn your phone into a WiFi Hotspot
- May require additional service charges

Airplane mode
- One button turns off all radios
- Cellular, WiFi, Bluetooth, NFC
- You can re-enable features without enabling cellular features
- Useful when the airplane has WiFi

VPN - Virtual Private Network
- Turn your phone into a VPN endpoint
- Integrated into the phone OS
- No additional software required
- May require some additional setup
- May support multifactor authentication, i.e., RSA SecureID

Configuring Email on Mobile Devices

Email configurations
- Retrieving mail - POP3, IMAP - Sending mail - SMTP
- Corporate email - Microsoft Exchange
- Commercial providers - Google, Yahoo, Outlook.com, iCloud, etc.

POP3 - Post Office Protocol version 3
- Used for downloading mail to local mail client, tcp/110
- Downloads and (optionally) deletes from server
- POP3S (SSL encryption) settings - tcp/995

IMAP - Internet Message Access Protocol
- Access mail on a central server, tcp/143
- Mail is generally stored on the server
- Supports folders and server-side searching
- IMAPS (SSL encryption) settings - tcp/993

SMTP - Simple Mail Transfer Protocol
- Send mail from a device to a mail server
- You usually must send from a local or trusted server
- Authentication usually required

Microsoft Exchange
- Enterprise email - Includes contacts, calendars, reminders, etc.
- Configure with Email, server, domain, username, password
- Integrated message encryption with S/MIME
  - Secure/Multipurpose Internet Mail Extensions
  - Encrypt and digitally sign

Commercial email providers
- Gmail - Google email, splits inbox into tabs, IMAP, POP3
- Yahoo Mail - IMAP and POP3 support
- Outlook.com - Microsoft free personal email, IMAP and POP3
- iCloud Mail - Apple Mail, IMAP support only

Mobile Device Synchronization

Synchronizing your data
- No single desktop - Many different devices
- Complete mobility - Access anything from anywhere
- Many different types of data - Email, calendar, apps, etc.
- All devices must stay synchronized - Most of it is invisible to us
- Mutual authentication - Client and server must authenticate with each other

Data types
- Contacts, Programs, Email, Pictures, music, video, Calendar, Bookmarks, Documents, Location data, Social media data, eBooks

Synchronizing to the desktop
- Application requirements - OS and disk space
- Operating System - Mac, Windows
- Memory - Relatively minimal
- Storage space - Enough to store backups, video, pictures
- iOS - Apple iTunes - syncs everything in the phone
- Android - Syncs online with Google
  - Use third-party apps to transfer movies and music
- Windows Phone - Windows Phone app
  - Media is synchronized, email, contacts, etc are not.

Synchronizing to the cloud
- Completely hands-off - No physical cables, no local files
- May be integrated into your Exchange or Gmail
- Apple iOS - Sync all data types to iCloud
- Android - Configure your Google account
- Windows Phone - Use your Microsoft account

Mobile Device Synchronization Connections

iOS
- USB - Proprietary - 30-pin, 8-pin Lightning
- 802.11 wireless
- Mobile network

Android and Windows Phone
- USB Micro-B
- 802.11 wireless
- Mobile network

USB Micro-B

Apple 8-pin Lightning

USB Standard Type A

Apple 30-pin

Common Security Threats

Malware
- Malicious software - gather information, keystrokes
- Unwilling participation in a group, such as a controlled botnet
- Extortion for big money
- Viruses and worms can ruin your day

Spyware
- Malware that spies on you - Advertising, identity theft, affiliate fraud
- Can trick you into installing - Peer to peer, fake security software
- Browser monitoring - Capture surfing habits
- Keyloggers - Capture every keystroke, send it back to the mothership

Viruses
- Malware that can reproduce itself -
- Reproduces through file systems or the network
- Running a program can spread a virus
- Some viruses are invisible, some are annoying
- Anti-virus is very common - Thousands of new viruses every week

Worms
- Malware that self-replicates - doesn't need you to do anything
- Uses the network as a transmission medium
- Can take over many PCs very quickly
- Worms can do good things - Nachi tried to patch your computer
- Firewalls and IDS/IPS can mitigate many worm infestations

Trojan horse
- Used by the Greeks to capture Troy from the Trojans
- Software that pretends to be something else
- Circumvents your existing security - Anti-virus may catch it
- The better trojans are built to avoid and disable AV
- Once it's inside it has free reign, and it may open the gates

Rootkits
- Originally a Unix technique - The "root" in rootkit
- Modifies core system files - Part of the kernel
- Can be invisible to the operating system or hides in the OS
- Also invisible to traditional anti-virus utilities

Ransomware
- Your data is held hostage until your provide cash
- Malware encrypts your data files - Pictures, documents, music, movies, etc.
- You must pay the bad guys to obtain the decryption key
- An unfortunate use of public-key cryptography

Phishing
- Social engineering with a touch of spoofing
- Often delivered by spam, IM, etc.
- Don't be fooled, Check the URL
- Spear phishing - Targeted and sophisticated phishing

Spoofing
- Pretend to be someone you aren't
- Modify your MAC or IP address - Change in driver configuration
- Fundamental with many DDoS attack types

Social engineering
- Major threat - Electronically undetectable
- Don't give any information over the telephone
- Look out for unattended persons, look for badges

Shoulder surfing
- You have access to important information
- Curiosity, industrial espionage, competitive advantage
- Airports / Flights, hallway-facing monitors, coffee shops
- Surf from afar with binoculars / telescopes
- Webcam monitoring

Zero-day attacks
- Many applications have vulnerabilities
- Someone is working hard to find the next big vulnerability
- Bad guys keep these yet-to-be-discovered holes to themselves
- Zero-day - The vulnerability has not been detected or published

Distributed Denial of Service (DDoS)
- Launch an army of computers to bring down a service
- Use all the bandwidth or resources - traffic spike
- A botnet can have millions of computers at your command
- Many people have no idea they are participating in a bonnet

Brute force
- The password is the key - secret phrase, stored hash
- Online - Brute force attacks - very slow
- Offline - Brute force the hash
- Large computational resource requirement

Dictionary attacks
- People use common dictionary words as passwords
- Many common wordlists available on the Internet
- This will catch the easiest and most common passwords

Common Security Threats (continued)

Non-compliant systems
- A constant challenge - There are always changes and updates
- Standard operating environments (SOE) are a set of tested and approved hardware/software systems
- Must have OS and application patches to be in compliance

Violations of security best practices
- There are many security best practices
- DLP, encryption, spam filters, patches, firewalls, education, etc.
- Constant audits are required
- Each missed practice is an opportunity

Tailgating
- Use someone else to gain access to a building
- Blend in with clothing - 3rd-party with a legitimate reason
- Once inside, there's little to stop you

Man-in-the-middle
- Bad guy can watch without you knowing
- Redirects your traffic, then passes it on to the destination
- You never know your traffic was redirected
- ARP poisoning - ARP has no security

Physical Security Prevention Methods

Door Access Controls
- Conventional lock and key, deadbolt, electronic, token-based, biometric, and multi-factor

Mantraps
- All doors normally unlocked
  - Opening one door causes others to lock
- All doors normally locked
  - Unlocking one door prevents others from being unlocked
- One door open / other locked
  - When one is open, the other cannot be unlocked
- One at a time, controlled groups

Securing physical documents
- Secure backups, laptops, hard drives, passwords
- Protection against the fire and water
- Makes it difficult to steal - Very heavy
- Must be carefully managed

Protect your rubbish
- Secure your garbage - Fence and a lock
- Shred your documents - This will only go so far
- Governments burn the good stuff

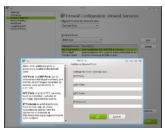
Cable locks
- Connect your hardware to something solid
- Cable works almost anywhere - Useful when mobile
- Most devices have a standard connector
- Not designed for long-term protection

Privacy filters
- Be aware of your surroundings
- Use privacy filters
- Keep your monitor out of sight

Badges and entry control roster
- Security guard - Physical protection
- ID badge - Picture, name, other details
- Entry control roster - Physical list of names

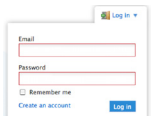
Digital Security Prevention Methods

Anti-virus and anti-malware
- Anti-malware software runs on the computer
- Large organizations need enterprise management
- Mobility adds to the challenge

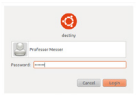


Host-based firewalls
- "Personal" firewalls - Software-based
- Stops unauthorized network access
- Stateful firewall
- Blocks traffic by application or port number

Network-based firewalls
- Filters traffic by port number
- Can encrypt and proxy traffic across the network
- Most firewalls can be layer 3 devices (routers)



User authentication
- Identifier - something unique
- Credentials - Password, smart card, PIN code, etc.
- Profile - Information stored about the user



Strong passwords
- Weak passwords can be difficult to protect against
- Passwords need complexity and constant refresh

Multi-factor authentication
- Something you are, something you have, something you know, somewhere you are
- Something you do

Directory permissions
- NTFS permissions - Much more granular than FAT
- User permissions - Everyone isn't an Administrator

VPN (Virtual Private Network) concentrator
- Encrypt (private) data traversing a public network
- Concentrator - Encryption/decryption device
- Used with client software

Data Loss Prevention (DLP)
- SSN, credit card numbers, medical records
- Stop the data before the bad guys get it
- Often requires multiple solutions

Disabling unused ports
- This is a good best-practice
- Requires additional maintenance and vigilance
- Plan on periodic reviews

Access control lists (ACLs)
- Permissions associated with an object
- Used in file systems, network devices, operating systems, and more

Smart cards
- Must have physical card to provide digital access
- Multiple factors - Card with PIN or fingerprint

Email filtering
- Stop it at the gateway before it reaches the user
- On-site or cloud-based
- Scan and block malicious software

Trust/untrusted software sources
- Consider the source
- Trusted sources - Internal apps, known publishers
- Untrusted sources - Email links, drive-by downloads

Security Awareness

Security policy training and procedures
- All of your policy information is on the Intranet
- Consider in-person mandatory training sessions
- General security best practices
- Specific security training

Network policies
- Each organization has their own philosophy
- Closely associated with the security policy
- Acceptable use policy
  - All-encompassing and specific set of rules for network use
  - May require a signature before getting network access

Principle of least privilege
- You only get the rights necessary to perform the job
- Management gets to choose the rights, IT administers it
- Physical and digital controls - Business processes, permissions

Workstation Security Best Practices

Password complexity and length
- No single words, no obvious passwords
- Mix upper and lower case, use special characters
- A strong password is at least 8 characters
- Set password expiration, require change
- System remembers password history, requires unique passwords

Password expiration and recovery
- All passwords should expire (30 days, 60 days, 90 days, etc.)
- Critical systems might change more frequently
- Some organizations have a very formal recovery process

Desktop security
- Require a screensaver password, lock after a timeout
- Disable autorun through the registry
  - autorun.inf in Vista, no Autorun in Windows 7 or 8/8.1
- Consider changing AutoPlay

Password best practices
- Changing default usernames/passwords
- Supervisor/Administrator BIOS password: Prevent BIOS changes
- User BIOS password: Prevent booting
- Always require passwords - No blank passwords, no automated logins

Restricting user permissions
- Everyone isn't an Administrator
- Assign proper rights and permissions
- Assign rights based on groups - Difficult to manage per-user rights
- Login time restrictions - Only login during working hours

Disabling unnecessary accounts
- Not all accounts are necessary - disable/remove the unnecessary
- Disable interactive logins - Not all accounts need to login
- Change the default usernames - Helps with brute-force attacks

Account lockout and disablement
- Too many bad passwords will cause a lockout
- Disable user accounts - You don't want to delete accounts

Data encryption
- Full-disk encryption - Encrypt the entire drive
- Filesystem encryption - Individual files and folders
- Removable media - Protect those USB flash drives
- Key backups are critical - You always need to have a copy

Patch and update management
- Keep OS and applications updated for security and stability
- Deployment may be managed internally
- Many applications include their own updater

Windows Security Settings

Users
- Administrator - The Windows super-user
- Guest - Limited access
- Standard Users - Everyone else

Groups
- Power Users - Not much more control than a regular user

NTFS vs. Share permissions
- NTFS permissions apply from local and network connections
- Share permissions only apply to connections over the network
- The most restrictive setting wins - Deny beats allow
- NTFS permissions are inherited from the parent object
  - Unless you move to a different folder on the same volume

Shared files and folders
- Administrative shares
  - Hidden shares (i.e., C$) created during installation
  - Local shares are created by users
- System files and folders
  - C$ - \
  - ADMIN$ - \Windows
  - PRINT$ - Printers folder
- Computer Management / Shared Folders - `net share`

Explicit and inherited permissions
- Explicit permissions - Set default permissions for a share
- Inherited permissions
  - Propagated from the parent object to the child object
  - Set a permission once, it applies to everything underneath
- Explicit permissions take precedence over inherited permissions
  - Even inherited deny permissions

User authentication
- Authentication - Prove you are the valid account holder
  - Username / Password - Perhaps additional credentials
- Single sign-on (SSO), i.e., Windows Domain
  - Provide credentials one time, managed through Kerberos

Run as administrator
- Administrators have special rights and permissions
- Use rights and permissions of the administrator
  - You don't get these by default, even if you're in the Administrators group
- Right-click the application, Run as administrator
  - Or Ctrl-Shift-Enter

BitLocker
- Encrypt an entire volume - Not just a single file
  - Protects all of your data, including the OS
- Lose your laptop? Doesn't matter without the password
- Data is always protected
  - Even if the physical drive is moved to another computer
- BitLocker To Go - Encrypt removable USB flash drives

EFS (Encrypting File System)
- Encrypt at the filesystem level on NTFS
- OS support:
  - Vista Business, Enterprise and Ultimate
  - 7 Professional, Enterprise and Ultimate
  - 8 and 8.1 Pro and Enterprise
- Uses password and username to encrypt the key
- Administrative resets will cause EFS files to be inaccessible

Securing Mobile Devices

Screen Locks
- Fingerprint - Built-in fingerprint reader
- Face Unlock - Face recognition
- Swipe - Choose a pattern
- Passcode - Choose a PIN or add complexity
- Failed attempts:
  - iOS: Erase everything after 10 failed attempts
  - Android: Lock the device and require a Google login
  - Windows Phone: Delays next attempt or factory reset

Locator applications and remote wipe
- Built-in GPS - And location "helpers"
- Find your phone on a map
- Control from afar with sounds and messages
- Wipe everything remotely

Remote backup
- Difficult to backup something that's always moving
- Backup to the cloud for constant backup
- Backup without wires - use the existing network
- Restore with one click - authenticate and wait

Antivirus and Antimalware
- Apple iOS - Closed environment, tightly regulated
- Android - More open, apps can be installed from anywhere
- Windows Phone - Closed environment, apps run in a sandbox

Patching/OS updates
- All devices need updates, even mobile devices
- Device patches - security updates
- Operating system updates - New features, bug fixes

Biometric authentication
- Multi-factor authentication - More than one factor
- Passcode, password, swipe pattern
- Fingerprint, face, iris
- A phone is always with you, and you're a good source of data

Authenticator apps
- Pseudo-random token generators
- Carry around physical token devices
- Use a token generator app

Full device encryption
- Encrypt all device data - Phone keeps the key
- iOS 8 and later - Personal data is encryption with your passcode
- Android - Full device encryption can be turned on
- Windows Phone 8/8.1 - Full device encryption only available with Exchange ActiveSync or managed by an MDM

Trusted vs. untrusted sources
- Once malware is on a phone,it has a huge amount of access
- iOS - All apps are curated by Apple
- Android - Downloaded from Google Play or sideloaded
- Windows Phone - Apps are curated by Microsoft
  - Sideloading available in enterprise environments

Firewalls
- Mobile phones don't include a firewall
- Some mobile firewall apps are available, most for Android
- Enterprise environments can control mobile apps

Policies and procedures
- Manage company-owned and user-owned mobile devices
- BYOD - Bring Your Own Device
- Set policies on apps, data, camera, etc.
- Force screen locks and PINs on these single user devices

Data Destruction and Disposal

Physical destruction
- Shredder - Heavy machinery - Complete destruction
- Drill / Hammer - Quick and easy - Platters, all the way through
- Electromagnetic (degaussing) - Remove the magnetic field
- Destroys the drive data and the electronics
- Incineration - Fire will remove everything

Certificate of destruction
- Destruction is often done by a 3rd party
- You need confirmation that your data is destroyed
- Destruction service should include a certificate

Disk formatting
- Low-level formatting - Provided at the factory
  - Not possible by the user
- Standard formatting / Quick format
  - Sets up the file system, installs a boot sector
  - Clears the master file table but not the data
  - Can be recovered with the right software
- Standard formatting / Regular format
  - Overwrites every sector with zeros
  - Windows Vista and later
  - Can't recover the data

Hard drive security
- File level overwriting - Sdelete – Windows Sysinternals
- Whole drive wipe secure data removal - DBAN - Darik's Boot and Nuke
- Physical drive destruction - One-off or industrial removal and destroy

Securing a SOHO Network

SSID management
- Service Set Identifier - Name of the wireless network
- Change the SSID to something not-so obvious
- Disable SSID broadcasting?
  - SSID is easily determined through wireless network analysis
  - Security through obscurity

Wireless encryption
- All wireless computers are radio transmitters and receivers
- Solution: Encrypt the data - Everyone gets the password
- Only people with the password can transmit and listen

Antenna placement
- Central coverage to reach all areas of the building
- Don't overlap frequencies

Power level controls
- Usually a wireless configuration - Set it as low as you can
- Consider the receiver - High-gain antennas can hear a lot

MAC address filtering
- Media Access Control - The "hardware" address
- Keeps the neighbors out - Additional administration with visitors
- Easy to find working MAC addresses through network analysis
- MAC addresses can be spoofed
- Security through obscurity

Using WPS (Wi-Fi Protected Setup)
- Allows "easy" setup of a mobile device
- Different ways to connect
  - PIN configured on access point must be entered on the device
  - Push a button on the access point
  - Near-field communication - Bring the mobile device close
  - USB method - no longer used

Securing a SOHO Network (continued)

The WPS hack
- December 2011 - WPS has a design flaw
- PIN is seven digits and a checksum
  - Seven digits, 10,000,000 possible combinations
- The WPS process validates each half of the PIN
  - First half, 4 digits. Second half, 3 digits.
  - First half, 10,000 possibilities. Second half, 1,000 possibilities
- It takes about four hours to go through all of them

Default usernames and passwords
- All access points have default usernames and passwords
- The right credentials provide full control/admin access
- Very easy to find the defaults for your WAP or router

IP addressing
- DHCP (automatic) IP addressing vs. manual IP addressing
- IP addresses are easy to see in an unencrypted network
- If the encryption is broken, the IP addresses will be obvious
- Security through obscurity

SOHO firewalls
- Small office / home office appliances
- Wireless access point, router, firewall, content filter
- May not provide advanced capabilities, i.e., dynamic routing, etc.
- Install the latest software - Update and upgrade the firmware

Firewall settings
- Inbound traffic - Extensive filtering and firewall rules
  - Allow only required traffic
  - Configure port forwarding to map TCP/UDP ports to a device
- Outbound traffic
  - Blacklist - Allow all, stop only unwanted traffic
  - Whitelist - Block all, only allow certain traffic types

Disabling ports
- Enabled physical ports - conference rooms, break rooms
- Always administratively disable unused ports
- Use Network Access Control (NAC) - 802.1X controls

Content filtering
- Control traffic based on data within the content
- Corporate control of outbound and inbound sensitive data
- Control inappropriate content - not safe for work, etc.
- Protection against evil - Anti-virus, anti-malware

Physical security
- Physical access = Relatively easy hack
- Door access - Lock and key, electronic keyless
- Biometric - Eyeballs and fingers
- Always have a documented and well established process

Operating System Troubleshooting

Bluescreens and spontaneous shutdowns
- Startup and shutdown BSOD
  - Bad hardware, bad drivers, bad application
- Apple pinwheel/beach ball
  - Hang or constant retries by application / resource contention
- Use Last Known Good, System Restore, or Rollback Driver
  - Try Safe mode
- Reseat or remove the hardware, if possible
- Run hardware diagnostics
  - Provided by the manufacturer
  - BIOS may have hardware diagnostics

Boot errors
- Can't find operating system - OS missing
- Boot loader replaced or changed - Multiple OSes installed
- Check boot drives - Remove any media
- Startup Repair
- Modify the Vista/7/8/8.1 Boot Configuration Database (BCD)
  - Formerly boot.ini
  - Recovery Console: bootrec /rebuildbcd

Improper shutdown
- Windows Error Recovery window
  - "Windows did not shut down successfully"
- Should recover normally - may just have problems again
- "Launch Startup Repair" can fix most issues
  - F8 or run from Windows Error Recovery window

Missing GUI
- No login dialog, no desktop - Driver or OS file corruption
- Start in VGA mode - F8 for startup options
- Run SFC - System File Checker - Run from recovery console
- Update driver in Safe Mode - Download from known good source
- Repair/Refresh or recover from backup

Startup Repair
- Missing NTLDR
  - Run Startup Repair or replace manually and reboot
- Missing operating system
  - Run Startup Repair or manually configure BCD store
- Boots to Safe Mode
  - Run Startup Repair

Missing GRUB/LILO
- GNU GRand Unified Bootloader (GRUB) - Linux boot loader
- LInux LOader (LILO) - An older and less common boot loader
- Missing boot loaders - Can be overwritten by other OSes
- Boot-repair LiveCD or command line recovery

Starting the system
- Device not starting
  - Remove or replace driver
- "One or more services failed to start"
  - Try starting manually
  - Check account permissions
  - Confirm service dependencies
  - Windows service; check system files
  - Application service; reinstall application

Slow system performance
- Task Manager - Check for high CPU utilization and I/O
- Windows Update - Latest patches and drivers
- Disk space - Check for available space and defrag
- Laptops may be using power-saving mode - Throttles the CPU
- Anti-virus and anti-malware - Scan for bad guys

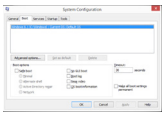
Kernel panic
- Unix and Linux systems, Mac OS X - Non-recoverable fatal error
- Error message provides some insight, Hardware failure, OS bug

Multiple monitor misalignment
- Monitors aren't "aligned" - Mouse won't move between screens
- Drag monitors into alignment - Move into any location

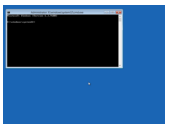
Operating System Troubleshooting Tools

BIOS/UEFI tools
- Built-in diagnostics - Check for temps and status
- Run some basic hardware tests

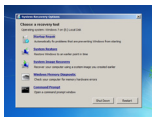
SFC
- System File Checker
- Integrity scan for operating system files



Logs
- Windows - Event Viewer, boot logs
  - System Configuration - C:\Windows\ntbtlog.txt
- Linux - Individual application logs - `/var/log`
- Mac OS X - Utilities / Console.app

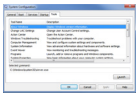


Windows Command Prompt
- Windows Vista/7
  - System Recovery Options / Command Prompt
- Windows 8/8.1
  - Choose Other Options / Troubleshoot / Advanced Options / Command Prompt
- Use, copy, rename, or replace OS files and folders
- Enable or disable service or device startup
- Repair the file system boot sector or the master boot record (MBR)
- Create and format partitions on drives

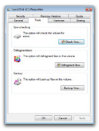


System Repair Disk
- Boots the computer - Provides system recovery options in Windows Vista/7/8/8.1
- Backup and Restore - Create a System Repair Disk

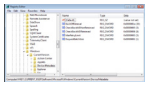
Pre-installation environments (PE)
- A minimal Windows operating environment
- Used for troubleshooting and recovery
  - And during Windows Vista/7/8/8.1 setup



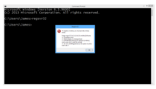
MSCONFIG
- Microsoft System Configuration
- Set boot parameters and startup apps/services



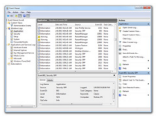
Defragmentation
- Moves file fragments so they are contiguous
- Improves read and write time
- Graphical version in the drive properties



REGEDIT - Registry Editor
- The Windows Registry - a hierarchical database
- REGEDIT - Modify registry settings
- Add / modify / delete keys, import and export



REGSVR32 - Microsoft Register Server
- Register/unregister a DLL
- Updates the registry



Event Viewer
- Central event consolidation
- Application, Security, Setup, System
- Information, Warning, Error, Critical, Successful Audit, Failure Audit

Options at boot time
- Press F8 before during boot for Windows Advanced Options
- Options for Safe Mode, Windows Recovery Console, Last Known Good Configuration

Safe Mode
- Press F8 on boot - Windows Advanced Options
- Safe Mode
- Safe Mode with Networking
- Safe Mode with Command Prompt
- Enable low-resolution (VGA Mode)

Automated System Recovery
- Last resort of Windows XP recovery
  - Try Safe Mode and Last Known Good first!
- Accessories / System Tools / Backup
  - Requires a floppy disk
- Recovery requires ASR floppy, system backup, and Windows CD
- Restores disk signatures, volumes, and partitions
- Destructive! You will lose your data!
- Starts a data restore from a separate backup
- ASR does not back up or restore your data!

Uninstall/reinstall/repair
- A clean install can fix many things
- Windows 8/8.1 includes a built-in refresh
  - Clean out Windows without losing your files
- If you really want to start fresh, you can reset
  - Back to factory defaults

Troubleshooting Common Security Issues

Bluescreens and spontaneous shutdowns
- Pop-ups in your browser - May look like a legitimate application
- Update your browser - Use the latest version with pop-up blocker
- Scan for malware - Rebuild from scratch or known good backup

Browser redirection
- Instead of your Google result, your browser goes elsewhere
- Malware is the most common cause
- Use an antimalware/antivirus cleaner - Not the best option
- Restore from a good known backup

Browser security alerts
- Security alerts and invalid certificates
- Look at the certificate details
- May be expired or the wrong domain name
- The certificate may not be properly signed (untrusted CA)

Malware network symptoms
- Slow performance, lock-up
- Internet connectivity issues, OS updates failures
- Rebuild from scratch or known good backup

Malware OS symptoms
- Renamed system files
- Files disappearing or encrypted
- File permission changes
- Access denied
- Restore from a good known backup

System lock up
- Completely stops - No status light changes
- May still be able to terminate bad apps
  - Windows and Linux Task Manager (Ctrl-Alt-Del / Task Manager)
  - Mac OS X Force Quit (Command-Option-Esc)
- Check logs when restarting
- May be a security issue - Perform a virus/malware scan
- Perform a hardware diagnostic

Troubleshooting Common Security Issues (continued)

Application crashes
- Application stops working
- Check the Event Log - Often includes useful reconnaissance
- Check the Reliability Monitor - A history of application problems
- Reinstall the application - Contact application support

Virus alerts and hoaxes
- Rogue antivirus - May include recognizable logos and language
- May require money to "unlock" your PC
- May require a specific anti-malware removal utility or technique

Email security
- Spam - Unsolicited email messages
  - Advertisements, phishing attacks, virus spreaders
  - Spam filters can be helpful
- Hijacked email
  - Infected computers can become email spammers
  - You receive odd replies from other users
  - You receive bounce messages from unknown email addresses

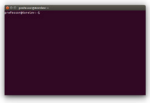
Tools for Security Troubleshooting

Anti-virus and anti-malware software
- Stop malicious software from running
- Keep your signatures updated

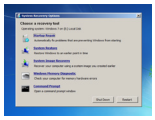
Recovery Console / Command Prompt
- Use, copy, rename, or replace OS files and folders
- Enable or disable service or device startup
- Remove malicious software components
- Windows Vista/7
  - System Recovery Options / Command Prompt
- Windows 8/8.1
  - Troubleshoot / Advanced options / Cmd Prompt

System Restore
- Go back-in-time to correct problems
- Windows Vista and 7:
  - All Programs / Accessories / System Tools / System Restore
- Windows 8/8.1:
  - Control Panel / System / Advanced System Settings
- Doesn't guarantee recovery from malware

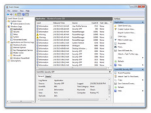
Windows Refresh (Windows 8/8.1)
- Reinstall Windows
- Keep your personal files and settings



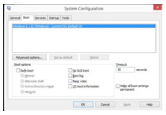
LVM (Linux Logical Volume Manager) snapshots
- The Linux version of Windows System Restore
- Common on high-availability servers
- Works very quickly
  - Initial snapshot is comprehensive
  - Only snapshots what's changed
- Restore from the snapshot
  - Many different file versions and points in time



Windows Pre-installation (PE) environments
- A minimal Windows operating environment
- Resolve security issues, copy and recover data
- Create your own Windows Anti-malware boot disk



Event Viewer
- Central event consolidation
- Get details around security events
- Authentication and application information



MSCONFIG / System Configuration
- Safe boot: Minimal
- Safe mode GUI with minimal services, no network
- Safe boot: Alternate shell - with minimal services
- Safe boot: Active Directory repair
- Safe boot: Network - File explorer in safe mode

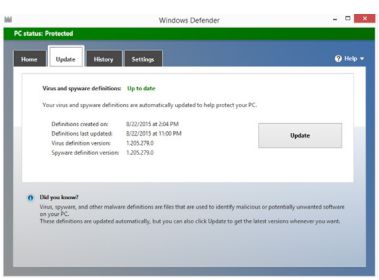
Best Practice Procedures for Malware Removal

Step 1: Identify Malware Symptoms
- Odd error messages, application failures, security alerts
- System performance issues - slow boot, slow applications

Step 2. Quarantine infected systems
- Disconnect from the network - Keep it contained
- Isolate all removable media
- Prevent the spread - Don't transfer files, don't try to backup

Step 3. Disable System Restore
- Malware infects restore points, so a restore will reinfect the PC
- Disable System Protection
  - No reason to save an infected config
- Delete all restore points
  - Remove all infection locations

Step 4a. Remediate: Update antivirus
- Signature and engine updates
- Automatic vs. manual
- Manual updates are almost pointless
- Your malware may prevent the update process



Step 4b. Remediate: Scan and remove
- Use a known-good anti-virus scanner
- Consider a malware-specific scanner such as Malwarebytes, etc.
- The virus may have a stand-alone removal app
- The only guaranteed removal is to delete it all and rebuild
- May require Safe Mode or working at the Recovery Console
- May also require repair of boot records and sectors

Step 5. Schedule scans and run updates
- Built into the antivirus software
- Automated signature updates and scans
- Automate the operating system updates

Step 6. Enable System Protection
- Now that you're clean, put things back to normal
- Create an initial restore point as a starting point

Step 7. Educate the end user
- One on one - Personal training
- Posters and signs - High visibility
- Message board posting - Physical postings in a visible area
- Login message - These become invisible over time
- Intranet page - Always available

Mobile Device App Troubleshooting

Dim display
- Difficult to see the details, even in low light
- Check the brightness setting
  - iOS: Settings / Display and brightness
  - Android: Settings / Display / Brightness level
  - Windows Phone: Settings / Brightness
- Replace the bad display - backlight issue

Wireless connectivity
- Intermittent connectivity
  - Move closer to access point, try a different access point
- No wireless connectivity
  - Check/Enable WiFi, check security key configuration
  - Hard reset can restart wireless subsystem
- No Bluetooth connectivity
  - Check/Enable Bluetooth, check/Pair Bluetooth component
  - Hard reset to restart Bluetooth subsystem

Cannot broadcast to monitor
- Broadcast to a TV - Apple TV, Xbox, Playstation, Chromecast, etc.
- Check app requirements - Every broadcast device is different
- All devices must be on the same wireless network
- Signal strength is important

Non-responsive touchscreen
- Touchscreen completely black or touchscreen not responding
- Apple iOS restart
  - Press power button, slide to power off, press power button
  - Hold down power button and Home button for 10 seconds
- Android device restart
  - Remove battery, put back in, power on
  - Hold down power and volume down until restart

App issues
- Apps not loading, slow app performance
- Restart the phone - Hold power button, power off
- Stop the app and restart
  - iPhone: Double-tap home button, slide app up
  - Android: Settings/Apps, select app, Force stop
- Update the app - Get the latest version

Unable to decrypt email
- Built-in to corporate email systems
- Each user has a private key - You can't decrypt without the key
- Install individual private keys on every mobile device
  - Use a Mobile Device Manager (MDM)

Short battery life
- Bad reception - Always searching for signal
- Disable unnecessary features - 802.11 wireless, Bluetooth, GPS
- Check application battery usage
  - iPhone: Settings/General/Usage
  - Android: Settings/Battery
- Aging battery - There's only so many recharges

Overheating
- Phone will automatically shut down to avoid damage
- Charging/discharging the battery, CPU usage, display light
- Check app usage - Some apps can use a lot of CPU

Avoid direct sunlight - Quickly overheats

Frozen system
- Nothing works - No screen or button response
- Soft reset - Hold power down and turn off
- Hard reset
  - iOS: Hold power and home button for 10 seconds
  - Android: Various combinations of power, home, and volume
- Ongoing problems may require a factory reset

No sound from speakers
- No sound from a particular app
  - Check volume settings - Both app and phone settings
  - Bad software / delete and reload
  - Try headphones
- Sound starts but then stops
  - Dueling apps / keep app in foreground
- No speaker sound from any app (no alarm, no music, no audio)
  - Load latest software
  - Factory reset

Inaccurate touch screen response
- Screen responds incorrectly or is unresponsive
- Close some apps - Low memory can cause resource contention
- Restart the device - Soft reset, unless a hard reset is required
- May require a hardware fix - Replace the digitizer / reseat cables

System lockout
- Too many incorrect unlock attempts
- iOS: Erases the phone after 10 failed attempts
- Android: Locks or wipes the phone after failed attempts
- Windows Phone: Locks after failed attempts

Mobile Device Security Troubleshooting

Signal drop / weak signal
- Drops and weak signals prevent traffic flows
- Make sure you're connecting to a trusted WiFi network
  - Never trust a public WiFi Hotspot, tether with your own device
- Run a speed test

Power drain
- Power drains faster than normal
  - Heavy application use
  - Increased network activity
  - High resource utilization
- Check application before install - Use an App scanner
- Run anti-malware - Check for malicious activity
- Perform a clean install - Factory reset, reinstall apps

Slow data speeds
- Unusual network activity
- Unintended WiFi connections, data transmission overlimit
- Check your network connection - Run a WiFi analyzer
- Check network speed - Run speed check / cell tower analyzer
- Examine running apps for unusual activity
  - Large file transfers, constant activity

Unintended Bluetooth pairing
- Connect with a device that isn't yours
- Remove the Bluetooth device - Re-pair the device again
- Disable Bluetooth radio - No communication at all
- Run an anti-malware scan - Check for malicious apps

Mobile Device Security Troubleshooting (continued)

Leaked information
- Unauthorized account access
- Determine cause of data breach
- Factory reset and clean install
- Check online data sources

Unauthorized location tracking
- Real-time tracking information and historical tracking details
- Run an anti-malware scan
- Check apps with an offline app scanner
- Perform a factory reset

Unauthorized camera / microphone use
- Third-party app captures intimate information
- Run an anti-malware scan
- Confirm that loaded apps are legitimate
- Factory refresh

Managing Electrostatic Discharge

Electrostatic Discharge
- Static electricity - Electricity that doesn't move
- ESD can be very damaging to computer components
- Silicon is very sensitive to high voltages
- Feel static discharge: ~3,500 volts
- Damage an electronic component: 100 volts or less

Controlling ESD
- Humidity over 60% helps control ESD - Won't prevent it all
- Touch the exposed metal chassis before touching a component
- Always unplug the power connection
- Try not to touch components directly, touch only the edges

Computer Safety Procedures

WARNING
- Power is dangerous - Remove all power sources before working

Equipment grounding
- Most computer products connect to ground
- Diverts any electrical faults away from people
- Also applies to equipment racks - Uses a large ground wire
- Don't remove the ground connection - It's there to protect you

Personal safety
- Remove jewelry and name badge neck straps
- Lifting technique - Lift with your legs, keep your back straight
  - Don't carry overweight items
- Electrical fire safety - Remove the power source
  - Use carbon dioxide, FM-200, or other dry chemicals
- Cable management - Avoid trip hazards - Use cable ties or velcro
- Safety goggles - Useful when working with chemicals
- Air filter mask - Dusty computers, printer toner

Handling toxic waste
- Batteries from uninterruptible power supplies (UPS)
  - Dispose at your local hazardous waste facility
- CRTs - Cathode ray tubes
  - Glass contains lead
  - Dispose at your local hazardous waste facility
- Toner
  - Recycle and reuse
  - Many printer manufacturers provide a return box

Local government regulations
- Health and safety laws - Keep the workplace hazard-free
- Building codes - Fire prevention, electrical codes
- Environmental regulation - High-tech waste disposal

Managing Your Computing Environment

Disposal procedures
- Read your Material Safety Data Sheets (MSDS)
  - United States Department of Labor,
  - Occupational Safety and Health Administration (OSHA)
- Provides information for all hazardous chemicals
  - Batteries, display devices / CRTs, chemical solvents and cans, toner and ink cartridges
- Product and company information, composition / ingredients, hazard information, first aid measures, fire-fighting measures, accidental release / leaking, handling and storage, etc.

Room control
- Temperature - Devices (and humans) need constant cooling
- High humidity promotes condensation
- Low humidity promotes static discharges
- Computers generate heat - Don't put everything in a closet

UPS (Uninterruptible Power Supply)
- Provide backup power and protect against brownouts
- Types: Standby UPS, Line-interactive UPS, On-line UPS
- Features may include auto shutdown, battery capacity, outlets, phone line suppression, etc.

Surge suppressor
- Not all power is "clean" - Self-inflicted power spikes and noise
- Storms, power grid changes
- Spikes are diverted to ground
- Noise filters remove line noise - Higher Db is better
- Surge absorption is measured in Joules - higher is better
- Surge amp ratings - Higher is better
- UL 1449 voltage let-through ratings - Lower is better

Protection from airborne particles
- Enclosures - Protect computers on a manufacturing floor
  - Protect from dust, oil, smoke
- Air filters and masks - Protect against airborne particles
  - Dust in computer cases
  - Laser printer toner

Dust and debris
- Cleaning - Use neutral detergents
  - No ammonia-based cleaning liquids
  - Avoid isopropyl alcohol
- Vacuum - Use a "computer" vacuum
- Compressed air pump - Try not to use compressed air in a can

Prohibited Activity and End-user Policies

Incident response: First response
- Identify the issue - Logs, in person, monitoring data
- Report to proper channels - Don't delay
- Collect and protect information relating to an event
- Many different data sources and protection mechanisms

Incident response: Documentation
- Security policy - An ongoing challenge
- Documentation must be available - No questions
- Documentation always changes - Constant updating
- Have a process in place - Use the wiki model

Incident response: Chain of custody
- Control evidence - Maintain integrity
- Everyone who contacts the evidence - Use hashes
- Label and catalog everything - Seal, store, and protect

Content policies
- A security policy - Every organization has a different philosophy
- Block policies - URL, application, user name / group
- Block everything, only allow certain traffic types
- Allow everything, block only certain traffic types

Licensing / EULA
- Closed source / Commercial - Source code is private
  - End user gets compiled executable
- Free and Open Source (FOSS) - Source code is freely available
  - End user can compile their own executable
- End User Licensing Agreement
  - Determines how the software can be used
- Digital Rights Management (DRM)
  - Used to manage the use of software
- Personal license - Designed for the home user
  - Usually associated with a single device or small group of devices owned by the same person
  - Perpetual (one time) purchase
- Enterprise license - Per-seat purchase / Site license
  - The software may be installed everywhere
  - Annual renewals

PII (Personally identifiable information)
- Part of your privacy policy - How will you handle PII?
- Not everyone realizes the importance of this data

Communication

Communication skills
- One of the most useful skills for the troubleshooter
- One of the most difficult skills to master
- A skilled communicator is incredibly marketable

Avoid jargon
- Abbreviations and TLAs - Three Letter Acronyms
- Avoid acronyms and slang - Be the translator
- Communicate in terms that everyone can understand
  - Normal conversation puts everyone at ease
  - Decisions are based on what you say
- These are the easiest problems to avoid

Avoid interrupting
- But I know the answer!
- Why do we interrupt?
  - We want to solve problems quickly
  - We want to show how smart we are
- Actively listen, take notes
  - Build a relationship with the customer
  - Don't miss a key piece of information
  - Especially useful on the phone
- This skill takes time to perfect
  - The better you are, the more time you'll save later

Clarify customer statements
- Ask pertinent questions
  - Drill-down into the details
  - Avoid an argument
  - Avoid being judgmental
- Repeat your understanding of the problem back to the customer
  - Did I understand you correctly?
- Keep an open mind
  - Ask clarifying questions, even if the issue seems obvious
  - Never make assumptions

Setting expectations
- Offer different options - Repair or replace?
- Document everything - No room for questions
- Keep everyone informed - Even if the status is unchanged
- Follow up afterwards - Verify satisfaction

Professionalism

Maintain positive attitude
- Positive tone of voice - Project confidence
- Problems can't always be fixed
  - Do your best, provide helpful options
- Your attitude has a direct impact on the customer experience

Avoid being judgmental
- Cultural sensitivity - Use appropriate professional titles
- You're the teacher - Not the warden
  - Leave insults on the playground
- Make people smarter - They'll be better technologists
- You're going to make some BIG mistakes - Remember them.

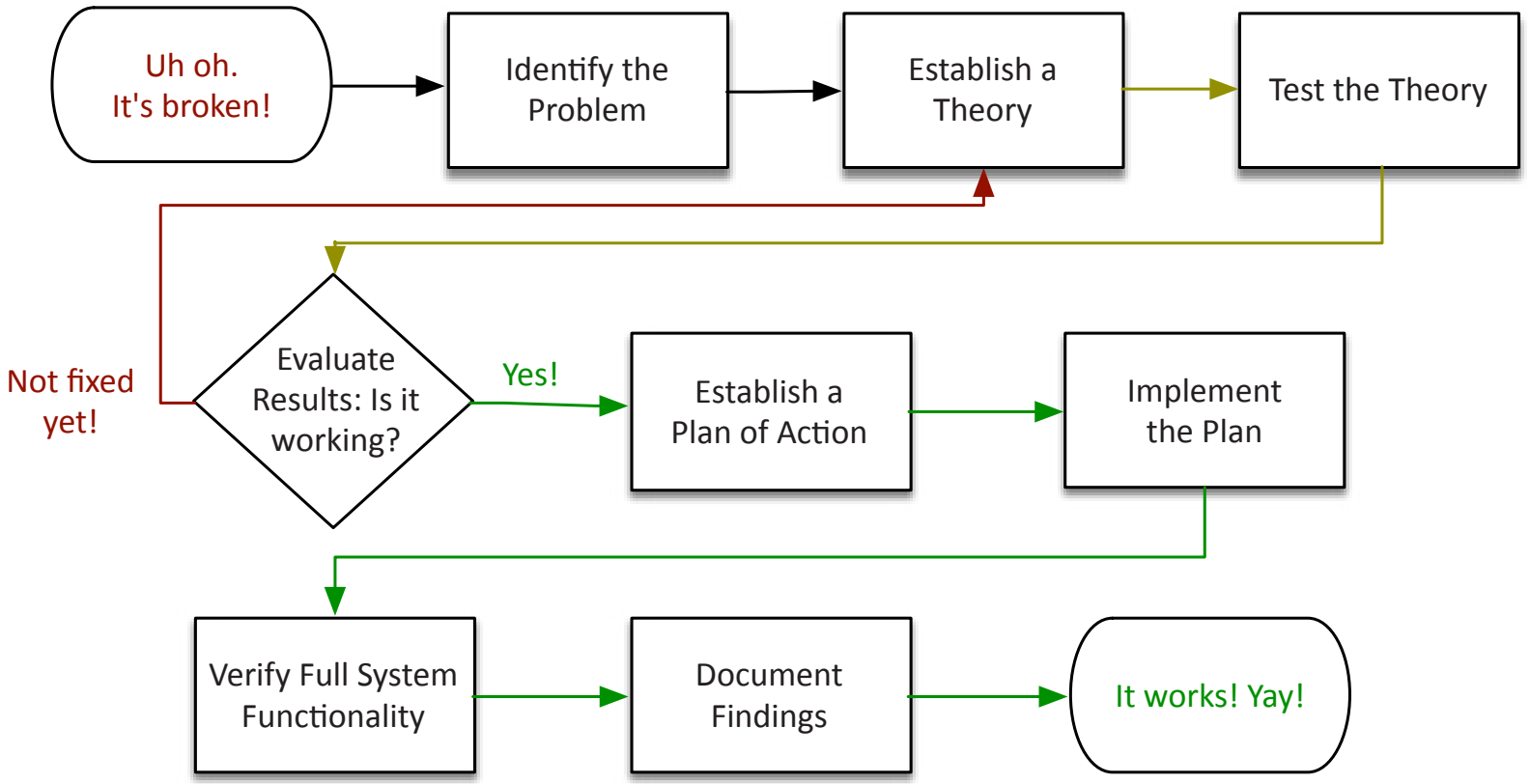
Be on time and avoid distractions
- Don't allow interruptions - No calls, no texting, no Twitter
  - Don't talk to co-workers
- Apologize for delays and unintended distractions
- Create an environment for conversation
- In person - Open and inviting
- On the phone - Quiet background, clear audio

Difficult situations
- Technical problems can be stressful
- Don't argue or be defensive - Don't dismiss, don't contradict
- Diffuse a difficult situation with listening and questions
- Communicate, even if there's no update
- Never take the situation to social media

Don't minimize problems
- Technical issues can be traumatic -
  - Often money and/or jobs on the line
- Even the smallest problems can seem huge
  - Especially when things aren't working
- Part technician, part counselor
  - Computers don't have problems, people have problems

Maintain confidentiality
- Privacy concerns
- Sensitive information on the computer, desktop, or printer
- IT professionals have access to a lot of corporate data
- Personal respect - Treat people as you would want to be treated

The Troubleshooting Process



Identify the problem
- Information gathering - Get as many details as possible
  - Duplicate the issue, if possible
- Identify symptoms - May be more than a single symptom
- Question users - Your best source of details
- Determine if anything has changed - Who's in the wiring closet?
- Approach multiple problems individually
  - Break problems into smaller pieces

Establish a theory
- Start with the obvious - Occam's razor applies
- Consider everything - Even the not-so-obvious
- Make a list of all possible causes
  - Start with the easy theories
  - And the least difficult to test

Test the theory
- Confirm the theory - Determine next steps to resolve problem
- Theory didn't work?
  - Re-establish new theory or escalate - Call an expert

Create a plan of action
- Build the plan
  - Correct the issue with a minimum of impact
  - Some issues can't be resolved during production hours
- Identify potential effects
  - Every plan can go bad - Have a plan B and a plan C

Implement the solution
- Fix the issue - Implement during the change control window
- Escalate as necessary - You may need help from a 3rd party

Verify full system functionality
- It's not fixed until it's really fixed
  - The test should be part of your plan
  - Have your customer confirm the fix
- Implement preventative measures
  - Let's avoid this issue in the future

Document findings
- It's not over until you build the knowledgebase
- Consider a formal database
  - Help desk case notes, searchable database

Study Tips

Exam preparation

- Download the exam objectives, and use them as a master checklist
- Use as many training materials as possible. Books, videos, and Q&A guides can all provide a different perspective of the same information.
- It's useful to have some hands-on, especially with command-line features and Windows recovery options.

Taking the exam

- Use your time wisely. You've got 90 minutes to get through everything.
- Choose your exam location carefully. Some sites are better than others.
- Get there early. Don't stress the journey.
- Manage your time wisely. You've got 90 minutes to get through everything.
- Wrong answers aren't counted against you. Don't leave any blanks!
- Mark difficult questions and come back later. You can answer the questions in any order.