Mr.X.'s TWEAKING AND OPTIMIZING WINDOWS DOC

Updated January 09 2003
x9000@techie.com

(set your page setup to A4 and all margins to 20mm or 2 cms for optimal display and go into options and change to wrap to ruler)

winxp
win2000
biostweaking
internetsecuritysites

INTRODUCTION

I have been messing around with various operating systems for many years now and there's nothing I like better then to get the best performance and stability possible from a system. This text file and its associated files represent some of the best optimising and tweaking tips available on the Windows platform. A lot of these tips I have found out myself and also from various contributors and websites which are listed in these tips. These tips will tell you indepth, the various things you can do to tweak your Windows system and to give you a lot more horsepower.

The tips are split up into sections, Windows 9x, ME, NT, 2000 and XP etc. Also in this document are tips for overclocking your computer, tips for tweaking your Bios, security tips, links to tweaking websites and a small list of some of the more useful programs that I have found on my travels.

Remember backup your data - everyone says it - so do it. Don't go performance crazy and make big broad changes to your system all at once if you are new to tweaking. This just digs you a deep hole real fast and you won't have any idea how to get out. I find the best way to use this document is just to dip in and read.

INDEX

CHAPTER [1]

OPTIMIZING WINDOWS 9x TIPS

(most of these apply for ME, NT, 2000 & XP also)

I shall go through many, many tips here. Some of these tips are only for the more experienced users out there and unless performed right will result in the death of your operating system - you are warned !

One of the biggest performance increases you can do straight away is to make sure you have adequate RAM installed in your machine. The more Ram the better ! - aim for a minimum of 512 meg Ram upwards ! I personally recommend 512 meg Ram for a normal machine as the price of Ram is very good nowadays.

1. Always do a clean install of your Windows operating system
Never upgrade over an existing system. This way you will wont have obsolete files scattered around and the all important registry is kept to a minimum. Only install the Windows components that you really need and always do a custom install e.g. no one needs desktop themes and paint etc installed.

2. Make sure that your hardware is functioning at its best
You don't have to spend a lot of money to get good performance. Make sure you have the very latest drivers for all your devices - if not get onto the manufacturers websites and download them. Also make sure you have the very latest Bios updates for all your hardware devices. Generally speaking if you install the latest operating system available than you will have some of the latest drivers installed onto your computer.

For example here are some areas you should upgrade your drivers for:-
BIOS
Bus Master
DirectX

Gfx
Modem
Network
Scanner
Software e.g. Internet Explorer
Sound

There are some good links to driver sites contained in this document (under internet sites\drivers). If you have a piece of hardware e.g. Modem and havent got a clue who the manufacturer is then check out this useful site
www.fcc.gov/oet/fccid/
Open up your computer case, and take out the no name card. Write down the FCC ID number on the card. Plug the card back in and close up your machine. Go to above web page. Type in the FCC ID number, and then search their database. You will know now who made your no name card and then you can search the web for updated drivers."

3. Cleanliness and organisation / planning drive partitions / downloading files
Install all of your programs onto another drive e.g. into D:\Programs and make some folders up in there to categorise everything e.g. Design, Business, Utils, Comms, Music, Multimedia, Misc etc and install your programs into there. E.g. I would install Photoshop into the Design folder and PC Anywhere into the comms folder. If you are serious about a certain subject than categorise it further e.g. Make folders up in the Utils folder for Diagnostic, Security, Backup, Cleanup, Archivers etc. Replicate this structure into your start menu and so instead of having a start menu that is virtually going across the screen it is only about 10 layers in height. The reason why I install programs onto another drive or partition is so that I can image back the computers operating system very quickly if problems arise - I create 2 main images, using DriveImage - one for the OS and one for the programs.

Before I install a program onto my computer I test it out, either on another computer or on the same computer utilising the excellent program VMWare, available from www.vmware.com - VMWare creates a virtual operating system which programs can be installed into without messing up your system. It is great for testing and evaluating programs as VMWare can revert all changes made to the machine. As you have no doubt gathered the cleaner your computer the quicker it will go ! You could also DriveImage or Ghost your computer and then when you have finished testing programs, restore the last image of your computer, resulting in the same process as the above. Included in this archive is a program I have written called 'Xen' - especially written to remove various temporary files etc that are left over on your hard drive.

PLANNING YOUR PARTITIONS
Besides general convenience, the main advantages of carefully planning and optimising your partitions are that it will make your computer run faster, crash less and be more efficient in general. Besides the broad, important issues of keeping fragmentation down (and thus enhancing system performance overall) with swap file and temp file partitions, separate partitions also makes defragmentation of your hard drive contents go much faster. Having extra partitions also means your data will be a lot easier to recover from accidental deletion because windows won't be writing all its temporary files etc to your data drive and so data recovery will be easy. Pretty much all of the advice given below is appropriate for drives across this entire range of sizes, and even larger.

The best program for organising your partitions is Partition Magic from www.powerquest.com/partitionmagic/index.html

KEEP YOUR C: DRIVE SIMPLE (1st hd - C drive) - 5 gb+ without program files - imaged regularly
Reserve the C: partition for just Windows, and for things that will not work unless they are installed on C: (there aren't many, but there are a few.) Relocate the movable part of Internet Explorer off of the C: drive (it's a little tricky to do that, but it can be done) to save lots of space. Once you decide how much room you really need on C:, allow a little extra 'growing room' - perhaps 200-500 MB.

PROGRAM FILES PARTITION (1st hd - D drive) - 10 gb+ - imaged regularly
Its up to you on this, whether you want to keep your program files and windows together. If windows gets broken restoring a simple ghost or driveimage of windows will take considerably less time to restore, than a big image with all the program files on as well. I have a program files partition of quite a large space and about 15 gig+. One disadvantage is that if I want to test programs etc out I have to image back 2 images (windows and program files images) instead of just one image. Just lately I have just been having one partition for my system and program files and have a partition size of around 10 gig +

TEMPORARY FILES PARTITION (1st hd - E drive) - 500mb at most - never backed up
A handy partition to create is one to hold all of your temporary files and folders. These change most rapidly, and are easily discardable. If they are left on a partition with Windows, with your apps, or with the swap file your computer can get very fragmented and will slow down your computer. I have a 500 MB partition for this (just because I have the room), but rarely use even 25 MB of it. Transfer such folders as MSDownLd.tmp, Recent, Temp, and Temporary Internet Files to this folder. Don't just drag them! Move them as follows:

-Temporary Internet Files (TIF)
Move this from inside of Internet Explorer (Tools | Internet Options), or from the Internet Options applet in the Control Panel. In either case, it is on the General tab, Temporary Internet Files box, Settings button, Move Folder button.

-Temp
You need to relocate this in two places. The first is in your AUTOEXEC.BAT file. To move the Temp folder to the H: partition, for example, the lines would be:
SET Temp=H:\TEMP
SET Tmp=%TEMP%
You must also make a change in the Registry. Go to the following key:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\Temporary Files
Edit the Folder value (in the right pane) to be the location you desire for the Temp folder.

-Recent
You move Recent with TweakUI. Change the value for "Recent Documents."

-Msdownld.tmp
This one needs manual changing from a Registry hack; search for it with RegEdit and alter "C:\WINDOWS\" to whatever partition you are using for this. (I am intentionally vague about how to make this last change. Leave the old (empty) versions of these folders in their old locations. This prevents some general problems with Windows thinking they are there.

DATA PARTITION (on 1st hd or another drive) - size depends on data being created - backed up regularly
One advantage of the My Documents folder is that it gives one common location for all such content. You can just backup the one folder and all of its subfolders, and their subfolders - your entire document hierarchy. But, you might consider moving My Documents from its default location. I have one partition set aside for this. Using TweakUI, as you did for the 'Recent' folder, move My Documents to its own partition. On some versions of Windows, this is even easier: Right-click the My Computers desktop icon, select Properties, then edit the 'Target Folder Location' box.

For one, it ensures greater protection against data loss in the event of a crash or bad shutdown, and especially for a wrongly deleted file. When you delete a file, it is usually possible to undelete it so long as the same part of the hard drive hasn't been overwritten. The Windows partition, and especially the partiton(s) of the swap file and temporary files, will have quite a lot of write activity, even during the course of a reboot. By isolating data files from these, you decrease the chance your wrongly deleted data will be overwritten.

DEDICATED SWAP FILES PARTITION (2nd hd or least used fast drive) - size depends on swap file size - not backed up
You will get your best gain from moving the swap file if you have two physical hard drives. Put the swap file partition as the first partition on the second drive. If you do not have two separate hard drives, the performance gains from this placement will be offset by certain performance degradations, and only by experimentation on your unique computer with your unique usage pattern can you determine whether the net change is a gain, a loss, or no difference at all. Also there is no need to backup this partition as your swap file is created automatically when its deleted.

STORAGE DRIVE (2nd hd or another drive) - much as you can spare - backed up fairly regularly
I have devoted much of my secondary 15 GB drive, about 5 GB of it, to holding downloads of the programs that I commonly use so that I can execute right off the hard drive, rather than off the much slower CD-ROM drive. Most importantly, I have downloaded the entire cab files of the OS CD to my hard drive. That means that any time I want to make any change in my Windows installation, I do not have to put in the CD -it is all onboard and works very fast. Notice that this type of partition does not need to be backed up in your routine backups, since nothing is modified on it. In the event of a crash and data loss, just recopy the CDs to the hard drive anytime you want. You could also put folder below into this partition (incoming files folder).

INCOMING FOLDER (2nd hd - maybe on new partition)
I have a folder on computer that contains all the files coming into the computer. This is checked extensively by virus checkers etc. You could locate this folder on another partition if required but bear in mind files in this folder are constantly being created and deleted and fragmentation will occur.

MULTIPLE OS SYSTEMS ETC
If you are booting multiple operating systems I would use VMWare available from http://www.vmware.com

TEST PROGRAM FILES PARTITION
If you test out loads of programs etc you may want to consider making a test partition for this purpose and when finished you can delete all the files in this partition and just image back your system partition (windows). Or use the excellent VMWare.

Downloading files
Remember these simple rules when downloading files
1 - Read tip 3 in security tips on virus checking etc
2 - Good software will not write to your Registry unnecessarily, nor will it access your proprietary system areas.
3 - Good software will make your puter purr - perhaps even more so than before.

4. Use ram memory rather than the swap file
(Only do this on systems with 256+ megs of ram) Start / Search / Files type and enter: "system.ini" then click on it and open it in Notepad and add this line after [386Enh] (without quotes) "ConservativeSwapfileUsage=1"
This will stop a lot of hard drive accessing and you will notice a definite speed difference.

5. Set file system to cache about many times higher than its default setting
If you goto control panels\system\FileSystem\Performance\typical role of this computer you will probably have desktop computer set here. You can further increase these settings BEYOND the Win9x GUI limit, to the
next level, otherwise unavailable from the System applet, to have your computer cache up to 3 (THREE) times more files and directories, and speed up hard disk performance substantially.
The only disadvantage is that this way Windows will allocate up to 3 times more physical RAM to the file cache, which is taken from the available memory pool, normally used by applications/games. Therefore I recommend doing this ONLY IF your system has at least 32 MB of installed RAM. This works best on computers with 64 MB and up... and who cares about RAM "shortage" if you happen to have 128 MB or more?

Copy & paste the text below in Notepad to create a REG file, and save it for example as MAXCACHE.REG, making sure when you goto save in notepad you change the save as type to all files and then run it. Remember to restart Windows after each change.

-----Begin cut & paste here-----
```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\FS Templates]
@="Max Cache"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\FS Templates\Super Cache]
@="Super Cache"
"NameCache"=hex:00,ff,00,00
```

```
"PathCache"=hex:ff,00,00,00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\FS Templates\Max Cache]
@="Max Cache"
"NameCache"=hex:00,18,00,00
"PathCache"=hex:c8,00,00,00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\FS Templates\Huge Cache]
@="Huge Cache"
"NameCache"=hex:80,13,00,00
"PathCache"=hex:90,00,00,00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\FS Templates\Large Cache]
@="Large Cache"
"NameCache"=hex:a0,0f,00,00
"PathCache"=hex:80,00,00,00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\FS Templates\Medium Cache]
@="Medium Cache"
"NameCache"=hex:20,0f,00,00
"PathCache"=hex:50,00,00,00

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\FileSystem]
"NameCache"=hex:00,18,00,00
"PathCache"=hex:c8,00,00,00
------End cut & paste here------
```

NEW Setting	Cached Files	Cached Directories	KiloBytes [KB]
Super Cache	65280	255	2170 KB (2.1 MB)
Max Cache	6144	200	150 KB
Huge Cache	4992	144	108 KB
Large Cache	4000	128	80 KB
Medium Cache	3872	80	64 KB

Win9x Default	"NameCache"	"PathCache"	Memory (RAM) Used
OLD Setting	Cached Files	Cached Directories	KiloBytes [KB]
Network Server	2729	64	40 KB
Desktop Computer	677	32	16 KB
Mobile/Docking	160	16	4 KB

Alternatively you can use Cacheman which I use for Win9x at www.outertech.com

Now that you have changed the size of the file cache next change the size of the disk cache :-
This tweak allows you control the minimum and maximum amount of memory being allocated as disk cache. It can be used to speed up your system and possibly avoid some memory problems. Using notepad or another text editor, open your SYSTEM.INI file from your Windows directory. Find the section starting with [vcache], and add the following two lines, or modify them if they already exist.

```
MinFileCache=0
MaxFileCache=4096
```

These values set the amount of memory in kilobytes to be used for disk caching, if you have more the 16Mb of RAM you may want to increase the MaxFileCache size, to about 25% of your total RAM (i.e. if you have 128Mb use "MaxFileCache=32768") Restart Windows for the change to take effect. Note: If you are receiving an error like "Error: An I/O subsystem driver failed to load" try increasing the maximum size to 6144.

Alternatively you can use Cacheman for Win9xwhich I use at www.outertech.com

6. Only run the very minimal amount of programs on computer bootup
I have seem some peoples taskbars almost full with the amount of unnecessary applications that are running. Not only does your computer boot up slowly with all these programs loaded, but your system resources are very low. With Windows 98, SE, ME, 2000 and XP versions you can control what programs are loaded at bootup by typing 'msconfig' from startmenu run - click the 'Startup' tab and it will give you a list of all the programs with a tick box next to each one. You can copy MSConfig from 98 onto NT and it will work.

From here you can tick the items you want to run. See if anything unnecessary is running all the time - Press CTRL + ALT + DEL at the same time, after you have first booted up and see what programs are loaded. You may find several programs running that don't need to run all the time. Most of them, if actually needed, can be loaded from the Start / Programs menu or from a home made batch file. Use CTRL+ALT+DEL to end tasks one by one and test the effect. Do not end the Explorer task - being the shell, this is required at all times. And contrary to belief, SysTray is only loaded when required, to run the system tray services it provides: Battery Meter, PC Card Status and Volume Control. When you are satisfied that a program or service is not essential, remove it permanently.

If you have Windows 95/NT you can edit the registry to get at the items that start up from there.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce'
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
Also in the startmenu\startup folder are programs designated to run on bootup.

Startup items in detail
At the very minimum, Windows will quite happily run with no startup options whatsoever. However, depending on your configuration there may be one or two programs which are necessary for certain hardware and software to function correctly.

Power Management - you'll find two entries for LoadPowerProfiles in the registry. These should not be removed if you want to use power management. The reason for having two entries is simple: one is run prior to logon, the other after logon. This makes sense if you bear in mind that with a manual logon it's possible that a user may logoff, leaving the logon prompt on the screen indefinitely. If no power profile is present, this could lead to burn-in.
(Over an extended period it is best to allow the hard-drives to power-down. Likewise with the CPU, if Standby is available). I always remove these entries from startup because I don't need them.

System Tray (systray.exe) - is a program which provides three very specific services that run from the System Tray itself. Note that it doesn't actually provide the System Tray (sometimes referred to - correctly - as the Status Area) since that is fundamentally built-in to the Taskbar provided by the Explorer shell. The three services are: Battery Meter, PC Card Status and Volume Control.

Other items - in the System Tray (next to the clock on the Taskbar) can be removed by simply selecting and opening the System Tray icon (either by a right- or left-click). Usually there are options to disable the item at startup on the icon's pop-up menu. The RealPlayer SmartStart is one such example. If you right-click the System Tray icon, you should find an option to Disable SmartStart. If no option exists on the icon menu, open up the main application itself and look for startup options there.

Task Scheduler - seems to cause many people problems. Selecting Stop using... from the Advanced menu doesn't seem to be sufficient to stop it loading at the next boot. The cause has nothing at all to do with Task Scheduler itself, but to do with the Critical Update Notification that Microsoft "insists" you install. A quick manual check of the Corporate Update site, every week or so, will soon tell you if there are any updates you need - you can even subscribe to one of the many Microsoft bulletins to be alerted of updates as they become available. Use the Add/Remove Programs applet to remove the offending Critical Update Notification and Task Scheduler will remain disabled forever more. You can also if you have it disable Windows Update by using the Update control panel. When you synchronise manually, Task Scheduler is launched automatically. However, it will be disabled at the next boot.

QucikRes - if you need to change resolutions regularly, you may have a QuickRes style icon in the System Tray. If you don't need it, it can normally be removed with Control Panel > Display Properties (or by right-clicking the desktop and selecting Properties). Examine the Settings tab and select the Advanced button. The new General tab normally has the option to disable the System Tray icon. On some systems, right-clicking the desktop has no effect. The cause is generally the QuickRes utility. It loads via rundll and the only way to gain access to the display properties is by using CTRL+ALT+DEL to end all RUNDLL tasks. By disabling the icon from loading in the first place, RUNDLL won't be loaded.

ATI - you may notice another icon in the System Tray. This can be enabled/disabled via the ATI Displays tab of the same dialogue. You may have something similar but the option should appear in the Display Properties dialogue somewhere.

Here are some of the programs I run from here :-

'ScanRegistry'	- Takes a backup of the registry at the first boot of the day and stores it in 'Windows\SysBckup' as a compressed file. By default Windows will keep the last five backups. (Part of operating system)
'RegTest'	- Registry RunGuard program that informs you of anything that has put itself into Windows Startup. Very handy.
'Tweak UI'	- A Microsoft 'powertoy'. Very handy control panel that tweaks many Windows settings. Only use TweakUI 2000 by Microsoft - the one that came on the cd with the first version of Windows was plagued by bugs.
'SchedulingAgent'	- I have routine maintenance and housekeeping chores automated.

The only main programs I have running all the time is a good virus checker which is always kept up to date with the latest definitions and a good firewall. Go to control panels, system and then performance tab - you should aim to have your system resources at around 95%+ once your system has booted up. A useful site that lists a lot of programs and their descriptions on startup is:- www.pacs-portal.co.uk/startup_index.htm

7. Disable "Automatic check for Windows Explorer updates
From the IE "Tools" menu click on "Internet Options" then go to "Advanced" and uncheck the 4th box.

8. Backup your computer using imaging/ghosting software
I back mine up using 'imaging' software called 'DriveImage Pro'. This software will do an identical backup, including all the hard drive sizes etc and create a set of boot disks. You can backup onto various devices. I personally back up onto multiple cd's or even better dvd's If needs be I could have my computer restored back to how it was in less than 15 minutes ! Other good imaging software is 'Norton Ghost' from Symantec.

Image/Ghosting to computer with different hardware
- Using disk image floppies, install your disk image to the new machine. On a new machine, with Windows pre-installed, you could also install to a second partition. That would provide the option of testing the success of the operation before erasing the pre-installed version. You'll need to then set that partition active in order to boot it.

- Boot the new copy.....Windows will be confused. There may be a different motherboard, video card or chip, etc.

- Open Regedit to HKEY_LOCAL_MACHINE and delete the entire Enum key.
(That key holds a record of all hardware ever installed on your computer.... but now it's all wrong and will cause Device Manager to list multiple instances of many components.)

- Reboot and let Plug and Play find the new hardware.

You'll need to make sure you've got access to any drivers that might be needed for the new hardware. If you can put them on a data partition beforehand it might save some trouble. If Plug and Play is not finding the new hardware there may be a driver conflict.....you might try selective installation to narrow down the problem. There will likely also be editing required of system files such as autoexec.bat and system.ini. These files may contain references to an old sound card, video card, etc. Once Windows is settled in its new home you'll need to make a new disk image.

9. Defrag your hard drives on a regular basis
I defrag mine every 2 weeks. Also defrag if possible with a third party defrag utility e.g. Diskeeper or O&O Defrag because. Before you defragment your hard drives make sure you have a fair amount of space on them or you will find your defrag program working away for days on end ! (clear some space before running).

10. Shrink your registry
From Dos type 'SCANREG /FIX'. This will compact the registry and the smaller the registry the quicker your machine will go! Also from Dos type 'SCANREG /OPT' - this only works in Windows Millennium I think. If the registry contains more than 500 KB of empty data blocks, Windows Registry Checker automatically optimizes it on boot (equivalent to doing a scanreg /fix). More details on this page.http://support.microsoft.com/default.aspx?scid=kb;EN-US;q183887

11. Increase Modem Speed
I have seen literally hundreds of tips to increase your modem speed and I must say the majority of them do not make any difference whatsever. The best way to increase your modem speed is to buy a decent modem e.g. US Robotics V90 and have the latest drivers for it installed on your computer. Also make sure that you have no noise on your line - if you have get it sorted. You could also ask your telephone provider to increase the gain on your line.

The next thing you want to do is to increase the speed of your ports - goto controlpanels\system\device manager\ports, click on com1 and goto port settings - change the bits per second from 9600 (default) to 921600. Also change the flow control from Xon /Xoff (default) to Hardware. Do the same to your other com ports e.g. com2.
On a normal line you should get connection speeds from between 44k-51k. Even better get rid of your old analogue modem and get a cable modem or ADSL (if in your area) and banish those awful speed problems forever.

I advise looking into broadband and see if it is available in your area and doing away with your old analogue modem once for all !

Faster Modem Dialing
Waiting to long for your modem to dial? This tip lets you reduce the time it takes your modem to dial, and increase your overall modem connection speed. Open Control Panel | Modems, select your modem and click on Properties. Select the Connection tab, and click on 'Advanced'. In the text box that is labelled 'Extra Settings' at the following text (without the quotation marks) 'S11=40'. The number specified after S11= (in this case 40) is the time for each tone in milliseconds. Lower numbers equals faster dialling. If your having problems connecting try increasing the number until it works. This may not work as planned in some countries and with some modems.

Speed Up ISP Logon Time
On some systems it can take a long time to connect to the Internet, you can decrease the time required to connect to your ISP by trying these simple steps. Open the Dial-Up Networking folder, right click on the icon for your ISP and select 'Properties'. Chose the 'Server Types' tab, and then under Advanced Options uncheck the 'Log on to network' box, and make sure that 'Enabled Software Compression' is checked. From under Allowed Network Protocols uncheck 'NetBEUI' and 'IPX/SPX Compatible'. Next time you connect to your ISP, the connection should be a little faster.

Show proper connection speed
The connection icon in the System Tray may say that you're connected at '115200' (or some other bogus number), when you're actually connected at 26400. This is because Windows may be reporting the port speed (not the actual speed the user at which the user is connected). Open the 'Dial-Up Networking' folder (in 'My Computer').
Right-click on an Internet service icon, select 'Properties,' press the 'Configure' button, click the 'Connection' tab, then press the 'Advanced' button. In the 'Extra settings' field, try adding 'W2' to your initialization string. Upon doing this, you may see a more accurate connection rate the next time you connect to the Internet.

Cable Modem/DSL Tweaks
To increase your broadband Cable Modem speed tip visit www.speedguide.net
Also visit www.x9000.net and download XenTweak
They have some excellent registry and inf files to download specially for cable access.

12. Speedier Boot
Below are some of my own MSDOS.SYS file (located in the root folder of your Win98/95 boot drive, C:\ by default) settings. I am referring here to the [Options] section lines that might give you a few extra seconds at bootup (depending on your System speed and configuration). Here are the lines that might speedup your Win9x bootup.
To edit your MSDOS.SYS take off the read only attribute, double click on it and open it in notepad (make sure you don't have ticked make default program).

```
[Options]
BootDelay=0
BootGUI=1
```

BootKeys=1
BootMenu=0
BootMenuDefault=1
BootWin=1
DisableLog=1
Doublebuffer=X - if have large FAT32 partition (10 Gigs+) or a SCSI hd, I use setting of 1 for the X.
if have a FAT32 partition, (under 10 Gigs), or using FAT16, disable this by inserting a 0 for the X
Drvspace=0 - should be 1 if you are using a compressed drive
Dblspace=0 - should be 1 if you are using a compressed drive
LoadTop=0
Logo=0
Network=0

Uncheck floppy search
Go to control panels\system\ - click on filesystem and then floppy disk tab and uncheck search for new floppy disk drives each time your computer starts for a quicker boot up.

13. Edit system.ini for best settings
Goto windows folder, right click on system.ini and click edit. Change or add these settings under [386Enh]

32BitDiskAccess=ON
To turn on 32-bit disk access in Windows for maximum performance. To disable 32-bit access ONLY for troubleshooting purposes (NOT recommended), replace ON with OFF.

ConservativeSwapfileUsage=1
Windows 98/ME ONLY: To disable the "PageFile_Call_Async_Manager" feature that allows the Memory Manager to asynchronously write out swap file buffers during VFAT idle times. This reverts swap file usage back to Windows 95 style, and forces the use of the computer's physical memory (faster) first, before the use of the slower hard disk virtual memory (swap file). Default is enabled (0). Only recommended if you have 256 meg + RAM.

DMABufferSize=64
This ensures that your DMA devices always have enough memory allocated.
(Note: Only use if you have one or more DMA enabled devices installed and enabled). Affects ALL I/O (Input/Output) DMA operations: soundcard FM/wavetable, MIDI playback/recording, disk buffered reads/writes. Default value is 16. In Windows 9x/ME this can also be done in: Control Panel -> System -> Device Manager tab -> System devices -> Direct memory access controller -> Settings tab -> check Reserve DMA buffer box -> 64 K bytes reserved -> OK -> OK

PageBuffers=32
This setting buffers the hard drive to RAM which is more efficient than letting Windows dynamically handle the buffer .

Change or add these settings under [vcache]

Minfilecache= ?
Set the minimum value to 10% of your installed system RAM, multiplied by 1024.
(Example: 256 x .10 = 25.6 x 1024 = 26214).
I prefer using Cacheman for this purpose http://www.outertech.com

Maxfilecache= ?
Set the maximum value to 25% of your installed system RAM, multiplied by 1024.
(Example: 256 x .25 = 64 x 1024 = 65536). I prefer using Cacheman for this purpose.

Chunksize= ?
The most commonly used values are 128, 256, 512, 1024, and 2048 . On WinMe,1024 seems to work the best.
If you have a very large Harddrive, (30Gig +), you may want to set this value to either 2048 or 4096. I prefer using Cacheman for this purpose.

As a rough guide :-

RAM	MinFileCache	MaxFileCache
8 MB	1024	2048
16 MB	2048	4096
32 MB	4096	8192
64 MB	8192	16384
128 MB	16384	32768
256 MB	32768	65536

14. Use a RamDisk
The ram disk XMS which in my view is the best can be extended to up to 2 GB, depending on the installed RAM. This RAMdisk driver works with EMS and XMS. Here is a solution to keep your hard drives "filthy clean". I use XMS/EMS RAMdisk v1.9i for DOS
ftp.simtel.net/pub/simtelnet/msdos/ramdisk/fu_rd19i.zip
to create a 46MB RAM disk (H:) in extended memory, by adding a Autoexec.bat line

LH XMSDSK.EXE 46080 H: /C1 /T /Y

46080 = RAM size in k
H: = desired drive letter

/C1 = cluster size of 512 Bytes. /C2 = 1024, /C4 = 2048 (only doubling works, not 3 or 5).
/T = use RAM from top in 1 block (highly recommended for proper operation).
/Y = to disable the confirmation prompt for uninterrupted operation.
If using a folder other than the root folder of your RAM drive (recommended!)
for the MS IE temporary cache files, you need to add another Autoexec.bat line
below the line that loads XMSDSK to create the respective directory (example
using the same RAM drive letter above). Add next line to Autoexec.bat also

MD H:\TEMP

I load XMSDSK in upper memory by using UMBPCI.SYS [Uwe Sieber's freeware upper memory manager] in my Config.sys:
DOS=HIGH,UMB
DEVICE=C:\WINDOWS\HIMEM.SYS /NUMHANDLES=120 /TESTMEM:OFF /Q
DEVICE=C:\MAX\RAM\UMBPCI.SYS

You can turn on or off your RAMdisk by running XMSDSK again with the /U
switch: XMSDSK.EXE /U /Y or you can disable it altogether by typing a double colon (::) or REM in front
of the XMSDSK Autoexec.bat line.

Note that I have 256MB of RAM installed in my computer, so I can "afford" to spare 46MB for a RAM disk. I recommend a 20-30MB RAM disk for users with 128MB RAM installed. Users with less than 128MB RAM may want to skip this procedure altogether, to avoid taking needed system memory away from Windows.It is necessary to use a large RAM disk because MS IE [all versions] needs space to hold all temporary files (including zips, mp3s, movies, pics etc) downloaded from the net into its cache until the download is completed [no matter if the IE Download folder is located somewhere else].

I also modified the Registry (using Regedit) to change all temporary/internet folders (Recent, MS IE 5's Cookies, Favorites, Links, History, Temporary etc) to the H:\TEMP directory on the ram drive (H). I did this because I prefer erasing the entire IE cache every time my computer boots, instead of keeping the internet files, which can only add to disk bloat. If I want to save an HTML page or a pic I do it manually from the IE's File menu [Save as...]. These are the relevant Registry keys for setting IE's folders on the temporary RAM disk [long key names between square parenthesis may wrap in and they need to be on a single row for proper operation]. Text below can be saved (using cut & paste) as a REG file [I called it TEMPRAM.REG].

You will have to customise these paths e.g. H:\\Temp to suit your own liking:-

-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Special Paths\Cookies]
"Directory"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Special Paths\History]
"Directory"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths]
"Directory"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\Path1]
"CachePath"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\Path2]
"CachePath"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\Path3]
"CachePath"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\Path4]
"CachePath"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Extensible Cache\MSHist011999032319990324]
"CachePath"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Content]
"CachePath"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Cookies]
"CachePath"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet

Settings\Cache\History]
"CachePath"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Url History]
"Directory"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\UrlHistory]
"Directory"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content]
"CachePath"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies]
"CachePath"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History]
"CachePath"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist011999092319990924]
"CachePath"="H:\\TEMP"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist011999032319990324]
"CachePath"="H:\\TEMP"

[HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders]
"Favorites"="H:\\TEMP"
"Cache"="H:\\TEMP"
"Cookies"="H:\\TEMP"
"History"="H:\\TEMP"

[HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders]
"Favorites"="H:\\TEMP"
"Cache"="H:\\TEMP"
"Cookies"="H:\\TEMP"
"History"="H:\\TEMP"
------End cut & paste here------

The RAM disk can also be used to hold the TEMP directory used by Windows 9x and MS-DOS 7 to the RAM drive, but beware of installing large programs that require megabytes of disk space to hold their temporary files during installation, and which will not fit into a small RAM disk.
Default Win9x TEMP folder [if not changed in Autoexec.bat or Config.sys] is C:\WINDOWS\TEMP.
I changed mine point to my fastest hard drive (D), by adding these lines to my Config.sys:
SET TEMP=D:\TEMP
SET TMP=D:\TEMP
where I also keep my Win98 swap file, by adding these lines to my System.ini file [located in C:\Windows], which can be edited in Sysedit, Notepad or Msconfig [this last one can be used only by Win98/98 SE owners]:
PagingDrive=D:
PagingFile=D:\TEMP\WIN386.SWP

Another way to redirect (and empty periodically by deleting all temporary files) your MS IE 4/5/6 Cache, Cookies, Favorites and History folders to a different (single) location (i.e. a RAM disk) is to use these 98lite CacheCloak INF files from www.98lite.net

To learn how to install a RAM disk in Windows NT 4.0 or 2000, install the free MS Win2000 RAMDISK.SYS:
http://support.microsoft.com/support/kb/articles/q257/4/05.asp
http://download.microsoft.com/download/win2000ddk/sample01/1/NT5/EN-US/Ramdisk.exe
and read these guides:
www.cyberwizardpit.com/article3.html
http://msclub.cs.nwu.edu/projects/Ramdisk/

15. Fonts
Make sure that you only have the bare minimum standard fonts installed on Windows for performance. If you want to add more than use a font manger program, such as Adobe Type Manager and don't activate more than 500 as your system may refuse to boot. Xen's major cleanup option copys all your fonts into a _fontbak folder and just keeps the fonts supplied with windows and is useful for clearing out countless numbers of useless fonts. If you find a program needs a particular font you can always copy it back to your fonts folder from _fontbak.

16. Increase your hard disc access speed, enable DMA 66 and Scsi drives
Goto control panels\system and click on device manager. Goto disk drives and click on your hard drive, goto properties and click

the settings tab and then tick the DMA box. Do this for all your hard drives. If on next boot the tick disappears then one or more of your hard drives don't support DMA access.

Windows sees your hard drives as though they were on one IDE channel. You may be able to squeeze a few more drops of performance out of those disks by: right-clicking on 'My Computer' and pulling up its 'Properties', selecting the Device Manager tab, then opening the Hard Disk Controllers section. At that point, you should see your device controller at the top of the list (something with the words Bus Master in it, most likely); pull up its Properties and flip to the Settings tab. Select 'Both IDE Channels Enabled' from the drop-down menu, reboot, and see if you've made a difference.

By default support for Ultra DMA 66 is not enabled. The registry settings below will enable Ultra DMA 66. Ultra DMA 66 has a maximum bus transfer of 66mb/sec this is twice the bandwidth of Ultra DMA 33. While this will inherently not enhance the speed of devices on the bus it will provide more maximum bandwidth. This tip is needed on PCs that contain hard disks that support Ultra DMA 66.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}\0000
add a new DWORD value called EnableUDMA66 with a value of 1.

Scsi Hard Drive Speedup
SCSI hard disks are usually used in high end systems and servers where data protection is more important then performance. This is why the write cache is disabled by default. This can be enabled. Enabling the write cache on a drive will increase its write performance considerably. On the other hand, data is physcially written to the disk after a few second delay. If power is lost during this time data loss and corruption can occur.
Right click my computer. Go into device manager, double Click Disk Drives, right click the appropriate drive, click properties, click the disk properties tab, click write cache enabled, click ok, reboot if neccessary.

17. Installing numerous copies of the OS?
Edit msbatch.inf to place the CD key into the setup for you.

18. Delete temporary files at bootup
By putting this line in your autoexec.bat DELTREE /Y C:\WINDOWS\TEMP*.* or even better put xenclean into your startup folder (which comes with Xen from www.x9000.net) you can cleanout your temporary files on startup.

19. Increase your CPU Priority
This will speed things up by using the fastest priority to the CPU when opening any program, and works with 99% of the PCs I've tried it on.To reset to Windows 9x default, type 3 in place of 1 in CPU Priority field.

-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\BIOS]
"CPUPriority"=dword:00000001
"FastDRAM"=dword:00000001
"PCIconcur"=dword:00000001
------End cut & paste here------

To reset to Windows 9x/ME default, type 3 in place of the 1. Here are other DWORD Values (Decimal) you can use to tweak your CPU Priority even further (under the same Registry key above):

PCIConcur = 1 (enabled)
FastDRAM = 1 (enabled)
AGPConcur = 1 (enabled) [if your video controller is AGP based].
These settings speed up hardware specific operations by allowing installed devices to use extra CPU cycles: PCI, AGP and/or DRAM based I/O transfers from the motherboard interface/bus/bridge (PCI, AGP, DRAM) [-> to the motherboard chipset/bus/bridge where applicable] -> to the CPU, and the other way around."

20. Turn off modem logging in Windows 9x
By default all modem activity is logged into a text file called after your modem's name installed in Control Panel -> System -> Device Manager -> Modem-> Your modem name. This file is located in your Windows folder (default), and has the .LOG extension. Example: if the name of your installed modem is "US Robotics 56K Fax INT PnP". But you can disable ALL modem logging by applying a simple Registry change. First, make sure your modem is completely disconnected (offline). Then run Regedit and go to:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\Modem\0000
Your modem might be found under the 0001, 0002, 0003 etc keys, depending on your particular setup, and on how many modems were installed on your system (i.e. if you replaced your old modem with a new one). The String to modify is "LoggingPath". Double-click on it and delete ALL characters found there.

21. Turn off Read-ahead optimization
Read-ahead optimization was intended to speed up hard drive access. If activated, Windows reads some blocks more that needed from the HD and 'hopes' the program will need the data later. It will work if you use only 1 application at once, but this is not always the case. As soon as 2 programs try to access the hard drive at the same time the Read-ahead reading will slow down things up to 50% !In many cases DISABLING Read-ahead optimization will give your a huge performance boost - just give it a try ! Go to control panels\system\performance\file system and turn down read ahead optimization. This setting retrieves cached data and can actually interfere with high data rates. In short, less is more.

22. Control your recycle bin
This applies to all windows versions. By default, both the Recycle Bin and Internet Explorer's Cache want to consume ridiculous amounts of your hard drive space. Right click on the Recycle Bin, select Properties, and on the Global tab, decide how much space you want the Recycle Bin to consume, either for all drives in your system, or on a per-drive basis. It's a percentage of the total space. I adjust the slider way to the left, so I'm using "only" a few hundred megs of space for trash.

Similarly, open Internet Explorer, and select Tools/Internet Options. Under Temporary Internet Files, click the Settings button and select a reasonable size for this cache area. Generally speaking, if you have a fast connection, 5 Mbytes to 10 Mbytes is adequate; 25 Mbytes or so is usually enough with a slower dial-up connection.

23. Asynchronous or Synchronous
Windows uses Synchronous Buffer Commits by default i.e. it checks that data has been correctly written to the disk drive. This alteration will enable Asynchronous Buffer Commits. There will not be a check to ensure data has been written to disk. Therefore there is a possibility of data loss should an 'event' occur.
Consider carefully before deciding to use this, even though the speed benefit may be notable.

Backup the Registry, run RegEdit, and locate the Key below
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem]
In the right pane, alter the Value Data of AsyncFileCommit to either:
0 for Synchronous
1 for Asynchronous

This can be also achieved the easy way by running Control Panel -> System -> Performance tab -> File System button -> Troubleshooting tab -> place (asynchronous mode) or remove (synchronous mode) the check mark in the "Disable synchronous buffer commit" box -> restart Windows.

24. Disable sound effects
Goto control panels\sound and multimedia and switch all your sounds to none. This way you wont have annoying startup, shutdown and other sounds all the time and a slightly quicker boot and shutdown time.

25. When installing new software
If there is an option for Custom settings, it is often best to choose it. This way, you can install only those features you want, and avoid those you don't. This means the program will take up less disk space.

26. Analyse whats booting up
Right for this next tip I would advise doing a backup before performing it. Do you find that your computer takes an unusually long time to load into Windows? - well this tip could make your windows machine boot up like its on steroids !! First download 'BootLog analyser' from www.vision4.co.uk/vision4 and install it onto your computer. Reboot your computer, press 'F8' or ' CTRL' key at bootup and choose the "Step-by-step confirmation" option from the "Windows 9x Startup Menu". Type Y for "Yes" to "Load all Windows drivers" when prompted. Now have your stop watch ready and start timing from the moment you press Y. Then stop the timer when the Win9x "Working in Background" cursor stops spinning or until it is replaced for the last time by the default "Normal Select" cursor. Or you can create a bootlog file for the analyser to analyse, hit F8 (or CTRL) at bootup and select option 2. Logged (\BOOTLOG.TXT).

Open BootLog Analyzer and take a look at all the drivers that loaded successfully. Mark down the longest times (10 seconds and above). Possible "culprits" that you might not even need on your particular Win9x system setup, and should consider removing (most of them located in C:\Windows\System and/or C:\Windows\System\Iosubsys), are:
- VNBT.386
- NDISWAN.VXD
- other Networking (LAN, WAN, Novell, IBM etc) .386, .DLL, .DRV, .EXE or .VXD drivers/executables, ONLY IF you know you are NOT connecting to or using such Networks.
- DRVWPPQT.VXD
- DRVWQ117.VXD

The first 2 drivers on this list belong to the "Microsoft Virtual Private Networking Adapter", which is NOT setup/used on my machine. BootLog Analyzer reported these 2 were EACH taking about 15-20 seconds to load! Geez... Talk about time wasting! So I moved them "PRONTO" from C:\Windows\System to a backup folder Further more, BootLog Analyzer reported a total loading time of 15 seconds for all the "TAPEDETECTION" sections (about 6 of them!) in my BOOTLOG.TXT. Since I don't use, or have any intention of getting a tape drive, I started a Registry search using the Windows 9x built-in Registry Editor (Regedit.exe, located in the Windows folder) for the TapeDetect string: click Edit -> select Find -> type the text string you want in the "Find what:" box (TapeDetect in this case). Then I deleted ALL references (Registry keys, subkeys and values) returned by the search (but I made a full registry backup), and also moved the two .VXDs (DRVWPPQT.VXD and DRVWQ117.VXD above) from C:\Windows\System\Iosubsys to the backup folder. Then I rebooted one more time. Guess what? This way I managed to "shave off" almost an entire minute from the GUI loading time. Now we're talking!

Bootlog.txt Failures in logfile
When you review the BOOTLOG.TXT file in the root folder on your hard disk, you may see the following lines even though your computer seems to function properly:-

LoadFailed = dsound.vxd LoadFailed = ebios LoadFailed = ndis2sup.vxd LoadFailed = vpowerd LoadFailed = vserver.vxd LoadFailed = vshare InitCompleteFailed = SDVXD

The following lines may appear only in the Windows 98 BOOTLOG.TXT file:

SysCritInitFailed = JAVASUP DeviceInitFailed = MTRR
These load failures do not necessarily mean that there is a problem. It is common for some, if not all, of these to fail, depending on your system configuration.

DSOUND
Many sound drivers are DirectSound enabled. DirectSound is part of Microsoft DirectX, a set of libraries used by most newer Windows-based games. When a DirectSound-enabled sound driver is loaded, it attempts to register with the DirectSound library so that games can use it. If no DirectX-based games are installed on your computer, the DirectSound library fails to load. This is normal.

EBIOS
The extended BIOS driver did not find an extended BIOS, so it does not load.

NDIS2SUP.VXD
The NDIS 2 support driver did not find any NDIS 2 drivers to support, so it does not load.

VPOWERD
The Advanced Power Management (APM) driver determined that your computer does not support APM, so it does not load, or APM support may be disabled. To determine if you have inadvertently disabled APM in Device Manager, follow these steps:

In Control Panel, double-click System.
Click the Device Manager tab. Double-click the System Devices branch to expand it. Double-click the Advanced Power Management Support branch. (If this branch does not exist, your computer does not support APM.) Click the Settings tab. Verify that the Enable Power Management Support check box is selected.

VSERVER.VXD
Vserver.vxd does not load statically so that it can save memory by loading later in the boot process only if it is needed. For example, Vserver.vxd might not be needed when you start a laptop computer while it is out of its docking station.

VSHARE
If you examine the Bootlog.txt file, you will notice that VSHARE loaded successfully earlier in the boot process. The second copy of VSHARE detects that VSHARE is already loaded and does not load.

FONT FAILURES
When Font Manager searches the hard disk for fonts, it may find shortcuts in the fonts folder (C:\WINDOWS\FONTS), which point to font files (e.g., TTF files) which are in the fonts folder already. The solution is to remove those font shortcuts from the fonts folder.

INITCOMPLETEFAILED=SDVXD
Windows 95/98 automatically loads a miniature disk cache to increase the speed of the boot process. When the boot process is complete, the miniature disk cache is unloaded from memory. When it is unloaded, the above line is added to the Bootlog.txt file to indicate that the miniature disk cache has been removed from memory.

This next part is normal behaviour...

SYSCRITINITFAILED=JAVASUP
The Java Support driver is not needed on your computer, so it did not load. Java is a programming language used on the World Wide Web (WWW). Microsoft Internet Explorer versions 3.0 and later include a Java subsystem.

DEVICEINITFAILED=MTRR
Memory Type Range Registers (MTRR) is a .vxd file responsible for manipulating memory ranges. This file is loaded with DirectX 5.0, however, none of the DirectX core components use the service provided by MTRR. However, NTKERN and some display drivers do use the service provided by MTRR to change memory ranges.

27. Case of filenames
Stop Windows from changing the case of your filenames to upper or lower case and have them changed to how they are bloody typed in! Start regedit.exe.

-----Begin cut & paste here-----
REGEDIT4

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"DontPrettyPath"=dword:00000001
------End cut & paste here------

Set the value to 1 to keep the case as you type it or 0 to adjust the case as Explorer requires.
Click OK. Close regedit.

28. Defrag the registrys hive files
I do NOT recommend performing this tip on Windows 95 - only on Windows 98. If using this tip on Windows 95 than you will more than likely get a corrupt registry so don't do it on Windows 95!

What we are going to do is compact the registry. This process can take up to a couple of hours to perform so only do it if you can spare the time. Before you perform this option I suggest you run Microsofts RegClean (see programs I recommend further down this file). Regclean doesnt actually take the entries out of the registry but marks them as not being used anymore. Basically we are going to export the registry into one big file and import it again and it MUST be done in these steps !

a - Run Microsofts RegClean program
b - Boot up in pure dos mode, using a bootdisc (do not use restart in dos mode on shutdown)
    Or press 'F8' at startup and boot the computer to a command prompt.
c - Type 'smartdrv.exe 2048 16' - this will speed up copying.
d - In pure dos mode type 'regedit /e c:\export.reg'
    (Will take some time- the e switch exports the registry)
e - Rename the existing registry files e.g.
    rename c:\windows\classes.dat _classes.dat
    rename c:\windows\user.dat _user.dat
    rename c:\windows\system.dat _system.dat
f - Type 'regedit /c c:\export.reg' (Will take some time - the c switch condenses the registry)

g - Restart your computer once step f has finished and if there is a problem you can delete the new registry and rename back the registry you renamed. If everything is fine which it should be than you can delete the export.reg from your c drive.

I've found that you can significantly shorten the overall processing time by exporting the registry using the GUI version inside Windows, then rebooting to the command prompt and then start at step e above. Either way will do the same thing. Thats it the registry has now been recreated and if you compare the file sizes of the registry files you have probably saved in most cases megabytes in file size ! Think of it as a major defrag of the registry because it does defragment the registrys hive files.

UPDATE : goto startmenu, run, type command and press enter. Type 'scanreg /OPT' and reboot if necessary.
Repeat but type 'scanreg /FIX'

29. Change default IE pages

Internet explorer default pages for events such as navigation canceled, navigation failed, offline information, and blank page are stored in the registry. You can replace these pages with your own.

Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\AboutURLs
Modify the key values to the full path on the hard drive. C:\page.htm

30. Save your Dial up password

Go to 'Control Panel' and click 'Network'. Make sure you have 'Client for Microsoft Networks' to save trouble. If you don't have it this is why your Internet Dial-up Password wouldn't save. Click on 'Dial-Up Adapter' and select Advanced. Go to 'IP Packet Size' and experiment with Small, Medium, and Large packets to see which one works best for you. This is similar to the program MTUSpeed that would change this setting for you. Also there is a value in your registry called 'SLOWNET' and it is usually set at '01' change this to '00' It won't dramatically increase your transfers but it will reduce timeouts. The key is as follows:
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\Net\0001]

31. Remove duplicate devices

To improve your system's reliability and gain some more speed, you should remove the multiple devices that build up when changing drivers and hardware. Restart your PC in Safe mode (Press F8 while system is booting and choose Safe Mode from the menu). Right-click on the "My Computer" icon, choose "properties", open the "Device Manager" tab. Check all the device categories, and remove all but the first instance of the devices on your system.
Note: Don't change your devices' properties while in Safe Mode.

32. Increase simultaneous HTTP connections

To abide by the HTTP specifications Windows limits the number of simultaneous connections that it will make to a single HTTP (web) server. This affects all Windows Internet applications that use the standard API, including Internet Explorer. The behavior can be seen when downloading multiple files from a web site only a certain number (2 or 4) will be active at any one time.

Create two new values, or modify the existing values, called 'MaxConnectionsPerServer' and 'MaxConnectionsPer1_0Server'. Change the values to equal the number of simultaneous requests allowed to a single HTTP server, the default values are 2 and 4 respectively.

```
-----Begin cut & paste here-----
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Setting]
"MaxConnectionsPerServer"=dword:00000004
"MaxConnectionsPer1_0Server"=dword:00000008
------End cut & paste here------
```

33. Problem installing/updating a device?

Here's a fix that applies to both Windows 98 and Me. If you have problems installing or updating drivers for a device, you may want to make a totally clean start. To do that, physically unplug the device and uninstall it via Device Manager. Then, go to the C:\Windows\Inf\Other directory and remove any files you find there for the device. (The Inf directory is hidden, so you'll need to set Explorer to view hidden files in Tools | Folder Options.) Next, remove the files DRVDATA.BIN and DRVIDX.BIN from c:\Windows\Inf and reboot. Windows will recreate those two files when you reboot and it detects the hardware again.

34. Turn off Throbbers in Windows 98, IE4, IE5 and IE6

A "throbber" is theanimated graphic that appears in the upper right corner of most web browsers. The function of a throbber is to let the user know, by displaying animation, that the browser is busy retrieving information. I find windows open and close quicker with these turned off. As usual copy and paste the details into notepad, put an extension onto the end called .reg and change the save as type to all files, save it and double click it to enter the details into the registry.

To turn throbbers OFF in Internet Explorer :-

```
-----Begin cut & paste here-----
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\WebBrowser]
"ITBarLayout"=hex:0c,00,00,00,4c,00,00,00,74,00,00,00,1a,00,00,00,10,00,00,00,\
  17,00,00,00,05,00,00,00,6a,00,00,00,26,00,00,00,01,00,00,00,e0,00,00,00,e0,\
  01,00,00,02,00,00,00,29,00,00,00,44,00,00,00,04,00,00,00,09,00,00,00,33,00,\
  00,00,03,00,00,00,09,00,00,00,42,00,00,00
------End cut & paste here------
```

To turn throbbers back ON in Internet Explorer :-

```
-----Begin cut & paste here-----
REGEDIT4
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\WebBrowser]
"ITBarLayout"=hex:0c,00,00,00,4c,00,00,00,74,00,00,00,18,00,00,00,1f,00,00,00,\
  74,00,00,00,01,00,00,00,e0,00,00,00,a0,0f,00,00,05,00,00,00,22,00,00,00,26,\
  00,00,00,02,00,00,00,21,00,00,00,a0,0f,00,00,04,00,00,00,01,00,00,00,e3,01,\
  00,00,03,00,00,00,01,00,00,00,67,00,00,00
------End cut & paste here------
```

To turn throbbers OFF in the shell:-

```
-----Begin cut & paste here-----
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\ShellBrowser]
"ITBarLayout"=hex:0c,00,00,00,4c,00,00,00,74,00,00,00,1a,00,00,00,10,00,00,00,\
  17,00,00,00,05,00,00,00,6a,00,00,00,26,00,00,00,01,00,00,00,e0,00,00,00,56,\
  00,00,00,02,00,00,00,29,00,00,00,57,00,00,00,03,00,00,00,a8,00,00,00,00,00,\
  00,00,04,00,00,00,09,00,00,00,55,01,00,00

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\Explorer]
"ITBarLayout"=hex:0c,00,00,00,4c,00,00,00,74,00,00,00,1a,00,00,00,13,00,00,00,\
  33,00,00,00,05,00,00,00,6a,00,00,00,26,00,00,00,01,00,00,00,e1,00,00,00,df,\
  01,00,00,04,00,00,00,01,00,00,00,bd,00,00,00,02,00,00,00,20,00,00,00,8d,01,\
  00,00,03,00,00,00,09,00,00,00,b8,00,00,00
------End cut & paste here------
```

To turn throbbers back ON in the shell:-

```
-----Begin cut & paste here-----
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\ShellBrowser]
"ITBarLayout"=hex:0c,00,00,00,4c,00,00,00,74,00,00,00,18,00,00,00,1f,00,00,00,\
  74,00,00,00,01,00,00,00,e0,00,00,00,a0,0f,00,00,05,00,00,00,22,00,00,00,26,\
  00,00,00,02,00,00,00,21,00,00,00,a0,0f,00,00,04,00,00,00,01,00,00,00,77,01,\
  00,00,03,00,00,00,01,00,00,00,35,00,00,00

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar\Explorer]
"ITBarLayout"=hex:0c,00,00,00,4c,00,00,00,74,00,00,00,18,00,00,00,1f,00,00,00,\
  74,00,00,00,01,00,00,00,e0,00,00,00,a0,0f,00,00,05,00,00,00,22,00,00,00,26,\
  00,00,00,02,00,00,00,21,00,00,00,a0,0f,00,00,04,00,00,00,01,00,00,00,a0,0f,\
  00,00,03,00,00,00,01,00,00,00,00,00,00,00
------End cut & paste here------
```

35. Unload DLLs upon closing

Windows Explorer will usually try and cache DLL's by keeping them in memory even after the application using them has been closed. This can cause performance problems on low memory systems, and can be annoying when developing on Windows and the DLL's remain in use. This applies for all versions of Windows

```
-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer\AlwaysUnloadDLL]
@="1"
------End cut & paste here------
```

36. Idle your CPU when not busy

Don't do this for NT, 2000 or XP as they have somthing similar built in.

```
-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\CPUIdle]
"Idle"=dword:00000001
------End cut & paste here------
```

37. Increase mouse rate

A slow mouse sample rate can cause "frag lag" in a 3D shooter, as the mouse movement will trail the frame rate of a fast system. You need either a USB mouse or a tool like PS2Rate. PS2Rate Plus changes the refresh rate of your PS/2 Mouse from the default 40hz up to a whopping 200hz!! Perfect for gamers wanting that extra bit of precision, or just a really slick mouse for your desktop. The plus version comes with an installer and a utility for testing your current mouse rate. Goto www.students.tut.fi/~zibbo/other/ps2rate/ps2rate.zip to download this.

If you have a Logitech mouse than you can increase the PS2 rate of it. This will stop your mouse from flickering and give you a better edge in online gaming !

```
-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\Software\Logitech\MouseWare\CurrentVersion\Technical]
"PS2ReportRate"="40"
------End cut & paste here------
```

38. Keep IE crash free
Here's a tip for keeping IE crash free. Go to the control panel start, settings, control panel and open Internet Options. Under the General tab you'll see Temporary Internet Files and two buttons called "delete files" and "settings", click the settings tab. Click View Objects. You should see 1 or more downloaded programs. Select all and delete them. Do this regulary. Also keep your temporary internet files to a minimum and clear them out regularly.

39. Save Icon positions 1
You've got all your windows sized, icons placed the way they look great.... explorer crash!
(Or, the thing crashes not that much anymore, but it seems to forget sometimes...) And there you go again.. but, there's a way to recover all your settings, that's windows placing, sizing and icon positions, with just one click. First, make it all look, once more, just the way you want it to be. Now these settings are in the Registry, open it and go to:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer

- Launch RegEdit and select:
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Streams
and export it to a file called "MyWindows1.reg" (don't type the quotes).

- Launch RegEdit and select:
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StreamMRUand export it to a file called "MyWindows2.reg".

- In Notepad, open "MyWindows2.reg", select all text except the first line (REGEDIT4), and press Ctrl+C to copy the selected text to the clipboard.

- In Notepad, switch to "MyWindows1.reg", go to the end of the text, and
press Ctrl+V to paste the text copied from "MyWindows2.reg".

- In Notepad, save the modified "MyWindows1.reg" to a directory on the hard disk. Eventually, change its name to "MyWindows.reg", or any other name you like.

40. Icon Positions 2
In Windows 95/98/ME/NT/2000/XP you can lock down the position of the Desktop icons, using a couple of files from the MS Windows NT 4.0 Resource Kit. Copy Layout.dll into C:\Windows\System for Windows 9x or into your system32 folder if using NT, 2000 or XP and doubleclick on layout.reg.
Then right-click on the "Recycle Bin" or "My Computer" icon, and choose to "Save [or Restore] Desktop Icon Layout".
There are several 3rd party tools that also do this, but these files are free and only 14 KB in size."
http://borg.isc.ucsb.edu/ftproot/pub/windows/winnt40/RESKIT/Server-Post_Installation/

41. Overclock your Gfx card
(also see section in this guide on overclocking your gfx card)
If you are using an Nvidia card or 3dfx card with the drivers v32x or v40x than this Regedit add-on will give you an additional window in your display control panel. It appears under Hardware Options under Additional Properties which is under the Advanced Controls in the display properties. Only overclock to another 10% of original values.

If you have an NVIDIA card copy & paste the text below in Notepad to create a REG file, and save it for example as GeForce.REG, making sure when you goto save in notepad you change the save as type to all files and then run it. Remember to restart Windows after each change.

-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\Software\NVIDIA Corporation\Global\NVTweak]
"CoolBits"=dword:ffffffff
------End cut & paste here------

If you have a 3DFX copy & paste the text below in Notepad to create a REG file, and save it for example as 3DFX.REG, making sure when you goto save in notepad you change the save as type to all files and then run it. Remember to restart Windows after each change.

-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\Software\3dfx Interactive\3dfx Tools\Installed\Tools\{AB040305-8AA1-11D2-8DD1-00104BB5EAD6}]
"CompleteRegistration"=dword:00000001
------End cut & paste here------

42. Make sure your IDE Controller is set to use DMA
Right click on the My Computer icon, select manage, click on device manager, expand IDE ATA/ATAPI controller, right-click on Primary IDE channel, click on properties, click on the advanced settings tab. In the Transfer Mode section, select DMA if available. Do this for both devices in both the Primary and Secondary Controllers. After you reboot you can go back in and see what the controller is now actually using.

43. Set your swap/paging file correctly
Open up System monitor (Click on Start, Programs, Accessories, System Tools, System Monitor), select Edit then Add item. Add Swapfile size as shown below. These are the items that System monitor will now track for you. You can remove/add other items by clicking on Edit then Add/Remove item. Over the next few days load up System monitor & let it track your Swapfile size. Click on Options then Chart & set the update interval as you see fit I'd recommend setting it to 30 seconds or 1 minute, depending on how

long you intend to be monitoring for. Make sure to Start logging (Click on File then Start logging) & save the logs so that you'll be able to reference usage over the days.
It would be best to start tracking your usage when you go to play a game or something that will put your PC under a bit of stress. Run a few time-demos or play Unreal tournament against some bots. This will give you an idea of your Virtual memory needs, however don't go overboard with the testing you want to track normal usage, not excessive usage. The graph to be concerned with is the Swapfile size. Once you're satisfied with your monitor it's time to consult your log. Open the sysmon.log (or whatever you saved it as) with Notepad.

Unfortunately the size is saved in byte size, rather than in MB's. To convert into MB's, take the largest value from the log & divide it by 1048576 (1024*1024). So in the above example it would be 113246208/1048576=110MB (108 rounded up). Obviously you should only be concerned with calculating the highest value, rounding up to the nearest 10 MB'S, e.g. if you get 143.8MB round it up to 150MB.

Based on your results, there are 2 different methods that should be considered when setting the Virtual memory. 1 is to create a permanent fixed swapfile; the other is to create a semi-permanent one. The benefit of a Semi-permanent one is that if needed, Windows can enlarge the size of it. This will remove any chance of Out of memory errors occurring. Afterwards Windows will bring the Swapfile back to its original, Minimum size.

Permanent swapfile - (NOT recommended) then set the size about 30-50MB's larger than the value you've calculated, E.g. given the values calculated earlier you'd set both the Minimum & Maximum to 150MB. This will allow for most unforeseen circumstances where extra Virtual memory is needed. Given the large size of hard drives today you should have no problem allowing for the extra space needed for this. There's no point in creating a 1GB swapfile if you only need 100MB for most tasks. Monitoring the swapfile size from time to time will determine whether your minimum is suitable. Eg if it resizes above your minimum often, then your minimum is clearly not suitable.

Semi Permanent swapfile - don't set the maximum and minimum to the same value. The only way to avoid "out of memory" errors when both are set to the same value would be to set them both far higher than you would ever need. This is wasteful and inefficient (indeed, it can actually reduce performance). Remember that swapfile size is based upon allocated memory, not used memory. You can easily allocate more than 2GB of memory (disk-space permitting, of course) yet only actually use 128MB. However, under normal usage, the swapfile will "top-out" at some value that is unique to your way of working, and that is the size your swapfile should be minimised to. By leaving the maximum open, any attempt to exceed your normal workload will not be hindered, and the swapfile will shrink back to its minimum when that overhead is no longer required. Your actual usage of the swapfile may well be a lot less than your minimum, however if you can't allocate the memory in the first place, you can't make use of it either...

I have a swap file located on the fastest hardly used drive. Once you've decided on which method you want to choose, take the following steps. NOTE - Some recommend disabling Virtual memory first. Rebooting, then defragmenting the hard drive. Then setting the Virtual memory options. I do not recommend this as it won't help you much in the sense that it won't do anything that defragmenting with the Swapfile enabled won't do (Unless you have a defragmenter that can move the swap file to the outer edge of the hard drive that is). Also I would recommend putting your swapfile\pagefile on the fastest hard drive e.g. preferably a fast scsi drive that is not used much. Also do not put two hard drives on the same IDE channel. NEVER put a swapfile\pagefile onto a separate partition (except the first) of the same hard drive - this is because the hard drive head as to move all the way across the disk each time and you will notice a major performance decrease ! For users with one hard drive c:\ will be fine.

- Right click on My computer & select Properties. Select the Performance tab.
- Select Virtual memory. Choose Let me specify my own virtual memory setting.
- Select step A or B depending on which path you choose to take.
---If you've chosen to use a Permanent fixed Swapfile set it (substituting in your own values)
---If you've chosen to use a Semi-Permanent Swapfile set it (substituting in your own values).
-For the Maximum value however set it to whatever amount of hard disk you have free.
-Reboot your PC for the changes to take effect

The Swapfile is best placed on the outer edge of the hard disk it is located on. Windows 9x\Me Disk Defragmenter won't do this unfortunately. You'll need a disk defragmenter like Norton speed disk to do so.

Swap File Myths

Swap-File myth #1:
Create a permanent Swap-File 2 1/2 or 3 times the amount of physical memory. I read that at least one of the popular PC Magazines and some web sites are still perpetuating this one. Fortunately it can't hurt you, it's just bad information.

Fact:
Virtual memory (Swap-File) is a substitute for physical memory. Common sense tells you the more physical memory you have, the less virtual memory you need. Conversely (all other things being equal) the less physical memory you have the more virtual memory you will need. There is no reasonable "rule of thumb" formula for setting the size of a permanent Swap-File.

Swap-File myth #2:
Set the 'min' and 'max' size the same for the Swap-File. This one can cause you grief.

Bad advice!!! Some seem to think of the Swap-File like an insect trap, if you don't have a lid on it, all of those Ks and Ms of bytes and bits will fly out all over the HD. Not so!!! It may help to think of your Swap-File as a water glass sitting on the table (The level within this container will rise and fall as demands change and it is emptied whenever you shut W95 off), the only time it will overflow is if you try to put more into it than it can hold, (your 'min' size setting) and that is the reason you 'never' want to place a 'max' size for your Swap-File, you want it to overflow if it needs to. (This is an analogy, it will not overflow, the Swap-File will increase in size if need be, possibly using non contiguous HD space until it shrinks to your 'Min' size setting again.) Win9x will 'never' exceed your 'min' size unless it needs to, if it can't (because of a 'max' size setting) it will revolt, usually with a "Out of Memory!! Shut down one or more programs to continue" warning. It is doubtful you will associate this warning with the 'max' setting you placed on your Swap-File months ago when your usage habits were less demanding.

44. Switch off Dos memory manager
Delete or uncomment out this line (if you have it) from your config.sys and/or autoexec.bat. These are located in your root directory where Windows is installed.
DEVICE=C:\WINDOWS\EMM386.EXE
This is a DOS memory manager, some switches to this line can place a limit on RAM available in Windows.

45. Disable the Windows animation function
It can slow down your PC. Open your registry and change the value of 'MinAnimate' found in the key below, set the value to '0' for disabled or '1' for enabled. If the value doesn't already exist simply create a new string value and name it 'MinAnimate'.
[HKEY_CURRENT_USER\Control Panel\Desktop]

46. Disable Windows smooth scrolling
This setting allow you to disable the Windows smooth scrolling function, which on an low-powered system can cause performance degradation. Using RegEdit find the key below. Modify the value of 'SmoothScroll' to either '00 00 00 00' for disabled, or '01 00 00 00' for enabled. If the value doesn't already exist create a new REG_BINARY value, naming it 'SmoothScroll'.
[HKEY_CURRENT_USER\Control Panel\Desktop]

47. Configure the contiguous file allocation size
This tip forces by Windows to ignore larger amounts of fragmented diskspace, and avoids splitting larger files the same time using windows maintenance tools e.g. defrag. If you are using disk intensive applications than configure the contiguous file allocation size. This also applies to NT, 2000 and XP.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\FileSystem

Right-click in the right hand pane -> select New -> DWORD -> name it "ContigFileAllocSize" (no quotes).
Now double-click on it -> check the Decimal box -> give it an integer value between 1024 (1 MB) and 4096 (4 MB). Default is 512 (512 KiloBytes = 1/2 MB). If you have any newer/"monster" multi-GigaByte size hard disk(s), you may want to set this value to "high": 2048 - 4096. If you don't work/"play" frequently with multi-MegaByte size files, you may want to set it to "low": 512 - 2048. Close the Registry Editor and restart Windows when done.

5 gig drive = "ContigFileAllocSize"=dword:00000200
10 gig drive = "ContigFileAllocSize"=dword:00000400
15 gig drive = "ContigFileAllocSize"=dword:00000600
20 gig drive = "ContigFileAllocSize"=dword:00000800
20 gig drive = "ContigFileAllocSize"=dword:00000a00
25 gig drive = "ContigFileAllocSize"=dword:00000c00
30 gig drive = "ContigFileAllocSize"=dword:00000c00
35 gig drive = "ContigFileAllocSize"=dword:00000e00
40 gig drive = "ContigFileAllocSize"=dword:00001000

48. Office Assistants !
Turn off those bloody office assistants always popping-up when you least expect it! This tweak will let you remove them for good! Open you're registry and find the key below. Then delete all the values under the key.
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\8.0\Common\Assistant]

49. Hide Links Folder on Favorites Menu
Internet Explorer persistently creates a Links folder on the Favorites menu, this tweak allows you to hide it.Although not a registry tweak, this tweak appears to be the only way to hide the automatically recreated Links folder. Using Explorer find the location of your Favorites folder (e.g. C:\Documents and Settings\Joe Bloggs\Favorites) within that folder will be a sub-folder named Links. Select the Links folder and right-click (or secondary click) and click on Properties, check the Hidden checkbox and click OK. From now on the Links folder should be hidden from the Favorites list. Note: This works for any other folder or link on the favorites menu as well.

Another method is to edit the registry.
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar
Locate the string "LinksFolderName" Right Click on it and select delete.

50. Hide the Internet Explorer Icon
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Value Name: NoInternetIcon
Data Type: REG_DWORD
Data: (0 = disabled, 1 = enabled)

51. Add Command Prompt Here to Every Folder
If you're from the old school and still use the DOS prompt regularly, then this tip is for you! It creates a new right-click option to open a command prompt window at the directory you are currently working from. Open your registry and find the key below.

Create a new sub key called 'CommandPrompt' as in [HKEY_CLASSES_ROOT\Directory\shell\CommandPrompt]. Change the value of '(default)' within the key to equal the text you would like on the right-click menu, for example 'Command Prompt Here'. Create another new sub-key under the key created above, name this subkey 'command' as in:
[HKEY_CLASSES_ROOT\Directory\shell\CommandPrompt\command]. Change the value of '(default)' within this key depending on your operating system to equal either:

Windows 9x
command.com /k cd "%1" or

Windows NT
cmd.exe /k cd "%1"

Now right-click on a folder and the new option of 'Command Prompt Here' should be available.

52. Easily Use Notepad to Open a File
Enabling this setting will allow you to use Notepad to open a file by simply right clicking on the icon. Also the Notepad will be used to open the files by default if no association already exists.
- Go to the key "HKEY_CLASSES_ROOT*\shell", if it doesn't exist create it.
- Under shell create a new key called open, and edit the string "(Default)" to read "Open With Notepad".
- Under open create a new key called command, and edit the string "(Default)" to read "notepad.exe %1".
Now when you right click on a file you should see "Open with Notepad" as one of the options.

53. Automatic Logon without Name or Password
This setting allows Windows clients to logon without entering a user name or password, bypassing the logon box.
- Using Regedit, open the key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon
- Create a new String Value, and name it 'Default Password'.
- Modify the data of 'Default Password' to match the default users password.
Reboot and the system should automatically logon.

The default username can be found at [HKEY_LOCAL_MACHINE\Network\Logon\Username]
The password is stored in clear text, therefore anyone with access to the registry can see the default password!

54. Remove the 'Shortcut to...' Text on Shortcuts
Don't like having 'Shortcut to...' appended to every Shortcut? You're not alone. With this tip you can stop Windows for adding this text when creating links.

Open your registry and find the key
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer

Create a new BINARY value name 'link', of modify the existing value, to equal '00 00 00 00' to have the Shortcut text disabled. This tweak can also be applied to the
[HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer] key, to change all users.
Restart your computer.

55. Remove various items from start menu

Remove the Favorites Folder from the Start Menu
Open your registry and find the key below.
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Create a new DWORD value, or modify the existing value, called 'NoFavoritesMenu' and set the value to '1' to disable the Favorites folder. Exit you registry and restart for the change to take effect.
Note: Create the same value under the HKEY_LOCAL_MACHINE hive for the change to be system wide.
For example, the setting may look like: NoFavoritesMenu 0x00000001 (1)

Remove the Documents Folder from the Start Menu
Open your registry and find the key below.
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Create a new binary value, or modify the existing value called 'NoRecentDocsMenu' set the value to equal '1' to enable the restriction. Also create a new binary value, or modify the existing value called 'NoSMMDocs' set the value to equal '1' to enable the restriction. Also create new binary value or modify existing called 'NoRecentDocsHistory' - set the value to '1'. Exit registry, you may need to restart for the changes to take effect.

For example, the setting may look like:
NoRecentDocsHistory 0x00000001 (1)
NoRecentDocsMenu 0x00000001 (1)
NoSMMyDocs 0x00000001 (1)

Remove the Help Option from the Start Menu
Open your registry and find the key below.
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Create a new DWORD value, or modify the existing value called 'NoSMHelp' set the value to equal '1' to enable the restriction. Exit your registry, you may need to restart for the changes to take effect.

For example, the setting may look like:
(Default) (value not set)
NoSMHelp 0x00000001 (1)

56. Stop PC Speaker Beeping on Errors
If you get annoyed by the beeps and noises coming from your PC speaker but can't find a way to turn it off, then use this tip to disable it.

Open your registry and find the key
[HKEY_CURRENT_USER\Control Panel\Sound]
Locate the value 'Beep' if it doesn't already exist create it, by selecting Edit | New | String Value and naming the new value 'Beep'.
Modify the value of 'Beep' to either 'Yes' beeping enabled, or 'No' beeping disabled.

57. Change the Location of Windows Installation Files
If you have moved your installtation files etc and want to put in correct location here is where it is stored.
Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup]

Data: D:\WIN95

58. Clear Recent Documents When Windows Exits
Open your registry and find the key.
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Create a new DWORD value, or modify the existing value called 'ClearRecentDocsOnExit' set the value to equal '1' to enable the tweak.

For example, the setting may look like:
(Default) (value not set)
ClearRecentDocsOnExit 0x00000001 (1)

59. Remove Cached Command Lines from the Run Menu
Got a lot of items in the Start Menu's run command history? This tip will allow you to remove any extraneous commands. Delete the value corresponding to the command you want to remove, or remove all the entries to clear the list completely.

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU]

60. Tired of waiting for Windows to restart?
Sometimes it can take ages to completely shutdown, then your have to wait for the PC to reset as well. Try this tip to speed up your computer's shutdown procedure. You can reduce the time it takes for Windows to restart by holding down the SHIFT key while you select 'Shutdown'. This will restart Windows only, and not your whole computer. This tip only works on Windows 9x and not Win ME.

61. Increase Cached Icons
To reduce your hard drive thrashing and decrease potential delays you might experience when you right-click to bring up a context menu or a dialog box and to avoid a permanent refresh of your Desktop icons. If you desktop icons are redrawing too frequently, it could be because the icon cache is full. Try increasing the size by changing this setting.

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer]
Create a new string value, or modify the existing value, called "Max Cached Icons" and set it to "2000". Restart Windows for the change to take effect. The default value is 500, which means the maximum number of icons that are cached by the OS. You need to restart your machine after this change (sometime multiple times.)

62. Removing Programs listed in the Add/Remove Programs Box
All Windows 9x or NT compatible programs must include an Uninstall program, sometimes though the program may get removed but entry in Add/Remove programs doesn't, from this key you can remove those orphaned entries.
Using Regedit open the key below.
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall]
Under this key will be a number of sub-keys, each representing an installed application.

To see which application each sub-key represents, open it and there should be at least two values 'DisplayName' and 'UninstallString'. 'DisplayName' is the name used in the Add/Remove programs list, and 'UninstallString' is the program used to uninstall the application. To remove a program from the list you can simple delete the sub-key representing that program.

63. Fix the fonts folder
A font may seem to be installed correctly but does not appear in the Fonts folder because the Fonts key in the registry is missing or damaged. Move the contents of the Fonts folder to an empty folder. By opening the Fonts folder, select all the fonts, copy them, and paste them to a new folder. Open your registry and find the key below appropriate to your operating system. Highlight the key and press DELETE. Once the key has been deleted create a new key to replace it, by selecting Edit | New | Key and name the new key [Fonts].

Restart the computer, then re-install the fonts by opening the Control Panel, double-click on 'Fonts'. And from the File menu select 'Install New Fonts...' adding the fonts that were previously copied to the temporary directory.

Windows 95
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Fonts]

Windows NT
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts]

64. Backup ISP
Navigate to HKEY_CURRENT_USER\RemoteAccess in the registry.
Click RemoteAccess to select it, then choose Registry, Export Registry File. When the Export Registry File dialog box appears, type a name and choose a location for your new file. Now click Save to save the file and close the dialog box. If you need to restore the settings, locate your ISP REG file and double-click its icon. This merges the file with the Registry and restores your original settings.

65. Disable Power Management (not recommended for everyone)
If you encounter random system errors while trying to open a program, see a yellow exclamation sign next to one of these Control Panel -> System -> Device Manager items: "Advanced Power Management support", "Display adapters", "Modem", "Network adapters", "PCMCIA devices", "Universal Serial Bus controllers" etc, even if you know there are NO IRQ/COM port conflicts, are bothered by intermitent CRT display flicker upon "waking up" after being
in "stand by"/"suspend" mode (which may in time wear off your monitor), get knocked out frequently from your otherwise functional Internet/modem/network hookup, experience (too) long delays when your monitor/hard disk(s) "wake up" after "hibernation" mode, you may want to turn off completely ALL your Windows 9x power management
features (like I did).

a. First enter your BIOS/CMOS Setup by pressing the appropriate key specified in your computer/motherboard manual during the bootup POST (Power On Self Test) screen, and DISABLE ALL (Advanced) Power Management (APM/ACPI) settings, like: "Doze Mode", "Standby Mode", "Suspend Mode", "HDD Power Down", "Video Off" etc. Save your changes and reboot.
b. After your Win9x GUI comes up: open Control Panel -> Power Management -> select the "Always on" Power scheme -> make sure the "Turn off monitor" and "Turn off hard disks" boxes show "Never" -> Click OK/Apply to save the changes.
c. Edit your SYSTEM.INI file (found in your Windows folder) with Notepad or Sysedit (but BACKUP IT UP FIRST!) -> go to the: [boot] section -> look for the "power.drv" entry on the "drivers=" line -> move it to a new line of its own starting with a semicolon (;) to disable it e.g :-

[boot]
drivers=mmsystem.dll whatever.vxd
; power.drv
DO NOT remark/disable ANY other filenames on the "drivers=" line!

[386enh] section -> look for the "device=*vpowerd" line -> disable it by placing a semicolon (;) in front of it e.g :-
[386enh]
; device=*vpowerd
Save your file.

d. Go in registry and goto:
HKEY_LOCAL_MACHINE and then to:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VCOMM
Under each key above -> double-click on the "EnablePowerManagement" DWORD/Binary (depending on your Win9x release) value in the right hand pane -> change ALL characters to read 0 (zero) -> click OK/press Enter.
e. Click Edit from the Regedit menu -> select Find -> start 3 separate Registry searches: type "power.drv", "vpower" and "vpowr" respectively (no quotes) in the "Find what..." box -> delete ALL found keys/entries.
f. Move to a safe BACKUP location these 2 files from C:\Windows\System: POWER.DRV and VPOWERD.VXD.
g. Disable ANY Power Management entries from the System Agent (Task Scheduler)
h. Reboot. Your Win9x machine should perform smoother from now on, without annoying interruptions or intermittent errors. :)

66. Diagnostic Info
At the Run command Type the following: HWINFO /UI - you'll get a ton of info, where in the registry it's located and any problems you might have (although sometimes it says you got problems when are ok.

67. Got problems and don't want to reinstall...
Don't wanna lose any of your settings or software? There's a command line option that'll get you back on your feet in no time. Boot up your PC with a Windows 98 boot disk, pop in your Windows 98 CD, and once you're at the command prompt, type your CD-ROM drive letter immediately followed by a colon. So, if your CD was set to "D" you'd enter D: and then hit ENTER. At this point, type the following command: SETUP /pf. This switch will restore all of Windows critical files to their factory state, and in 99% of situations doing this will fix whatever problems you were having in Windows 98.

68. Increase refresh rate of windows
If you want to possibly speed up the refresh rate in Console Windows, add the following to the [386Enh] section of SYSTEM.INI: WindowsUpdateTime=10 (the value is the refresh rate in milliseconds). Using values less than 15-20ms requires a fast machine and a good video card. Otherwise your system will become very slow when a DOS Box or Win32 Console Application is running). Make sure to reboot your system after setting the tweak.

69. Having shutdown problems ?
Try these registry switches
-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Shutdown]
"FastReboot"="0"
------End cut & paste here------

And if you have Windows Millennium :-
-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon]
"PowerDownAfterShutdown"="1"
------End cut & paste here------

Also check out these websites:-
http://www.aumha.org/a/shutdown.htm
http://www.pcforrest.freeserve.co.uk/shutdown_errors.htm

70. Faster Startup After Adding Network Card
After adding a network card to your Windows 95/98 installation you may notice a 10 to 20 second delay when Windows is loading at the graphic splash screen. This is caused by Windows attempting to poll your network for a TCP/IP address. Under normal circumstances Windows will not be able to find one and will manually assign you one.
The delay you experience is the process where Windows is polling the network. To eliminate this follow these steps:

Go to your network neighborhood, right click and bring up the properties dialog.
Scroll down in the install protocols list until you see an entry marked "TCP/IP -> [Network Card Name]".
DO NOT select the one marked "TCP/IP -> Dial-up Adapter" as this is your modem and your Internet service provider will normally assign you a TCP/IP address upon connect.

Click on the property tab for this protocol and go to the "IP Address" tab.
Click "Specify an IP Address" and type in any IP address. Do not include "zeros" in any of the four fields.
For example, mine is set to 192.198.1.11.
Change the subnet mask to 255.255.255.0
Click "OK" and Windows will inform you it needs to restart. Let it.
The delay should now be gone. IP addresses for a small, local network are not too terribly important. Just be sure that you give EACH computer on the network a unique IP address. For consistency sake, always keep the first 3 set of numbers the same. There are technical details about why, but suffice it to say it's the best option.

71. Block those bloody net adverts
There is an easy and free way to eliminate many of these ads with the added benefit of speeding up the serving of web pages; the "HOSTS" file can be used as a tool to block these ads, and it can be customized by each user to suit their browsing habits. The Hosts file shows the IP address [in the form of xxx.xxx.xxx.xxx] and name of various domains. Generally, if a domain has a constant IP address browsing is speeded up as Windows will consult the Hosts file first when translating domain names to IP addresses. In the Windows folder, there is a file named "Hosts.sam" [meaning sample] file.

There is an IP address reserved for all local computers (yours and mine) which is the same for everyone; that address is 127.0.0.1. Since Windows will look in the Hosts file first to translate a domain name to an IP address, if the domain names of advertisers are listed in your Hosts file with the IP address of 127.0.0.1, then Windows will, of course, not find the real IP address of the advertiser and no advertisement will be sent to you. When you browse to a web page which has ads from the domains listed in your Hosts file, the web page will show one to several blank spots where the ad would be and Windows won't miss them or wait for them. And, you, the surfer, will be served up content without the wait for and clutter of ads.

Download an excellent up to date hosts file from :-
http://www.smartin-designs.com/hosts_info.htm

Making a HOSTS File
a - Find the Host.sam file in your Windows folder. (If the extension does not show, open Windows Explorer; on the Menu Bar, select "Tools/Folder Options/View Tab". Uncheck "Hide file extensions for knowm file types.")
b - Copy/paste it back into the Windows folder.
c - Rename the "copy of hosts.sam" file to "Hosts" [no quotes]. Notice that there is no extension. Windows will complain about renaming it but ignore the nag.
d - The Hosts file can be opened & edited with any text editor such as Notepad.exe. Don't edit it with a word processor such as Wordpad.exe. Fortunately, there already exists lists of common ad serving domains neatly compiled with the 127.0.0.1 address in a Hosts friendly format. One such list can be found at
http://www.ecst.csuchico.edu/~atman/spam/adblock.shtml . Copy, then paste the list of ad server domains with the 127.0.0.1 IP addresses from that webpage into your Hosts file.

Customizing Your HOSTS File
Your new Hosts file will now block the major ad serving domains from placing ads on the web pages you access. However, depending on what software you use (such as free ISPs) and where you browse, many ads will still get through. To add your own entries to the Hosts file, use IE4/5's cache of browsed files; it is a gold mine of ad server domain names. The name of the cache folder is Temporary Internet Files (AKA TIF).
a - First, clear the TIF, from "Internet Options/General Tab/Delete Files". Check "Delete all offline content", select OK twice.
b - Put a shortcut to the TIF and the Hosts file on your Desktop.
c - After browsing various websites (especially, the larger, commercial ones) with one or more of your ISPs and signing off, open the TIF shortcut to find ads which may have appeared on webpages you accessed. (Note: Set your TIF view to "Details" by selecting View on the Menu Bar.) Ads are usually "gif" files whose URLs appear to be from ad servers. The domain names of these ad servers can be copied from the Address Bar if you open the "gif" or from "Properties" when right clicking on the "gif". Paste just the domain name, not the entire file name into the Hosts file after entering 127.0.0.1 and a space. Each entry in the Hosts file should be on a separate line. (Note: If, when trying to open a TIF file, you receive a message that "Running a system command on this item might be unsafe. Do you wish to continue?", select Yes. If you get a message that "Your current security settings do not allow you to perform system commands on this item.", then enable or prompt "Launching programs and files in an IFRAME" in Internet Options/Security Tab.)

More Ad Blocking Strategies
1 - If you use AOL and have placed Ad Server domain names with 127.0.0.1 in your Hosts file, browse the web OVER the AOL shell; in other words, open your browser as a standalone application when you want to access websites that use advertisements.
2 - Some websites serve ads from their own domains often with other graphics. One example [without naming names], is a news-type website whose main page consists of about 26kb [2 files] of text content and 107kb [46 files] of graphics [which are a mixture of ads and standard navigation or identification pictures]. Loading the page with graphics turned on is materially slower than loading the same page with graphics turned off. [Graphics in IE can be turned off by unchecking "Show Pictures" on the Advanced Tab of Internet Options.]
3 - Turning off graphics solves much of the problem of ad clutter, but it is overkill as all pictures are turned off when another website is accessed. You can turn graphics back on by checking "Show Pictures", but this can become a time consuming and clumsy approach. You can solve this problem by putting some sites in a graphics permitted category and other sites in a no graphics category as follows:
a - Start a browsing session with graphics turned on, that is with the "Show Pictures" option checked.
b - When you want to access a website that is known to serve its own ads from its own domain [examining the TIF periodically will reveal the origin of the ads], run a Registry entry to turn off graphics & open a separate instance of your browser. Now you will have two instances of IE open; one will show graphics [it will be on the left side of the Taskbar]; the other will show no graphics [it will be on the right side of the Taskbar].
c - The above graphics on & off works because the first instance of IE is "looking at" a Registry that says to Show Pictures while the second instance of IE is "looking at" a Registry thats says do not Show Pictures. With these two instances of IE open, you can browse in graphic & non-graphic mode by alternating between the left side [graphic] & right side [non-graphic] browsers.
4 - Some ads [gifs] are served from a domain name that looks like http://xxx.xxx.xxx.xxx where "x" is a number. ,Putting these numbers in the HOSTS file is useless; since Windows gets the IP address from the web page, it doesn't need to refer to the HOSTS

file. When you spot these kinds of URLs in the Cache, make a note of which website is using IP address served ads. To defeat these ads, use the same "pixs-off" strategy for domains that mix ads with standard graphics.

Redirect
Some websites redirect you to another page whether you want to go there or not. One such website is Hotmail; when the visitor logs off from Hotmail, the MSN home page [www.msn.com] is served up. To stop this behaviour, one can put www.msn.com into the HOSTS file; a "The page cannot be displayed" message will appear.

Blank Message
With Internet Explorer & an active HOSTS file, a typical blocked ad will return a red X . When an entire domain is blocked via the HOSTS file such as "www.doubleclick.net", browsing to that location will return "The page cannot be displayed" message. This same message will appear [at least partially depending on the size allocated to the ad] if that domain is embedded [such as through layering or Iframes] on a webpage of another domain [e.g. www.pcworld.com]. This message is embedded in the file "shdoclc.dll" [in the Windows\System folder] as common HTML code; to make this message less verbose [and annoying], open a copy of shdoclc.dll [pasted into a non-Windows locale] with a word processor; browse to the sections that hold "The page cannot be displayed" message and other text with an Edit/Find operation; change the font color from "black" to "white". It is strongly advised to save the original "shdoclc.dll", rename it to something like "shdoclc0.dll" [I prefer the 0 (zero) to denote original]; then copy your revised copy of "shdoclc.dll" to the Windows/System folder. NOTE: If you had been previously working with IE, Windows may complain about the rename & paste operations; a reboot may be necessary. Also the rename & paste operations can be made from native MS-DOS or from another OS if you dual boot.

The new error message will show small icons with the red links for "Refresh", "Detect Network Settings", & "Back" still intact & functional; the background will be white. NOTE: If your system experiences problems, replace the original shdoclc.dll. Some problems have been reported with right click [context] menu functionality after the font color changes were made. If a white background is not to your liking, you can change the "bgcolor" of the relevant message sections to "black" from "white" and not change the font color. This will give a black backgound with the red links still intact & functional. Whether you prefer the white or black background, another change can be made to the Title Bar message which appears when the Hosts file blocks a domain. The standard Title Bar message is "Cannot Find Server"; browse to that phrase and change it to "Domain HOST Listed".

72. Having problems getting AGP 4x support from your Geforce card !
Check your BIOS setup, usually in the Chipset Features Setup, for something called the AGP Driving Value. This value controls the timing of the AGP driver in Windows. The value you place here can make AGP4X stable. This value is a hex value from 00-FF. In order to place a value here you might need to change another BIOS setup feature called the AGP Driving Control. This should appear with the AGP Driving Value. Set this to MANUAL if not already. The other option is AUTO. Try setting this value to DA or EA. Try DA for a VIA Apollo Pro 133A motherboard. On a KT133 motherboard you might want to try E7. Save your options and reboot your machine. Make sure you are running AGP4X and try some 3D games. Where they might have hung or crashed before they should now be running fine.
If not, then go back into the BIOS Setup and try another value. I've found that values that end in an 'A' seem to work the best.

Enabling AGP 4x in Windows 9x only

-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\Software\NVIDIA Corporation\Global\System]
"EnableVia4X"=dword:00000001
------End cut & paste here------

Enabling AGP 4x in Windows 2000 only

-----Begin cut & paste here-----
REGEDIT4

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nv4\Device0
"EnableVia4X"=dword:00000001
------End cut & paste here------

73. Increase your memory
Free up to 75% of your RAM. Open notepad and put this in it:
Mystring = Space(80000000)
Now save it as memory.vbs and place it on your desktop. Just single or double click on it and presto, quick and easy.
It's an easy way to gain 75% memory! How it works
It's a VB script that makes use of an operating system 'trick' that many memory freeing programs use. It allocates a huge chunk of your memory, forcing Windows to dump out the current contents of your RAM to the hard drive and giving you a nice load of free RAM in return. Nice, simple and it works. Just be careful not to allocate too much memory or you might make Windows grind your hard drive for a while (annoying, but not a major problem).

74. Cache write delay
This applies only to Windows 98 SE and ME, and consists in a workaround, by creating a Registry Value that allows enough time to write all data stored in the memory cache buffer back to the hard disk while Windows shuts down.
This happens because newer hard drives have their own built-in memory cache buffers, which do NOT send proper signals to the drive controller and therefore their cache will NOT empty (flush) correctly upon OS shutdown.

To do this, run Regedit and go to:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

Right-click in the right hand pane -> create a New DWORD Value called "CacheWriteDelay".
Click OK -> double-click on it -> check the Decimal box -> type 2000 (2 seconds delay measured in milliseconds)

75. Speed up your startmenu
The default speed of the start menu is pretty slow, but you can fix that by editing a Registry Key.
This works for all windows versions up to XP.

HKEY_CURRENT_USER \ Control Panel \ Desktop \ MenuShowDelay
By default, the value is 400. Change this to a smaller value, such as 0, to speed it up.

76. Speed up and browse faster
Normally Windows scans for shared files for Scheduled Tasks. And its turns out that you can experience a delay as long as 30 seconds when you try to view shared files across a network from as Windows is using the extra time to search the remote computer. Note that though the fix is originally intended for only those affected, Windows users will experience that actual browsing speed of both the Internet & Windows Explorers improving significantly after applying it since it doesnt search for the Scheduled Tasks anymore.

Open up the Registry and go to :
HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/Current Version/Explorer/RemoteComputer/NameSpace

Under that branch, select the key :
{D6277990-4C6A-11CF-8D87-00AA0060F5BF} - and delete it.

This fix is so effective that it doesn't require a reboot and you can almost immediately determine yourself how much it speeds up your browsing processes.

77. Remove ads from MS Messenger
Go into the links.txt in MS Messenger folder and delete everything in it, and then change it read only. Don't delete the file, only what's in it. This only works on older versions of Messenger - Messenger Plus is a program that is good at blocking adverts for new versions of MSN.

78. Raid - create an optimiszed stripe set
A stripe set is a group of hard drives that is accessed threw the operating system as one drive. For example, if you have three hard disks and created a stripe set with parity(RAID 5) the drive would have the combined space of all three drives and the files would be striped across all three. When you format a stripe set with parity (RAID 5) you lose the size equal to one of the drives in the set. For example, if you have three 9GB drives in a RAID 5 configuration the total size of the stripe will be 18GB.

79. Switch off devices you don't use and free up resources
You can disable some hardware you don't use in Windows. You can think of Joystick ports, MPU-401 (compatible)-port, CD-ROM Controllers on you soundcard if you don't use them, etc. If you havent got any USB devices then disable it - you get the idea. Goto control panesl\system\ - doubeclick the device you want to disable, select disable this device in the hardwar profile, click ok, repeat this with other devices and restart windows.

The devices you have chosen, are not enabled in Windows, so you can't use them. Because they're disabled, the needed drivers aren't loaded now. This results in having more RAM and more system recourses free for other use.

80. IE Full Screen Bar
This tip applies to ALL Microsoft Internet Explorer releases beginning with V4. I have been using MS IE 4.01 in full screen mode for some time, but I have never been able to adjust IE's menu bar to include all basic items, like:
File, Home, Back, Forward, Reload, Full screen, Help etc, and the same time display the URL address bar and get rid of IE's annoying title bar.

Export the registry key that will be modified further below just in case.
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar
Next copy and paste below into notepad and save as IE4bar.reg file and double click it

-----Begin cut & paste here-----
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar]
"Theater"=hex:0c,00,00,00,4c,00,00,00,74,00,00,00,18,00,00,00,1b,00,00,00,5c,\
00,00,00,01,00,00,00,e0,00,00,00,a0,0f,00,00,05,00,00,00,22,00,00,00,26,00,\
00,00,02,00,00,00,21,00,00,00,a0,0f,00,00,04,00,00,00,01,00,00,00,a0,0f,00,\
00,03,00,00,00,08,00,00,00,00,00,00,00
------End cut & paste here------

81. CD/DVD Max Speed
When you right-click on My Computer and select Properties, the System Properties applet opens. Click the Performance tab, click File System and choose the CD-ROM tab. Look at the "Supplemental cache size". When you move this slider all the way up to the right, Windows 95/98/ME allocates a maximum of 1238 KB from your computer's memory. You can increase these settings even further. The table below shows all the "CacheSize" and "Prefetch" values you need to modify for cd-roms/dvds of different speeds, starting with 4x (maximum allowed by Windows) and up to 52x
The maximum values Windows allows are.

Hex values:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\FileSystem\CDFS
"CacheSize"=hex:6b,02,00,00
"Prefetch"=hex:e4,00,00,00

DWORD values:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\FileSystem\CDFS
"CacheSize"=dword:0000026b
"Prefetch"=dword:000000e4

CD-ROM/CD-R/CD-RW/DVD-ROM/DVD-R/DVD-RW/DVD-RAM "CacheSize" values:

Cache Size	Decimal | KB	Hex	DWORD
Small [Default]	619 | 1238	6b,02,00,00	0000026b
Medium	1238 | 2476	d6,04,00,00	000004d6
Large	2476 | 4952	ac,09,00,00	000009ac

CD-ROM/CD-R/CD-RW "Prefetch" Registry values:

CD-ROM Speed	Decimal	Hex	DWORD
4x [Default]	228	e4,00,00,00	000000e4
8x	448	c0,01,00,00	000001c0
12x	672	a0,02,00,00	000002a0
16x	896	80,03,00,00	00000380
20x	1120	60,04,00,00	00000460
24x	1344	40,05,00,00	00000540
32x	1792	00,07,00,00	00000700
40x	2240	c0,08,00,00	000008c0
44x	2462	a0,09,00,00	000009a0
48x	2688	80,0a,00,00	00000a80
52x	2912	60,0b,00,00	00000b60

DVD-ROM/DVD-R/DVD-RW/DVD-RAM "Prefetch" Registry values:

DVD Speed	Decimal	Hex	DWORD
1x	448	c0,01,00,00	000001c0
2x	896	80,03,00,00	00000380
4x	1792	00,07,00,00	00000700
6x	3584	80,0a,00,00	00000a80
8x	4096	00,10,00,00	00001000
10x	5376	00,15,00,00	00001500
12x	6400	00,19,00,00	00001900
16x	8192	00,20,00,00	00002000

Larger cache/buffer size means using more memory and you need at least 64mb before playing with these settings. You can test your settings by using CDCheck from ftp://ftp.cdrom.com/pub/sac/utildisk/chkcd101.zip

82. CD Keys
If your Win9x system (or your Windows applications: MS Plus!, MS Office etc) become corrupted, and you have misplaced the installation cd-rom key (which is usually shown on the cd-rom sleeve or on the manual cover), there is still a way to find it, so you can reinstall your OS/app from scratch. This procedure requires a working copy of Windows. To make it easier to find them all, start a Registry search: click Edit, select Find, type "ProductID" (no quotes) in the search box, and hit Enter.

With the GUI started, open Regedit and go to:
MS Windows 9x:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProductID
MS Windows NT:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductId

83. Click here to begin !
To get rid of the annoying "Click here to begin" moving arrow and message, which appear on the Taskbar every time you load the Windows GUI.

HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Policies/Explorer
Modify the "NoStartBanner" DWORD value to read:
"NoStartBanner"="01 00 00 00"
by double-clicking on it, and then type: 01000000

84. Disable homepage to speed up launch
By using a blank home page internet explorer does not have to use additional cpu time and uses the hard drive less. After all most of the time you want to go to a different site right away so it is not going to affect your productivity at all. Launch Internet Explorer. Select the Tools from the menu bar. Then select Internet Options... from the drop down menu. Once the internet options has loaded click on the general tab. Under the home page section click the use blank button. Click OK

85. Get free domain name and setup web/ftp server etc
The first thing you'll need to go is head over to http://www.dyndns.com and register for your own domain name.
The totally free way is DynDNS which is a dynamic domain naming service. This way, you'll get a free third level domain name that maps to the public IP address of the computer that is running the client software. A third level domain name is something such as tweaker.d2g.com. The advantage of this system is that it is totally free and dynamic. The bad news is that it's not a second level domain name, such as 3dfiles.com.

By the use of this client software, every time your computer is online, you can access your computer by typing "yourdomain.d2g.com" or whatever other domain you specify at DNSDNS. This is much easier than typing in a numerical IP address, especially if if changes every time you connect to your service. DynDNS will email you a special key that will unlock the DynDNS client. You can enter in different kinds of information to keep your connection alive if need by, as well as where to direct the user if the client if offline.

The second way is free, depending on how you do it. The first step is getting your own REAL Domain name. www.register.com is a good place to get a .com, .net, or .org domain name for a small fee every year. Most places on the internet charge £18 per year for a .com, .net, and .org domain name. Using this process, you can have your own domain to the tune of www.yourname.com, ftp.yourname.com, and anythingyouwant.yourname.com. There are many places that will sell you a domain name but be careful there are a lot of companys that tie you in and a lot of small ones have gone bust.

When you buy a domain name, that's only half the ordeal. You have to tell DNS Servers out on the internet what IP is equal to that domain name. DynDNS will do this automatically via the use of their client for a small fee. I urge you to check their site out if you haven't already.

www.granitecanyon.com is a Public DNS Server. They have three domain servers that will tell other DNS servers what IP is equal to your domain name. Using this method, you must have a Static IP which costs extra from your ISP...usually, a lot extra. Because it's so expensive to have a static IP, I will not go in depth on how to use granitecanyon.com, because I feel their site covers itself very well.

86. Use SFC (system File Checker)
SFC.EXE is a valuable tool to check your system files. Windows ME, 2K and XP will check and restore critical system files automatically. Since the bulk of people are still using Windows 9x, we need to fix Microsoft's problems ourselves. Unfortunately, Windows doesn't integrate it into your user-shell, thus it must be run from the command line.
Select Start > Run, type: "SFC", Click OK.

SFC will check your system files for their correct versions and will give you a logfile. Its best to run SFC before you put anything onto your system as you can check for changes in the since it was last updated.

87. Run programs at shutdown
With windows XP you have the option to run programs a shutdown but how do you do it in the other MS systems ?
All you need here is Notepad - to create a batch file. Batch files are simply plain-text files,launch Notepad and begin.

For example, suppose we want to run Windows Scandisk on all drives without notification (unless errors are found) and then shutdown the system. Since we'd need to wait for Scandisk to complete before we shutdown, we need the START /W command to launch Scandisk. The final command will be the shutdown command itself. Since we don't need to wait for the shutdown to complete, START (without the /W switch) will be used. The batch file to do all this would be:
You will see the number 1 at the end of the above lines - you can change the number and the numbers mean:-
0 Logoff
1 Shutdown
2 Reboot
4 Force
8 Poweroff

```
@ECHO OFF
START /W C:\WINDOWS\SCANDSKW.EXE /A /N
START C:\WINDOWS\RUNDLL32.EXE C:\WINDOWS\SYSTEM\shell32.dll,SHExitWindowsEx 1
```

or simpler shorter version:-

```
@ECHO OFF
START /W SCANDSKW /A /N
START RUNDLL32 shell32,SHExitWindowsEx 1
```

Save the batch file with a meaningful name such as shutdown.bat and stick it on your desktop or some convenient location. Note that all batch files must have the .BAT extension in order to execute. Double-click the shortcut when you're ready to shut down. When the scandisk process completes, Windows will shut down. Perfect. Just change scandisk to whatever you want to run on shutdown. You can run as many or as few as you like, but the final command should always be the shutdown command itself - without the /W switch.

Probably the hardest bit is to work out which switches or parameters the program requires in order to fulfil the function you require. Check the documentation for the program you want to run to ensure your command line arguments (switches and parameters) are correctly set. Note that programs residing in the C:\Program Files folder (or any folder using long-filenames) should be quoted in full. e.g. if the program were C:\Program Files\Long Filename.exe, we'd use:

```
@ECHO OFF
START /W "C:\Program Files\Long Filename.exe"
START C:\WINDOWS\RUNDLL32.EXE C:\WINDOWS\SYSTEM\shell32.dll,SHExitWindowsEx 1
```

CHAPTER [2]

OPTIMIZING WINDOWS MILLENNIUM TIPS

As well as the tips above here are some modifications that I have made to Windows ME to gain SIGNIFICANT increase in speed, performance and security. I have tested these settings for over a month and haven't encountered any problems. After applying these tweaks and rebooting the free resources are in their high 90's.

1. Disable System Restore and uninstall PC Health
Open Control Panel -> System -> Performance Tab -> File System - >
Troubleshooting area -> Disable System Restore
(While you are in this window click on the Floppy Disk tab and uncheck the box so the system doesn't check for a NEW floppy drive every time it starts.)

If you want to use system restore in Millennium and have loads of hard drive space you may not want to remove it from my instructions in steps 1 & 2 because you can revert your operating system back to a previous day or week. Create a restore point - type msconfig in run from the start menu, launch system restore. Here you will have two options, one to create a restore point and the other to revert your system back to a previous time. Doing this will effectively uninstall any programs etc that you may have installed that went wrong etc, etc. The space governed by system restore is in control panels, system, performance, file system - in here it says the amount of space used by system restore. I always have it on minimum. If you don't keep regular backups than leaving system restore and health on would be a good idea.

Uninstall PC Health
Start / Run "\windows\pchealth\support\pchsetup /uninstall"
This also removes the Help engine. You can put it back by using 98lite.

Disable these settings in the start menu
Start / Run type and enter: "Msconfig" then click on Startup and UNCHECK PcHealth, StateMgr, SchedulingAgent and Taskmon
Then allow the system to reboot so all these changes will take effect. If you want your programs optimised during defrag then don't untick Taskmon (I personally think Taskmon is a waste of time).

Delete _Restore Folder
Run Windows Explorer and click on Tools / Folder Options / View andselect "Show hidden files and folders" then browse the c: drive and delete the _Restore folder. Hold your shift key so it doesn't move it to the recycle bin while you press del. This folder can have hundreds of megs of temp files if you have been running ME for a while with the system Restore and PC Health on. If you get an error message saying there is a sharing violation you haven't successfully turned off Pc Health and Restore. The _Restore folder should NOT appears again in the future (unless you update a key Microsoft program like IE). Update: Download System Restore Remover from http://defsoft.iwarp.com/ which will get rid of these files on every startup without removing help engine.

2. Make System File Protection work when PC Health disabled
If you uninstall PCHealth as described in ME System File Protection will stop working. Therefore to make system file protection work and todisable PCHealth AND System Restore do as follows:
1. Open Control Panel -> System -> Performance Tab -> Troubleshooting area ->check the "Disable System Restore" box.
2. Open Regedit and change the RunServices State Manager item from:
"*StateMgr"="C:\WINDOWS\System\Restore\StateMgr.exe" to read:
"Stmgr.exe"="C:\WINDOWS\System\Restore\Stmgr.exe"
either manually (don't type the quotes), or by running this REG file:

-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
"Stmgr.exe"="C:\\WINDOWS\\System\\Restore\\Stmgr.exe"
"*StateMgr"=""
------End cut & paste here------

This will allow System File Protection ONLY to run AND protect system files from being overwritten.

3. Turn off Automatic Updating
(This will hog your modem for 30mins every day when you first go on line if you don't turn it off.)
Start / Settings / Taskbar / Advanced then check Expand Control Panel and close and go to
Start / Settings / Control Panel / Automatic Updates and turn OFF Automatic Updating

4. Install ME on slower computer
Windows Me has a built-in CPU checking function that prevents you from installing it on computers with a CPU slower than 150 MHz. If you're a patient type, you can bypass this check at setup time. Type 'setup /nm'.

5. Make Win98 Boot floppy
Want to "Ghost" or "Image" your Windows 98 installation before installing WinMe? WinMe's "crippled" DOS doesn't directly support DOS-mode utilities such as Norton Ghost and Drive Image, but there's an easy workaround. Make a Win98 boot floppy, remove the extra stuff from it, put a copy of Ghost.exe or DriveImage on it and boot with it.

6. Installation of different versions
You can trick an OEM version of Windows ME (intended to be installed on a completely blank hard drive) into upgrading an existing Windows 98 installation. Go to your windows directory in DOS. Rename win.com and winver.exe (to any other names) and run setup.

7. Passwords Forgotten
If you've installed or upgraded to Win Me and now your dial-up networking configuration seems to have forgotten how to remember your password, install File and Print Sharing (Network Control Panel>Services). This addition will enable this feature, even if you don't share any files or printers.

8. Want Real mode DOS back in Windows ME?
There are two patches - you can use any one. This patch enables DOS mode straight from boot via the F8 key. All instructions are included in the ZIP file.
Unofficial Windows ME Real DOS-Mode Patch v1.3 http://www.geocities.com/mfd4life_2000/
Unofficial Windows ME DOS Fix v2.0 http://www.overclockers.com.au/techstuff/a_dos_me/

CHAPTER [3]

OPTIMIZING WINDOWS NT TIPS

(some of these also apply to 2000 and XP)

God I'm not a great lover of NT, because it has a bloody mind of its own sometimes, but when you are forced to use it you havent got much of a choice. I would advise anyone to install XP in preference to NT. Anyway here are a few tips that I hope will make your life a bit easier with this old, outdated piece of crap operating system :-)
As usual I have only listed the tweaks that apply for NT only, because no configuration is perfect for anyone.
Because NT is such a pain in the arse I have listed 8 pointers for you to follow and trust me you will want to heed this advice. If you do these pointers than you will not have a problem.

a. Never assume an upgrade will go smoothly because all the others have.
b. Do a backup.
c. Create an Emergency Repair Disk.
d. Do not do the upgrade when you are jet-lagged or tired.
e. Make sure the WinNT install disks are around.
f. Have a serial number for NT handy.
g. Have a backup disk configuration, especially if you are using striping or mirroring.
h. Keep a log of server configuration changes

1. Defrag your drive
Microsoft in there infinite wisdom decided not to include a disk defragmenting utility with NT, because they said the NTFS file system didnt need defragmenting - this is complete and utter crap. Install a third party defrag utility, such as Diskkeeper etc. Free version of diskkeeper is available at www.execsoft.com/dklite/

2. Cut down on services loading in at bootup
Also see option 2 in Windows 2000 (very detailed list of services) and option 1 in Windows XP as they also apply to NT. Before we go on one point to remember is that by changing the Startup Type of services to Manual, Windows can still start the service if it's needed.

Overview of editing services

Automatic: the service starts at Start-up, provided that you have more than 12 MB of RAM.
Manual: the service starts when/if the system starts it, which it will only do in a time of need
Disabled: the service cannot be started, even by the system, without user intervention.
Most services don't need to be disabled. Setting them to manual will give you some safety, since the system is pretty smart about firing up what it needs. Setting some services to manual will reduce your systems boot time, but it will also extend the amount of time it takes to fire up anything that needs that service, since the service will then have to be started on the fly.

The defaults here are representative of what you get, as an end user, when you install Windows NT from the media. It doesn't necessarily represent what you get on an OEM machine with Windows NT pre-installed. So, I've listed all of the standard services here, even the ones that seem extremely innocuous, just so you can compare the default media config with what you have. You'll sometimes notice that settings that I claim are default, or enabled on your machine, and vice-versa. That's usually the doing of the OEM, or perhaps another piece of software you've installed.

THE SERVICES

Alerter
Process Name: Services.exe
Default Setting: Manual (Workstation), Automatic (Server)
Description: Distributes administrative alerts to users specified in Alert box in Server properties, on behalf of a computer (via the Messenger service). A common example of such an alert is a performance monitor threshold. To function properly, this service requires the Messenger and Workstation services to be started. Furthermore, this service is used by other services, like Server and several 3rd-party applications.
Recommendation: For most folks running Workstation, remaining at a **manual** status is the way to go. In this state, the service will only run when the OS or a prog requires it. As for the Server edition, if you know that something server-side is using it go ahead and leave it set on automatic. However, if you're using Server more like a Workstation (which many folks do), setting it to manual will shave some fat off the size of that services.exe process, which actually governs a few services.

Clipbook Server
Process Name: Clipsrv.exe
Default Setting: Manual (Workstation), Manual (Server)
Description: While some still use this collaboration tool, it is mostly a relic from the NT 3.x days. This service provides support for the Clipbook Viewer, which allows the clipboard of the source machine to be accessed remotely on target computer's Clipbook Viewer.

Recommendation: For the most part, if you're wanting such functionality I suggest looking at NetMeeting. The bulk of you that aren't using this tool, leave the status set to **manual** (or disable if you're really compulsive).

Computer Browser

Process Name: Services.exe
Default Setting: Automatic (Workstation), Automatic (Server)
Description: Actively collects the names of NetBIOS resources on the network, creating a list so that it can participate as a master browser or basic browser (one that takes part in browser elections). This maintained list of NetBIOS resources (computers) is offered to and displayed in the Network Neighborhood & Server Manager.
Recommendation: This decision is straightforward. If you're using Server or Workstation on a machine that is not connected to a LAN (stand-alone), or will not participate as a master browser and/or take part in elections, then feel free to change the status of this service to disabled (or manual, service will not start in manual status). Keep in mind this does not equate to disabling TCP/IP, but will kind of resemble being on a windows network without WINS (empty Network Neighborhood). This change will squeeze the services.exe process down a little more, and will have a more noticeable effect as a result of dropping those browser duties. If this doesn't sound like your type of scenario, stick with the **automatic** setting.

Directory Replicator

Process Name: Lmrepl.exe
Default Setting: Manual (Server only)
Description: This service simply replicates specified files & directories between computers. The host is referred to as the export server, and the target machines are called import computers. This replication is configured under Server in the Control Panel.
Recommendation: By default Workstation does not install this service, so only folks with Server need worry about this. This is another easy judgment call--if your server is doing any replication you'll need to set this service to automatic. If not, keep the status set to **manual**. DCs are set to automatic by default, and this shouldn't be tampered with (Netlogon share).

Event Log

Process Name: Services.exe
Default Setting: Automatic (Workstation), Automatic (Server)
Description: This service supports the recording of the three categories of events: System, Security, and Application. The events recorded can be viewed under the system tool Event Viewer
Recommendation: Most of you are going to want to leave this service started, whether you're using Workstation or Server. However, some of you using either edition as a personal workstation might consider disabling the service. Do this only if you're not worrying about security events, and are willing to start the service retroactively if/when you happen to have NT probs. Personally, I almost never have such problems, so this "reporter" does me little good. If you don't agree with my logic in **disabling it**, leave this set to automatic.

License Logging Service

Process Name: Llssrv.exe
Default Setting: Automatic (Server only)
Description: As can be derived from the name for the most part, this service provides support for license tracking on a server or DC (Domain Controller).
Recommendation: Now I'd be crazy to recommend compromising any piece of the licensing model MS has. However, keep sharp you folks using Server on a stand-alone machine (for testing purposes only of course). Once upon a time there was a myth floating about that MS monitored Servers and their licensing status through this service, over the Internet. However, analysis has shown this not to be true.

Messenger

Process Name: Services.exe
Default Setting: Automatic (Workstation), Automatic (Server)
Description: Processes the delivery of pop-up messages sent by the Alerter service, or an administrator. The messages appear on the recipient's machines, and must be clicked OK to disappear. This service is also required to receive any messages sent by the Messenger service from another machine.
Recommendation: Oh boy, yet another chance to squeeze down the size of the Services.exe process. For stand-alone machines running either edition of NT, go ahead and **disable** this service. For machines in some kind of NT environment on a network, you may want to also consider disabling this service for security. Misuse of the 'net send' command-line util has caused many admins to disable this service, in order to avoid varying forms of misuse and abuse. If these scenarios don't include you, or you dream up another, go ahead and leave this service set to automatic.

Net Logon

Process Name: Lsass.exe
Default Setting: Automatic (Domain), Manual (Workgroup)
Description: Responsible for network authentication including the following sub-components: maintains a synced domain directory database between the PDC and BDC(s), handles authentication of respective accounts on the DCs, and handles the process of authentication of domain accounts on networked machines. FYI - LSASS (Local Security Authority Subsystem), is an acronym you'll see thrown around alot in discussion of NT Security.
Recommendation: By default this service is set to automatic for machines residing in domains, and manual for machines that aren't. That's about as tweak-a-rific as it gets. Sometimes I've notice that OEM machines can come with this service set to automatic, however, so you might want to check this one for sure.

Network DDE

Process Name: Netdde.exe
Default Setting: Manual (Workstation), Manual (Server)
Description: Supports network transport of DDE (Dynamic Data Exchange) connections. Such connectivity is mostly a relic from the NT 3.x days, and interaction with Windows for Workgroup clients. Some Win32 NetDDE APIs are still used, but such APIs are thunked down to 16-bit.

Recommendation: This service will function properly when called upon with a status of **manual**, so no change need be made. If you notice the nddeagnt.exe process running frequently, you're better off not disabling this service (not that you'd gain anything in particular by disabling it in the first place).

Network DDE DSDM

Process Name: Netdde.exe
Default Setting: Manual (Workstation), Manual (Server)
Description: This service manages the shared DDE conversations (from shares like: \\computername\ndde$). The Network DDE service above requires this "father" service to be started. For what's it worth, the full-name is Network Dynamic Data Exchange Share Database Manager.
Recommendation: Take the same approach for this service as you would for its complement, just above.

NT LM Security Support Provider

Process Name: Services.exe
Default Setting: Manual (Workstation), Manual (Server)
Description: Extends NT security to Remote Procedure Call (RPC) progs using various transports other than named pipes. This activity is quite common, as most apps going the RPC route don't use named pipes.
Recommendation: As I implied in the description, this is activity is common, so don't be messin' here. The functionality offered by the service is viable with a setting of **manual**, so changing it to automatic is unnecessary.

Plug and Play

Process Name: Services.exe
Default Setting: Automatic (Workstation), Automatic (Server)
Description: A service that fudges some functionality of Plug and Play, standard in Windows 9x. For those of you having used unimodem modems in NT4, you should be quite familiar with this service (as it's needed to detect and use such modems). Other than that, we all know what PnP is.
Recommendation: Unless you specifically require this service's abilities to support a certain piece of hardware, I suggest setting the status to **manual** and saving yourself some memory.

Protected Storage

Process Name: Pstores.exe
Default Setting: Automatic (IE4, or higher)
Description: A service coming from the IE development team, starting with IE4. NT uses PS to encrypt and store secure info like SSL certificates, passwords for apps (like Outlook, Outlook Express, etc.), info stored by Profile Assistant, info maintained by MS Wallet, and digitally signed S/MIME keys.
Recommendation: After installing IE4 or higher, the pstores.exe process will start **automatically** on system boot. Many folks originally changed the service's status to manual, without suffering any obvious ill-affects. I did the same until IE5, as I now use the MS Wallet. Additionally, since the IE Dev folks just seem to keep piling more and more dependency on this, we might as well get used to having it around right now. I figure those of us not using Netscape should just suck it up, and leave this guy running (even though the process seems to start itself, even when set on manual).

Remote Procedure Call (RPC) Locator

Process Name: Locator.exe
Default Setting: Manual (Workstation), Manual (Server)
Description: Maintains the RPC name server database, and requires the RPC service (just below) to be started. In a two-tier distributed model, the server half registers its status with the maintained database, while the clients query said database to locate available server applications.
Recommendation: Because the service starts on demand, there's **no need to alter the status** setting of this service. Disabling the RPC Locator service would be highly detrimental to your machine, especially if that machine took part in a NT networked environment.

Remote Procedure Call (RPC) Service

Process Name: Rpcss.exe
Default Setting: Automatic (Workstation), Automatic (Server)
Description: As is evident by the process name alone, this service is a subsystem. This RPC subsystem is crucial to the operations of any RPC activities taking place on a system (most DCOM stuff, Server and User Manager, etc.). Rpcss.exe is also known as dcomss.exe (Distributed Common Object Model).
Recommendation: Changing its status from automatic (to either manual or disabled) would be highly problematic for the continued health of the machine, especially if it's networked. Don't mess! Leave on **automatic**.

Schedule

Process Name: atsvc.exe
Default Setting: Manual (Workstation), Manual (Server)
Description: As the process name eludes to, this service is also referred to as the AT service. This service is required for the use of the AT (or SOON) command, which allows the scheduling of commands or progs to be run on a specific computer, at a specified time & date. NT admins are no strangers to this tool, and a domain administrator account is often used in the Run Service As option.
Recommendation: Unless you plan to be sending AT jobs to the machine in question, there's no need to have this service started. Therefore, go ahead and **leave the status of this service alone**.

Server

Process Name: Services.exe
Default Setting: Automatic (Workstation), Automatic (Server)
Description: Provides support for file, print, and named pipe sharing via the SMB services. As a whole, this can be thought of as a subsystem for NT sharing (directories and printers).
Recommendation: Believe it or not, MS actually recommends folks running IIS to disable this service! I suggest that the rest to choose between automatic and manual, with the key distinction being whether or not you plan to do sharing on the machine. If not, go with **manual** ... if so, just say automatic.

Spooler
Process Name: Spoolss.exe
Default Setting: Automatic (Workstation), Automatic (Server)
Description: This service exists as the printing subsystem of NT. This process accepts (from clients), stores, and sends print jobs (one at a time) to available specified print devices when made available. The model is very similar to the post office and snail mail.
Recommendation: If you have a printer attached locally, or are supporting remote printers, you'll need to stick with the **automatic** status. However, if you don't print, you don't need the subsystem, and thus you don't need said subsystem eating up your physical RAM (set it to manual or disabled).

TCP/IP NetBIOS Helper
Process Name: Services.exe
Default Setting: Automatic (Workstation), Automatic (Server)
Description: Provides support for name resolution via a lookup of the LMHosts file. This is an alternative to the more standard DNS lookup, but some still make use of it (even though it sucks, IMO).
Recommendation: Managing this service is fairly straightforward. If you use and maintain a LMHosts file for resolution, leave the status set to automatic. You'll know if you use LMHosts. If you don't (and you probably don't), set it to **manual**.

Telephony
Process Name: Tapisrv.exe
Default Setting: Manual (Workstation), Manual (Server)
Description: A necessary service for all unimodem modems, much like PnP. Not sure exactly why this is a service, but who am I to question the Telephony capabilities of NT4.
Recommendation: All users can leave the status of this service at **manual**, as the service will start on demand if ever needed (will use no resources in the meantime).

UPS
Process Name: Ups.exe
Default Setting: Manual (Workstation), Manual (Server)
Description: Provides support for and manages over the Uninteruptable Power Supply (UPS) physically connected (local) to the machine.
Recommendation: Another easy choice folks, as you only need to deviate from the default status of **manual** if you have a UPS connected to the machine.

Workstation
Process Name: Services.exe
Default Setting: Automatic (Workstation), Automatic (Server)
Description: Also referred to as Lanman Workstation service, this service is needed for communications and network connections. Several other services (Alerter, Messenger, and Net Logon) are dependant on this being started.
Recommendation: Unless you're tweaking an IIS box, and not using any UNC paths, you pretty much need to stick with the default status of **automatic** here. Or in a further extreme, if you're sure you want to basically can communications to and from the machine, disabling this service is all you Fox.

Chances are you'll only remove the automatic setting from a few of the services that are set to load at boot.
Here's a list of those services which are, in a normal installation, set to automatic by default:
Alerter, Computer Browser, Event Log, Messenger, Plug and Play, Protected Storage, RPC Service, Server, Spooler, TCP/IP NetBIOS helper, Workstation.
You'll only be able to turn off more than a few if you're tweaking a stand-alone box. As you might guess, a Network OS (NOS) can have more than a few of its services stopped if it's not existing on a network. Even then, there's two levels of networking to consider: Internet networking, and LAN-networking. Most home users will only want to muck with settings that address the LAN question.

For my NT Server, which I use for home development, and which is not not on a network, I stopped the following seven services:
Alerter
Computer Browser
Event Log, Messenger
Plug and Play
Server
Spooler
TCP/IP
NetBIOS Helper

All in all, after turning off the above services I regained a total of about 4450KB of RAM initially, that is, right after boot. Additionally, I trimmed 6 seconds off my boot time. One thing to keep in mind is that my recommendations of status setting is based on the OS. So if you're having some weird software problem you hadn't had before after stopping some services, plug that into your troubleshooting. Don't get me wrong, these are logical choices to be making, but it may be the case that your new super-fab app that prints out recipes from the 'net needs the Clipboard server running or something. I've seen stranger things happen.

Disable the Computer Browser service
This service enables the local computer to maintain a list of available PCs on a LAN. This is not needed on workstations on a network because the servers function as the master browser. By disabling this function on every PC on a network it can reduce network traffic when choosing a Master Browser as each workstation will not be participating. Every service that is running also consumes memory and CPU cycles.

3. Plug and Play
Windows NT 4.0 does not officially support Plug N Play devices. Luckily, you can install support for Plug N Play devices such as modems, sound cards, network cards, and more in Windows NT 4.0. Without this support installed, Windows NT very well might not

detect and/or recognize your hardware device. Another bonus, it is very easy to install this support. Simply insert your Windows NT 4.0 CD-ROM and navigate to the \Drvlib\Pnpisa\X86\Pnpisa folder/directory.
Right-click the "Pnpisa.inf" file and choose "Install" from the resulting menu. Reboot Windows NT 4.0 and it will recognize most Plug N Play devices just as Windows 95 and Windows 98 do. As in services in tip 2 for NT I would leave the services on manual until needed, saving memory.

4. Rollback not
Windows NT 4.0 comes with a "utility" named "ROLLBACK.EXE" which will corrupt your registry in most cases and render your system unusable, forcing you to reinstall Windows NT from scratch. Don't use Rollback !

5. Service Packs
Install the last service pack for NT - which is service pack V6a - some people say that you must install the service packs in order e.g. install service pack 3, than 4, than 5 etc but this is complete crap. Service Pack V6a will install all the fixes, updates and enhancements from all the previous service packs - and believe me there are thousands of fixes!

6. Pagefile (also see pagfile tip in XP tips)
Make sure your pagefile is set correctly for you. The settings you need to change are in control panels\system\performance. It doesn't matter if you've got 128 or even 256MB of RAM - if your pagefile isn't in tip-top shape, you're taking a performance hit, and that extra RAM you paid for isn't truly paying off. But how much RAM do you need in the first place?

To see how much Virtual Memory you really need, you've got to put your box through its paces, and them some. Use your computer as you normally would. Then use it some more. Run Quake, Access, or whatever you can find to really push your system. Leave it on all day. Abuse it by loading and closing your programs all day long. The point of all of this is to push your machine to the natural limits of your usage pattern. Don't just thoroughly abuse it by loading 500MB files if you never do that sort of thing - we're trying to get an accurate picture of your most intense user scenario.

After you've put the box through its paces, let's have a look at the Task Manager. You can access the Task Manager either by evoking the almighty Ctrl-Alt-Del and clicking "Task Manager," or by choosing "Task Manager" when you right click on the taskbar. OK, got it up? You'll want to have a look at the goodies hiding behind the "Performance" tab. As you can see to the left (or above, depending on your font size), I've highlighted the lower left-hand section of the "Performance" tab's contents in red. This is the "Commit Charge" meter, and it's one of your best tickets to figuring out how much RAM and how much Virtual Memory you should have.

Total refers to the total amount of system memory, real and virtual, that you are using right at that moment. It's the least significant figure. Limit is, you guessed it, your system's combined memory limit, or, the amount of RAM you have plus the amount of Virtual Memory you have allocated. Don't forget, they are displaying these values in 'K' not 'MB,' and there's 1024 'K' in 1MB. Peak is where the truth comes to light. This is the highest total system memory usage during this session.

If your peak number is higher than your limit, you're seriously under-allocated in terms of total system memory. You need more virtual memory, and perhaps you need more RAM. How do you determine which you need more of? Well, in the world of NT, it's easy to get a peak reading that's higher than your total physical RAM. Ideally, you should strive to have more RAM than your peak needs, but not everyone is made of money. As you can see above, my Peak for this session was 170,376K. That's a good deal under 256MB, but it's far above 128MB of RAM. That's why I've got 512MB - it makes life that much smoother.

By default, NT will place your pagefile where ever %winnt% lives, so if you've got NT on D:\, that's where it is.
That's hardly optimal in most situations. Here's how to figure out where to put it: whether your using SCSI or IDE, try to split up your pagefile across your physical drives. Don't waste precious power on splitting up the pagefile across multiple partitions on the same physical drives - that defeats the purpose of what we're trying to do. NT is pretty adept at making multiple simultaneous I/O calls to hardware. This capability enables NT to work with your pagefile in as many locations as it can get access to in any given moment. You can see, now, why NT would take a hit if you split up a pagefile over a partition on one logical drive: hard drives cannot serve two requests simultaneously, IDE or SCSI. However, two different drives can. You cannot move the pagefile from C: but you can reduce the size of the original file and set up a larger paging file on the other drive. The minimum size you can set your pagefile to is 2mb on the boot drive. My advice is to put a paging file on a hard disk (or multiple hard disks) that does not contain the operating system or a paging file should be on a dedicated non RAID FAT partition.

So, if you have multiple drives, spread that pagefile out. On an IDE system, it's best to have them on different chains if possible, too. When it comes to the format of that drive, use NTFS. It's far superior to FAT for the pagefile's needs. So, keeping it on the Win 9x partition on C: probably isn't the best performance-minded decision to make. There is one caveat: if you want to be able to write a full dump when you bluescreen, you have to have a pagefile that is at least the size of your RAM on your boot partition (in NT Speak, the boot partition is the partition with %winnt%, not necessarily C:\ ).

7. The L2 Cache myth
One of the most infamous NT tweaks since the introduction of NT4 has got to be the "L2 cache" tweak, a lone registry entry which stipulates the amount of L2 cache (or secondary cache) that the OS will make use of. Well, as with many things in life, the effects of this tweak are not so black and white. If you're using a processor that implements a direct-mapped L2 cache design (like Pentium I's), then this registry adjustment is indeed for you. However, if you own any Intel processor post-PI, or any modern AMD processor (K6-2 and newer), then your processor is using a set-associative L2 cache design, and thus you need not specify your L2 cache size. Despite the technical logistics of this model, the fact remains that numerous accounts exist of users claiming that after setting this tweak, they received a serious boost in performance. Tests have revlealed that the tweak made absolutely no difference on PII or PIII processors. However, if you wish to save your system the HAL call, and just supply the accurate L2 cache size (or preempt an unlikely HAL error), feel free to set the static value for your processor. Or, if you still have a PI (heaven forbid), continue on.

HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
(take note of the space in "Memory Management")

In this key, double-click on the SecondLevelDataCache registry value to open a DWORD editor window.

The registry key defaults to zero which means 256KB. Change the DWORD value to 0x200 for 512KB or 0x400 for systems with 1MB of L2 cache. Reboot to make this change. I've made this change on a few servers and workstations. It makes a noticeable difference. This tweak can be implemented by using XenTweak.

8. Increase your I/O

Originally considered a tweak for high volume file systems only, the mad progression of yesterday's server-power into the home has changed the audience of those optimising the IOPageLockLimit registry value. By default, the value is set to 0, which NT translates into 512KB. For most users with an ample amount of physical memory (RAM), leaving this setting as 0 will not negate them any caching performance increase. A machine with heavy file I/O traffic and a fair amount of unused physical memory is just begging for this tweak. Such a system would likely benefit from having an IOPageLockLimit of 64 to 128 times the total physical memory size measured in MB, but then recorded in KB (you'll see what I mean in a second). So, for example, a 128MB system should be set between 8192KB and 16384KB, as the decimal setting. This is a good formula for systems with 128MB of RAM, and higher.

For machines with less memory, I suggest starting with a value of 1024KB, and utilizing a "real-world" benchmarking suite like ZDNet's Winbench 99 to bench the performance effect of raising the number of bytes locked for I/O operations. Raise this value by 1024KB per trial, until you see a point of diminishing performance returns. This very well may be 1024KB, 4096KB, or even higher. Each system really requires a different setting. Not all systems experience the same amount of file I/O operations, and not all systems experience disk I/O bottlenecks in the same way, since processor power, disk access & transfer rate, and memory size all play a part in overall performance. So, be prepared to tweak here and there.

How To Implement:

Make certain that you've got everything else in working order, including UDMA (if you have devices that support it). Launch a registry editing tool of your choice (regedit.exe or regedt32.exe will do).

Advance down to the following registry key:

HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management

In this key double-click on the IOPageLockLimit registry value to open a DWORD editor window
(default value of 0 = 512KB).

Change from Hex (hexadecimal) to Decimal, change the value in the data field to reflect your preferred allocation size in KB (1024, 2048, etc.).

Close the registry editor app, and reboot to implement the change.

RAM (MB)	IoPageLockLimit Decimal	Hex
4	4096	1000
8	8192	2000
16	16384	4000
32	32768	8000
64	65536	10000
128	16384	
256	65536	
512	131072	

But I've seen the value in bytes, not KB. In my years of using NT I've come across a few folks who've claimed that the numerical values for this tweak should be entered in bytes, and not kilobytes (e.g., 4096000, not 4096). Nonetheless, the KB values work like a charm.

9. Disable extra sub-systems

If you use the UNIX tools that accompany the NT Server Resource Kit, you won't want to kill POSIX. Other than that, chances are - you don't need these. Umm, most everyone who is a tried and true NT tweaker should busta cap in these two subsystems. Other than that, chances are - you don't need these suckas. There's a lot of debate concerning just how much a tweak like this will earn ya in terms of improved performance. I have consistently argued that the performance benefit for implementing this optimization is marginal at best, but what I have noticed (as have many others) is that the CSRSS.exe process earns a smaller footprint. Additionally, the process /seemed/ to grow a little less aggressively the more I opened and closed applications. This is a tweak for the true Tweak freak. Unlike some of our more apocalyptic tweaks (the UDMA tweaks constantly brings in reports of people loosing bowel control after witnessing the improvements gained), this is for the NT lover who just knows that there's no sense in these subsystems being enabled when they're not ever put to use.

How To Implement:

Launch Windows NT Explorer, and browser to the %windir%\system32 subdirectory.
Rename these files: OS2.exe, OS2SS.exe, and PSXSS.exe (to filename.3x3, or whatever you prefer)
Shutdown any open programs, and reboot to implement the change. Laugh at how seriously easy this is.

10. Use large system cache

While Windows NT Server and Workstation are alike in many ways, the default methods they use for disk caching differ greatly. The Large System Cache option is one that can affect your disk I/O performance up to 50%! On NT Server, the Large System Cache option is enabled, but disabled on Workstation. The two different settings effect how the cache manager allocates free memory. If the Large Cache option is on, the manager marks all the free memory, which isn't being used by the system and/or applications, as freely available for disk caching. On the flip-side (with a small cache), the manager instead only sets aside 4MB of memory for disk caching in an attempt to accelerate the launch of applications. Or in a more technical approach, if enabled the system will favor system-cache working sets over process working sets (with a working set basically being the memory used by components of a process).

This setting may very well benefit users with less than 96MB of physical RAM who don't have more than 2-3 applications open at the same time (those of you with 64MB or less are probably pushing it here). However, without testing this tweak on such a machine, I'd have to suggest 96MB of RAM or more as the rule for implementing this change. I've tested the change on my machine (Celeron 300a @ 450Mhz, 256MB PC100 RAM, WD Expert 18gb 7200rpm drive), and have posted some Winbench benchmark results below.

It should almost certainly benefit users with more than 96MB of RAM, allowing them to more effectively use their available resources, which would otherwise be idle. The Peak Memory Limit item on the Performance tab of the Task Manager is an excellent indicator of how much memory you use on a regular basis. If that number is lower than the amount of physical memory in your computer, this tweak is for you!

How To Implement:
Advance down to the following registry key:
HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
In this key double-click on the LargeSystemCache registry value to open a DWORD editor window
(default value of 0 = small cache).
Change the Hex (hexadecimal) or Decimal value to 1.
Reboot to implement the change.

As can be seen below, the impact of enabling the large cache model is quite noticeable where one would expect it with more high-end (A/V) intensive applications that are I/O intensive.

		Before	After	% difference
Business Disk WinMark 99		6660	6700	0.6
High-End Disk WinMark 99		15000	17000	**13.3**
AVS/Express 3.4	17800	17400	-2.2	
FrontPage 98		69900	74200	**6.2**
MicroStation SE		25400	25800	1.6
Photoshop 4.0		7090	7100	0.1
Premiere 4.2		12400	16100	**29.8**
Sound Forge 4.0	14300	21800	**52.4**	
Visual C++ 5.0		15700	18700	**19.1**

11. Enable UDMA for your hard drives:-
Step 1: Be sure that you have a UDMA-capable hard drive and Motherboard. Don't know? Read the manuals! Take note of all the devices on your IDE chains and whether or not they're UDMA compatible. Most importantly: understand that UDMA can only be enabled on a per-chain basis. So, if you have a CD-ROM and a Hard Drive on your first IDE Chain, both MUST support UDMA for this to work. It's all or nothing. If possible, you might consider rearranging your devices to get your UDMA capable hardware on the same chains. Otherwise, yer broke. Also, it's been reported that CD-Rs react very poorly to this tweak. So, you might or might not be able to get this to work if you have a CD-R running off the IDE chain.

Step 2: Install Service Pack 6 (and reboot). But then, you've already done that, haven't you? Haven't you? And you probably already have an update Rescue Disk, right? If not, make one.

Step 3: Grab CLIBench, a small easy to use Benchmark that'll give you enough accuracy to determine if applying SP6 was enough to do the trick (and if your system came from an OEM with NT pre-installed, you can see if they'd already set it up). Run a Disk Throughput check on any hard drives that are UDMA-capable. http://www.ncpro.com/clibench/clibench.htm

Step 4: Grab dmacheck.exe (from Microsoft), and run it. Enable DMA on any channels you've got DMA capable devices on. Reboot. http://support.microsoft.com/download/support/mslfiles/Dmachcki.exe

Step 5: Run the Disk Throughput check again. If there's a major change (unlikely, but see Step 7 for some reference numbers), you're golden, if not, crack open regedt32.exe. See, although dmacheck.exe may report that UDMA is enabled, it's not necessarily working. But you can force it.

Step 6: Head over to

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\atapi\Parameters\Device0
or
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\atapi\Parameters\Device1

(depending on which channel you want to enable UDMA) and find the DmaDetectionLevel key. It has three possible values, 0x0, 0x1, and 0x2. The first value is what dmacheck sets for channels with the Disable radio button selected, and 0x1 is what dmacheck sets for channels with the Enable radio button selected. Now, here's the funky bit: 0x1 doesn't turn DMA on, but only allows for DMA to be turned on if NT detects that all the hardware is appropriate. If you know that your hardware is good, but 0x1 isn't doing it for you, you can edit the registry key to read 0x2, which forces UDMA on. Sadly enough, most people gotta force it.

If at any point you find you can't boot after making your changes, load the "Last Known Good" and you'll be set (hopefully) - if not restore that last registry backup manually.

Step 7: Run the Disk Throughput test on your drive one more time and see if all rox out. If you're experience was anything like mine, it'll be obvious if it worked. For reference, a Celeron 300A system with the Maxtor DiamondMax 10GB drive averages 13MB/sec on average sustained transactions, with 5% CPU usage. Before modifying the registry, it was clocking in around 6MB/sec, and 90% CPU usage during intense operations. Chew on those numbers!

12. Disable paging of NT executive components:-
On systems with large amount of RAM this tweak can be enabled to force the core Windows NT system to be kept in memory and not paged to disk. If you have 512 megs or more of memory, you can increase system performance
by having the core system kept in memory.
Start Regedit
Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\DisablePagingExecutive
Set the value to be 1. Reboot the computer
Since I've made this registry change, I've have a slight but noticeable decrease in OS caching to disk.
With that said, according to Winbench 99 the "OS performance" increase is ...

		Before	After
Business Disk WinMark 99		6760	6760
High-End Disk WinMark 99		17700	**17900**
AVS/Express 3.4	74300	**74800**	
FrontPage 98		27200	**27400**
MicroStation SE		17100	**17400**
Photoshop 4.0		7050	7030
Premiere 4.2		16600	**17900**
Sound Forge 4.0	21600	21600	
Visual C++ 5.0		18900	**19300**

13. MSConfig
If you like to use MSCONFIG from Windows98, you can still use it with Windows NT. Just copy the file to a place in your path (e.g. \WINNT). You will get an error about a file Regenv32.exe. It will work fine without it but I just copied that file from Windows 98 as well.

14. Stop NTFS volume from generating MS-DOS compatible 8.3 file names
Disabling this feature can increase the performance on heavily used NTFS partitions that have large amount of files with long filenames. Warning: Some 16 bit installation programs may have problems with this option enabled, you can either re-enabled 8.3 creation during the install or use directory names in the non LFN format i.e. "c:\progra~1\applic~1"

Registry Settings:
Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]
Value Name: NtfsDisable8dot3NameCreation
Data Type: REG_DWORD
Data: (0=disable, 1=enable)

15. Increase NTFS Peformance by Disabling the Last Access Time Stamp
When Windows NT accesses a directory on an NTFS volume, it updates the LastAccess time stamp on each directory it detects. Therefore, if there are a large number of directories, this can affect performance. Open your registry and find the key below. Create a new DWORD value, or modify the existing value, named "NtfsDisableLastAccessUpdate" and set it to "1" to prevent the LastAccess time stamp from being updated. Restart Windows for the change to take effect.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem
NtfsDisableLastAccessUpdate 0x00000001 (1)

16. Increase your network performance
If you increase the number of buffers that the redirector reservers for network performance, it may increase your network throughput. Each extra execution thread that you configure will take 1k of additional nonpaged pool memory, but only if your applications actually use them. To configure additional buffers and threads, edit:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters

Modify or Add Value of type REG_DWORD for 'MaxCmds' The range is 0 - 255 and the default is 15
'MaxThreads' Set it to the same value as MaxCmds. You may also want to increase the value of 'MaxCollectionCount'. This REG_DWORD is the buffer for character-mode named pipes writes. The default is 16 and the range is 0 - 65535.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]
Data Type: REG_DWORD

17. Change the Default Printer Spool Directory, priority and other printing tips
This applies for NT, 2000 and XP. If the system is acting as a print server, it is possible that the default location may have insuffcient disk space.

- Create a new directory to act as the Printer spool directory.
- Using Regedit open the key:-
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers]
- Change the value of 'DefaultSpoolDirectory" to equal the full path of the directory you created on other drive.
- Reboot Windows NT, or stop and start the 'Spooler' service.

The default directory is: %SystemRoot%\system32\spool\PRINTERS
To change the spool directory for a specific printer only, find the sub-key under the key below that corresponds to the printer in question. Modify the value of 'SpoolDirectory' to equal the directory you want to use.
Note: If the directory doesn't exist, Windows will use the default.

or
Click Start, click control panel, click printers, click file, click server properties, click the advanced tab, type the name of the new directory in the spool folder dialog box and click ok.

Increase the priority of the spooler subsystem
Prioritize the server for printing on a heavily used server or a server being used for multiple tasks.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print
and add the following key SpoolerPriority
with the REG_DWORD value of 0(Idle Priority), 9(Normal Priority) and 13(High Priority) in decimal.

Other printing tips
You can prioritize for printing speed, application response and efficient network printing.

Click start. click settings. click printers, right click the specific printer you wish to change, click properties, click the details tab, click spooler settings.

-Optimize for quickest return to application
Click spool print documents so program finishes printing faster, click start printing immediately, click ok.

-Optimize for shortest printing time
The application will be unavailable until all printing has been completed.
Click print directly to the printer and click ok.

-Optimize for efficient network printing
This option is best used with applications that take a long time to spool each page.
Click spool print documents so program finishes printing faster, click start printing after last page is spooled and click ok.

18. Disable Print Job Notification in Event Viewer
By default Windows NT server adds an entry in the event log for every print job occuring on the spooler. This can quickly fill up the event log with redundent information.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers]
To disable this function, change the DWORD value for EventLog to "0".

19. Create a Useful Name for My Computer
This tweak will rename "My Computer" to "Username on Computername" making it simple to determine which computer you are logged on to and which username you are logged on as. Using REGEDT32.EXE (this is necessary for REG_EXPAND_SZ) open your registry and find the key below.

[HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}]

Delete the existing value called "No Name" and add a new REG_EXPAND_SZ value with an empty value name and set the string to equal "%USERNAME% on %COMPUTERNAME%". Exit the registry editor, click on your desktop and press F5 (for refresh). The "My Computer" icon should now be rename to "Username on Computername".

20. Auto Logon to a Windows NT/2000 Machine
If you're running Windows NT servers from a locked closet or server room, you can make them fully bootable. This means they won't require human intervention to carry out initial log-ins and run startup batch files. It allows you to automatically logon to the machine and network, bypassing the Winlogon dialog box. This tip also works with 2000.

To enable this function you need to add several new values to the
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] key.

- Add a new value of 'DefaultUserName' and set the data to the username you wish to automatically logon as.
- Add a new value of 'DefaultPassword' and set this to the password for the username above.
- Add a new value of 'DefaultDomainName' and set this to the domain of the user.
  Ignore this value if the NT box is not participating in NT Domain security. This should be the local Windows NT Advanced Server domain on Advanced Server networks, or Machine Name on standalone Windows NT systems.
- Add a new value of 'AutoAdminLogon' and set it to either '1' to enable auto logon or '0' to disable.
- Exit and reboot, Windows should not ask for a password and automatically show the desktop of the user.

Warning: The password is stored in registry, which means anyone who has access to the machine has access to the password and should not be used on secure systems. You can also do the above with TweakUI.

21. Automatically Close Non-Responding Applications
Occasionally when Windows, NT, 2000 and XP shuts down, a task will return as 'Not Responding' and you are given the option to 'End Task'. This tweak automatically closes any non-responding applications. Open the registry and find the key below. This tip also works with all other Microsoft Os's.

[HKEY_USERS\.DEFAULT\Control Panel\Desktop]
Modify the value of 'AutoEndTasks' to equal '1' to automatically end tasks or '0' to prompt for action.

Also we will change the HungAppTimout - Right-click -> select New -> String Value -> call it "HungAppTimeout" (no quotes). Double-click on "HungAppTimeout" and give it a value of 1000 (default is 5000 milliseconds = 5 seconds). This value sets the manual timeout until a program is terminated by using System (Task) Manager.

Next Right-click -> select New -> String Value -> call it "WaitToKillAppTimeout" (no quotes). Double-click on "WaitToKillAppTimeout" and give a value of 2000 (default is 20000 milliseconds = 20 seconds).
This value sets the automatic timeout until Windows shuts down/restarts, while trying to close all open programs.

For example, the setting may look like:
AutoEndTasks "1"
HungAppTimout "1000"
WaitToKillAppTimeout "2000"

22. Delete Cached Copies of Roaming Profiles
If this settings is enabled, when users with roaming profiles log off, the system will delete the cached copy of their roaming profile. This will help to save disk space where that are lots of roaming users. This tip also works for 2000.

Registry Settings:
Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

Value Name: DeleteRoamingCache
Data Type: REG_DWORD
Data: (0 = disabled, 1 = enabled)

23. Reduce the Time the Startup List is Shown on Boot
30 Seconds is a long time when you're waiting for Windows NT or 2000 to boot. With this tip you can decrease the time the system waits for a selection, or remove the time-out all together. The simple way to modify the time-out is to open Control Panel > System. Then click on the 'Startup/Shutdown' tab and change the value of 'Show list for'. Any value between 1-999 is valid, if you choose '0' the system will wait forever for you to make a selection. If you would like to boot Windows without waiting for the time-out the process is slightly more difficult. Using Windows explorer find the file called BOOT.INI on your system drive. Make the file writeable, by right clicking on it and choosing Properties, and then under Attributes, uncheck 'Read-only' and click OK. Now double-click on BOOT.INI, and it should open in Notepad. There is a line under the [boot loader] section labeled timeout=. The number after the '=' sign is the time in seconds Windows will wait for a selection. To make Windows boot instantly change this value to '-1' (i.e. timeout=-1). Save the file, and the next time you reboot Windows NT won't wait for a selection and just load the default OS choice.

24. View Which HotFix Patches Have Been Installed
Periodically Microsoft releases HotFix's to patch bugs in Windows NT and other products, this key contains information about which Hotfix's have been installed.
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix]

25. Removing Orpahned NT Devices and Services
Sometimes it is possible to get orphaned services remaining in the registry. These services can be remove be modifying this key.

Under this key are subkeys representing each device and service installed on the machine.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services]
To remove, first stop the service through Control Panel / Services, then locate the subkey corresponding to device or service and delete it.

26. Stop Error Messages When Booting
Stops the annoying Windows pop-up messages notifying you a device is not functioning when you boot-up Windows NT. Create a REG_DWORD value of 'NoPopupsOnBoot' in the key below (if it doesn't already exist). Set the value to '1' to disable pop-up messages from appearing.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows]

27. Delay Occurs When Unlocking Workstation
Sometimes a noticeable delay occurs when the logged on user or an administrator attempts to unlock a workstation. This because when you unlock the workstation Windows NT will update the domain list if the cached list's age exceeds two minutes (by default). This age limit can be modified.

Open the registry and find this key and value, if they don't exist already create them.
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
Modify the value of 'DcacheMinInterval' to equal the new cache time-out.

28. Connect More Than 10 Clients
If you have a retail version of Windows NT server, and you are still unable to connect more the 10 users concurrently, then have a look at this tip. Open the key below, and find the value of 'Users', if the value doesn't exist then create a new DWORD value. Change the value to equal 'FFFFFFFF' in hex and reboot.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]

29. Tune your server
Improve NT Server systems performance by adjusting the way the network Server object uses memory. Start Control Panel / Network, select the Server object and click on the Configure button. You then have four choices for optimizing the server.

- minimize Memory Used is good choice for workstations and servers on very small networks (up to five sessions).
  balance is good for servers on medium-sized networks (up to 64 sessions).
- maximize Throughput for File Sharing is best for Advanced Server systems that provide resource sharing for large networks (more than 64 sessions)
- maximize Throughput for Network Applications is best for Advanced Servers like SQL Server that provide application services for large networks. Reboot the computer after you change this setting.

30. Unfragment your registry
With time the files that contain the registry become fragmented. While Windows NT is running defragmentation of these files is not possible because they must be opened for exclusive access and cannot because the operating system is using them. An optimal registry is recommended for best performance. This procedure unfragments the files containing the registry. It is always wise to have a backup. Make sure your Emergency Disk is up to date. This procedure requires used of PageDefrag a third party utility program developed by SysInternals. This utility also defragments the paging file. Download PageDefrag from http://www.sysinternals.com. Diskeeper is also very good at this.

31. Unfragment the master file table
The MFT is actually a file usually stored at the beginning of the volume. It is a database which stores file location and attributes. It also stores data about the volume. The MFT only exists on drives using the NTFS file system. Any file accessed on a drive must also access the MFT. A heavily fragmented MFT can cause extremely bad performance. Even if the file is contiguous if the MFT is fragmented it will take several I/O's to access the file.

This procedure cannot be ran on volumes using the FAT file system and this procedure requires Diskeeper.

Click Analyze, click ok, click Action, click view report, scroll threw the report and look for Total MFT Fragments. One Fragment is the optimal number. To defrag the MFT click Action, click Boot-TIme Defragmentation, click on the appropriate drives, click Defragment the MFT, click Set, restart the PC. The MFT is defragged during the boot process and can be lengthy.

32. Increase master file table allocation
When a NTFS drive is formatted it by default reserves 12.5% of that drive for the Master File Table. The MFT contains information about the files on the drive. This includes size, date and permissions. If lots of files are expected to be added to this drive it is recommended to increase the size of the MFT before formatting the drive. When a file is accessed Windows 2000 must also read the MFT for file attributes. A heavily fragmented MFT will slow access to files on the drive. By default Windows NT allocates 12.5% of the drives free space to the MFT. The values for this registry setting are 1=12.5% 2=25% 3=37.5% 4=50%.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem
and add the key NtfsMftZoneReservation with the REG_DWORD value of 2.

33. Increase interval of printer browsing announcement packets
This will decrease network traffic and increase local and wide area network speed. By default Windows NT sends out broadcast packets every 36,000 milliseconds (36 seconds) by default to update the printers list. You can increase this interval to decrease network broadcast traffic.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print
and change the following key
ServerThreadTimeout with the REG_DWORD value of 72,000 milliseconds (number of ms).

34. Reboot on blue screen of death
There are those rare cases when a system fault/error/crash ends up freezing the OS at the dreaded BSOD (Blue Screen Of Death), which displays the cause of the crash and gives some details about the state of the system when it crashed. If you are a system administrator, requiring your servers to run non-stop 24/7, this can be a pain in the neck. To bypass the BSOD altogether and enable the instant "Auto Reboot" feature, run Regedit and go to:

- Windows NT/2000:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CrashControl

- Windows XP/2002:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl
Right-click on the "AutoReboot" String value in the right hand pane -> select Modify -> change it to read 1 -> click OK

CHAPTER [4]

OPTIMIZING WINDOWS 2000 TIPS

(i also advise reading through XP and NT tips as a lot of these also apply)

1. Add/Remove Win2K Components
A common complaint about Windows 2000 Professional is that once you set up the OS, you don't have the option to change the installed components such as WordPad, Calculator, and so on. It turns out there's a relatively easy fix. Using Notepad or another plain-text editor, open up the SYSOC.INF file from the \Windows\Inf folder, and remove all instances of the word HIDE. Save the file and re-open the Add/Remove Program applet in Control Panel. You should now have the option to change components.

2. Turn off not needed services
See Option 1 in Optimizing Windows XP chapter 4, as this is the same and explains what each service does in detail. Also check out Black Vipers website at www.blkviper.com as this details the services very well indeed. Before we go on one point to remember is that by changing the Startup Type of services to Manual, Windows can still start the service if needed.

System services are actually small helper programs that provide support for other larger programs in Windows 2000. Many of the services are set up to run automatically each time you start Windows 2000. However, if you're not using the larger programs that these services are designed to support, these services are simply wasting RAM that could be put to better use by your applications. While the word 'Disable' is used here to describe the idea that you'll remove these services from memory, what you'll really be doing is changing the startup setting from Automatic to Manual. When you do, the services won't automatically start each time you launch Windows 2000 Professional. However, Windows 2000 will be able to manually start the services if they're needed. That way you won't be unnecessarily wasting RAM, but you won't be crippling your system either.

If you have 2000 on a LAN at home you can probably crank all these off... Unless you do peer to peer style workgroup networking without your NT box as a Domain Server or controller! Inside Control Panel, Set these Services to manual via the MMC.EXE console in the Administrative Tools folder.

Description of services in windows 2000

Alerter
notifies selected users and computers of administrative alerts. If this service is turned off, applications that use the NetAlertRaise or NetAlertRaiseEx APIs will be unable to notify a user or computer (by a Message Box from the Messenger service) that the administrative alert took place. Set to **Manual** if you aren't connected to a network. If you are connected to a network set it to Automatic, this will enable your System Administrator to be informed when something goes wrong in your system, which may aid them in Diagnosing, & fixing the issue

Application Management

provides software installation services, such as Assign, Publish, and Remove. This service (known as appmgmts) processes requests to enumerate, install, and remove applications deployed via a corporate network. When you press the Add button in Add/Remove Programs on a computer joined to a domain, the applet calls in to the service to retrieve the list of your deployed applications. The service is also called when you use Add/Remove Programs to install or remove an application, and in cases when a component, such as the shell or COM, makes an install request for an application to handle a file extension, COM class, or progid that is not present on the computer. The service is started by the first call made to it-it does not terminate once started. If the service is disabled, users will be unable to install, remove, or enumerate applications deployed in the Microsoft Active Directory™ service through IntelliMirror® management technologies. Leave this set to **Manual**.

Boot Information Negotiation Layer (BINL)

provides the ability to install Windows 2000 Professional on (Pre Execution Environment) PXE remote boot-enabled client computers. The BINL service, the primary component of Remote Installation Services (RIS), answers PXE clients, checks Active Directory for client validation, and passes client information to and from the server. The BINL service is installed when you either add the Remote Installation Services component from Add/Remove Windows Components, or select it when initially installing the operating system. If turned off, PXE clients requesting RIS installations will fail to get a reply. If BINL is no longer needed on the system, the proper way to discontinue its use would be to use Add/Remove Windows components to remove the Remote Installation Services component. IF turned off, Remote Installation Services will fail to allow client machines to install the OS remotely.

Certificate Services

creates, manages, and removes X.509 certificates for applications such as (Secure/Multipurpose Internet Mail Extensions) S/MIME and (Secure Sockets Layer) Cliff this service is stopped, certificates will not be created. If this service is disabled, any services that explicitly depend on it will fail to start.

Clipbook

enables the Clipbook Viewer to create and share "pages" of data to be viewed by remote computers. This service depends on the NetDDE/Network Dynamic Data Exchange (DDE) service to create the actual file shares that other computers can connect to, while the Clipbook application and service allow users to create the pages of data to share. This service is turned off by default, and it is only started when a user starts the Clipbook. If you disable or remove the service, Clipbrd.exe will time out on startup and notify the user that it cannot be started and remote access is not available. However, Clipbrd.exe can still be used to view the local Clipboard (where data is stored when a user highlights text and then goes to the Edit menu and selects Copy, or types Ctrl+C). Set this to **Manual** to enable users to be able to view information on the Clipbook server. You shouldn't ever need to set this to Automatic.

Cluster Service

defines a cluster as a group of independent computer systems, referred to as nodes, that work together to provide a unified computing resource. There are two different types of cluster solutions in the Windows platform that support different application styles: Server Clusters and (Network Load Balancing) NLB clusters. Server clusters provide a highly available environment for long-running applications such as database or file servers by providing failover support with tightly integrated cluster management. Network load balancing clusters provide a highly available and highly scalable environment for applications that have no long running state such as front-end web servers by load balancing client requests among a set of identical servers. This service applies to the server clusters and is the essential software component that controls all aspects of the server cluster operation and manages the cluster database. Each node in a cluster runs one instance of the cluster service

COM+ Event System

provides automatic distribution of events to subscribing (Component Object Model) COM components. COM+ Events extend the COM+ programming model to support late-bound events or method calls between the publisher or subscriber and the event system. Instead of repeatedly polling the server, the event system notifies interested parties as information becomes available.
COM+ Events handles most of the event semantics for the publisher and subscriber. Publishers offer to publish event types, and subscribers request event types from specific publishers. Subscriptions are maintained outside the publisher and subscriber and are retrieved when needed. This simplifies the programming model for both. The subscriber does not need to contain the logic for building subscriptions-building a subscriber is as easy as building a COM component. The life cycle of the subscription is separate from that of either the publisher or the subscriber. Subscriptions can be built prior to either the subscriber or publisher being made active.
If the service is turned off, System Event Notification (SENS) stops working: Login and logoff notifications will not occur. Other inbox applications, such as Volume Snapshot service, will not work correctly. Set this to **Automatic**.

Computer Browser

maintains an up-to-date list of computers on your network, and supplies the list to programs that request it. The Computer Browser service is used by Windows-based computers that need to view network domains and resources. Computers designated as browsers maintain browse lists, which contain all shared resources used on the network. Earlier versions of Windows applications, such as My Network Places, the NET VIEW command, and Windows NT® Explorer, all require browsing capability. For example, opening My Network Places on a computer running Windows 95 displays a list of domains and computers, which is accomplished by the computer obtaining a copy of the browse list from a computer designated as a browser. There are several different roles a computer may perform in a browsing environment. Under some conditions, such as failure or shutdown of a computer designated for a specific browser role, browsers-or potential browsers-may change to a different role of operation. Windows NT assigns the following special roles to computers running the Computer Browser service:
Domain Master Browser. Used only in domain environments. By default, the primary domain controller (PDC) for a domain operates in this role. The domain master browser collects and maintains the master browse list of available servers for its domain, in addition to any names for other domains and workgroups used in the network. It also distributes and synchronizes the master browse list for master browsers on other subnets that have computers belonging to the same domain.
Master Browser. Collects and maintains the list of available network servers in its subnet. The master browser fully replicates its listed information with the domain master browser to obtain a complete browse list for the network, and distributes it to backup browsers located on the same subnet.
Backup Browser. The backup browser receives a copy of the browse list from the master browser for its subnet, and distributes it to other computers upon request.
Potential Browser. Capable of becoming a backup browser when instructed to by the subnet's master browser, the potential browser operates similarly to a non-browser under normal conditions.

Nonbrowser. A nonbrowser is configured so it cannot become a browser, and it does not maintain a browse list. It can operate as a browse client, requesting browse lists from other computers operating as browsers on the same subnet. When the Computer Browser service is turned off there is no mechanism to discover other computers to populate the My Network Places, and so on. If you are connected to a network set it to **Automatic** as it will enable you to browse through My Network Places & such.

DHCP Client

Dynamic Host Configuration Protocol Client manages network configuration by registering and updating IP addresses and Domain Name Server (DNS) names. You do not have to manually change the IP settings when a client, such as a roaming user, travels throughout the network. The client is automatically given a new IP address regardless of the subnet it reconnects to-as long as a DHCP server is accessible from each of those subnets.
There is no need to manually configure settings for DNS or Windows Internet Name Service (WINS). The DHCP server can give these settings to the client, as long as the DHCP server has been configured to issue such information. To enable this option on the client, simply select the Obtain DNS Server Address Automatically option button. There are no conflicts caused by duplicate IP addresses. If this service is turned off you will not be able to obtain an IP address. You will have to configure a static IP address. If you on a network or have a permanent internet connection, connected to a specified DCHP server set this to **Automatic**. Those who are not connected to a network (or specific DCHP server) set this to Manual

DHCP Server

using the Dynamic Host Configuration Protocol (DHCP), this service allocates IP addresses and allows the advanced configuration of network settings such as DNS servers, WINS servers, and so on to DHCP clients automatically. If the DHCP Server service is turned off, DHCP clients will not receive IP addresses or network settings automatically.

Distributed File System (DFS)

manages logical volumes distributed across a local or wide area network. DFS is a distributed service that integrates disparate file shares into a single logical namespace. This namespace is a logical representation of the network storage resources that are available to users on the network. If the DFS service is turned off, users will be unable to access network data through the logical namespace; in order to access the data, users will need to know the names of all the servers and shares in the namespace, and access each of these targets independently.

Distributed Link Tracking (DLT)

Client-maintains links between the NTFS file system files within a computer or across computers in a network domain. The DLT Client service ensures that shortcuts and (Object Linking and Embedding) OLE links continue to work after the target file is renamed or moved. When you create a shortcut to a file on an NTFS v5 volume, distributed link tracking stamps a unique object identifier (ID) into the target file, known as the link source. Information about the object ID is also stored within the referring file, known as the link client.
Distributed link tracking can use this object ID to locate the link source file in any combination of the following scenarios that occur within a Windows 2000 domain:
The link source file is renamed.
The link source file is moved to another folder on the same volume or to a different volume on the same computer.
The link source file is moved from one NTFS volume to another within the same domain. (The NTFS volumes must be on computers running Windows 2000. The NTFS volumes cannot be on removable media.)
The computer containing the link source file is renamed.
The shared network folder containing the link source file is renamed.
The volume containing the link source file is moved to another computer within the same domain.
Distributed link tracking also attempts to maintain links even when they do not occur within a domain, such as cross-domain, within a workgroup, or on a single computer that is not connected to a network. Links can always be maintained in these scenarios when a link source is moved within a computer, or when the network shared folder on the link source computer is changed. Typically, links can be maintained when the link source is moved to another computer, though this form of tracking is less reliable over time.
Distributed link tracking uses different services for client and server:
The DLT Client service runs on all Windows 2000-based computers. In non-networked computers, the Client service performs all activities related to link tracking.
The DLT Server service runs on Windows 2000 Server domain controllers. The server service maintains information relating to the movement of link source files. Because of this service and the information it maintains, links within a domain are more reliable than those outside a domain. For computers that run in a domain, the DLT Client service takes advantage of this information by communicating with the DLT Server service.
Note: The DLT Client service monitors activity on NTFS volumes and stores maintenance information in a file called Tracking.log, which is located in a hidden folder called System Volume Information at the root of each volume. This folder is protected by permissions that allow only the system to have access to it. The folder is also used by other Windows services, such as Indexing Service.
If the DLT Client service is disabled, you won't be able to track links. Likewise, users on other computers won't be able to track links for documents on your computer. Set this to **Manual**. Although its highly unlikely many of you will use this particular Service. If however you are connected to a Windows 2000 domain & use the NTFS file system, set it to Automatic

Distributed Link Tracking (DLT) Server

stores information so that files moved between volumes can be tracked for each volume in the domain. The DLT Server service runs on each domain controller in a domain. This service enables the DLT Client service to track linked documents that have been moved to a location in another NTFS v5 volume in the same domain
If the DLT Server service is disabled, links maintained by the DLT Client service may be less reliable, especially over time. The "NtfsDisableDomainLinkTracking" policy should be enabled in the File system policy group to prevent DLT clients from repeatedly trying to reach the disabled service.

Distributed Transaction Coordinator

coordinates transactions that are distributed across multiple computer systems and/or resource managers, such as databases, message queues, file systems, or other transaction-protected resource managers. The Distributed Transaction Coordinator is necessary if transactional components are going to be configured through Component Services (COM+). It is also required for transactional queues in Message Queuing (MSMQ) and Microsoft SQL Server™ operations that span multiple systems. Disabling this service prevents these transactions from occurring. Leave this set to **Manual.**

DNS Client
resolves and caches (Domain Name Server) DNS names. The DNS client service must be running on every computer that will perform DNS name resolution. An ability to resolve DNS names is crucial for locating domain controllers in Active Directory domains. Running the DNS client service is also critical for enabling location of the devices identified using DNS names. If the DNS client service is disabled your computers may not be able to locate the domain controllers of the Active Directory domains and internet connections. The computers with disabled client service will not be able to locate the devices identified using DNS names; for example a Web server identified using DNS name www.example.com. Set this to **Automatic** if you are connecting to a specific DNS server on a network

DNS Server
enables DNS name resolution by answering queries and update requests for Domain Name Server (DNS) names. Presence of the DNS servers is crucial for locating devices identified using DNS names and locating domain controllers in Active Directory. If there is no DNS authoritative for a particular portion of the namespace, then locating devices in that portion of the namespace will fail. Not having the DNS server authoritative for the DNS namespace used to resolve Active Directory domains results in an inability to locate the domain controllers for such domain.

Event Log
logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer. The Event Log service writes events sent by applications, services, and the operating system to log files. The events contain diagnostic information in addition to errors specific to the source application, service, or component. The logs can be viewed programmatically through the Event Log APIs or through the Event Viewer in a Microsoft Management Console (MMC) snap-in. If the event log is disabled, you will be unable to track events, which reduces your ability to quickly diagnose problems with your system. In addition, you won't be able to audit security events. Leave this set to **Automatic**.

Fax Service
enables you to send and receive faxes. Disabling this service will render the computer unable to send or receive faxes. Set this to **Manual.**

File Replication
maintains file synchronization of file directory contents among multiple servers. File Replication is the automatic file replication service in Windows 2000. It is used to copy and maintain files on multiple servers simultaneously and to replicate the Windows 2000 system volume SYSVOL on all domain controllers. In addition, it can be configured to replicate files among alternate targets associated with the fault-tolerant Distributed File System (DFS). If this service is disabled, file replication will not occur, and server data will not be synchronized. In the case of a domain controller, stopping the File Replication service may seriously impair its ability to function.

File Server for Macintosh
enables Macintosh users to store and access files on this Windows server machine. If this service is turned off, Macintosh clients will not be able to view any NTFS shares.

FTP Publishing Service
provides (file transfer protocol) FTP connectivity and administration through the Internet Information Service (IIS) snap-in. Features include bandwidth throttling, security accounts, and extensible logging. Set to **Manual**.

Gateway Services for Netware
provides access to file and print resources on Netware networks.

IIS Admin Service
allows administration of Internet Information Services (IIS). If this service is not running, you will not be able to run Web, FTP, NNTP, or SMTP sites, or configure IIS. If you have IIS 5.0 installed & configured to provide an FTP/Website on your machine set this to **Manual** to allow you to configure it whenever needed.

Indexing Service
indexes contents and properties of files on local and remote computers and provides rapid access to files through a flexible querying language. It also enables quick searching of documents on local and remote computers and a search index for content shared on the Web. The Indexing Service builds indexes of all textual information in files and documents. Once the initial index build is complete, the Indexing Service maintains its indexes whenever a file is created, modified, or deleted.
Initial indexing can be resource-intensive. By default, the Indexing Service will index only when the computer is idle. Using MMC, you can configure the Indexing Service to be more aggressive in its approach. MMC also allows configuration of resource allocation in the service to be optimized for query or indexing usage patterns. If this service is either stopped or disabled, all search functionality is provided by traversing the folder hierarchy and scanning each file for the requested string. With the service turned off, search response is typically much slower. Most of you should be fine leaving this set to **Manual**. Although if you wish to maintain regular index updates set this to Automatic

Internet Authentication Service (IAS)
performs centralized authentication, authorization, auditing, and accounting of users who are connecting to a network (LAN or Remote) using Virtual Private Network Equipment (VPNs), Remote Access Equipment (RAS), or 802.1x Wireless and Ethernet/Switch Access Points. Internet Authentication Service implements the IETF standard Remote Authentication Dial-In User Service (RADIUS) protocol, which enables use of heterogeneous network access equipment. If IAS is disabled or stopped authentication requests will fail over to a backup IAS server, if available. If none of the other backup IAS servers are available, users will not be able to connect.

Internet Connection Sharing (ICS)
provides network address translation (NAT), addressing and name resolution services for all computers on your home or small-office network through a dial-up or broadband connection. When Internet Connection Sharing is enabled, your computer becomes an "Internet gateway" on the network, enabling other client computers to share one connection to the Internet, share files, and use the same printers. This service is turned off by default. If this service is stopped or disabled services such as internet connection sharing, name resolution, and addressing will not be available to clients on the network. Therefore clients on the home or small office network may not be able to get to the Internet, and their IP addresses will expire, resulting in some clients using Automatic

Private IP Addressing (APIPA) for peer-to-peer networking connectivity. If no Internet connection is being shared you can set this to **Manual** instead.

Intersite Messaging (ISM)
allows sending and receiving messages between Windows Server sites. This service is used for mail-based replication between sites. Active Directory includes support for replication between sites by using SMTP over IP transport. SMTP support is provided by the SMTP service, which is a component of IIS. The set of transports used for communication between sites must be extensible; therefore, each transport is defined in a separate add-in dynamic link library (DLL). These add-in DLLs are loaded into the ISM service, which runs on all domain controllers that are candidates for performing communication between sites. The ISM service directs send requests and receive requests to the appropriate transport add-in DLLs, which then route the messages to the ISM service on the destination computer.

IPsec Policy Agent
manages IP security (IPsec) policy, starts the Internet Key Exchange (IKE) and coordinates IPsec policy settings with the IP security driver. If you aren't connected to a Windows 2000 Domain you may set this to **Manual**. If you are connected to a Windows 2000 Domain set this to Automatic.

Kerberos Key Distribution Center
enables users to log on to the network using the Kerberos version 5 authentication protocol. If this service is stopped, users will be unable to log on to the domain and access services.

License Logging Service
tracks Client Access License usage for server products, such as IIS, Terminal Services, and File and Print services, as well as other products such as SQL Server and Microsoft Exchange Server. If disabled, licensing for these programs will work properly, but usage will no longer be tracked.

Logical Disk Manager
watches Plug and Play events for new drives to be detected and passes volume and/or disk information to the Logical Disk Manager Administrative Service to be configured. If disabled, the Disk Management snap-in display will not change when disks are added or removed. The Logical Disk Manager uses an administrator service and a watchdog service. The service should not be disabled if dynamic disks are in the system. Set this to **Automatic**.

Logical Disk Manager Administrative Service
performs administrative service for disk management requests. This service is started only when you configure a drive or partition, or a new drive is detected. This service does not run by default, but it does get activated by whenever dynamic disk configuration changes occur or when the Disk Management MMC snap-in is open. Such changes include converting a basic disk to dynamic, recovery of fault tolerant volumes, volume formatting, or changing your page file. The service starts, completes the configuration operation, and then exits. This Service may be set to **Manual**.

Message Queuing
a messaging infrastructure and development tool for creating distributed messaging applications for Windows. Such applications can communicate across heterogeneous networks and can send messages between computers that may be temporarily unable to connect to each other. Message Queuing provides guaranteed message delivery, efficient routing, security, support for sending messages within transactions, and priority-based messaging. Message Queuing provides both Win32® and COM APIs for all programmatic functionality including administration and management. Disabling MSMQ affects a number of other services including COM+ Queued Component (QC) functionality, some parts of WMI, and the MSMQ Triggers service.

Messenger
sends and receives messages to or from users and computers, or those transmitted by administrators or by the Alerter service. If disabled, Messenger notifications cannot be sent to or received by the computer or by users currently logged on; NET SEND and NET NAME will no longer function. If you aren't connected to a network you may set this to **Manual**.

Net Logon
supports pass-through authentication of account logon events for computers in a domain. This service is started automatically when the computer is a member of a domain. It is used to maintain a secure channel to a domain controller for use by the computer in the authentication of users and services running on the computer. In the case of a (domain controller) DC, It also handles the registration of the computer's DNS names specific to DC locator discoveries. In the case of a DC, it also allows pass-through authentication from other DCs running Net Logon that (pass-through authentication) is forwarded to the destination domain controller where the logon credentials are validated. If this service is turned off, the computer will not operate properly in a domain. Specifically, it may deny NTLM authentication requests and, in case of DC, it will not be discoverable by client machines. If you aren't connected to a Windows 2000 Domain you may set it to **Manual**.

NetMeeting Remote Desktop Sharing
allows authorized users to remotely access your Windows desktop from another PC over a corporate intranet by using Microsoft NetMeeting®. The service must be explicitly enabled by NetMeeting, and can be disabled in NetMeeting or shut down via a Windows tray icon. Disabling the service unloads the NetMeeting display driver used for application sharing. For security reasons I'd recommend you set this to **Disable** unless you really need to give others remote access to your Desktop via NetMeeting, in which case set this Service to Manual.

Network Connections
manages objects in the Network and Dial-Up Connections folder, in which you can view both network and remote connections. This is the service that takes care of network configuration (client side) and displays status in the notification area on the desktop (the area on the taskbar to the right of the taskbar buttons). You may also access configuration parameters through this service.
Disabling this service results in a number of consequences including but not limited to the following:
Because connections do not appear in the Connections folder, you will not be able to dial out or configure your local area network (LAN) settings.
Other services that use it to check for Network Location aware Group Policies will start to have undefined behavior
You will not receive events about media connect and disconnect.

Internet connection sharing will not work.
You will not be able to configure incoming connections, wireless settings, or your home network.
You will not be able to create new connections. Leave this set to **Automatic** unless your system is not connected to a Network/Internet, in which case you may set this to Manual.

Network DDE
provides network transport and security for dynamic data exchange (DDE) by applications running on the same computer or on different computers. You can create Network DDE "shares" programmatically or by using DDEshare.exe on your computer, and make them visible to other applications and computers. Traditionally, the user creating the share will create and run a server process to handle incoming requests from client processes and/or applications (running on the same computer or remotely); once connected, these processes can exchange any kind of data over a secure network transport.
This service is turned off by default, and it is only started when invoked by an application that uses NetDDE, such as Clipbrd.exe or DDEshare.exe. In addition, applications running on remote computers can send messages to other computers that will invoke the NetDDE service. If you disable or remove the service, any application that depends on NetDDE will time out when it tries to start the service. If an application on a remote computer is trying to start NetDDE on a different computer, it will appear as if that remote computer is not found on the network. Set this to **Automatic** if you use DDE connections

Network DDE DSDM
manages shared dynamic data exchange (DDE) and is used by Network DDE. This service is used only by Network DDE to manage shared DDE conversations. You can create and "trust" DDE shares by using DDEshare.exe to allow remote computers and applications to connect and share data. This service maintains a database of these DDE shares, including information on which ones are trusted. For each request for a connection from, or "conversation" with, an application, this service queries the database and validates your security settings to determine if the request should be granted. Set this to **Automatic** if you have set the Network DDE Service to Automatic. Otherwise, set it to Manual.

Network News Transfer Protocol (NNTP)
makes the Windows 2000-based server a news server. You can use a news client such as Outlook® Express messaging client to retrieve newsgroups from the server and read headers or bodies of the articles in each newsgroup. You can then post back to the server. NNTP is an Internet standard. (Note that the version included in Windows 2000 doesn't support feeds, where two news servers replicate their contents between each other. However, the version included in Exchange 2000 does include this functionality.) If the service is off, client computers won't be able to connect and read or retrieve posts.

NT LM Security Support Provider
enables users to log on to the network using the NTLM authentication protocol. If this service is stopped, users will be unable to log on to the domain and access services. NTLM is used mostly by Windows versions prior to Windows 2000. For improved security with RPC Applications you should set this to **Automatic**. If you don't use many of these you may save some Memory by setting this to Manual.

Online Presentation Broadcast
links audio and/or video with your PowerPoint® presentation program slides as you deliver a presentation. This can occur either in real time (people on the other end), or asynchronously while at your desk preparing a presentation to be stored on a server and later viewed. There are no other dependencies on this service.

Performance Logs and Alerts
configures performance logs and alerts. This service is used to collect performance data automatically from local or remote computers that have been configured using the Performance Logs and Alerts snap-in. You can use the snap-in to define the performance data you want to collect, the conditions under which alerts should be sent to a user, the start and stop times for the collection, and additional parameters that you can save as a user-defined log collection setting. The Performance Logs and Alerts service then starts and stops performance data collections based on the information contained in the named log collection setting. This service only runs if there are collections scheduled. If the service is running and is then stopped by a user, currently running data collections will terminate and no future scheduled collections will take place. If your system isn't configured like this leave it set to **Manual**.

Plug and Play
enables a computer to recognize and adapt to hardware changes with little or no user input. With Plug and Play, a user can add or remove devices, without any intricate knowledge of computer hardware, and without being forced to manually configure hardware or the operating system. For example, a user can plug in a USB keyboard and Plug and Play will detect the new device, find a driver for it and install it. Or, a user can dock a portable computer and use the docking station's Ethernet card to connect to the network without changing the configuration. Later, the user can undock that same computer and use a modem to connect to the network-again without making any manual configuration changes. Stopping or disabling this service will result in system instability. Set this to **Automatic**. It will make hardware installation far easier.

Print Server for Macintosh
enables Macintosh clients to route printing to a print spooler located on a computer running Windows 2000 Server. If this service is stopped, printing will be unavailable to Macintosh clients.

Print Spooler
queues and manages print jobs locally and remotely. The print spooler is the heart of the Windows printing subsystem and controls all printing jobs. It manages the print queues on the system and communicates with printer drivers and input/output (I/O) components (such as the USB port, TCP/IP, and so on). If the spool service is disabled, you will not be able to print. If you have a printer installed, or intend to install a printer then set this to **Automatic**.

Process Control Service
a Datacenter Server tool that helps you organize and manage the processes on your system and the resources they use. The service monitors all processes starting and stopping on the system and applies the rules you have defined using the Process Control interface. Before stopping this service refer to the product documentation for Process Control.

Protected Storage

provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services processes or users. (Protected Storage) P-Store is a set of software libraries that allows applications to fetch and retrieve security and other information from a personal storage location, hiding the implementation and details of the storage itself. The storage location provided by this service is secure and protected from modification. P-Store uses the Hash-Based Message Authentication Code (HMAC) and the SHA1 cryptographic hash function to encrypt the user's master key. This component requires no configuration. Disabling it will make information protected with this service (for example, private keys) inaccessible to you. P-Store is an earlier service that has been supplanted by the Data Protection API (DPAPI), which is currently the preferred service for protected storage. Unlike DPAPI, the interface to P-Store is not publicly exposed. Set to **Automatic**.

QoS Admission Control (RSVP)
provides network signaling and local, traffic-control, setup functionality for (Quality of Service) QoS-aware programs and control applets. Leave this set to **Manual**, most users will not be using such programs & have no need to set it to Automatic.

QoS RSVP
invoked when an application uses the (Generic Quality of Service) GQoS API requesting a specific quality of service on the end-to-end connection it uses. The services signals its peer and they agree (or not) on the parameters. The RSVP messages can also be intercepted by routers who can veto the resource request if it cannot guarantee it. Once a successful negotiation happens, the service then sets up appropriate flows with the Packet Scheduler which then ensures that a packet rate for that specific flow does not exceed the negotiated rate. If disabled or removed, QoS is not guaranteed to the application and must then decide whether to accept best-effort (the default) or refuse to run.

Remote Access Auto Connection Manager
creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address. This service (sometimes called the autodial service) detects an attempt to resolve the name of a remote computer or share, or an unsuccessful attempt to send packets to a remote computer or share. The service is activated only when there is no network access. In that case, the service brings up a dialog which offers to make a dial-up or virtual private network (VPN) connection to the remote computer. To assist users, the service maintains a local database of connections that were used in the past to reach named computers or shares. When the service detects an unsuccessful attempt to reach a remote computer or share, it will offer to dial the connection that was last used to reach this remote device. Disabling the service has no effect on the rest of the operating system. You will have to set up connections to remote computers manually. In most instances you should be able to set this to Manual without any issue. Although if you are using a modem to provide Internet connectivity it is recommended you set this to **Automatic.**

Remote Access Connection Manager
creates a network connection. This service manages the actual work of connecting, maintaining, and disconnecting dial-up and VPN connections from your computer to the Internet or other remote networks. When you double-click a connection in the Network and Dial up Connections folder and select the Dial button, this generates a work request for this service that is queued with other requests for creating or destroying connections.
This service will unload itself when there are no requests pending. But in practice, the Connections folder calls on this service to enumerate the set of connections and to display the status of each one. So unless there are no connections in the Network Connections folder, the service will always be running. The service cannot be disabled without breaking other portions of the operating system, such as the Network Connections folder. Leave this set to **Automatic** if you are connecting to a network. Those not connected to a network should be able to set this to Manual.

Remote Procedure Call (RPC)
provides the endpoint mapper and other miscellaneous RPC services. This is the RPC endpoint mapper and the COM Service Control Manager (SCM). If this service is turned off, the computer will not boot. Set this Service to **Automatic**. Setting it to Manual/Disable can cause problems, in my experience at least it will stop any Internet activity from occurring.

Remote Procedure Call (RPC) Locator
provides the name services for RPC clients. This service supports the RpcNs family of APIs. It helps locate RPC servers that support a given interface within an enterprise (also known as an RPC named service).
This service is turned off by default. If stopped, depending on the role the particular server was playing in the discovery process, RPC clients that rely on RpcNs* APIs from the same computer may not be able to find RPC servers supporting a given interface, or if the service is turned off on a domain controller, RPC clients using the RpcNs* APIs and this domain controller may experience interruption of service while trying to locate clients. Note that no OS component uses the RpcNs* APIs so having this service turned on is only necessary if third part code requires it. Leave set at **Automatic**.

Remote Registry Service
allows remote registry manipulation. This service lets users connect to a remote registry and read and/or write keys to it-providing they have the required permissions. It is usually used by remote administrators and perf counters. If disabled, it doesn't affect registry operations on the system it runs; therefore, the local system will run in the same manner. Other computers or devices will no longer be able to connect to this computer's registry. Set as **Disabled** for security.

Remote Storage Engine
migrates infrequently used data to tape. It leaves a marker on disk allowing the data to be recalled automatically from tape if you attempt to access the file.

Remote Storage File
manages operations on remotely stored files.

Remote Storage Media
controls the media used to store date remotely. If you have such devices, e.g. Tape drives (not CD\DVD\Floppy drives), then this set to Automatic. Otherwise you may leave it on Manual. NOTE - If set to **Manual** you will need to Start this service before using the Backup program with such backup devices.

Remote Storage Notification
allows Remote Storage to notify you when you have accessed an offline file. Because it takes longer to access a file that has been moved to tape, Remote Storage will notify you if you are attempting to read a file that has been migrated and also allow you to

cancel the request. If the services is turned off, you won't receive any additional notification when you try to open offline files, nor will you be able to cancel an operation that involves an offline file.

Removable Storage

manages removable media drives and libraries. This service maintains a catalog of identifying information for removable media used by a system, including tapes, CDs, and so on. If the system also has automated devices for maintaining removable media (such as a tape autoloader or CD jukebox), Removable Storage also operates the robotics to mount, dismount, and eject media. It is used by applications such as Backup and Remote Storage to handle media cataloging and automation.
This service stops itself when there is no work to do. If there are no automated devices attached to the system, Removable Storage only runs while there are applications using it, so stopping it should never be necessary. If it is stopped on a system that has automated devices, then starting an application such as Backup or Remote Storage can take a very long time. When started in these circumstances, Removable Storage frequently needs to inventory the complete contents of attached autoloaders and jukeboxes, which includes mounting each media in a drive.

Routing and Remote Access

offers routing services in local area and wide area network environments. Routing and Remote Access service provides:
Multiprotocol LAN-to-LAN, LAN-to-WAN, VPN, and NAT routing services
Dial-up and VPN remote access services.
If this service is turned off, incoming remote access and VPN connections, dial-on-demand connections, and routing protocols will not be available. In a routing context, Routing and Remote Access service drives the TCP/IP stack forwarding engine. The forwarding code can be enabled outside the service for various reasons, most notably Internet connection sharing (ICS). Offers routing services to businesses in local area & wide area network environments. If that description fits your system/network type then set this to Automatic, otherwise leave it set it to **Manual**.

RunAs Service

allows you to run specific tools and programs with different permissions than your current logon provides.
It is good practice for administrators to use an account with restrictive permissions to perform routine, non-administrative tasks, and to use an account with broader permissions only when performing specific administrative tasks. To accomplish this without logging off and back on, log on with a regular user account and use the runas command to run the tools that require the broader permissions. You should set this to **Manual**.

SAP Agent

advertises network services on an IPX network using the (Inter Packet eXchange) (Service Advertising Protocol) IPX SAP protocol. It also forwards advertisements on a multi-homed host. Some products such as Microsoft's File and Print Services for Netware rely on the SAP Agent. If this service is turned off, these products may not function correctly.

Security Accounts Manager

startup of this service signals other services that the Security Accounts Manager subsystem is ready to accept requests. This service should not be disabled. Doing so will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to not start correctly. Leave this set to Manual if you haven't changed any Security policies via the Local Security Policy editor. If you have made Security Policy changes set this to **Automatic** in order that the policies may be applied at User logon.

Server

provides RPC support and file print and named pipe sharing over the network. The Server service allows the sharing of your local resources (such as disks and printers) so that other users on the network can access them. It also allows named pipe communication between applications running on other computers and your computer, which is used for RPC.
Disabling this service results in:
An inability to share files and printers on your computer with other computers on the network.
An inability of your computer to service RPC requests.
An inability to communicate via named pipes between machines. If you have IIS 5.0 installed & active on your machine it is recommended that you set this to **Manual**. Set this to Automatic should you wish to make Offline files available to others

Simple Mail Transfer Protocol (SMTP)

transports e-mail across the network.
The SMTP service is used as an e-mail submission and relay agent. It can accept and queue e-mail for remote destinations and retry at specified intervals. Windows domain controllers use the SMTP service for intersite e-mail-based replication. The Collaboration Data Objects (CDO) for Windows 2000 COM component can use the SMTP Service to submit and queue outbound e-mail.
Other applications may use the SMTP Service as the basis for the SMTP support in their product, for example, Microsoft Exchange 2000 Server. Should your machine provide an SMTP server then set this to **Automatic**. You may leave it set to Manual at all other times.

Simple TCP/IP Services

implements support for the following protocols:
Echo (port 7, RFC 862)
Discard (port 9, RFC 863)
Character Generator (port 19, RFC 864)
Daytime (port 13, RFC 867)
Quote of the Day (port 17, RFC 865)
Once the service is enabled, all five protocols are enabled on all adapters. There is no provision for selectively enabling specific services or enabling this service on per-adapter basis. Disabling the service has no effect on the rest of the operating system.

Single Instance Storage (SIS) Groveler

an integral component of Remote Installation Services (RIS). In an effort to reduce the amount of disk space used by a RIS Server's installation folders, SIS will grovel through the partition containing the RIS installation directory, searching for redundant files, storing them centrally, and replacing them with symbolic links. Although the SIS Groveler is installed by default in Windows Server installations, it is set to disabled unless you either add the Remote Installation Services component from Add/Remove Windows Components, or select it when initially installing the operating system.

If the service is turned off, RIS installation images will consume their full image size, and no space savings can be realized. If the SIS Groveler is no longer needed on the system, you should use Add/Remove Windows components to remove the Remote Installation Services component, which will disable it.

Site Server ILS Service

as part of IIS, this service scans TCP/IP stacks and updates directories with the most current user information. Windows 2000 is the last version of the operating system to support the Site Server ILS service.

Smart Card

manages and controls access to a smart card inserted into a smart card reader attached to the computer. The smart card subsystem is based on personal computer/smart card (PC/SC) consortium standards and consists of the following components:
The Resource Manager. This component manages access to readers and smart cards. To manage these resources, it performs the following functions:
Identifies and tracks resources.
Allocates readers and resources across multiple applications.
Supports transaction primitives for accessing services available on a given card.
The resource manager also exposes a subset of the Win32 API to provide applications with access to these functions.
A Card/Reader Selection UI. This component allows simple smart card aware applications to access a card and reader with minimum coding. Disabling the smart card subsystem will result in a loss of smart card support in the system. If you use a SmartCard (not likely for home users) then you can set this to **Disabled** or Manual. If you do happen to use a smart card system set this to Automatic.

Smart Card Helper

provides support for earlier smart card readers attached to the computer. This component is designed to provide enumeration services for the smart card subsystem so that earlier non Plug and Play smart card reader devices can be supported. Turning off this service will remove support for non-Plug and Play readers. If you use a SmartCard (not likely for home users) then you can set this to **Disabled** or Manual. If you do happen to use a smart card system set this to Automatic.

SNMP Service

allows incoming (Simple Network Management Protocol) SNMP requests to be serviced by the local computer. SNMP includes agents that monitor activity in network devices and report to the network console workstation. If the service is turned off, the computer no longer responds to SNMP requests. If the computer is being monitored by network management tools, the tools won't be able to collect data from the computer or control its functionality via SNMP.

SNMP Trap Service

receives trap messages generated by local or remote SNMP agents and forwards the messages to SNMP management programs running on the computer. If the service is turned off, SNMP applications won't receive SNMP traps that they are registered to receive. If this computer is being used to monitor network devices or server applications using SNMP traps significant system occurrences could be missed.

Still Image Service

loads necessary drivers for imaging devices (scanners and digital still image cameras) and manages events for those devices and associated applications and maintains device state. The service is needed to capture events generated by imaging devices (button presses, connections). If the service is not running, events from imaging devices are not captured and processed. In addition, for device drivers, relying on state, access to respective devices will be disabled.

System Event Notification (SENS)

tracks system events such as Windows logon network and power events. Notifies COM+ Event System subscribers of these events.
SENS is an AutoStarted service that depends on COM+ EventSystem service.
Disabling this service has the following effects:
Win32 APIs IsNetworkAlive() and IsDestinationReachable() won't work well. These are mostly used by mobile applications and on portable computers.
SENS interfaces don't work properly. In particular, SENS' Logon/Logoff notifications will not work.
Internet Explorer 5.0 or later uses SENS on portable computers to trigger when to go offline or online (the "Work offline" prompt).
SyncMgr (Mobsync.exe) will not work properly. It depends on connectivity information and Network Connect/Disconnect and Logon/Logoff notifications from SENS.
COM+ EventSystem will try to notify SENS of some events, but will not be able to.
I'd recommend leaving this set to Manual, or **Automatic** depending on how your system is configured (particularly if on a network). Nearly all home users (like myself) can leave this set to Manual with any problems.

Task Scheduler

enables a program to run at a designated time. This service enables you to perform automated tasks on a chosen computer. The Task Scheduler monitors whatever criteria you choose and carries out the task when the criteria for it have been met. For example, you can have the computer run ScanDisk at 7:00 P.M. every Sunday.
Task Scheduler is automatically installed with Windows 2000 and is started each time the operating system is started. It can be run from Windows 2000 (by means of the Task Scheduler graphical user interface [GUI]) or through the Task Scheduler API. If Task Scheduler is disabled, jobs that are scheduled to run won't run at their designated time or interval. Scheduled Tasks using local accounts won't run without a password.
Any task that is using a local account (non-domain account) as the account under which the scheduled task is to run requires a password. If the local account doesn't have a password one needs to be created for that account, and then the task needs to be scheduled using that account name and password. You can create a password for an account by going to Control Panel, User Accounts, Create a Password. Any valid password is acceptable, but it cannot be a blank password. Personally I leave this set to **Disabled** & run the programs myself, although if you need to have task to schedule then set it to Automatic

TCP/IP NetBIOS Helper Service

enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution. This service is an extension of the kernel mode NetBT. It should be considered an integral part of NetBT, not a normal service. It does two things for NetBT, which cannot be done in kernel mode:

It performs DNS name resolution.
It pings a set of IP address and returns a list of reachable IP addresses.
If this service is disabled, NetBT's clients, including Redirector (RDR), SRV, Netlogon, and Messenger, could stop responding. As a result, you may not be able to share files, printers, and logon.
If your Internet connection is setup to enable LMHOSTS Lookup then set this to **Automatic**. Otherwise you may set this to Manual.

TCP/IP Print Server
enables TCP/IP-based printing using the Line Printer Daemon protocol. If this service is stopped, TCP/IP-based printing will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Telephony
provides Telephony API (TAPI) support for programs that control telephony devices and IP-based voice connections on the local computer and through the LAN on servers that are also running the service. The telephony service enables applications to act as clients to telephony equipment such as PBXs, telephones, and modems. The service supports the TAPI under which different wire protocols that communicate with telephony equipment can be supported. These protocols are implemented in Telephony Service Providers (TSPs). The telephony service cannot be stopped if there is another dependent service, such as Remote Access service, currently active. If no other dependent service is running and you stop the telephony service, it will be restarted when any application makes an initialization call to the TAPI interface. If the service is disabled, no program that depends upon it, including modem support, will be able to run.
Leave this set to **Automatic**, generally this Service is started when you load Windows 2000 anyway, even when set to Manual.

Telnet
allows a remote user to log on to the system and run console programs by using the command line. A computer running the Telnet service can support connections from various TCP/IP Telnet clients, including UNIX-based and Windows-based computers. If the Telnet service is stopped, remote users won't be able to connect to the computer using telnet clients. You should **Disable** it altogether, this will improve system security as well.

Terminal Services
provides a multisession environment that allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server. Terminal Services allows multiple users to be connected interactively to a computer and to the display of desktops and applications to remote computers.

Terminal Services Licensing
installs a license server and provides registered client licenses when connecting to a Terminal Server. The Terminal Services License Service is a low-impact service that stores the client licenses that have been issued for a Terminal server and tracks the licenses that have been issued to client computers or terminals. If this service is turned off, the server will be unavailable to issue Terminal Server licenses to clients when they are requested. If another License Server is discoverable on a DC in the forest, the requesting Terminal Server will attempt to use it.

Trivial FTP Daemon
TFTP (trivial file transfer protocol) is an integral part of the Remote Installation Services, this implements support for the TFTP protocol defined in the following RFCs:
RFC 1350 - TFTP
RFC 2347 - Option extension
RFC 2348 - Blocksize option
RFC 2349 - Timeout interval, transfer size options
To disable this service, uninstall Remote Installation Services. Disabling the service directly will cause Remote Installation Services to malfunction.

Uninterruptible Power Supply
manages communications with a UPS connected to the computer by a serial port. If this service is turned off, communications with the UPS will be lost. In the event of power loss on the AC line, the UPS will be unable to direct the PC to shut down while the UPS battery discharges toward a critically low state. This could result in loss of data. If you are connected to such a power supply leave this set to **Automatic**, otherwise leave it Manual.

Utility Manager
starts and configures accessibility tools from one window. Utility Manager allows faster access to some accessibility tools and also displays the status of the tools or devices that it controls. This program saves users time because an administrator can designate that certain features start when Windows 2000 starts. Utility Manager includes three built-in accessibility tools: Magnifier, Narrator, and On-Screen Keyboard. If you don't use (or have Uninstalled) the Accessibilty Tools in Windows 2000 you should set this to **Disabled/Manual**. If you use Accessibility Tools set this to Automatic.

Volume Snapshot
manages volume snapshots used by backup applications. This service manages the volume snapshots. When a backup application attempts to start a backup utilizing the new snapshots infrastructure, the backup application calls methods to determine the number of writers that are running on the service, then queries each writer to gather the required metadata. Following this, the backup application can collect the volumes that need to get a snapshot to ensure a successful backup session. The volumes are presented to the snapshot coordinator and a snapshot is created. The snapshot creates volumes that match the original volumes at the snapshot point of time. If turned off, no snap shot backups can be done.

Windows Installer
installs, repairs, or removes software according to instructions contained in .MSI files provided with the applications. If disabled, the installation, removal, repair, and modification of applications that make use of the Windows Installer will fail. Some applications make use of this service while running, and those applications might not run. You should set this to **Disable** this if you don't wish others to have the ability to change any software installation, or to install Programs/Hardware which use the Windows Installer.

Windows Internet Name Service (WINS)

enables NetBIOS name resolution. Presence of the WINS server(s) is crucial for locating the network resources identified using NetBIOS names. WINS servers are required unless all domains have been upgraded to Active Directory and all computers on the network are running Windows 2000.
Disabling or turning off WINS results in the following:
Location of the Windows NT 4 domains fails.
Location of Windows 2000 Active Directory domains by Windows NT 4 clients fails.
NetBIOS name resolution fails unless a device whose name should be resolved is on the same subnet as the device attempting name resolution and the latter is configured to attempt NetBIOS name resolution using broadcast.

Windows Management Instrumentation (WMI)
provides system management information. WMI is an infrastructure for building management applications and instrumentation shipped as an integral part of the current generation of Microsoft operating systems. Its primary purpose is to reduce cost of ownership for Microsoft operating systems and applications.
WMI makes applications and systems less expensive and easier to manage by providing comprehensive, easily accessible information about applications and services, including management events those applications and services may generate. WMI provides access to the management data through a number of interfaces, including COM API, scripts and command-line interfaces. WMI is compatible with previous management interfaces and protocols, such as Simple Network Management Protocol (SNMP) WMI is a crucial part of Microsoft Operations Manager 2000 infrastructure, and the service is used by internal and external partners to access management information. If this service is turned off, this valuable information will be unavailable. Leave this set to **Automatic**.

Windows Management Instrumentation Driver Extensions
tracks of all of the drivers that have registered WMI information to publish. If the service is turned off, clients cannot access the WMI information published by drivers. However, if the APIs detect that the service is not running, it will attempt to restart it. This should be set to **Automatic** as it seemingly gets Started even if you set it to Manual. Setting it to Disable (Or attempting to Stop the service) will display the following error window.

Windows Media Monitor Service
provides services to monitor client and server connections to the Windows Media™ services.

Windows Media Program Service
roups Windows Media streams into a sequential program for the Windows Media Station Service.

Windows Media Station Service
provides multicasting and distribution services for streaming Windows Media content.

Windows Media Unicast Service
provides Windows Media streaming content on-demand to networked clients.

Windows Time Service (W32Time)
sets the computer clock. W32Time maintains date and time synchronization on all computers running on a Microsoft Windows network. It uses the Network Time Protocol (NTP) to synchronize computer clocks so that an accurate clock value, or timestamp, can be assigned to network validation and resource access requests. The implementation of NTP and the integration of time providers makes W32Time a reliable and scalable time service for enterprise administrators. For computers not joined to a domain, W32Time can be configured to synchronize time with an external time source. If this service is turned off, the time setting for local computers will not be synchronized with any time service in the Windows domain, or an externally configured time service. You may leave this Service set to **Manual**.

Workstation
provides network connections and communications. The workstation service is a user-mode wrapper for the Microsoft Networks redirector. It loads and performs configuration functions for the redirector, provides support for making network connections to remote servers, provides support for the WNet APIs and furnishes redirector statistics. If this service is turned off, no network connections can be made to remote computers using Microsoft Networks. Should you have the Alerter or Messenger Services set to **Automatic** then set this to Automatic also. Otherwise you should be able to safely set this to Manual instead.

World Wide Web Publishing Service
provides HTTP services for applications on the Windows platform. The service depends on the IIS administration service and kernel TCP/IP support. If this service is turned off the operating system will no longer be able to serve act as a Web server. If you have IIS 5.0 installed, & is configured to provide a Website on your machine set this to Automatic, otherwise leave it set to **Manual**.

Should you find that any of the Services you have attempted setting to Manual are Started when Windows 2000 is loaded you should set them to Automatic instead. You may verify this by checking the Status tab in the Services Utility in Administrative Tools. By now you should have finished customizing your system Services settings. Hopefully by now you will have reduced the amount of Memory consumed by the Services program (services.exe), disabled certain Services to improve your systems security or just configured the Services to enhance your Networked environment, or Standalone operating environment.

3. MSConfig
If you like to use MSCONFIG from Windows98, you can still use it with Windows2000.
Just copy the file to a place in your path (e.g. \WINNT). You will get an error about a file Regenv32.exe. It will work fine without it but I just copied that file from Windows 98 as well.

4. Turn off Windows 2000 system file protection
For the most part I view SFP as a good thing but there are reasons to disable it - many people dont want the OS spending cycles doing this, disk space may be light and the world made it this far without SFP so its not absolutely necessary. Howerver unless you routinely experience problems with it, it's probably either left alone or tweaked to a size that makes you comfortable.

Both registry keys in question are found at:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

The two relevant keys are SFCDisable and SfcQuota. The size of the dllcache can also be manipulated at the command prompt.

To disable (or create) the SFCDisable to REG_DWORD 'ffffff9d'. (It should be currently set to '0')
Reboot. indows will not clean up the files, so if you want to trash them, you can, but leave the folder. Check your event log and see that Windows has truly disabled it.
Other reports on the 'net indicate that a value of '1' will disable WFP, but this seems to reset after another reboot.

To manage the size of dllcache you have two options 1) the registry, and 2) the easier command prompt option. In the registry, set SfcQuota to the hexadecimal value that's equivalent to the number of MB you'd like for the dllcache to take up.

If you don't know hex, here's some samples:
00000099 = 153 (MB).
0000004b = 75 (MB).
00000032 = 50 (MB).
0000000a = 10 (MB).
FFFFFFFF = Unlimited (default setting now)

When you're done, run sfc /snannow for good measure, and reboot.
Using the sfc command, it gets much easier. At the command prompt, type:
sfc /cachesize=X
where X is measured in MB. For instance, X=50 sets the cache to 50MB.
When done, run sfc /snannow for good measure, and reboot.

How to relocate the dllcache
You will need to create a registry key in this location. Use regedt32 for this operation:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Create a value of SFPGDllCacheDir, with data type REG_SZ_EXPAND. The string is the path where you want the folder to live. It will append the folder to that location. Some examples:
%systemroot%\system32 (the default)
\\PhatServer\sneakypoo$\admin (the admin folder in the hidden share sneakypoo, on the server PhatServer)

5. Drive Data
By default, Win2k is set to collect physical drive data. Home users we don't need this.
To disable the disk performance counters: Start, Programs, Command Prompt, 'diskperf -n', reboot
And if you ever want to return to defaults - type 'diskperf -yd' in command prompt

6. VCache
Win2K handles its system cache (known as Vcache in Win9x) very differently depending on which version you have. Server and above have this setting enabled, and they see a substantial disk I/O increase because of it. It is more effective than you would think because programs with native support for Win2k are supposed to already be programmed so that they can be run directly from the cache. I personally don't recommend enabling this value unless you have at least 256 MB of RAM.

To enable the setting here are the registry keys:-
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\MemoryManagement
"LargeSystemCache"=dword:00000001

To disable it:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\MemoryManagement
"LargeSystemCache"=dword:00000000

7. Relocating the pagefile.sys
You can set this in the performance tab but I have had no luck at all so try this.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement
Scroll to pagefile.sys and you'll see the letter for your pagefile.sys just highlight letter and select a new drive letter.

8. Install Recovery Console
Very useful for troubleshooting. Go to where your 2000 cab files are and type '\i386\winnt32.exe /cmdcons'. Where 'd:\' is cd drive or hard drive. Commands available when Recovery Console is installed :-

LISTSVC	List services
ENABLE/DISALBE	Enable/disable service
DISKPART	Equivalent of FDISK
FIXBOOT	Create a new boot sector on the system partition
FIXMBR FDISK /MBR	equivalent (problems with RAID etc)
LOGON	List installation of Windows 2000 and can choose which to work on
SYSTEMROOT	Move to the system root
MAP	Display a list of drives and ARC paths. Useful to fix boot.ini probs.

9. Cable Modem & xDSL Speed Tweak
To increase your broadband Cable Modem speed tip visit www.speedguide.net
Also visit www.x9000.net and download XenTweak
They have some excellent registry and inf files to download specially for cable access.

10. Speed up modem data
Speed up buffering of data between your modem and your modem port. This enables your modem to retrieve information faster. Right click my Computer, Click Properties, Click Hardware, Click Device Manager, Double Click Ports, Double Click the appropriate Com port, Click Port Settings, Click Bits per second and change it to the highest supported speed, Click Flow Control and change it to Hardware, Click OK. Click OK. OK.

11. Adaptive Menus
Microsoft Office 2000 introduced personalized menus (a.k.a. adaptive menus) that remembers which items you use regularly and hides items you don't. This tweaks allows you to enable or disable this functionality. Exit all open Office 2000 applications, including Word, Excel, Access and Outlook. Then open your registry and find the key below, if it does not exist create it.
[HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Common\Toolbars]
Create a new DWORD value named 'AdaptiveMenus' and set the value to '0' for disabled and '1' for enabled.

12. Control Smart Menus
Switch them off ! Windows 2000 included a new feature called 'Personalized Menus', which remembers which items you use regularly and hides items you don't. This tweaks allows you to enable or disable this functionality.

Open your registry and find the key mentioned below.
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
Create a new string value, or modify the the existing value, named 'IntelliMenus'.
Modify the value to equal 'YES' to enable smart menus or 'NO' to disable them.

By using the same key except under the [HKEY_LOCAL_MACHINE] tree the tweak can be enforced system wide, instead of only user based. Restart your machine.

13. Create a Useful Name for My Computer
This tweak will rename "My Computer" to "Username on Computername" making it simple to determine which computer you are logged on to and which username you are logged on as.
Using REGEDT32.EXE (this is necessary for REG_EXPAND_SZ) open your registry and find the key below.

[HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}]
Rename the value named "LocalizedString" to "LocalizedString.old". Create a new REG_EXPAND_SZ value named "LocalizedString", and copy the contents of the original value to the new value except change the words "My Computer" to equal "%USERNAME% on %COMPUTERNAME%". For example, the new "LocalizedString" value may equal "@C:\WINNT\system32\shell32.dll,-9216@1033,%USERNAME% on %COMPUTERNAME%".

14. Hide or Display Administrative Tools Menu
As with Windows NT, Windows 2000 has an 'Administrative Tools' folder on the Start Menu. This folder contains powerful administration utilities and therefore can be hidden to avoid accidental use.

Open your registry and find the key mentioned below.
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]

For example, the setting may look like:
(Default) (value not set)
StartMenuAdminTools YES

Create a new string value, or modify the the existing value, named 'StartMenuAdminTools'. Modify the value to equal 'YES' to show the administrative tools folder or 'NO' to hide it. By using the same key except under the [HKEY_LOCAL_MACHINE] tree the tweak can be enforced system wide, instead of only user based.
Exit your registry and log off for the changes to take effect. Note: Hiding the folder does not stop the use of the tools, it only make it more difficult to locate them.

15. Show Favorites on the Start Menu
This setting controls whether the Favorites folder is shown on the Start Menu.

Open your registry and find the key mentioned below.
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
Create a new DWORD value, or modify the the existing value, named 'StartMenuFavorites'. Modify the value to equal '1' to enable Favorites or '0' to disable them.

For example, the setting may look like:
(Default) (value not set)
StartMenuFavorites 0x00000001 (1)
By using the same key except under the [HKEY_LOCAL_MACHINE] tree the tweak can be enforced system wide, instead of only user based. Log off for the changes to take effect.

16. Group Policy Editor in 2000/XP
Various settings can be altered by accessing administrator setup. At the Start\Run prompt type "gpedit.msc". This will open a management console which gives access to various administrator settings.

17. Hidden Devices
In Device Manager, there is an option to show hidden settings: from the menu go to View/Show Hidden Devices.
I had a couple of items here that were not installed correctly.

18. Disable Last Access Time
To prevent ntfs from updating the last access time of each directory, open the following registry key:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem
Add a new DWord Value and name it NtfsDisableLastAccessUpdate: set the value to 1 to disable this feature.

19. Speed up and browse faster
Here's a great tip (a bug actually) to speed up your browsing of 2000 machines. Its actually a fix to a bug that by default of a normal Windows 2000 setup that scans for shared files for Scheduled Tasks. And its turns out that you can experience a delay as

long as 30 seconds when you try to view shared files across a network from as Windows 2000 is using the extra time to search the remote computer. Note that though the fix is originally intended for only those affected, Windows 2000 users will experience that actual browsing speed of both the Internet & Windows Explorers improving significantly after applying it since it doesnt search for the Scheduled Tasks anymore.

Open up the Registry and go to :
HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/Current Version/Explorer/RemoteComputer/NameSpace

Under that branch, select the key :
{D6277990-4C6A-11CF-8D87-00AA0060F5BF} - and delete it.

This is key that instructs Windows to search for Scheduled Tasks. If you like you may want to export the exact branch so that you can restore the key if necessary. This fix is so effective that it doesn't require a reboot and you can almost immediately determine yourself how much it speeds up your browsing processes.

20. Manage performance using Microsoft Management Console
To best manage the performance of your Windows 2000 and XP installation, I recommend using the Microsoft Management Console to customise the tools available to you. To bring up the MMC, type "MMC" in the Start/Run box. This will open a blank MMC. Then select Add/Remove Snap In from the Console menu, and select the items you wish to use. You will probably want to add Defragmenter, Services, Event Viewer and Device Manager as a minimum. When you are finished save your changes, and create a desktop shortcut to the file you have saved. If you wish you can set Event Viewer to show error messages only: right click on Application, Security and System in turn, select Properties and uncheck the options you do not require.

21. PMTU Discovery
You can configure Windows 2000 to calculate the MTU between your machine and a remote host, e.g. your ISP. This avoids fragmentation of information sent over the connection, and can improve internet connection speeds.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Right click in the right hand pane, and select New Dword Value.
Name this value "EnablePMTUDiscovery" and then set the value to 1.

22. Increase the time NetBIOS names remain in the cache
If your Windows 2000/XP domain is not using active directory name resolution will be provided by WINS. WINS provide names resolution to IP addresses and this will reduce the number of broadcasts. Lans not using active directory should use a WINS server instead of broadcasting or using a LMHOST file. The WINS server maintains a cache of the NetBIOS names. By increasing how long these names are kept in the cache broadcasting will be further reduced.

Edit the key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters\CacheTimeout.
Modify the key Cache timeout to a value of 900000(millisceonds) which is 15 minutes.

23. Tune your server
This also applies to NT and XP. Improve 2000 Server systems performance by adjusting the way the network Server object uses memory. Start Control Panel / Network, select the Server object and click on the Configure button. You then have four choices for optimizing the server.

- minimize Memory Used is good choice for workstations and servers on very small networks (up to five sessions).
  balance is good for servers on medium-sized networks (up to 64 sessions).
- maximize Throughput for File Sharing is best for Advanced Server systems that provide resource sharing for
  large networks (more than 64 sessions)
- maximize Throughput for Network Applications is best for Advanced Servers like SQL Server that provide
  application services for large networks. Reboot the computer after you change this setting.

CHAPTER [5]

OPTIMIZING WINDOWS XP TIPS

(i also advise reading through XP and NT tips as a lot of these also apply)

1. Turn off unneeded services and save 25-30 meg of ram
put here list of services

2. Uninstall unwanted components
It seems that some components in Windows XP can't be uninstalled. Well they can. Use this trick to uninstall MSN Messenger, MSN Explorer and Microsoft Games. First, make a copy of sysoc.inf
found on the hard disk at \windpws\inf\sysoc.inf before proceeding so that you can restore the initial configuration if necessary. Give the copy a different name, such as sysoc2.inf.

Open the Sysoc.inf file. Each line of text in the file represents a component that can be displayed in the Add/Remove Windows Components dialog. Delete the word HIDE for any component that you want to see in the dialog (do not erase the commas). Save the Sysoc.inf file, then close it, and reboot your computer. The Add/Remove Windows Components dialog will now display the items you want.

3. Speed up Internet Explorer 6 Favorites
For some reason, the Favorites menu in IE 6 seems to slow down dramatically sometimes. I've noticed this happens when you install Tweak UI 1.33, for example, and when you use the preview tip to speed up the Start menu. But here's a fix for the problem that does work, though it's unclear why. Just open a command line window (Start button -> Run -> cmd) and type sfc, then hit ENTER. This command line runs the System File Checker, which performs a number of services, all of which are completely unrelated to IE 6. But there you go: It works.

4. Remove the Shared Documents folders from My Computer
One of the most annoying things about the new Windows XP user interface is that Microsoft saw fit to provide links to all of the Shared Documents folders on your system, right at the top of the My Computer window. I can't imagine why this would be the default, even in a shared PC environment at home.

Simply fire up the Registry Editor and backup and then delete the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\My Computer\NameSpace\DelegateFolders\{59031a47-3f72-44a7-89c5-5595fe6b30ee}"(Default)"=dword:00000

If you do this, all of the Shared Documents folders (which are normally under the group called "Other Files Stored on This Computer") will be gone.

5. Sort the default My Documents folders out
Microsoft Windows XP uses a lot of folders for each user. Everything from "My video" to your personal documents folder. Below is where you can view the locations of these folders and can change them.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
Right click on the folders and select Modify. Change the path to a new path if you want to change the path.

Delete My EBooks and other special folders in My Documents
Click Start, then Run and type: regsvr32 /u mydocs.dll
then delete them

6. Do an unattended installation
The Windows XP Setup routine is much nicer than that in Windows 2000 or Windows Me, but it's still an hour-long process that forces you to sit in front of your computer for an hour, answering dialog boxes and typing in product keys. But Windows XP picks up one of the more useful features from Windows 2000, the ability to do an unattended installation, so you can simply prepare a script that will answer all those dialogs for you. If you want to dual-boot Windows XP with another OS, you're going to have to go through the interactive Setup just like everyone else: An unattended install will wipe out your hard drive and install only Windows XP, usually.

To perform an unattended installation, you just need to work with the Setup Manager, which is located on the Windows XP CD-ROM in D:\SupportTools\DEPLOY.CAB by default. Extract the contents of this file and you'll find a number of useful tools and help files; the one we're interested in is named setupmgr.exe. This is a very simple wizard application that will walk you through the process of creating an answer file called winnt.sif that can be used to guide Windows XP Setup through the unattended installation.

One final tip. There's one thing that Setup Manager doesn't add. Your product key. However, you can add this to the unattend.txt file manually. Simply open the file in Notepad and add the following line under the [UserData] section:

ProductID="RK7J8-2PGYQ-P47VV-V6PMB-F6XPQ"
You'll have to substitute your actual product key for the string listed above, of course. Key above is a 60 day key.

Then, just copy winnt.sif to a floppy, put your Windows XP CD-ROM in the CD drive, and reboot: When the CD auto-boots, it will look for the unattend.txt file in A: automatically, and use it to answer the Setup questions if it's there.
Finally, please remember that this will wipe out your system! Back up first, and spend some time with the help files in DEPLOY.CAB before proceeding.

7. XP product activation
Microsoft believes that the activation process is solid, and will work in this situation so that you will not be left stranded at all. But, suppose you don't have a working phone line where you are, so that both telephone and modem contact are unavailable to you, and you really need to get your computer up and running now! There's a fix you can do on the spot. It involves backing out of the last hardware change, and restoring the hardware configuration to the way it was when you activated, or close enough to that. Here's how to do it:

- Boot Windows XP into non-networked Safe Mode.
- Press and hold the F8 key right after the POST is finished, and selecting the correct option from a menu.
- At the command prompt, navigate to the System32 folder: cd \windows\system32
- Backup the file WPA.DBL - rename it something like OLDWPA.DBL; do not name it WPA.BAK.
- Copy the file WPA.BAK to WPA.DBL. - copy and not rename because you may want WPA.BAK file another time.
- Reboot the computer. It should load Windows XP in normal mode, and you're back in business.

Here's how to check if your copy of XP is Activated
Go to the run box and type in oobe/msoobe /a and hit ok ...theirs your answer

Avoid XP Registration
To avoid registering your copy of Windows XP with Microsoft altogether, and to force XP into thinking you have already completed the registration process, just follow these steps:

- Physically disconnect/unplug your network cable/connection (if any).
- Turn on (power up) your computer.

- Start WinXP Setup and answer NO when asked to use Windows Dynamic Update, which would (if enabled) connect to the Microsoft web site for registering purpose.
- If you are installing XP unattended (automatic Setup), you MUST add/modify your Unattend.txt "DisableDynamicUpdates" line under the [Unattended] section to read:
[Unattended]
DisableDynamicUpdates=yes
- Right after your XP installation is completed, either: reboot to Safe mode, or
avoid setting up your Internet connection when asked to, upon the first reboot. Click Next or Skip instead. At this point the Internet Connection Wizard will eventually crash, after clicking the Next button, but don't worry, everything is cool

Click the Start button -> select the Run box -> type:
regsrv32 -u regwizc.dll

Click OK or hit Enter. Then click OK or hit Enter again to close the following confirmation dialog box, which unregisters this DLL, thus making it "invisible" to Windows.
Optionally, you can also rename BOTH your Regwizc.dll files located in %systemroot%\System32 and %systemroot%\System32\Dllcache to something else (i.e. Regwizc.dlx), to avoid having to repeat these annoying steps all over again, whenever you install a Windows component/patch/update/etc that might re-register (reenable) Regwizc.dll, which would force WinXP to register with MS in the future, without your permission.

Run Regedit and go to:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion

Right-click on the "RegDone" String (REG_SZ) Value -> select Modify -> type 1 in the Value data: box -> click OK or hit Enter -> exit the Registry Editor.

Right-click on the Internet Explorer Desktop icon -> open Tools menu -> click Internet Properties -> change the default home page to ANYTHING EXCEPT ANY Microsoft or MSN web page -> click OK/Apply or hit Enter.

Reboot to Normal mode. Right AFTER XP reboots, but BEFORE before Windows GUI loads, make sure to plug back in/reconnect your network cable/connection (if any).

8. Switch off menu shadow and other useless effects

XP reserves a substantial amount of your CPU horsepower for things like animating various desktop elements, placing shadows under menus and cursors, and rounding the upper corners of open windows. In the aggregate, these visual effects can slow down screen-drawing operations significantly. Also, XP may have selected a "color depth" for your video system in excess of what you really need; this, too, can slow down screen operations.

To adjust XP's desktop animations and visual effects, right click on My Computer and select Properties/Advanced/Performance Settings. You can choose to activate/deactivate individual items or use the general "best performance/best appearance" buttons. When you've made a change, click Apply, and you'll see the effects almost immediately. (By the way: Selecting Best Performance makes your desktop look very much like the classic desktop in Win98/Win2K.) Experiment until you've found the mix of speed and visual effects that works best for you.

9. XP configuration tool

Modify virtually every feature in Windows XP without having to resort to regedit. It's called the Local Group Policy Editor, or gpedit for short. Select Start and then Run, then type gpedit.msc

10. Manage performance using Microsoft Management Console

To best manage the performance of your Windows 2000 and XP installation, I recommend using the Microsoft Management Console to customise the tools available to you. To bring up the MMC, type "MMC" in the Start/Run box. This will open a blank MMC. Then select Add/Remove Snap In from the Console menu, and select the items you wish to use. You will probably want to add Defragmenter, Services, Event Viewer and Device Manager as a minimum. When you are finished save your changes, and create a desktop shortcut to the file you have saved. If you wish you can set Event Viewer to show error messages only: right click on Application, Security and System in turn, select Properties and uncheck the options you do not require.

11. Memory Tweaks

Below are some memory tweaks and they apply to NT, 2000 and XP. They are located in the Windows
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

DisablePagingExecutive
You can read more on this in NT tips. When enabled, this setting will prevent the paging of the Executive files to the hard drive, causing the OS and most
programs to be more responsive. However, it is advised that people should only perform this tweak if they have a significant amount of RAM on their system (128 MB+), because this setting does use a substantial portion of your system resources. By default, the value of this key is 0. To enable it, set it to 1.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\DisablePagingExecutive
Set the value to be 1. Reboot the computer

LargeSystemCache
You can read more on this in NT tips. When enabled (the default on Server versions of Windows 2000), this setting tells the OS to devote all but 4 MB of system memory (which is left for disk caching) to the file system cache. The main effect of this is allowing the computer to cache the OS Kernel to memory, making the OS more responsive. The setting is dynamic and if more than 4 MB is needed from the disk cache for some reason, the space will be released to it. By default, 8MB is earmarked for this purpose. This tweak usually makes the OS more responsive. It is a dynamic setting, and the kernel will give up any space deemed necessary for another application (at a performance hit when such changes are needed). As with the previous key, set the value from 0 to 1 to enable.

Note that in doing this, you are consuming more of your system RAM than normal. While LargeSystemCache will cut back usage when other apps need more RAM, this process can impede performance in certain intensive situations.
According to Microsoft, the "[0] setting is recommended for servers running applications that do their own memory caching, such as Microsoft SQL Server, and for applications that perform best with ample memory, such as Internet
Information Services." I personally don't recommend enabling this value unless you have at least 256 MB of RAM.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\MemoryManagement
"LargeSystemCache"=dword:00000001

IOPageLockLimit
You can read more on this in NT tips. This tweak is of questionable value to people that aren't running some kind of server of off of their computer, but we will include it anyway. This tweak boosts the Input/Output performance of your computer when it is doing a large amount of file transfers and other similar operations. This tweak won't do much of anything for a system without a significant amount of RAM (if you don't have more than 128 MB, don't even bother), but systems with more than 256 MB of RAM will generally find a performance boost by setting this to between 8 and 16 MB. The default is 0.5 MB, or 512 KB. This setting requires a value in bytes, so multiply the desired number of megabytes
* 1024 * 1024. That's X * 1048576 (where X is the number, in megabytes). Test out several settings and keep the one which seems to work best for your system.

HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management
In this key double-click on the IOPageLockLimit registry value to open a DWORD editor window
(default value of 0 = 512KB).
Change from Hex (hexadecimal) to Decimal, change the value in the data field to reflect your preferred allocation size in KB (1024, 2048, etc.). Close the registry editor app, and reboot to implement the change.

RAM (MB)	IoPageLockLimit Decimal	Hex
4	4096	1000
8	8192	2000
16	16384	4000
32	32768	8000
64	65536	10000
128	16384	
256	65536	
512	131072	

12. Stop NTFS volume from generating MS-DOS compatible 8.3 file names
Disabling this feature can increase the performance on heavily used NTFS partitions that have large amount of files with long filenames. Warning: Some 16 bit installation programs may have problems with this option enabled, you can either re-enabled 8.3 creation during the install or use directory names in the non LFN format i.e. "c:\progra~1\applic~1"

Registry Settings:
Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]
Value Name: NtfsDisable8dot3NameCreation
Data Type: REG_DWORD
Data: (0=disable, 1=enable)

13. Increase NTFS Peformance by Disabling the Last Access Time Stamp
When Windows XP accesses a directory on an NTFS volume, it updates the LastAccess time stamp on each directory it detects. Therefore, if there are a large number of directories, this can affect performance. Open your registry and find the key below. Create a new DWORD value, or modify the existing value, named "NtfsDisableLastAccessUpdate" and set it to "1" to prevent the LastAccess time stamp from being updated. Restart Windows for the change to take effect.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem
NtfsDisableLastAccessUpdate 0x00000001 (1)

14. Automatically Close Non-Responding Applications
Occasionally when XP shuts down, a task will return as 'Not Responding' and you are given the option to 'End Task'. This tweak automatically closes any non-responding applications. Open the registry and find the key below. This tip also works with all other Microsoft Os's.

[HKEY_USERS\.DEFAULT\Control Panel\Desktop]
Modify the value of 'AutoEndTasks' to equal '1' to automatically end tasks or '0' to prompt for action.

Also we will change the HungAppTimout - Right-click -> select New -> String Value -> call it "HungAppTimeout"
(no quotes). Double-click on "HungAppTimeout" and give it a value of 1000 (default is 5000 milliseconds = 5 seconds). This value sets the manual timeout until a program is terminated by using System (Task) Manager.
Next Right-click -> select New -> String Value -> call it "WaitToKillAppTimeout" (no quotes). Double-click on "WaitToKillAppTimeout" and give a value of 2000 (default is 20000 milliseconds = 20 seconds).
This value sets the automatic timeout until Windows shuts down/restarts, while trying to close all open programs.

For example, the setting may look like:
AutoEndTasks "1"
HungAppTimout "1000"
WaitToKillAppTimeout "2000"

15. Turn off autoplay for CDs

Go to Start->Run->gpedit.msc. Computer Config -> Administrative Template -> System
Double clik Turn off Autoplay. Enable it.

16. Disable error reporting
Every time a program crashes I do not want to send a report to microsoft. Disable this stupid feature. Open Control Panel, Click on Preformance and Maintenance. Click on System. Then click on the Advanced tab. Click on the error reporting button on the bottom of the windows. Select Disable error reporting. Click OK twice.

17. Refresh Rate on your Nvidia Card
This tip is not documented that well on the net and is essential to get the best out of your gameplay.
Having trouble setting refresh rate on your Nvidia card when playing games ? There are 2 ways to sort this out. Basically you need to change refresh rate for all the resolutions that you play for games - for example if you play games using 800x600 and also 1024x768 and also 1280x1024 etc you need to goto your display control panel put your desktop into 800x600 and goto the monitor tab and put the refresh up to whatever your monitor can handle (normally 85hz) and then ok or apply it - you need to do this for the screen resolutions that you play and then when finished put your desktop back to the resolution you was using.

Another way to do it is to use Nvidia Refresh Rate Fix MkII from www.sheep-design.net - this program basically does the above for you.

18. Create a Bootable XP Floppy Disk
You can easily create a bootable floppy disk by following these steps:
Place a blank disk in the floppy disk drive. Click Start, and then click My Computer. Right-click the floppy disk drive, and then click Format on the shortcut menu. Click Create an MSDOS startup disk, and then click Start.
Now you're on your way to a bootable startup disk.

19. Control Automatic Boot Disk Optimization
Windows XP includes a new feature that will automatically optimize the the disks on boot if required.
This setting controls whether this feature is enabled.

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Dfrg\BootOptimizeFunction]
Create a new String value, or modify the existing value, called 'Enable' and edit the value - enter 'Y' for enabled or 'N' for disabled.

20. Configure your virtual memory pagefile properly
XP is very different - the best in depth article I have seen - http://aumha.org/a/xpvm.htm
This is the basis of the excellent article by James Eshelman...

Where is the page file?
The page file in XP is a hidden file called pagefile.sys. It is regenerated at each boot there is no need to include it in a backup. To see it you need to have Folder Options | View set to 'Show Hidden and System files', and not to 'Hide Protected mode System files'. In earlier NT systems it was usual to have such a file on each hard drive partition, if there were more than one partition, with the idea of having the file as near as possible to the 'action' on the disk. In XP the optimisation implied by this has been found not to justify the overhead, and normally there is only a single page file in the first instance.

Where do I set the placing and size of the page file?
At Control Panel, System, Advanced, click Settings in the Performance Section. On the Advanced page of the result, the current total physical size of all page files that may be in existence is shown. Click Change to make settings for the Virtual memory operation. Here you can select any drive partition and set either 'Custom'; 'System Managed' or 'No page file'; then always click Setbefore going on to the next partition.

Should the file be left on Drive C: **?**
The slowest aspect of getting at a file on a hard disk is in head movement ('seeking'). If you have only one physical drive then the file is best left where the heads are most likely to be, so where most activity is going on on drive C:. If you have a second physical drive, it is in principle better to put the file there, because it is then less likely that the heads will have moved away from it. If, though, you have a modern large size of RAM, actual traffic on the file is likely to be low, even if programs are rolled out to it, inactive, so the point becomes an academic one. If you do put the file elsewhere, you should leave a small amount on C: an initial size of 2MB with a Maximum of 50 is suitable so it can be used in emergency. Without this, the system is inclined to ignore the settings and either have no page file at all (and complain) or make a very large one indeed on C:

NOTE: If you are debugging crashes and wish the error reporting to make a kernel or full dump, then you will need an initial size set on C: of either 200 MB (for a kernel dump) or the size of RAM (for a full memory dump).. If you are not doing so, it is best to make the setting to no more than a 'Small Dump', at Control Panel | System | Advanced, click Settings in the 'Startup and Recovery' section, and select in the 'Write Debug information to' panel

Can the Virtual Memory be turned off on a really large machine**?**
Strictly speaking Virtual Memory is always in operation and cannot be turned off. What is meant by such wording is set the system to use no page file space at all. Doing this would waste a lot of the RAM. The reason is that when programs ask for an allocation of Virtual memory space, they may ask for a great deal more than they ever actually bring into use the total may easily run to hundreds of megabytes. These addresses have to be assigned to somewhere by the system. If there is a page file available, the system can assign them to it if there is not, they have to be assigned to RAM, locking it out from any actual use.

How big should the page file be**?**
There is a great deal of myth surrounding this question. Two big fallacies are:
- The file should be a fixed size so that it does not get fragmented, with minimum and maximum set the same
- The file should be 2.5 times the size of RAM (or some other multiple)
Both are wrong in a modern, single-user system. A machine using Fast User switching is a special case, discussed below.)

Windows will expand a file that starts out too small and may shrink it again if it is larger than necessary, so it pays to set the initial size as large enough to handle the normal needs of your system to avoid constant changes of size. This will give all the benefits

claimed for a 'fixed' page file. But no restriction should be placed on its further growth. As well as providing for contingencies, like unexpectedly opening a very large file, in XP this potential file space can be used as a place to assign those virtual memory pages that programs have asked for, but never brought into use. Until they get used probably never the file need not come into being. There is no downside in having potential space available.

For any given workload, the total need for virtual addresses will not depend on the size of RAM alone. It will be met by the sum of RAM and the page file. Therefore in a machine with small RAM, the extra amount represented by page file will need to be larger not smaller than that needed in a machine with big RAM. Unfortunately the default settings for system management of the file have not caught up with this: it will assign an initial amount that may be quite excessive for a large machine, while at the same leaving too little for contingencies on a small one.

How big a file will turn out to be needed depends very much on your work-load. Simple word processing and e-mail may need very little large graphics and movie making may need a great deal. For a general workload, with only small dumps provided for (see note to 'Should the file be left on Drive C:?' above), it is suggested that a sensible start point for the initial size would be the greater of (a) 100 MB or (b) enough to bring RAM plus file to about 500 MB. EXAMPLE: Set the Initial page file size to 400 MB on a computer with 128 MB RAM; 250 on a 256 MB computer; or 100 MB for larger sizes. But have a high Maximum size 700 or 800 MB or even more if there is plenty of disk space. Having this high will do no harm. Then if you find the actual pagefile.sys gets larger (as seen in Explorer), adjust the initial size up accordingly. Such a need for more than a minimal initial page file is the best indicator of benefit from adding RAM: if an initial size set, for a trial, at 50MB never grows, then more RAM will do nothing for the machine's performance.

Should the drive have a big cluster size**?**
While there are reports that in Windows 95 higher performance can be obtained by having the swap file on a drive with 32K clusters, in Windows XP the best performance is obtained with 4K ones the normal size in NTFS and in FAT 32 partitions smaller than 8GB. This then matches the size of the page the processor uses in RAM to the size of the clusters, so that transfers may be made direct from file to RAM without any need for intermediate buffering.

What about Fast User Switching then**?**
If you use Fast User Switching, there are special considerations. When a user is not active, there will need to be space available in the page file to 'roll out' his or her work: therefore, the page file will need to be larger. Only experiment in a real situation will establish how big, but a start point might be an initial size equal to half the size of RAM for each user logged in.

Problems with Virtual Memory
- It may sometimes happen that the system give 'out of memory' messages on trying to load a program, or give a message about Virtual memory space being low. Possible causes of this are: The setting for Maximum Size of the page file is too low, or there is not enough disk space free to expand it to that size.

- The page file has become corrupt, possibly at a bad shutdown. In the Virtual Memory settings, set to No page file, then exit System Properties, shut down the machine, and reboot. Delete PAGEFILE.SYS (on each drive, if more than just C:), set the page file up again and reboot to bring it into use.

- The page file has been put on a different drive without leaving a minimal amount on C:.

- With an NTFS file system, the permissions for the page file's drive's root directory must give Full Control to SYSTEM. If not, there is likely to be a message at boot that the system is unable to create a page file.

So to summarise**...**
1. always use virtual memory, never switch it off.
2. ideally keep pagefile from main hard drive and if you do move it make sure you leave an initial size of 2mb and a max of around 50mb on C:
3. do not set pagefile minimum and maximum to same
4. do not set pagefile to 2.5 times your memory
5. start minimum pagefile at a low size e.g. 50mb and maximum to say 700mb - if pagefile grows keep adjusting up minimum size until you find your mark.
6. best performance is gained with 4k clusters on hard drive with NTFS.

Swapfile management has been somewhat of a black art in previous versions of Windows, but the XP Help System actually has good information on the subject. Select Help And Support from the Start menu, and do a search for virtual memory. Be sure to check out the related topics delivered by the search for additional good information.

On XP I have 1 gig of ram on my system, I have the pagefile set at a minimum of 100 meg and a maximum of 800 meg. I have the pagefile on a fast hard drive that is hardly used and I have an initial size of 2MB with a Maximum of 50 is suitable so it can be used in emergency.

21. Stop opening explorer and opening my documents
To revert to the old way of launching My Computer by default rather than My Documents as the default, simply edit the shortcut to Windows Explorer, by right clicking on it, and left clicking "Properties" and changing the "Target" box to: "C:.EXE /n,/e," [adjust the path/drive letter if needed]. The key is to add the "/n,/e," to the end of the shortcut (don't type the quotes).

22. Speed up modem data
Speed up buffering of data between your modem and your modem port. This enables your modem to retrieve information faster. Right click my computer, click Properties, click Hardware, click Device Manager, double click ports, double click the appropriate com port, click port settings, click bits per second and change it to the highest supported speed, click flow control and change it to hardware, click ok. Click ok. ok.

23. Want to network but dont have all the stuff ?
If you want to network two WinXP machines together you don't have to install a full blown network setup, i.e. switches, hubs, routers, etc... All you need is two NIC cards (three if you want to share an Internet connection) and a cross over cable.

- Connect one NIC to your broadband connection device like normal.
- Install a second NIC in the machine with the broadband connection.
- Install a NIC in the second machine.
- Connect cross over cable between the second machine NIC and second NIC in the board band connection machine.
- Re-boot both.
- Run the networking wizard if necessary.

24. Software not installing?
If you have a piece of software that refuses to install because it says that you are not running Windows XP (such as drivers) you can simply edit HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows NT/CurrentVersion/ProductName to say Microsoft Windows 2000 instead of XP and it will install. You may also have to edit the version number or build number, depending on how hard the program tries to verify that you are installing on the correct OS. Don't forget to restore any changes you make after you get your software installed. You do this at your own risk.

25. Prefetch
This is an unique technique for XP, which could improve the performance significantly by tweaking the prefetcher. Recommended hardware: PIII 800 or higher, 512M RAM or more. This will decrease the boot time and increase the performance of XP.

- Run "regedit";
- Goto [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters\EnablePrefetcher];
- Increase the value ("5" is recommended) and reboot

Prefetch is a new and very useful technique in Windows XP. However, after using XP some time, the prefetch directory can get full of junk and obsolete links in the Prefetch catalog, which can slow down your computer notablely. My suggestion is: open C(system drive):/windows/prefetch, delete those junk and obsolete files,reboot. It is recommended that you do this every couple of months.

Do rebuild the prefetch manually type into startmenu/run:-
rundll32.exe advapi32.dll,ProcessIdleTasks

26. Automatically defrag drives with a new context menu item
Create a new Registry import file named context_defrag.inf in Notepad (be sure to save with it with the Save as type set to All Files and not Text Documents) and place the following text inside:

```
; context_defrag.INF
; Adds Defrag to the right click context menu in Windows XP

[version]
signature="$CHICAGO$"

[DefaultInstall]
AddReg=AddMe

[AddMe]

HKCR,"Drive\Shell\Defrag\command",,,"DEFRAG.EXE %1"
```

Then, right-click and choose Install. This will add a context menu to XP that allows you to automatically defrag drives, using the command line version of the built-in defragmentation utility. To use it, navigate to a drive in My Computer, right-click, and choose Defrag. A command line window will appear, and that drive will be defragged. When it's complete, the window just disappears.

Defrag with command prompt
You can now defrag in XP from the command prompt.

defrag volume [-a] [-f][-v] [-?]

-a Analyze only
-f Forces defragmentation volume regardless of whether it needs to be defragmented or even if free space is low
-v Verbose output

The volume must have at least fifteen percent free space for Defrag to completely and adequately defragment it. Defrag uses this space as a sorting area for file fragments. If a volume has less than fifteen percent free space, Defrag only partially defragments it. To interrupt the defragmentation process, at the command line, press CTRL+C.

27. Unfragment the master file table
The MFT is actually a file usually stored at the beginning of the volume. It is a database which stores file location and attributes. It also stores data about the volume. The MFT only exists on drives using the NTFS file system. Any file accessed on a drive must also access the MFT. A heavily fragmented MFT can cause extremely bad performance. Even if the file is contiguous if the MFT is fragmented it will take several I/O's to access the file.

This procedure cannot be ran on volumes using the FAT file system and this procedure requires Diskeeper.
Click Analyze, click ok, click Action, click view report, scroll threw the report and look for Total MFT Fragments. One Fragment is the optimal number. To defrag the MFT click Action, click Boot-TIme Defragmentation, click on the appropriate drives, click Defragment the MFT, click Set, restart the PC. The MFT is defragged during the boot process and can be lengthy.

28. Increase master file table allocation

When a NTFS drive is formatted it by default reserves 12.5% of that drive for the Master File Table. The MFT contains information about the files on the drive. This includes size, date and permissions. If lots of files are expected to be added to this drive it is recommended to increase the size of the MFT before formatting the drive. When a file is accessed Windows 2000 must also read the MFT for file attributes. A heavily fragmented MFT will slow access to files on the drive. By default Windows allocates 12.5% of the drives free space to the MFT. The values for this registry setting are 1=12.5% 2=25% 3=37.5% 4=50%.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem
and add the key NtfsMftZoneReservation with the REG_DWORD value of 2.

29. Display the Sharing Tab in Folder Properties
In Windows 2000, getting to the Sharing options for a folder was simple: Just right-click, choose Properties, and you'd see a Sharing tab. In Windows XP, this feature is missing by default, but you can make the system display the Sharing tab if desired. Simply open up Folder Options (My Computer, then Tools, Folder Options) and navigate to the View tab. In the Advanced Settings section, scroll down to the bottom and uncheck Use simple file sharing (Recommended). Now share your folders on the LAN as you would in Windows 2000.

30. Control System Restore
System Restore is an incredible space hog. It might be worth it, if System Restore were a truly complete and foolproof form of backup, but it's not. At best, System Restore can and will get the core operating system running again after a bad crash, but it doesn't return all files to the pre-trouble state, and it can't remove all traces of a program that went bad. As a result, System Restore's usefulness is limited, and so should be its appetite for disk space.

Right click on My Computer, select Properties, and select the System Restore tab. Select your main drive (usually C:), click Settings, and move the slider to reserve a reasonable amount of disk space. With a good regimen of backup images from Drive Image or Ghost you can even move the slider all the way to the left.

If you have more than one drive, you may wish to turn off System Restore entirely for non-system drives. There's little, if any, benefit to be gained by having them monitored. And if you're really religious about making a full backup before you alter your system or install new software, you may wish to completely turn off System Restore for all drives.

31. Backup your Fresh Install
After you complete your clean install and get all your software installed I would recommend that you use something like Drive Image to do an image of your install partition, then burn the image to CD or DVD or another hard drive and keep it. XP is a different creature for some people. If you mess it up when playing around with it, just bring the image back. You can be up and running again in 20 minutes vs. the two to three hours it will take to get the whole thing and all your
stuff installed again.

Note the default install of XP is about 1.5 GB and the download image may be larger that 700 MB. So don't install too much on the OS partition. To help downsize the Image I run the System File Checker and reset the cache size to 40 or 50 MB (it's well over 300 MB by default).

To run it open the command prompt and type:
SFC /?
SFC /purgecache
SFC /cachesize=50
and finally rebuild the cache with SFC /scannow (have the CD ready).
I also Delete the Pagefile.sys and Hibernate.sys files before running Drive Image, although I now have the pagefile on another drive and hibernation turned off in power management.

32. Install Java Virtual Machine
JVM will not appear on Windows Update site either. Some web sites will prompt you to install it upon visiting their pages. You can get the Java Virtual Machine (JVM) and have it ready to use when you Install XP:
http://download.microsoft.com

33. Install BootVis
This is a tweak for Windows XP that can result in a much faster boot time. Download bootvis
http://www.microsoft.com/hwdev/fastboot (look for BootVis.exe Tool)
Once you've unzipped Bootvis, run the .exe and you'll notice several checkboxes on the left. I only selected "Boot Activity". Then I chose "Trace", then "Trace Next Boot". When you reboot it will tell you how long it took to boot everything up. My PC took 35 seconds the first time I tried it. I had it down to 27 seconds after choosing the "Optimize System" feature under the trace menu and various other tweaks. I imagine it could go faster, but I was happy enough with that. My services took about 15 seconds before optimization.

34. Increase bandwidth for network connections - tame QOS !
XP reserves 20% of your bandwidth for quality of service - this is ridiculous and need to be sorted immediately !
XP seems to want to reserve 20% of the bandwidth for itself even with QoS disabled.

1. Make sure your logged on as actually "Administrator". do not log on with any account that just has administrator privileges. To log in as an administrator:

-click on start->logoff->logoff
-in the logon screen hold Ctrl+Alt+Del.
-in the user field type 'Administrator' <-case sensitive.
-in the password field type the password for the administrator (if you don't have one leave blank)
-press ok

2. Start - run - type gpedit.msc
3. Expand the local computer policy branch
4. Expand the administrative templates branch
5. Expand the network branch

6. Highlight the QoS Packet Scheduler in left window
7. In right window double click the limit reservable bandwidth setting
8. On setting tab check the enabled item
9. Where it says Bandwidth limit % change it to read 0. Click apply, OK, exit gpedit.msc.
10. Go to your Network connections (start->my computer->my network connection-> view network connections). Right click on your connection, choose properties then under the General or the Networking tab (where it lists your protocols) make sure QoS packet scheduler is enabled.
11. Reboot , now you are all done.

35. Corporate Windows Update
Microsoft Corporate Windows Update is useful as you can select and download patches to your computer, so you can easily transfer them to other XP computers etc.
http://v4.windowsupdate.microsoft.com/en/default.asp?corporate=true

36. Navigate easier with built in toolbar (also applies to Windows ME)
This tweak makes use of the much under utilized/under appreciated/despised links folder within favorites.

- Right click on your bottom taskbar, select toolbars and choose links.
- Drag the links partition OFF the taskbar (hold mouse down over the toolbar and drag it off)
- This will create a menu/folder view of links. Right click on folder and choose to open folder. Get rid of all the existing junk links in here. Create a new folder in here and put either valuable links or shortcuts to apps/software inside. Add shortcuts to apps directly in the links folder. Close this folder when done.
- Drag the links menu/folder to either the top of the screen or to either side. This will dock the menu.
- Right click on your new docked toolbar and select view small icons, check always on top and auto-hide.

This creates a new navigation menu with dropdown menus that you can access by moving ur mouse to the left/right side of the screen. Shortcuts to folders will launch that folder in a new window as opposed to displaying a drop down menu. You can create new toolbars and dock them to the other side of windows however the drop down feature only works within the links folder.

37. Reset folder view
Sometimes XP forgets it's folder view settings. Here is the solution. Backup these RegKeys.

[HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\BagMRU]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\Bags]
After that delete them. Restart windows to take effect. Now you can change each folder and the setting will stay.
Also this tweak is more enhanced with XenTweak.

38. Remove shortcut arrows from icons
Navigate to HKEY_CLASSES_ROOT\lnkfile in the registry. Delete the IsShortcut registry value.
Navigate to HKEY_CLASSES_ROOT\piffile in the registry. Delete the IsShortcut registry value.

39. DMA mode on IDE devices
Just like 2000, XP still fails to set the DMA mode correctly for the IDE device designated as the slaves on the primary IDE and secondary IDE channels. Most CD-ROMS are capable of supporting DMA mode, but the default in XP is still PIO. Setting it to DMA won't make your CD-ROM faster, but it will consume less CPU cycles. Here's how:

- Open the Device Manager. Right click on "My Computer", select the Hardware tab, and Select Device Manager.
- Expand IDE ATA/ATAPI Controllers and double-click on Primary IDE Channel
- Under Advanced Settings tab, check the Device 1 setting. More than likely, your current transfer mode is set to PIO.
- Set it to DMA if available.
Repeat the step for the Secondary IDE Channel if you have devices attached to it. Reboot.

40. Decrease shutdown with NVIDIA drivers
Shut Down can take up to 20 sec. with nvidia drivers. To reduce this delay:
Go start/excute type msconfig. Go to services tab. Uncheck Nvidia Driver Helper and reboot or

In config panel, administrator tools/services, look for Nvidia driver helper. Right click on it, select properties, select disabled. Reboot. Dont Know what the purpose of the driver helper, but no side effect so far !

41. Install XP from Dos
Boot with a Windows 98/ME Start Up disk.
Insert the Windows 98 CD into the CD reader
Run smartdrv.exe from the Win98 directory on the windows 98 CD (file caching)
Type cd.. to back up to the root directory
Insert Windows XP CD into the CD reader
Copy the i386 folder to C:\
Go into C:\i386 folder on C: and type winnt32.exe to launch the setup from the hard drive.

42. Shutdown command in XP
Command is shutdown -s -f -t 5

43. Change DVD regions as many times as you want !
This also applies to Windows 2000. When you clean install 2000/XP you can only change regions a couple of times but not any more !

[HKEY_LOCAL_MACHINE\Software\Microsoft]

Goto above key in registry and you should see a strange looking random letter key (for example "`dv:=/") as the first entry... Delete the entire key. Reboot the machine and... the first disc you'll use will be set as the new region, with 1 change left.... Works every time... try it and see.

Versions 3.75 and later of DVD Genie should be able to find this key for you and allow you to backup and erase the key with ease. This method has been confirmed to be working with Windows 2000 Service Pack 2 and Windows-XP!.

Other Method
Using the information above, instead of erasing the key, you can see that it has one REG_QWORD entry. What you can do is completely blank out the 'Value Data' field and then reboot your machine. After the boot, Windows should report your region as unselected and programs requesting the region should see this as "Region 0". The problem with "Region 0" is that it won't work on all titles, especially MGM and the new RCE titles (such as The Patriot). You can always export these registry entry and have them loaded automatically at boot time by creating a short cut that will run the registry file ("regedit.exe /s filename.reg") within the startup directory. This should be especially useful with the "Region 0" setting.

44. Add additional time servers
Browse to : www.eecis.udel.edu/~mills/ntp/servers.htm for a list of public NTP servers.
Save your list as a text file with the extension .reg
Here's a sample:

-----Begin cut & paste here-----
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\Servers]
@="1"
"1"="time.windows.com"
"2"="time.nist.gov"
"3"="clock.isc.org"
"4"="timekeeper.isi.edu"
"5"="usno.pa-x.dec.com"
"6"="tock.usno.navy.mil"
"7"="tick.usno.navy.mil"
-----End cut & paste here-----

45. Improve XP's folder views
Windows XP's default folder view, with its giant icons, makes me feel as though I'm staring at a coloring book instead of a business computer. But you can easily change the folder view to something more restrained, space-efficient, and useful. Open My Documents. In the View menu, select Status Bar, List, and Arrange Icons by Name. Next, right click on an empty spot in the My Documents toolbar and select Customize. Choose any of the Available Toolbar Buttons you wish and click Add. (I select the Undo, Delete, Cut, Copy, and Paste buttons.) Exit the dialog.

Now click to the Tools menu and select Folder Options. Under the View tab, tell XP to show you the full path, to show hidden and system files, not to hide any file extensions, and not to hide protected folders--plus any other settings you want. When you have the folder options set the way you desire, click the "Apply to all folders" button at the top of the dialog. This adjusts all windows opened by Explorer, so they'll inherit the visual choices you made for this one window.

46. Turn off automatic updates and error reporting
By default, XP wants to contact the Microsoft servers to auto-search for patches, downloads, and updates. It also wants to send Microsoft information about any crashes you experience. The former can be an annoyance if the auto-update cycle kicks in at an inopportune time. You can turn off both behaviors by right clicking on My Computer, selecting Properties, and first choosing the Automatic Updates tab. Select either Turn Off or, minimally, Notify me. Now select the Advanced tab and click on Error Reporting. Check "Disable error reporting," but leave "notify me when critical errors occur" checked.

47. Hidden devices
XP may deliberately hide certain system devices from you. While this might make a kind of sense in, say, XP Home edition, these devices remain hidden even in the Professional edition.

For example, if you're used to Windows 98's networking applet, you may be surprised by how clean and uncluttered XP's networking applet is. But XP may simply be hiding lots of networking elements from you. To see if this is the case, right click on My Computer, select Properties, Hardware, and Device Manager. In Device Manager, select View and Show Hidden Devices. Depending on how your system is set up, you may find other hidden devices, or no others. It varies hugely. But at least now you'll know if XP is hiding things from you.

48. Shorten bootup chkdsk delay
Want to shorten the boot up chkdsk delay of 10 secs on WInXP start from 10 secs to 3 ?

-----Begin cut & paste here-----
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager]
"AutoChkTimeOut"=dword:00000003
-----End cut & paste here-----

49. Speed up browsing with DNS cache
When you connect to a web site your computer sends information back and forth, this is obvious. Some of this information deals with resolving the site name to an IP address, the stuff that tcp/ip really deals with, not words. This is DNS information and is used so that you will not need to ask for the site location each and every time you visit the site. Although WinXP and win2000 has a pretty efficient DNS cache, you can increase its overall performance by increasing its size

-----Begin cut & paste here-----
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters]
"CacheHashTableBucketSize"=dword:00000001
"CacheHashTableSize"=dword:00000180
"MaxCacheEntryTtlLimit"=dword:0000fa00
"MaxSOACacheEntryTtlLimit"=dword:0000012d
-----End cut & paste here-----

50. Easier Searching
Remember the Quick Search powertoy for IE? Well, now it's built in. Load up TweakUI and expand the Internet Explorer menu. Under search, you can create new search options. For example: Create one with a prefix of "g" and a URL of "http://www.google.com/search?q=%s". Now, to search Google for, say, penguins, all you have to do is type "g penguins" in the Address bar. Nice and easy.

51. Remove balloon tips
With this setting, some of this pop-up text is not displayed. The pop-up text affected by this setting includes "Click here to begin" on the Start button, "Where have all my programs gone" on the Start menu, and "Where have my icons gone" in the notification area.

Type gpedit.msc in run box. Goto to user configuration, administrative templates, start menu and taskbar, find remove balloon tips on start menu items, check enabled, ok.

52. Turn off indexing service
Windows XP keeps a record of all files on the hard disk so when you do a search on the hard drive it is faster. There is a downside to this and because the computer has to index all files, it will slow down normal file commands like open, close, etc. If you do not do a whole lot of searches on your hard drive then I suggest turnning this feature off:

Open my computer, right click your hard drive icon and select properties. At the bottom of the window you'll see "Allow indexing service to index this disk for faster searches," uncheck this and click ok. A new window will pop up and select apply to all folders and subfolders. It will take a minute or two for the changes to take affect but then you should enjoy slightly faster performance.

53. Remove hibernation file
If you do not use hibernation, make sure you do not have it enabled, which reserves disk space equal to your RAM.
If you have a hidden file on the root directory of your C drive called hiberfil.sys, hibernation is enabled. To remove that file, go to Control Panel, select Performance and Maintenance, Power Options, Hibernate tab, and uncheck the Enable hibernation box.

54. Cache Folder Thumbnails
In WinXP to make folders with thumbnail images start up faster, go to control panel and then folder options. Click on the view tab and make sure "Do not cache thumbnails" is not checked.

55. Search the internet quicker
- Get TweakUI by installing XP Powertoys for Windows XP from: http://download.microsoft.com
- Start -> Programs -> Powertoys for Windows XP -> TweakUI for Windows XP
- Click the '+' next to 'Internet Explorer'
- Hightlight 'Search'
- In the right plane click on the 'Create' button.
- For the Prefix, type in 'Google' or if you're really lazy (like me) then just 'g'
- For the URL, enter: http://www.google.com/search?hl=en&q=%s&num=100

The 'hl' is language, the 'q' is the query, and the 'num' is the number of results per page. To search for multiple keywords at a time, use the format 'google monkey+cars' or just 'g monkey+cars' depending how you chose to set it up.

56. Mouse acceleration tweak
This resolves the XP mouse acceleration bug.

-----Begin cut & paste here-----
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Control Panel\Mouse]
"SmoothMouseXCurve"=hex:00,00,00,00,00,00,00,00,00,a0,00,00,00,00,00,00,00,40,\
01,00,00,00,00,00,00,80,02,00,00,00,00,00,00,00,05,00,00,00,00,00
"SmoothMouseYCurve"=hex:00,00,00,00,00,00,00,00,66,a6,02,00,00,00,00,00,cd,4c,\
05,00,00,00,00,00,a0,99,0a,00,00,00,00,00,38,33,15,00,00,00,00,00
-----End cut & paste here-----

57. Fresh install with no ACPI
An easy way to do a fresh install with no advanced configuration power management is when setup is loaded, the blue screen will ask if you have any raid devices, and to press F6. When it does that, press and hold F7 and no ACPI will be installed.

58. Hide users on the welcome screen and show Admin
When you add an account for certain users with Windows XP, their user names will appear on the Welcome Screen. Sometimes a user needs to be added to a Windows XP machine, because he needs access (via the network) to resources on the machine, but he will not be physically logging in on the computer. You can remove his name from the Welcome Screen, while still maintaining the user account. Start the Registry Editor Go to HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon \ SpecialAccounts \ UserList \ Right-click an empty space in the right pane and select New > DWORD Value Name the new value exactly as the Username Leave the Value data as 0 If you want to enable this user again on the Welcome Screen, either double-click the Username value, and change the Value data to 1, or delete the Username Close the registry editor.

To get Admin account on the "Welcome Screen" as well as the other usernames, make sure that there are no accounts logged in. Press "ctrl-alt-del" twice and you should be able to login as administrator!

59. Enable Cleartype on the welcome screen
Laptop users and other LCD owners are quickly realizing, Microsoft's ClearType technology in Windows XP really makes a big difference for readability. But the this feature is enabled on a per-user basis in Windows XP, so you can't see the effect on the Welcome screen; it only appears after you logon.

But you can fix that. Fire up the Registry Editor and look for the following keys:
(default user) HKEY_USERS \ .Default \ Control Panel \ Desktop \ FontSmoothing (String Value)
HKEY_USERS \ .Default \ Control Panel \ Desktop \ FontSmoothingType (Hexadecimal DWORD Value)

Make sure both of these values are set to 2 and you'll have ClearType enabled on the Welcome screen and on each new user by default.

60. Setup XP for different uses
WinXP allows multiple users [each with highly-separate system settings], which sounds like a rather useless capability for a single user system. However, I have set up my system as follows, and can see an almost limitless number of possibilities for those that want the most technically correct setup.

My main user, X , is pretty much what you would call a standard setup, providing Internet access, protected by a background Anti-Virus program and a personal firewall, CD-RW software, Instant Messenger software, etc. Even though I am the only user on this PC, I have a second user login, Gamer , which does not load all those background programs, and is as optimized as I could get it for game play. Another user, Graphics , also doesn't load the AV (but I can run it on demand), firewall, or IM program, but does load the CD-RW software and scanner program, for example.

61. Install Recovery Console
Very useful for troubleshooting. Go to where your XP cab files are and type '\i386\winnt32.exe /cmdcons'. Where 'd:\' is cd drive or hard drive. Commands available when Recovery Console is installed :-

LISTSVC	List services
ENABLE/DISALBE	Enable/disable service
DISKPART	Equivalent of FDISK
FIXBOOT	Create a new boot sector on the system partition
FIXMBR FDISK /MBR	equivalent (problems with RAID etc)
LOGON	List installation of Windows XP and can choose which to work on
SYSTEMROOT	Move to the system root
MAP	Display a list of drives and ARC paths. Useful to fix boot.ini probs.

62. Cable Modem & xDSL Speed Tweak
To increase your broadband Cable Modem speed tip visit www.speedguide.net
Also visit www.x9000.net and download XenTweak
They have some excellent registry and inf files to download specially for cable access.

63. Adaptive Menus
Microsoft Office 2000 introduced personalized menus (a.k.a. adaptive menus) that remembers which items you use regularly and hides items you don't. This tweaks allows you to enable or disable this functionality. Exit all open Office 2000 applications, including Word, Excel, Access and Outlook. Then open your registry and find the key below, if it does not exist create it.
[HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Common\Toolbars]
Create a new DWORD value named 'AdaptiveMenus' and set the value to '0' for disabled and '1' for enabled.

64. Control Smart Menus
Switch them off ! Windows 2000 included a new feature called 'Personalized Menus', which remembers which items you use regularly and hides items you don't. This tweaks allows you to enable or disable this functionality.

Open your registry and find the key mentioned below.
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
Create a new string value, or modify the the existing value, named 'IntelliMenus'.
Modify the value to equal 'YES' to enable smart menus or 'NO' to disable them.

By using the same key except under the [HKEY_LOCAL_MACHINE] tree the tweak can be enforced system wide, instead of only user based. Restart your machine.

65. Hide or Display Administrative Tools Menu
As with Windows NT and Windows 2000, XP has an 'Administrative Tools' folder on the Start Menu. This folder contains powerful administration utilities and therefore can be hidden to avoid accidental use.

Open your registry and find the key mentioned below.
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]

For example, the setting may look like:
(Default) (value not set)
StartMenuAdminTools YES

Create a new string value, or modify the the existing value, named 'StartMenuAdminTools'. Modify the value to equal 'YES' to show the administrative tools folder or 'NO' to hide it. By using the same key except under the [HKEY_LOCAL_MACHINE] tree the tweak can be enforced system wide, instead of only user based.
Exit your registry and log off for the changes to take effect. Note: Hiding the folder does not stop the use of the tools, it only make it more difficult to locate them.

66. Speed up and browse faster
Here's a great tip to speed up your browsing of XP machines. Its actually a fix to a bug that by default of a normal Windows XP setup that scans for shared files for Scheduled Tasks. And its turns out that you can experience a delay as long as 30 seconds when you try to view shared files across a network from as Windows XP is using the extra time to search the remote computer. Note that though the fix is originally intended for only those affected, Windows XP users will experience that actual browsing speed of both the Internet & Windows Explorers improving significantly after applying it since it doesnt search for the Scheduled Tasks anymore.

Open up the Registry and go to :
HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/Current Version/Explorer/RemoteComputer/NameSpace

Under that branch, select the key :
{D6277990-4C6A-11CF-8D87-00AA0060F5BF} - and delete it.

This is key that instructs Windows to search for Scheduled Tasks. If you like you may want to export the exact branch so that you can restore the key if necessary. This fix is so effective that it doesn't require a reboot and you can almost immediately determine yourself how much it speeds up your browsing processes.

67. Auto Logon to machine
If you're running servers from a locked closet or server room, you can make them fully bootable. This means they won't require human intervention to carry out initial log-ins and run startup batch files. It allows you to automatically logon to the machine and network, bypassing the Winlogon dialog box.

To enable this function you need to add several new values to the
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] key.

- Add a new value of 'DefaultUserName' and set the data to the username you wish to automatically logon as.
- Add a new value of 'DefaultPassword' and set this to the password for the username above.
- Add a new value of 'DefaultDomainName' and set this to the domain of the user.
  Ignore this value if the NT box is not participating in NT Domain security. This should be the local Windows NT Advanced Server domain on Advanced Server networks, or Machine Name on standalone Windows NT systems.
- Add a new value of 'AutoAdminLogon' and set it to either '1' to enable auto logon or '0' to disable.
- Exit and reboot, Windows should not ask for a password and automatically show the desktop of the user.

Warning: The password is stored in registry, which means anyone who has access to the machine has access to the password and should not be used on secure systems. You can also do the above with TweakUI.

68. Reboot on blue screen of death
There are those rare cases when a system fault/error/crash ends up freezing the OS at the dreaded BSOD (Blue Screen Of Death), which displays the cause of the crash and gives some details about the state of the system when it crashed. If you are a system administrator, requiring your servers to run non-stop 24/7, this can be a pain in the neck. To bypass the BSOD altogether and enable the instant "Auto Reboot" feature, run Regedit and go to:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl
Right-click on the "AutoReboot" String value in the right hand pane -> select Modify -> change it to read 1 -> click OK.

69. Temporarily assign yourself admin permissions
Many programs require you to have Administrative permissions to be able to install them. Here is an easy way to temporarily assign yourself Administrative permissions while you remain logged in as a normal user. Hold down the Shift key as you right-click on the program's setup file. Click Run as. Type in a username and password that have Administrative permissions. This will also work on applications in the Start menu.

CHAPTER [6]

SECURITY TIPS

Never get into a false sense of security - just because you have applied service packs and fixes to your system or server doesn't mean you are completely protected. There is no such thing as being completely protected - security is an ongoing process and needs to be looked at very frequently. New exploits are released all the time. My personal view is that every company should employ full-time someone who just looks at system security - a small price to pay considering that a employee/virus/malicious hacker etc could take down a company or even lose them a lot of money.

Before I go into some security tips here is what security is...

- Security is now that the blissful have been hit again, maybe they can get serious.
- Security is serious business - yes, even when you are using a computer for fun.
- Security is knowing that how you navigate the "information highways" affects others and taking responsibility for it.
- Security is taking the time, focusing on what you have to do and excluding all else. You work in your own best interests and you know it.
- Security is knowing your machine, knowing what's going on it it. So you know if something is compromised.
- Security is checking all ways of starting applications automatically at boot and making sure only applications you are familiar with are starting.
- Security is making sure, if you are running Windows, that you see all file extensions.

- Security is not opening attachments you haven't requested from people you know or do not know, but downloading them to disk and having a text editor or AV tool look them over instead. And even if it's not readable as text, and even if your AV tool doesn't say it's malicious, don't run it. Ask whoever sent it what it is and why they sent it before clearing it with you first. And even if your friend assures you that the file is not malicious, check it out with Blobview, Peeper, and BinText, and use InCtrl5 to open it.
- Security is disabling web scripting if you are running Windows.
- Security is trying to find a more secure emailer (than Outlook) if you are a home user.
- Security is making sure you are not broadcasting your presence on the Internet on a permanent IP. If you are running Windows, make sure ports 135 - 139 are closed. If you are running NT/2K/XP, make sure port 445 is closed and make doubly sure port 135 is closed.
- Security is installing and properly configuring a firewall if you have a permanent IP.
- Security is changing your IP regularly, even if you have a permanent connection.
- Security is never connecting to the Internet without your firewall up and running.
- Security is never using Java - anywhere. Disable it everywhere, especially in your email reader.
- Security is using an ad killer such as Silencer to kill as many banners as you can.
- Security is checking with sites such as Spychecker before even considering a download from the Internet.
- Security is reading email as text only. If people can't send you text email, tell them to get out of your mailbox. The Internet is built on text, and don't forget it. No winmail.dat cards, no VCF attachments - just text.
- Security is seriously considering disabling JavaScript when surfing and NEVER having it on while you are reading email.
- Security is disabling VBScript everywhere - unconditionally.
- Security is making sure ActiveX OCX's can't be downloaded and run on your box. Check your browser settings for this.
- Security is checking your firewall logs all the time. If you can't understand what they say - learn.
- Security is running AV often enough, even if you don't run AV all the time, and updating your lists as often as you can.
- Security is always checking with an up-to-date AV before sending or receiving anything via email.
- Security is visiting security sites where major advisories are posted. Keep up on "traffic hazards".
- Security is finding someone who can help you if you don't know all the technical stuff, someone who can help you when you need it. If you need a quick answer in a tight situation, write to radsoft.net.
- Security is checking your process list regularly so you know what should be there and so you immediately see when something that shouldn't be there is around.
- Security is playing around with GD and the netstat (and nbtstat) commands and learning how they work so you can be sure you don't have open ports you shouldn't have.
- Security is learning your own file system. When you see files there that look suspect - turn up their properties and see whose program it is. If it's from your operating system vendor (eg Microsoft) it may be ok, but if it has no version info or is from a company you never heard of, raise an eyebrow.
- Security is running an up-to-date copy of Ad-aware regularly, especially if you download and test new software all the time, and being suspicious of anything you download. Use InCtrl5 from ZD Net to check the effects of any program you download and run, and take the time, yes take the time, to study the logs of InCtrl5 so you know exactly what happened when the new program ran.
- Security is backing up your system regularly, and only when you are at least 100% positive it is not corrupted by virus, worm, trojan or other malicious software. Learn how to restore a system from a backup so you can do this and will do this immediately you recognise a need to.

1. Email security and scripts

Don't let windows run HTA, SHS and VBS Script automatically. Those file associations allow viruses to infect your system. Open Windows Explorer and click Tools / Folder Options / File Types and delete HTA, SHS and VBSscript. It is very unlikely a normal PC user would need those file associations turned on. If every person never had these filetypes recognised to the operating system than the effect of the 'LoveBug' virus would of been a lot less. Good program to stop various filetypes from launching is ScriptDefender - www.analogx.com/contents/news.htm

Configure Windows so that is always shows file extensions. In Explorer, clock on View, Folder Options, View tab. In the advanced list, uncheck 'Hide file extensions for known file types'. Never open attachments to emails or follow links to web pages that are contained in unsolicited emails. Ignore attachments that have sexual filenames, such as porn.exe. This is a common trick to tempt people into opening the attachment. Don't assume that because an attachment has the icon of a harmless file type such as txt or jpg the file is harmless. Check the actual file extension. EXE (executable) files can have any icon. Never accept attachments from strangers in online chat systems, such as IRC, ICQ or AOL messenger. Be wary of files downloaded from internet newsgroups. These forums are often used by virus writers to distribute their new viruses.

Check out
www.symantec.com/avcenter/venc/data/win.script.hosting.html
how to disable scripting. Scripting adds "functionality" that most people really don't need. In fact, that very functionality could be considerably dangerous with regard to VBS type malware infections that are spread primarily through email attachments.

2. Control Outlook Security

As Microsoft Outlook is a major victim and a major cause of trouble, consider using another email client, and make sure the client is not dependent on IE technology. Even webmail is better suited. Once you get rid of that Outlook address book a lot of worms will be lost. Other email clients are Eudora, Pegasus, Agent etc. If you must use Outlook then here are some tips for you.

Introduced into Outlook service packs was a security feature that disabled the ability to directly open executable (EXE) file. This tweak allows you to disable that functionality. Open your registry and find the key below.

HKEY_CURRENT_USER\Software\Policies\Microsoft\Security
Create a new DWORD value, or modify the existing value, called 'CheckAdminSettings' and edit the value according to the settings below.
CheckAdminSettings REG_DWORD 0x00000001 (1)

To Disable embedded scripting from Outlook
(or better dont use Outlook at all and use an alternative)
Disable embedded scripting from Outlook (or even better dont use it at all and use an alternative email program)

www.symantec.com/avcenter/security/Content/2000_05_26_a_i_dES.html
While you're at it, you should also familiarize yourself with Outlook E-mail Security Updates
http://support.microsoft.com/support/kb/articles/q262/6/31.asp?LN=EN-US&SD=gn&FR=0>

Outlook 2002 XP attachments
Microsoft Outlook 2002, included with Office XP, introduced new restrictions to stop possible unsafe e-mail attachments from being opened or saved. This tweak allows you to modify those restrictions.
Any files with following extension are prohibited from being opened or saved when received as e-mail attachments:
ade, adp, asx, bas, bat, chm, cmd, com, cpl, crt, exe, hlp, hta, inf, ins, isp, js, jse, lnk, mda, mdb, mde, mdz, msc, msi, msp, mst, pcd, pif, prf, reg, scf, scr, sct, shb, shs, url, vb, vbe, vbs, wsc, wsf, wsh
To change this behaviour open your registry and find the key below.

[HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Security]

Create a new String value, or modify the existing value, called "Level1Remove" and set it to equal a semi-colon seperated list of the extension you want to allow e.g. "bat;exe;hlp" (this would allow batch files, executables and help files through). Restart Outlook for the change to take effect.

Turn off Outlook Preview
Regarding Nimda and virus e-mails in general. Not sure if everyone can do this. OE defaults to three panes. Top-right is your list of messages and bottom-right is the message itself. The problem is that if you want to delete an e-mail, you have to select it. When you select it, the message opens automatically in the bottom-right panel.

If you go to View | Layout, you can turn off the preview pane. Now, you don't have to open a message in order to delete it. The advantages are a reduced likelihood of mail-borne viruses; you can delete spam without opening it and potentially setting cookies from a spammer's site. The disadvantage is if you want to view a new message, you have to double-click to open it up in a new window.

If there is something you see that you're not sure about, you can right-click the suspect e-mail, go to Properties, Details tab, and click the View Source button. Finally, you can forward spam to abuse at whatever.com without ever having to open the e-mail; you can read the headers from the detail tab of the properties window, etc. Anyway, it seems this logic protects me from yet another batch of e-mail viruses. Between the above tactic and my Hotmail email account which also lets me delete e-mails without having to open them. Everything so far is pretty good. As an aside, you can also turn off WAV file playing somewhere in IE's options. I think its Play Sounds under the Advanced section. Just a thought.

Do not allow attachments to be saved
In outlook options tick the box 'do not allow attachments to be saved or opened that could potentially be a virus'. When this option is ticked it will essentially disable the opening of email attachments. Untick it if you wish to save/run attachments from people whom you know

Create invalid entry in address book
Create ':' in address book and enter yourself as email address and if virus gets sent out it will email you also so you can then start investigating quickly.

Outlook and Exchange Site
Another useful site for Outlook and Exchange solutions is http://www.slipstick.com/

Turn off Java and Javascript
Turn off Java and JavaScript everywhere. If you run them in your email client you should have your head examined. It is childishly simple for a malicious website to write to your AUTOEXEC.BAT, force you to reboot by crashing your machine, and on reboot automatically wipe your entire hard drive clean. Turn if off in Internet Explorer by going to tools, internet options, security, custom and disabling java and scripts.

Other Outlook Stuff
Some email clients will automatically move to a new message when the one you're reading is moved or deleted. Make sure yours doesn't.

3. Virus Checking
Always have running an up to date virus checker and update the virus definitions on a weekly basis. Check everything that arrives on your computer. I personally use 3 virus checkers - I only have one loaded at any one time. Every file that comes into the computer, goes into an incoming folder. Everything in that incoming folder is left there for a period of 1 month before being executed. The reason for this is to allow another couple of updates to the virus definitions, just in case I have downloaded a very new virus that the virus checker cannot detect. Everything in that Incoming folder is then checked by 3 different virus checkers. Even then I have performed a relatively new system backup before anything is executed.

Commercial software is pretty much assumed safe from malicious code, but with the number of programs the average person downloads from the Internet, Trojan horses are becoming a major threat. Basically, a Trojan Horse is when you run a program to do one thing, but in the background it is doing another. These are often referred to as viruses, and frequently commercial antivirus programs will catch the most common ones, but they are easy to make, and can access anything the person running them can. As a rule of thumb, don't download new software and install it, unless you are sure it comes from a reputable source. Or Microsoft. Sorry, couldn't help myself.

Make it your business to be aware of what comes in in all forms: email, web pages you look at, diskettes and CDs, accesses from LAN or Internet when online, and junk pulled down by auto-updating-software. This is not as easy as it used to be as the old beliefs simply do not apply anymore.

Don't run or open unsolicited executables, documents, spreadsheets, etc. Be paranoid, if you don't know something to be virus-free, you must assume it isn't. (Have a strict policy in your organization that downloading executables and documents from the Internet

is not acceptable, and that anything that runs in your organization has to be virus-checked and approved first.) You may think I`m paranoid (well I am!) but having seen some of the damage and chaos that a virus can cause on peoples machines I am very careful indeed and you should be to! I have tested virtually every single virus detection program for the PC on the market and my favourites as I write this are: AVG and Norton. AVG is completely free for personal use and is very good.

Never open email attachments that have the file extensions VBS, JS, SHS or PIF. These extensions are commonly used by worms and rarely contain valid attachments. Never open attachments that appear to have double file extensions, for example, somefile.txt.exe.

Also in addition to a good virus checker, check your computer regularly with an up to date dedicated trojan scanning program e.g. Trojan Defence Suite or one available from www.agnitum.com

Never, ever:

- Open files or e-mail attachments from someone you don't know
- Open files or e-mail attachments forwarded to you even if they are from someone you know
- Never follow links to web pages from an unknown email
- Open files that have extensions VBS, JS, SHS or PIF - these are commonly used by worms
- Open unsolicited/unexpected e-mail attachments until confirmed the sender actually meant to send it
- Open a document with macros enabled, period
- Boot from a floppy unless you created it, write protected it and stored it in a locked safe since then
- Accept attachments from strangers in online chat systems, such as IRC, ICQ or Aol etc.
- Download files from internet newsgroups. These are often used by virus writers to distribute viruses

Always:

- Always scan file attachments or downloaded files before you run or open them
- Always scan floppy disks (including ZIP drive media)
- Always scan CDs
- Always keep your antivirus definitions upto date
- Always make backups and test your backups to ensure date integrity
- Check with your friends or colleagues if a message seems slightly strange e.g. I love you that they sent the email before opening

These issues are especially important if you are the administrator on a large network. While the average user has the rights to delete his or her files, most admins can delete everything on network drives, too. This is a bad thing.
If your computer does become infected with a virus, the **alt.comp.virus** newsgroup is a good place to go for help and/or information. You can ask for, or find advice from a number of professionals and other experienced users.

4. Display Hidden File Extensions

Even when you have configured Windows to display all file extensions, there are still some which remain hidden. This potentially allows dangerous files to be masked as safe files, fooling the user into executing them. This tweak helps expose those file extensions. It is possible for a malicious user to name a file so that it looks safe to open, when in fact it may be executable containing dangerous content.

For example, a file could be displayed as "readme.txt" in explorer, when it fact it is really name "readme.txt.shs" but since the ".shs" portion of the filename is hidden it is impossible to tell it apart from a simple text file. Then once a user double-clicks to open this file, instead of seeing a text page as expected, the file will be executed by Windows as a scrap object and potentially harm the system. To remove the potential to hide files, search through the registry for any values named "NeverShowExt", a common one is located at [HKEY_CLASSES_ROOT\ShellScrap]. To force the file extension to be shown highlight the value "NeverShowExt" and press delete. Now the full file extension should be shown and not masked. You may need to restart Windows for the change to take effect.

Registry Settings:
Key: [HKEY_CLASSES_ROOT] Value Name: NeverShowExt

You can also make sure that you turn off the option. Goto control panels, folder options, view, hide file extensions for known file types and uncheck the box.

5. Boot sequence

Change your CMOS bootup sequence to C: / A: -- or just C: -- this is so you don't boot from drive A: if you leave a floppy in your machine. This should stop all pure boot sector viruses from infecting you. If you do need to boot from a floppy disk the CMOS can be quickly switched back.

6. Update and download service packs and fixes

The next step is learning to be vigilant and wise about updating your system. There are several opinions concerning the best way to go about this. If you are a total security freak, and would rather be offline than unsecure, you can download hotfixes from Microsoft as soon as they are out. This can be a dangerous thing, since many of these "fixes" are not very well tested, or really are just registry changes that disable some of Window's features. Even if you are not going to install every fix as soon as it comes out, you should still keep up to date on what exploits have been found, and how (or even if) Microsoft is addressing them. To get the less biased but unofficial scoop on what exploits are out there, try NT Bug Traqs security mailing list. http://www.securityfocus.com/

I am not so worried about security on my home machine that I am willing to wade through the myriad of patches and reading the wordy Microsoft documents trying to figure out if they apply to me. The next best thing for security and best for stability is to make sure you are up to date on your service packs and critical updates. Do this by running the windows update wizard regularly. The fixes posted here are supposedly regression tested and should be quite stable. Apply any service packs to your computer, which will fix many security related problems. If you are still using NT than upgrade to Service Pack V6a which contains a lot of security fixes. Also apply service pack 2 for 2000. If you use Outlook especially install the latest security patches from Microsoft. I always recommend keeping Internet Explorer completely up to date e.g. latest at time of writing is IE6, which contains a lot of security fixes etc.

Downloads:-
http://corporate.windowsupdate.microsoft.com/en/default.asp
www.microsoft.com/windows2000/downloads/
http://support.microsoft.com/highlights/default.asp?pr=topsdn&cl=136&SD=TECH

Also download the Windows Critical Update Notification tool and never miss a Critical Update again. Whenever a new Critical Fix is released, you will be notified. You can install or uninstall Windows Critical Update Notification by using either of the following methods: Click Start, point to Settings, and then click Control Panel.
Double-click Add/Remove Programs. Click Microsoft Windows Critical Update Notification. Click Add/Remove.
http://support.microsoft.com/support/kb/articles/Q224/4/20.ASP
Also visit http://windowsupdate.microsoft.com/ and also see other Microsoft links in links further in this document.

As new security fixes become available it is important to apply these new fixes. Microsoft has created the Qchain tool to chain hotfixes together in order for only one reboot to be required when installing several fixes.
http://support.microsoft.com/support/kb/articles/Q296/8/61.asp

HFNetChk
One particularly important element of operating a secure system is staying up to date on security patches. It's critical to know which patches have been applied to your system and, more importantly, which haven't. Microsoft has released a tool called HFNetChk that will significantly aid system administrators in this task. HFNetChk is a command-line tool that enables an administrator to check the patch status of all the machines in a network from a central location. The tool does this by referring to an XML database that's constantly updated by Microsoft. HFNetChk can be run on Windows NT 4.0 or Windows 2000 systems, and will scan either the local system or remote ones for patches www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/hfnetchk.asp

Windows NT 4.0, Windows 2000, All system services, including Internet Information Server 4.0 and 5.0, SQL Server 7.0 and 2000 (including Microsoft Data Engine), Internet Explorer 5.01 and later

7. Subscribe

Subscribe to the Security Focus newsletters and check out there website at www.securityfocus.com/
Subscribe to the Security Admin newsletters and check out there website at www.secadministrator.com/

Subscribe to an email alert service that warns you about new, in-the-wild, viruses like the free service at
www.sophos.com/virusinfo/notifications

Subscribe to the Microsoft Security Notification Service. This is a free e-mail notification service that Microsoft uses to send information to subscribers about the security of Microsoft products. www.microsoft.com/technet/security/bulletin/notify.asp
Also keep an eye on Microsoft's security bulletins at
www.microsoft.com/security
www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp

Microsoft Personal Security Advisor
Microsoft Personal Security Advisor (MPSA) is an easy to use web application that will help you secure your Windows NT 4.0 and Windows 2000 computer system. Simply navigate to the MPSA site and press the Scan Now button to receive a detailed report of your computer's security settings and recommendations for improvement. MPSA will scan your system and build a customized report on items such as: missing security patches, weak passwords, Internet Explorer and Outlook Express security settings, and Office macro protection settings. More details on the specific features performed by MPSA are available by selecting the Features option on the MPSA toolbar.

For each weakness identified on your computer, MPSA provides easy to understand information on the security issue at hand, how to fix it, and links to additional information about the issue. Once you correct a reported deficiency, you can run the scan again and see the results of the change. Running MPSA on a regular basis will help ensure that your system stays up to date and secure.
www.microsoft.com/technet/mpsa/start.asp

8. Disable NetBios, clean up network bindings, protocol optimisation and internet connection sharing

If you are **NOT** connected to a local or wide area network and only use your dial up modem or cable modem for internet access then disable NetBios. Goto control panels, Network and examine every line beginning with "TCP/IP", click on properties and then remove all of the checkmarks from the services listed on the bindings tab!
(Note that when you click "OK" after unbinding everything, Windows will think you're nuts and will warn you that you "have not selected any drivers to bind with." Just click "NO" to proceed.)

It will quietly disappears from sight and your system's security skyrockets. You won't miss it at all, Windows will boot faster, and you'll have more memory for things you do need. And if you later decide to share your files with another computer (which is almost the only reason for Microsoft's networking) it's very easy to bring it back from the grave. Not only does unbinding TCP/IP from the Microsoft networking components prevent your computer's files from being accessed through abuses of Microsoft's networking. Unbind ALL network services from EVERY instance of the TCP/IP protocol!

You can also do this by the following registry settings. Copy these next lines into notepad, save as Disable NetBios.reg (remembering to change save as type to all files), double click the file you have just created and jey presto you are a lot more secure on the Internet. Remember every time you enter a new dial up networking setting you will need to disable NetBios. The advantage of doing this is that you will get a better transfer speed and a lot better security. To verify these settings you can go onto shields up site (https://grc.com) and test before and after putting these settings into your registry.

-----Begin cut & paste here-----
REGEDIT4

[-HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETBIOS]

[-HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP]
------End cut & paste here------

Single NT computers can be effectively protected from many kind of attacks by Unbinding NETBIOS and TCP/IP protocols. Workstation that does not need to share any disk, printer or other resources can be protected by shutting down SERVER service.

Clean up networking bindings
The next step in securing your system from prying eyes is to ensure your bindings are set appropriately and should only be used on machines that do not connect to other Windows-based machines. The next step will disable Microsoft Networking connections to and from your machine. This will make it a lot harder for external computers to access your shares, printers and other Server Message Block services on your computer. This will not stop them from exploiting non-Microsoft Networking services such as IIS (FTP, Web, Web file sharing, and Web shared printers). If you don't know what shares are, and if you're not attaching to an NT file server, chances are that you can take this top. Note that in this sense, we're not talking about a home network that solely uses Internet connection sharing network via Microsoft's own Internet Connection Sharing, or some other program that lets this machine assign IP addresses to your other computers (WinGate).

Right click on Network, select properties. Right click on the icon for your connection to the Internet and select Properties. Select the tab on the top named "Networking". In the box below that says, "Components used by this network connection" Uncheck everything but TCP/IP.

Protocol Optimization
The protocols should be ordered by the frequency that they are used. For example, the most used protocol should be first and the least used last.

Using Internet Connection Sharing
The Networking Wizard wants to use TCP as the main protocol for everything, both inside and outside the LAN. For example, with Internet Connection Sharing (ICS) set up on one PC, the Wizard will set up TCP, with Print and File sharing enabled, and with NetBIOS enabled (or actually in the default setting, which seems to be "enabled" in this case) on the ICS PC, and on each PC on which you run the Wizard. This sounds and can be dangerous, because TCP is the protocol or "language" of the internet: Using TCP for your local communications can make it easier for hackers to jump from the internet to your local network.

So, on the PC that's doing the sharing, you need to open the connection settings and unbind (remove) everything but TCP from the outbound network card- the one that connects to your ISP and the internet at large. That connection should have just plain-vanilla TCP- no file/print share, no "Microsoft Network Client," etc. Nothing but TCP, period. You also need a compatible firewall: On the Win98/WinME versions of ICS, you'll need to add an ICS-compatible firewall, such as Sygate Personal or Pro, or Zone Alarm Pro. On XP, the ICS setup will offer to enable the built-in firewall, and that's an OK place to start (better than nothing), although you may wish to install a more robust firewall.

With nothing but TCP going in or out, and with the connection firewalled, you should be pretty safe: Tests like ShieldsUp www.grc.com should show full stealthing of the ICS PC- all ports should be invisible to the outside world, and NetBIOS shouldn't be open to the internet. But it can operate on the safe side of the LAN, letting the PCs access each other, and share files locally. This is very different from the way things work with NATS and some proxies. The old Sygate NAT I used forever worked just fine with XP clients set up in the traditional safe way, for example, using NetBEUI or IPX for the internal, peer-to-peer communication. But that way wouldn't work for XP if Windows' own ICS was doing the connection-sharing; for that, I had to use the Wizard-style networking, adjusted as above.

A final note: Each PC on the safe side--- the inside--- of a shared connection needs its own firewall, too, even if the externally-connected PC is firewalled, and even if the firewalling is provided by a piece of hardware. Don't rely on a single line of defense against internet threats: See www.informationweek.com/840/langa.htm

9. Shares and Shared Resources
After you have decided what drives and printers you want the outside world to see, you have to share them. Do this by going to the resource you want to share and opening its properties. Go to sharing (not security), and select "New Share" for folders or "Shared as" for printers and assign the object the share name you want it to be seen as on the network. If you append a dollar sign to the share, it will not be displayed as browseable to the network, but it is still there. This doesn't really add security, but is a nice trick to use so you can share out your quake mods to your friends at work with out having a \\computername\quake share showing up in everyone's browse window.

Remove the everyone group
Now here's the important part: remove the Everyone group. In some ways, since we have disabled the Guest account this is redundant, but it is better to do a little extra work so that if you missed something, you still are secure at a second point (and in the NT 4.0 days, there was more than one exploit involving the "Everyone" group, so let's err on the side of being cautious). Now add the people or groups that you want to access your computer. This can be as wide open as the "Domain Users" or "Authenticated users" or as restrictive as just your user ID. One thing to remember is that regardless who has rights to the file system, if they don't have rights to the share they cant get to it. The same thing works in reverse, too. If you are sharing your MP3 collection as: \\computername\mp3s$

... and you set the share to allow full control to everyone in the Authenticated Users group, those settings will not override the filesystem settings. Therefore, if all of you MP3s are only readable by user 'frufruhead,' then your share security settings won't change that. Now you can see why shares default so that "Everyone" can read them: on the most basic level, "everyone" can try and browse the share, but the default permissions take over on the filesystem.

Here's a rhetorical question: do you already have shares on your machine? Windows 2000 (and Windows NT) comes with Administrative shares already enabled. This means that every file on every hard drive on your computer is shared to the network by default. Only members of your Administrators Group can get to these shares, but it still can make it easier for someone outside to access things that they shouldn't. They are shared from the root of the drive, so to remove them go to the properties of the drive, the sharing tab, and remove the C$ by selecting "Do not share this folder". This is ok on a home machine, but may get your administrator at work a bit miffed. If you are this concerned about security, you should also remove the administrative share at

your C:\Windows directory. This is the Admin$ share. These shares are on every NT workstation and server by default, but remember, because of the $ at the end, they don't show up in My Network Places. They are still there however, so be sure to lock them down if you are concerned about external users accessing your drives, including snooping admins :).

Disable the automatic creation of the administrative shares
such as C$, D$, Admin$, on 2000 and NT, change the value of the following registry key to 0. Create a new DWORD value of either 'AutoShareWks' for NT Workstation or 'AutoShareServer' for NT server. Then set the value to equal '0' to disable automatic sharing. If the values already exist then modify them to change the value.

For Server -
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer

For Workstation -
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks

A setting of zero (1) reenables the shares

Read and execute permissions
Make sure program file directories have just Read and Execute permissions. Try to separate public files from private files. Note the owners of directories. The owner can still change things inside a directory, despite permissions being reset.

Domain administrators global group
Add the domain administrator's global group to all of your workstation's local administrator group for control. Also remove the "Access this computer from network" logon right from administrators on domain controllers.

10. Protect files and directories and use strong permissions
Clean-installed Windows 2000 systems have secure default ACLs on the file system. However, upgrades from previous versions (eg NT 4) do not modify the previous security settings and should have the default Windows 2000 settings applied. Refer to document on the Microsoft TechNet Security Web site for instructions about applying default Windows 2000 settings.

--Go to Windows NT File Manager and give the following permissions to C:\ drive (propagate permissions through entire tree):
Full Control Administrators
Full Control SYSTEM.

--Use FileAdmin and add Users group with the following permissions:
List Only C:\ (propagate)
Add C:\TEMP
Read %SYSTEMROOT% (Propagate)
No Access %SYSTEMROOT%\Config
No Access %SYSTEMROOT%\Repair
Change %SYSTEMROOT%\system32\Spool\Printers
Add %SYSTEMROOT%\system32\Spool\Profiles

--Go to FileAdmin and add CREATOR OWNER group with the following permissions:
Full Control C:\TEMP
Full Control C:\Users (Propagate)

--Clone Users group permissions if necessary. Note: This is probably the minimum set of permissions required for users to logon on NT and run software installed by an Administrator.

In an EXISTING installation:
1. Create a new Windows NT user group, for example Every User;
2. Include all your existing users into this group;
3. Use Windows NT User Manager to substitute Everyone with Every User in all rights.
4. Use FileAdmin to replace Everyone with Every User on all your drives. Important: Propagate permissions through the entire directory tree.

Shared NT server if you are planning to access the registry remotely:
1. Create a new Windows NT user group, for example Every User;
2. Include all your existing users into this group;
3. Use User Manager to substitute Everyone with Every User in all rights;
4. Use RegAdmin to replace Everyone with Every User propagating permissions through the entire key tree on the following keys:
HKEY_LOCAL_MACHINE
HKEY_USERS

NT workstation or stand-alone server:
If you do not need to access server registry remotely you can effectively (and truly) "Unshare" entire registry by explicitly denying access to the NETWORK group. These settings are recommended for a stand-alone Internet server or for NT server used for file sharing only. Use RegAdmin to give NETWORK group "Special Access (None)" rights propagating the changes through entire key tree for All root keys.

No one will be able to access your registry remotely, including users with correct administrator password. Most of the remote administrator tools will work on this computer. User Manager for the Domain is an exception from this rule: you will need to log on locally to administer your local users.

NOTE: NT will restore everyone's read access to root keys and some subkeys after reboot. Make sure that special key \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

exists on your NT machine (this key exists in NT 4.0 server by default. You can create this key manually on NT 3.51 SP 2 or later and on NT 4.0 Workstation) since this key is responsible for the "Network Registry Sharing" i.e. access to this key specifies Network access to the HKEY_LOCAL_MACHINE registry key and some of its subkeys.

11. File and Print Sharing
Make sure that you have 'File and Print Sharing' disabled on your computer if you are connecting to the internet - this is a big security risk. Go to control panels\network, click on File and Print sharing and unclick both boxes. See tip 8 on internet connection sharing.

12. Disable Unnecessary Services
Also see tips regarding services in NT, 2000 and XP as they also apply to security.
After installing Windows NT, 2000 or XP you should disable any network services not required. In particular, you should consider whether you needs any IIS components and whether it should be running the Server service for file and print sharing. You should also avoid installing applications on servers etc unless they are absolutely necessary to the server's function. For example, don't install e-mail clients, office productivity tools, or utilities that are not strictly required for the server to do its job.

13. Ports and Firewalls
You can specify which ports you wish to be accessible using this. Together with the NTFS file system this provides very strong protection against inwanted access to your system through a network connection. Right-click the network connection you want to configure, and then click Properties. On the General tab (for a local area connection) or the Networking tab (all other connections), click Internet Protocol (TCP/IP), and then click Properties. Click Advanced. Click Options, click TCP/IP filtering, and then click Properties. You may then configure TCP, UDP and IP ports for the traffic you wish to allow. Note that this filters incoming traffic only, you will need a firewall to monitor outgoing traffic. You may need to install this from the Network and Dial Up Connections folder, by selecting Advanced/Optional Networking Components.

When Internet-based programs try to connect to your machine, they first locate the machine itself via an IP address (which itself is resolved from a hostname, like www.bbc.co.uk). Once your computer knows where to locate the other, it then attempts to talk to whatever service on the remote computer that you're requesting, be it HTTP, FTP, NNTP, etc.. Think of an IP address as a phone number to a large corporation, and ports as the extensions to the various departments and people in it. Some well-known ports are: the Web (HTTP, port 80 TCP), Telnet (21 TCP) or Outgoing Mail (SMTP, 25 TCP). If you where to shut off port 80, no one would be able to connect via HTTP to your machine.

By shutting down any ports that you don't use, you cut down on the number of ways that an intruder can break into your system. But Windows can use a lot of weird ports to communicate to do things like run the update wizard, but most programs that scan for open ports (strangely named "port scanners") only check the first thousand or two (known as "well known ports"), so this isn't a problem. To see some services that use ports, and the port associated with them, go to C:\windows\system32\drivers\etc\services. It is a plan text file, so use notepad to open it. (Note that your Windows directory name may be different).

Firewalls
There are two ways to approach this: shut them all down yourself by inspecting your system and being extra cautious, or by slappin' up something called a Firewall, and takin' it easy. With a firewall, you can leave the FTP port on your machine wide-open, but it won't be visible to the outside world (people on the otherside of the firewall, that is) because the firewall can control and block access. Firewalls can be implemented in software on individual machines, or in special hardware for LAN-type firewalls that protect entire network nodes. You can see why business love firewalls: one good firewall can protect a whole LAN from outside attacks quite easily. Of course, once behind the firewall, all bets are off. Even if your company has a firewall, the dude in the cube next to you will not likely be affected in any way when he tries to mess with your machine.

Always run a good configured firewall when connected to the internet. Whether it be a hardware or a software firewall always use one. These programs will help secure your home machine from the Internet, as well as logging external and internal attempts to access resources. This way you can tell if a cracker is trying to break into your baby, or if there is some nasty Trojan trying to send your IRC passwords to Dr. Primevil. (And you'll likely be amazed at the number of port scans that you'll discover being run. These products can be configured to let you know when someone is attempting to connect with these ports and log the IP they are supposed to be coming from. Just note: installing these applications will make serious changes to your computers outside connection to the world. Make sure you read up on them before installing. Put web, ftp, and any other public servers OUTSIDE the firewall, or in a DMZ between a couple of firewalls.

I have tested a lot of firewall security programs for the PC and there are 3 very good affordable software firewalls which are excellent - these are 'Outpost Pro' 'Kerio' and 'Sygate'. Outpost is great as it also has plugin support e.g. popup blocking and ad filtering etc and also it doesn't consume many system resources. Sygate has to be the most feature rich of all the firewalls and I rate it very highly indeed and doesn't consume many resources. Kerio takes a bit of setting up and uses the least resources of them all. If I was running a server I would probably use Kerio as I like messing about with firewall rules. But at the end of the day you cannot beat a hardware firewall, for which I would still use a software firewall. Norton firewall is another bloated programme from Symantec. Nothing is completely secure in computing but if you have a properly configured firewall than you can at least get a good nights sleep !
A good hardware firewall I recommend is 'Sonicwall Soho'. Even if you install a hardware firewall, you should still have firewall software. Tiny can still be used to block unauthorised outbound traffic.

If you are using a firewall, these will look at it, not your machine. This tells us two things: firewalls can be great for protection outside of your firewall, but remember that you may still be open to the public behind the firewall, i.e., the people on your local network. Consider using "internal" firewalls if you need to secure certain servers from certain groups of users, i.e. protect the accounting server from the disgruntled marketing group.

IP filters or Firewalls must protect all NT-based LANs connected to the Internet. All traffic from the Internet to the LAN on ports UDP 137, UDP 138 and TCP 139 must be disabled.

Note: many cable modem service providers are now blocking many ports on their network segments. For example, blocking the NT networking ports on my network segment. You may wish to check with your service provider to see what kind of protection is already in place.

There are three basic types of exploits that are used on TCP ports. The first is when someone sends many, many packets to your machine so that it freezes or blue screens under the electronic onslaught. This is a form of a denial of service (DoS) attack. The second is where they send a specially crafted packet that "overloads" the port, allowing them to either execute code or cause the service/OS to crash. This is called a buffer overrun. The last is when you haven't properly secured your services, and they can connect to your mail server, and then send commands to the OS under the credentials of the mail service. For the most part the last is not something you need to worry about on a Windows 2000 workstation. These products can be configured to let you know about all such noteworthy events, and they will make your home machine a lot safer from the malicious e-rabble in the process.

14. List connections to your machine
Type 'netstat -a' in a command prompt will tell you who if anyone is connected to your computer.

15. Test your network
Now that your network is set up and hopefully locked down, you can test it at a number of sites to see if you got the basics. Please note that these do NOT mean that your workstation is secure, and do NOT assume that because you pass this no one can break into your workstation. These are just tools letting you know that some of the most obvious exploits. Here are the sites.

http://grc.com/intro.htm
www.dslreports.com/r3/dsl/secureme
www.antionline.com/

16. Use NTFS
NTFS partitions offer access controls and protections that aren't available with the FAT, FAT32, or FAT32x file systems. Make sure that all partitions on your server are formatted using NTFS. If necessary, use the *convert* utility to non-destructively convert your FAT partitions to NTFS. Warning If you use the convert utility, it will set the ACLs for the converted drive to Everyone: Full Control. Use the fixacls.exe utility from the Windows NT Server Resource Kit to reset them to more reasonable values. Also no dual booting.

17. Encryption
If you are using the NTFS file system you can encrypt files or folders so that they cannot be opened by other users. Open Windows Explorer, and then browse to the file or folder to be encrypted. Right-click on the file/folder and click 'Properties'. On the 'General' tab, click 'Advanced'. Select the 'Encrypt contents to secure data' check box. Encrypting a folder automatically encrypts all its subfolders and files. The encryption of a file or folder is transparent to the person who encrypts it; that person can work with the file without restriction. Encryption protects against others opening that file or folder.

Never leave sensitive material on your computer e.g. credit card numbers etc unless it is properly encrypted. Use PGP software (Pretty Good Privacy, from Network Associates), to make an encrypted virtual drive. No one will be able to access the contents of the PGP drive unless the proper password is entered. To be really, really safe encrypt the contents of the items you put into the PGP drive once again. Never use the same password that you use for anything else for PGP. 95, 98 and NT passwords are very easy to crack. Make sure that your passphrase for PGP is over 25 characters long and contain non asci characters (see next tip). When making a new key make the new key 4096 bit and make sure that you use 256bit for the PGP Disc. Overkill I know but as computers are getting faster and faster everyday the cracking of highly encrypted files comes that one bit closer.

18. Use strong passwords
Windows 2000 allows passwords of up to 127 characters. In general, longer passwords are stronger than shorter ones, and passwords with several character types (letters, numbers, punctuation marks, and nonprinting ASCII characters generated by using the ALT key and three-digit key codes on the numeric keypad - see further below for complete list of non ASCII characters) are stronger than alphabetic or alphanumeric-only passwords. For maximum protection, make sure the Administrator account password is at least nine characters long and that it includes at least one punctuation mark or nonprinting ASCII character in the first seven characters. In addition, the Administrator account password should not be synchronized across multiple servers. Different passwords should be used on each server to raise the level of security in the workgroup or domain.

Also try to avoid words that are used in the English dictionary. Its common sense but never write your password down, never type your password in when someone is near by and never use passwords that have something in common with yourself e.g. if someone liked Harleys they may have Harley Davidson as the passphrase !

There's a lot of discussion on how complex/long you should make your password. One common misconception about hacking an account is that it is frequently done through brute force attacks. This is where a remote machine tries to log into your local one over and over, trying a different password each time. Don't worry too much about this because there are only two accounts that everyone has on their Windows 2000 workstation, Administrator (which you have renamed) and Guest (which you have disabled). There is one big if. IF someone has access to the physical medium you are using to connect to another computer (i.e. they are on the same Ethernet segment or sharing someplace else further down the line), they can attempt to sniff the packets off the wire. Since computers use electricity to send information over a network (ok, some use light, but really, how many of you have fiber to your desktop?), every computer on a network segment gets every packet passed on that segment (Unless you are switched to the desktop). Usually network cards ignore information not intended for them, but people of a mischievous bent can install programs that let them pick up and save information that is intended for other people's computers.

If you are using Telnet, FTP or clear text SMB connections (Some older network programs use this, SAMBA for instance), your passwords are there for the taking. It's that simple, they just run the program and read it. Even worse, Windows 9X and NT (pre-service pack 4) defaults to using the LAN Manager hash to encrypt passwords. This was a decently secure way to do it back in the day, but with today's powerful processors, programs like L0phtCrack can sniff and decode your NT/9X authentication session-in real time. This is not a good thing. Fortunately for the security conscious Windows user, Microsoft has made NTLMv2 the standard method of encryption for authentication for NT after SP4 and 2000 from the start. The gotcha is that if you are in communication with a machine that only supports an older version, Windows 2000 will communicate in a way the older machine understands, meaning a less secure method. The Windows 2000 CD has an update for Win9X that allows 9x to use NTLMv2.
It is found at Clients\Win9x\Dsclient.exe.

Remember, if your password is easy to guess, it doesn't matter how well encrypted it is, so use something unusual. Your phone number from your childhood home, your aunt's last name, or anything else that is:

- Not found in a dictionary
- Not directly related to you (don't use your name, address or the word "password", please),
- Mix the password with numbers and non asci characters if possible e.g. 43934!!!^BLAH&*"£$
- Don't use a blank one
- I mean it, don't use a blank one.

If you are sharing your machine with others, you should make sure that all the users use different ID's and passwords. You don't want your roommate to delete your term paper or be able to read your email. Windows 2000 has greatly improved on the Profiles that NT 4 used to keep your files separate from other user's. This will work if:

- You don't let everyone have Administrative rights to your workstation (or they can just take ownership of the file and assign any rights they like, although this should leave an auditing trail)
- You are all logging in as separate users. Make everyone an ID and make sure they use it. It can be easy to guess the password of someone you know, so you should consider requiring complex passwords. These are a lot harder to guess, because they have to be 6 characters long and have a mix of characters in them. This also prevents the user from using their username as the password.

To enable this:
- Open up MMC.
- Add the Group Policy Snap-in, selecting local computer
- Go to Windows settings > Security Settings > Account Policy
- Change "Passwords must meet complexity requirements" to Enabled

- Set the minimum password length to at least 8 characters
- Set a minimum password age appropriate to your network (typically between 1 and 7 days)
  (this is for the truly paranoid, because it comes into play when a user is forced to change password, and changes it 5 times in a row so they can get it back to what it was originally. Not a problem really.
- Set a maximum password age appropriate to your network (typically no more than 42 days)
- Set a password history maintenance (using the "Remember passwords" option) of at least 6

How strong is your password ?
If someone runs a password cracker, and if it starts at the good length, how much computations he could expect to do. This is very simple. First count how much different characters you use. If you use only letters, that is 26, if you use lowcase and upcase letters, it is 52 (26 + 26), if you use only figures it is 10, etc. Let's call this number p. Then count how long your password is. We shall call that number l To know how much possibilities there are, compute
p ^ l.

Be your password yh66p14kk. You used lowcase letters and figures, that makes 36 different characters (26 + 10). The password is 9 letters long. So there are more than 100,000,000,000,000 possibilities. (36 ^ 9 is about 1.016*10^14) It is an excellent password.

A thing you should be aware of, is that some systems does not account the case of your password. If that is the case, abc, ABC and aBc are the same password and you can only consider 26 different characters instead of 52. I advise you to use figures an some sings like (or /.

You can generate secure passwords by using a good password generator at
www.winguides.com/security/password.php

Also use Jeremy Allison's PWAudit program to monitor the keys that PWDump accesses. This way you can logs attempts at grabbing the password.

Non ASCII characters - use them in your password !
Alt - 0 = NUL
Alt - 1 = ?
Alt - 2 = ?
Alt - 3 = ?
Alt - 4 = ?
Alt - 5 = ?
Alt - 6 = ?
Alt - 7 = •
Alt - 8 = ?
Alt - 9 = ?
Alt - 10 = ?
Alt - 11 = ?
Alt - 12 = ?
Alt - 13 = ?
Alt - 14 = ?
Alt - 15 = ¤
Alt - 16 = ?
Alt - 17 = ?
Alt - 18 = ?
Alt - 19 = ?
Alt - 20 = ¶
Alt - 21 = §
Alt - 22 = ?
Alt - 23 = ?
Alt - 24 = ?
Alt - 25 = ?
Alt - 26 = ?
Alt - 27 = ?
Alt - 28 = ?
Alt - 29 = ?
Alt - 30 = ?

Alt - 31 = ?
Alt - 32 = SPACE
Alt - 33 = !
Alt - 34 = "
Alt - 35 = #
Alt - 36 = $
Alt - 37 = %
Alt - 38 = &
Alt - 39 = '
Alt - 40 = (
Alt - 41 =)
Alt - 42 = *
Alt - 43 = +
Alt - 44 = ,
Alt - 45 = -
Alt - 46 = .
Alt - 47 = /
Alt - 48 = 0
Alt - 49 = 1
Alt - 50 = 2
Alt - 51 = 3
Alt - 52 = 4
Alt - 53 = 5
Alt - 54 = 6
Alt - 55 = 7
Alt - 56 = 8
Alt - 57 = 9
Alt - 58 = :
Alt - 59 = ;
Alt - 60 = <
Alt - 61 = =
Alt - 62 = >
Alt - 63 = ?
Alt - 64 = @
Alt - 65 = A
Alt - 66 = B
Alt - 67 = C
Alt - 68 = D
Alt - 69 = E
Alt - 70 = F
Alt - 71 = G
Alt - 72 = H
Alt - 73 = I
Alt - 74 = J
Alt - 75 = K
Alt - 76 = L
Alt - 77 = M
Alt - 78 = N
Alt - 79 = O
Alt - 80 = P
Alt - 81 = Q
Alt - 82 = R
Alt - 83 = S
Alt - 84 = T
Alt - 85 = U
Alt - 86 = V
Alt - 87 = W
Alt - 88 = X
Alt - 89 = Y
Alt - 90 = Z
Alt - 91 = [
Alt - 92 = \
Alt - 93 =]
Alt - 94 = ^
Alt - 95 = _
Alt - 96 = `
Alt - 97 = a
Alt - 98 = b
Alt - 99 = c
Alt - 100 = d
Alt - 101 = e
Alt - 102 = f
Alt - 103 = g
Alt - 104 = h
Alt - 105 = i
Alt - 106 = j
Alt - 107 = k
Alt - 108 = l
Alt - 109 = m
Alt - 110 = n
Alt - 111 = o
Alt - 112 = p
Alt - 113 = q
Alt - 114 = r
Alt - 115 = s
Alt - 116 = t
Alt - 117 = u
Alt - 118 = v

Alt - 119 = w
Alt - 120 = x
Alt - 121 = y
Alt - 122 = z
Alt - 123 = {
Alt - 124 = |
Alt - 125 = }
Alt - 126 = ~
Alt - 127 = ¦
Alt - 128 = Ç
Alt - 129 = ü
Alt - 130 = é
Alt - 131 = â
Alt - 132 = ä
Alt - 133 = à
Alt - 134 = å
Alt - 135 = ç
Alt - 136 = ê
Alt - 137 = ë
Alt - 138 = è
Alt - 139 = ï
Alt - 140 = î
Alt - 141 = ì
Alt - 142 = Ä
Alt - 143 = Å
Alt - 144 = É
Alt - 145 = æ
Alt - 146 = Æ
Alt - 147 = ô
Alt - 148 = ö
Alt - 149 = ò
Alt - 150 = û
Alt - 151 = ù
Alt - 152 = ÿ
Alt - 153 = Ö
Alt - 154 = Ü
Alt - 155 = ¢
Alt - 156 = £
Alt - 157 = ¥
Alt - 158 = P
Alt - 159 = ƒ
Alt - 160 = á
Alt - 161 = í
Alt - 162 = ó
Alt - 163 = ú
Alt - 164 = ñ
Alt - 165 = Ñ
Alt - 166 = ª
Alt - 167 = º
Alt - 168 = ¿
Alt - 169 = ¬
Alt - 170 = ¬
Alt - 171 = ½
Alt - 172 = ¼
Alt - 173 = ¡
Alt - 174 = «
Alt - 175 = »
Alt - 176 = ¦
Alt - 177 = ¦
Alt - 178 = ¦
Alt - 179 = ¦
Alt - 180 = ¦
Alt - 181 = ¦
Alt - 182 = ¦
Alt - 183 = +
Alt - 184 = +
Alt - 185 = ¦
Alt - 186 = ¦
Alt - 187 = +
Alt - 188 = +
Alt - 189 = +
Alt - 190 = +
Alt - 191 = +
Alt - 192 = +
Alt - 193 = -
Alt - 194 = -
Alt - 195 = +
Alt - 196 = -
Alt - 197 = +
Alt - 198 = ¦
Alt - 199 = ¦
Alt - 200 = +
Alt - 201 = +
Alt - 202 = -
Alt - 203 = -
Alt - 204 = ¦
Alt - 205 = -
Alt - 206 = +

Alt - 207 = -
Alt - 208 = -
Alt - 209 = -
Alt - 210 = -
Alt - 211 = +
Alt - 212 = +
Alt - 213 = +
Alt - 214 = +
Alt - 215 = +
Alt - 216 = +
Alt - 217 = +
Alt - 218 = +
Alt - 219 = ¦
Alt - 220 = _
Alt - 221 = ¦
Alt - 222 = ¦
Alt - 223 = ¯
Alt - 224 = α
Alt - 225 = ß
Alt - 226 = Γ
Alt - 227 = π
Alt - 228 = Σ
Alt - 229 = σ
Alt - 230 = µ
Alt - 231 = τ
Alt - 232 = Φ
Alt - 233 = Θ
Alt - 234 = Ω
Alt - 235 = δ
Alt - 236 = 8
Alt - 237 = φ
Alt - 238 = ε
Alt - 239 = n
Alt - 240 = =
Alt - 241 = ±
Alt - 242 = =
Alt - 243 = =
Alt - 244 = (
Alt - 245 =)
Alt - 246 = ÷
Alt - 247 = ˜
Alt - 248 = °
Alt - 249 = ·
Alt - 250 = ·
Alt - 251 = v
Alt - 252 = n
Alt - 253 = ²
Alt - 254 = ¦
Alt - 255 = BLANK
Alt - 0127 = □
Alt - 0128 = €
Alt - 0129 = □
Alt - 0130 = ,
Alt - 0131 = *ƒ*
Alt - 0132 = „
Alt - 0133 = ...
Alt - 0134 = †
Alt - 0135 = ‡
Alt - 0136 = ˆ
Alt - 0137 = ‰
Alt - 0138 = Š
Alt - 0139 = ‹
Alt - 0140 = Œ
Alt - 0141 = □
Alt - 0142 = Ž
Alt - 0143 = □
Alt - 0144 = □
Alt - 0145 = ‘
Alt - 0146 = ’
Alt - 0147 = “
Alt - 0148 = ”
Alt - 0149 = •
Alt - 0150 = -
Alt - 0151 = -
Alt - 0152 = ˜
Alt - 0153 = ™
Alt - 0154 = š
Alt - 0155 = ›
Alt - 0156 = œ
Alt - 0157 = □
Alt - 0158 = ž
Alt - 0159 = Ÿ
Alt - 0160 = BLANK (my favourite))
Alt - 0161 = ¡
Alt - 0162 = ¢
Alt - 0163 = £
Alt - 0164 = ¤
Alt - 0165 = ¥

Alt - 0166 = ¦
Alt - 0167 = §
Alt - 0168 = ¨
Alt - 0169 = ©
Alt - 0170 = ª
Alt - 0171 = «
Alt - 0172 = ¬
Alt - 0173 =
Alt - 0174 = ®
Alt - 0175 = ¯
Alt - 0176 = °
Alt - 0177 = ±
Alt - 0178 = ²
Alt - 0179 = ³
Alt - 0180 = ´
Alt - 0181 = µ
Alt - 0182 = ¶
Alt - 0183 = ·
Alt - 0184 = ¸
Alt - 0185 = ¹
Alt - 0186 = º
Alt - 0187 = »
Alt - 0188 = ¼
Alt - 0189 = ½
Alt - 0190 = ¾
Alt - 0191 = ¿
Alt - 0192 = À
Alt - 0193 = Á
Alt - 0194 = Â
Alt - 0195 = Ã
Alt - 0196 = Ä
Alt - 0197 = Å
Alt - 0198 = Æ
Alt - 0199 = Ç
Alt - 0200 = È
Alt - 0201 = É
Alt - 0202 = Ê
Alt - 0203 = Ë
Alt - 0204 = Ì
Alt - 0205 = Í
Alt - 0206 = Î
Alt - 0207 = Ï
Alt - 0208 = Ð
Alt - 0209 = Ñ
Alt - 0210 = Ò
Alt - 0211 = Ó
Alt - 0212 = Ô
Alt - 0213 = Õ
Alt - 0214 = Ö
Alt - 0215 = ×
Alt - 0216 = Ø
Alt - 0217 = Ù
Alt - 0218 = Ú
Alt - 0219 = Û
Alt - 0220 = Ü
Alt - 0221 = Ý
Alt - 0222 = Þ
Alt - 0223 = ß
Alt - 0224 = à
Alt - 0225 = á
Alt - 0226 = â
Alt - 0227 = ã
Alt - 0228 = ä
Alt - 0229 = å
Alt - 0230 = æ
Alt - 0231 = ç
Alt - 0232 = è
Alt - 0233 = é
Alt - 0234 = ê
Alt - 0235 = ë
Alt - 0236 = ì
Alt - 0237 = í
Alt - 0238 = î
Alt - 0239 = ï
Alt - 0240 = ð
Alt - 0241 = ñ
Alt - 0242 = ò
Alt - 0243 = ó
Alt - 0244 = ô
Alt - 0245 = õ
Alt - 0246 = ö
Alt - 0247 = ÷
Alt - 0248 = ø
Alt - 0249 = ù
Alt - 0250 = ú
Alt - 0251 = û
Alt - 0252 = ü
Alt - 0253 = ý

Alt - 0254 = þ
Alt - 0255 = ÿ

Create a password reset disk
If you're running Windows XP Professional as a local user in a workgroup environment, you can create a password reset disk to log onto your computer when you forget your password. To create the disk:

Click Start, click Control Panel, and then click User Accounts. Click your account name. Under Related Tasks, click Prevent a forgotten password. Follow the directions in the Forgotten Password Wizard to create a password reset disk. Store the disk in a secure location, because anyone using it can access your local user account

19. Ensure that you have disabled the Guest Account
The 'Guest' account allows anonymous access to a machine. Making sure that this account is disabled will prevent people from using services you may have inadvertently left open. You can get to this from "Control Panel > Users and Passwords" Then, click on the "Advanced" tab, and choose "Advanced." You should know be able to modify the Guest account in the "Users" folder.

There is a tendency to confuse the "Everyone" group with the guest account/group. "Everyone" represents people that are authenticated in any way the client can verify, be locally or to a domain. If you are anyone, you are "Everyone". If a user doesn't have any other method of authentication, then they are allowed to access whatever the guest group/account has rights to. This is why you should disable your guest account. But keep in mind: anyone is everyone, including your own valid user. It is a common mistake for new users to set the filesystem permissions at the root of their system to "deny" Everyone access. Doing so will keep everyone, including you out. We're be covering filesystem permissions more in depth at another time.

20. Rename Administrator
Unlike other Accounts, the Administrator ID cannot be locked out. This means that people can try as many times as they like to crack this ID. To make this more difficult, rename your administrative account to something else. Make it very easy to remember, like "RealAdmin" or something similar. Next, I would recommend making a dummy Administrator account that has NO rights to anything, named "Administrator" with no privileges. Scan the event log regularly looking for attempts to use this account and giving it a log in script that writes the client machine's host name and IP address to a file whenever someone is able to log in using it, and then kicks the user off. To add a login script to the dummy administrators account, go to Console1 and the properties of the dummy account. Change it in the "Login Scripts" entry.

A login script, in the most simple terms, is just a batch file that a user runs when they login. This can be as simple as connecting a few network drives to as complex as, well, let it suffice to say it can get really complex. If you want to make a login script that puts the IP address info of the person logging into your machine into a log file, you would use something like this. Let's name the file Login.CMD, and let's create it in notepad just like any other text file.

```
rem Make it so the person logging in doesnt see the script run
@echo off
Rem get the ipaddress of the local machine along with some other settings, you can write another Rem script to parse out just the ip address, but if they are NAT'ed or PAT'ed then the whole thing is a Rem lot more useful
ipconfig >> \\<YourServer>\<SecureShare>\ipaddr.log
rem Exit the command shell
Exit
```

Please note a few things here:
You need to be very restirictive on the rights to the <secureshare> folder on your machine. Give authenticated users read/change permissions at the share level, then go to Security, Advanced, Permissions, select your dummy account, and click "Edit". Make all the options deny except the right to append to the file.

- You may want to enable quotas on this account as well, so a malicious user can't fill up your harddrive by repeatedly logging in, over and over.
- This will only catch people running Windows machines or other SMB clients that will run a login script.
- This is by no means the best way to detect an intruder. Use a firewall or some dedicated intrusion detection software.
- Enable auditing on the shared directory so you can tell what's happening.

Now it is time to create the ID you will actually be logging in with everyday. If it's your home desktop, go ahead and add this to the administrator's group for your local machine. Use this ID to log in for most things, reserving your renamed Administrator account for emergencies. If you are a member of a NT 4.0 domain or a Windows 2000 Active Directory tree, it is also a good idea to audit Logon Failures. This is not an option in Windows 2000 professional in a standalone configuration. Next enable account lockout on the real Administrator accounts by using the passprop utility from resource kit and disable the local computer's Administrator account.

21. Enable Auditing
Use Auditing - heavily if Internet connected. Read your logs daily. Use them as a guide, however don't blindly trust that every action is in the logs, and every action reflected in the logs should not be taken at face value. INVESTIGATE ODD THINGS.
Enable auditing and create a separate administrators account for auditing purposes only. For the highest security use separate administrator account for auditing this allows other administrators to be audited as well. Only enable auditing on the events you need because every item audited increases overhead.
1. Open User Manager or User Manager for Domains.
2. Create a new account. For example, auditor.
3. Make sure auditor is a members of the Administrators group and Domain Admins.
4. Click Policies. Click Audit.
5. Click Audit These Events
6. Select the events your wish to audit.
7. Click ok.
8. Click Policies.
9. Click User Rights.
10. Select Manage Auditing and security log.

11. Remove the default administrators group.
12. Add the account used for auditing.
13. Click ok.

22. Group Policy Editor
On 2000 and XP you can use the group policy tool to restrict access. If you would like to limit or control just about every aspect of your computer you can use a great tool called the group policy editor. Click Start and select Run. Type gpedit.msc in the text box and click on OK. The group policy editor will load. Navigate through the folders and you will discover hundreds of items that you can limit access to and control.

23. Security Templates
This applies to 2000 and XP. During installation, a set of standard security settings is applied to the system: these settings are known as a security template. To get a detailed analysis of the security settings on your machine, open the MMC and select Add/Remove Snap In from the Console Menu. Click on the Add button, and select the Security Configuration and Analysis, and Security Templates snap-ins.

If you view the Security Templates option, you will see a list of the basic security templates that are available to your system. You can view the security settings that each individual template applies by clicking on the plus sign next to each template. The basicwk template is the default workstation security template, the hisecws template provides higher security workstation settings while the compatws template provides maximum compatibility for non-Windows 2000 certified applications.

The template named Setup Security is the default setup template, by double-clicking on this you can see a list of the security settings that this template applies under each section of the system, i.e. Account Policies, Local Policies, Event Log, Restricted Groups, System Services, Registry and File System. Double clicking on each individual item will give you more detailed information on that particular setting. For example under the default Setup Security template, if you look under Account Policies, then Password Policy you will see the security setting for the system passwords.

To view the settings that are currently applied to your machine, right click on Security Configuration and Analysis and select Analyse Computer Now. To apply a different template, right-click on Security Configuration and Analysis and select Import Template. You can then choose from the selection of standard templates. You can also modify an existing template to your chosen settings, then choose Export Template and save it as a new template.

24. Disable or delete Unnecessary Accounts
You should review the list of active accounts (for both users and applications) on the system in the Computer Management snap-in, and disable any non-active accounts, and delete accounts which are no longer required.

25. Set account lockout policy
Windows 2000 and XP includes an account lockout feature that will disable an account after an administrator-specified number of logon failures. For maximum security, enable lockout after 3 to 5 failed attempts, reset the count after not less than 30 minutes, and set the lockout duration to Forever (until admin unlocks).

The Windows NT Resource Kit includes a tool that allows you to adjust some account properties that aren't accessible through the normal management tools. This tool, passprop.exe, allows you to lock out the administrator account: The */adminlockout* switch allows the administrator account to be locked out

26. Require CTRL-ALT-DEL before login
In 2000 and XP under Control Panel/Users & Passwords ensure that the "Users must enter a user name and password" box is checked, and under the Advanced tab, that "Require users to press CTR-ALT-DEL before logging on" is checked.

27. Don't Display Last User Name at logon
Either use TweakUI and clear the checkmark next to Clear Last User at logon in the Paranoia tab or utilise a registry entry. Enabling this will blank the username box on the logon screen. Preventing people that are logging on from knowing the last user on the system and also from preventing account lockouts for the wrong person.

Win9x Settings
Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon]
Value Name: DontDisplayLastUserName
Data Type: REG_SZ
Data: (1=enable, 0=disable)

NT Settings
Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
Value Name: DontDisplayLastUserName
Data Type: REG_SZ
Data: (1=enable, 0=disable)

If that doesn't fix it, follow this solution (make sure you have a note of all your ISP usernames and passwords)

First, delete your .PWL file from the C:\WINDOWS folder.
Next, delete the equivalent entry from C:\WINDOWS\SYSTEM.INI's [Password Lists] section.
Next, open Control Panel > Network and ensure Windows Logon is installed and that it is the Primary Network.
Reboot. When asked for a username and password, enter your usual username and hit Return. Do NOT enter a password- leave it blank. Hit Return to confirm the blank password. That's the last time you'll be asked to logon to Windows. When you logon to your ISP, you'll have to enter your username and password, but once connection is established, these will be remembered for future logons, provided you checkmark the appropriate box, of course.

If you're on a LAN, use Client for Microsoft Networks, instead. You will need to use Tweak UI's Logon instead.
If you WANT to logon, but can't, remove the following registry value:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\Real Mode Net
"autologon"="1"

28. Disable Password Caching
Normally Windows caches a copy of the users password on the local system to allow for additional automation, this leads to a possible security threat on some systems. Disabling caching means the users passwords are not cached locally. This setting also removes the second Windows password screen and also remove the possibility of networks passwords to get out of sync.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
Right-click on the white space in the left pane and select New/DWORD Value. Give the new value the name DisablePasswordCaching, and set the value to 0x00000001

When you're logging on to a WinNT domain it is preferable to disable password caching.
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network]
"DisablePwdCaching"=dword:00000001

29. Protect the registry from anonymous access
The default permissions do not restrict remote access to the registry. Only administrators should have remote access to the registry, because the Windows 2000 registry editing tools support remote access by default. To restrict network access to the registry:
Add the following key to the registry:
HKEY_LOCAL_MACHINE \SYSTEM Key \CurrentControlSet\Control\SecurePipeServers
Value Name \winreg Select winreg, click the Security menu, and then click Permissions.

Set the Administrators permission to Full Control, make sure no other users or groups are listed, and then click OK.
The security permissions (ACLs) set on this key define which users or groups can connect to the system for remote registry access. In addition, the AllowedPaths subkey contains a list of keys to which members of the Everyone group have access, notwithstanding the ACLs on the winreg key. This allows specific system functions, such as checking printer status, to work correctly regardless of how access is restricted via the winreg registry key. The default security on the AllowedPaths registry key grants only Administrators the ability to manage these paths.

30. Restricting Information Available to Anonymous Logon Users under NT
Windows NT has a feature where anonymous logon users can list domain user names and enumerate share names. Customers who want enhanced security have requested the ability to optionally restrict this functionality.

Go to the following key in the registry:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

On the Edit menu, click Add Value and use the following entry:
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Value: 1

Restart the computer for the change to take effect.

31. Hiding Servers from the Browser List on NT
If you have a secure server or workstation you wish to hide from the general browser list, add this registry setting.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Add value "Hidden" (REG_DWORD) and set it to "1".
Reboot the server. It may take up to ½ hour for the server to disappear from the browse lists.
(Same result can be acheived by executing NET CONFIG SERVER /HIDDEN:YES on the workstation.)

32. Require Validation by Network for Windows Access
By default, Windows 95 & 98 don't require a valid network username and password combination for a user to bypass the logon and access the local machine. This functionality can be changed to require validation by the network before allowing access. Your machine must be part of a Windows NT domain for this tweak to work, as the user must be authenticated by the network.

Open your registry and find the key
[HKEY_LOCAL_MACHINE\Network\Logon]
Create a new DWORD value, or modify the existing value, called "MustBeValidated" and set it to equal "1" to require successful authentication. Restart Windows for the change to take effect.

33. Mapped Drives
Windows stores the names of previously mapped drives, this can be a security threat if vunerable hidden shares are listed. An advantage is that this key can also be used to set default items for list, if for example inexperienced users where required to map common drives, your could store them here.

a. Open the registry and find the key below.
[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Network\Persistent Connections]

b. Listed under this key are all the shares Windows has stored for the current user, simply delete the entries you don't want to store. Or add new ones by adding a new string value, and name it by incrementing the alpha values already in the list. Set the data to equal the drive share you wish to add.
Note: This change affects only the current user, to change the defaults for all users modify
[KEY_USERS\.DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\Network\Persistent Connections] instead.

34. Restricting Access to the Event Logs
The Windows NT/2000 event log contains records documenting application, security and system events taking place on the machine.

These logs can contain sensitive data, and by default, the Guest account has access to view them. This tweak allows you to restrict access to administrators and system accounts only.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog]
Under this key are three sub-keys: Application, Security and System. These subkeys represent each section of the event log. To restrict access to each section create a new DWORD value of 'RestrictGuestAccess' under each sub-key and set it to equal '1'. To restrict access to only certain sections, then only add the value to that specific key. Restart Windows for change to take effect.
For example, the setting may look like :
RestrictGuestAccess 0x00000001 (1)

35. Stopping the KnownDLLs Vulnerability
In Windows NT, core operating system DLLs are kept in virtual memory and shared between the programs running on the system. This has exposed a vulnerability that could allow a user to gain administrative privileges on the computer the user is interactively logged onto. To enable stronger protection on system base objects such as the KnownDLLs list, change the value of 'ProtectionMode' to equal '1' in the registry key below.
Registry Settings:
Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager]
Value Name: ProtectionMode
Data Type: REG_DWORD
Data: (0 = disabled, 1 = enabled)

36. The ICMP Router Discovery Protocol
comes enabled by default on DHCP clients that are running MS Windows95 (with Winsock 2), Windows 98/98SE, Windows ME, and Windows2000 machines. Using router discovery, clients dynamically discover routers and can switch to backup routers if a network failure or administrative change is needed. However, by spoofing IRDP Router advertisements, a potential attacker can remotely add default route entries on a remote system. The default route entry added by the attacker will be preferred over the default route obtained from the DHCP server on Windows 9x/ME systems. The problem is not in IRDP itself, but rather that MS platforms use it even when DHCP is enabled and the DHCP setup specifies router information. To disable this vulnerability, you need to add the following entry to the Registry. This is intended for advanced users, please backup your Registry before making any changes.

Windows 9x / ME:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans\000n
(Where "000n" is your TCP/IP protocol. It contains "TCP/IP" assigned to the "DriverDesc" Value)
PerformRouterDiscovery="0" (DWORD value)
Note: Although according to Microsoft's documentation the value should be DWORD, they have moved to string values for most TCP/IP related Registry entries in Windows 98, so the documentation on the value type could be wrong.

-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans\0000]
"PerformRouterDiscovery"=dword:00000000

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans\0001]
"PerformRouterDiscovery"=dword:00000000

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans\0002]
"PerformRouterDiscovery"=dword:00000000

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans\0003]
"PerformRouterDiscovery"=dword:00000000

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Class\NetTrans\0004]
"PerformRouterDiscovery"=dword:00000000
------End cut & paste here------

Windows 2000:
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces*interface*
PerformRouterDiscovery="0"
(REG_DWORD, range 0,1,2, 0=disabled, 1=enabled, 2=enable only if DHCP sends the router discover option)
Note: IRDP support is disabled by default on NT4, and enabled on Windows 2000.

37. Prevent the Logon Screen Saver from Launching and use a security screensaver !
Windows NT has a default screen saver called login.scr, which runs even if no screen saver has been selected. This can be a security risk, as it can allow a local user to replace login.scr with another program and have it launched with system privileges.

[HKEY_USERS\.DEFAULT\Control Panel\Desktop]
Change the value of 'ScreenSaveActive' to '0' to disable the screen saver.

Restart for the change to take effect. An alternative screen saver can be used, if disabling is not an option, simple change the value of 'SCRNSAVE.EXE' in the same to key, to equal the full path of the screen saver you wish to use.

Security Screen Savers
The Security screen savers help remind users of basic security practices. One that displays the Ten Immutable Laws of Security, and one that displays the Ten Immutable Laws of Security Administration.
www.microsoft.com/technet/security/tools.asp

38. Maximum Number of Remote Access Authentication Attempts on NT
This setting controls the number of authentication retries before the remote access connection is terminated. Even better disable remote access.

Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters]
Value Name: AuthenticateRetries
Data Type: REG_DWORD
Data: 1 to 10

39. Automatically Disconnect Remote Access Callers on NT and 2000
Specifies the amount of idle time in minutes to wait before disconnecting the RAS client. This reduces browser traffic generated by the machine because it advertises its presence on the network. This change is highly recommended for WAN's connected using dial up lines to reduce costs on idle connections to the server.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\autodisconnect
Modify the REG_DWORD value from 15 minutes to 2 in decimal.

40. Disable Dial-In Access for Windows 9x and NT
It's possible for users to setup a modem on a Windows machine, and by using Dial-up Networking allow callers to connect to the internal network. Especially in a corporate environment this can cause a major security risk.

Key: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]
Value Name: NoDialIn
Data Type: REG_DWORD
Data: (0 = dial-in enabled, 1 = dial-in disabled)

41. Securing Network Access to NT CD-ROM Drives
This setting determines whether data in the CD-ROM drive is accessible to other users. Because the CD-ROM drive is a volume, by default, it is shared as an administrative share on the network. If the value of this entry is 1, the CD-ROM drive is allocated to the user as part of the interactive logon process and, therefore, only the current user can access it. This prevents administrators and remote users (and even the same user at a different workstation) from accessing the drive while the current user is logged on to the computer. The drive is shared again when the current user logs off the computer.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
Value Name: AllocateCDRoms
Data Type: REG_SZ
Data: (0 = enabled, 1 = disabled)
Value Meanings:
'0' = Compact discs in the CD-ROM drive can be accessed by all administrators in the domain.
'1' = Only the user logged on locally can access data on the compact discs in the CD-ROM drive.

42. Securing Network Access to NT Floppy Drives
This setting determines whether data in the floppy disk drive is accessible to other users. Because the floppy disk drive is a volume, by default it is shared as an administrative share on the network. If the value of this entry is 1, the floppy disk drive is allocated to the user as part of the interactive logon process and, therefore, only the current user can access it. This prevents administrators and remote users (and even the same user at a different workstation) from accessing the drive while the current user is logged on. The drive is shared again when the current user logs off.

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
Value Name: AllocateFloppies
Data Type: REG_SZ
Data: (0 = enabled, 1 = disabled)

Value Meanings:
'0' = Floppy disks in the floppy disk drive can be accessed by all administrators in the domain.
'1' = Only the user logged on locally can access data on the floppy disks in the floppy disk drive.

43. Dont save encrypted files to disk
When you connect to a site that is encrypted the data sent over the network is encrypted. Your browser has the key to decrypt and display the information. Why give someone a chance to crack the encryption. If you don't allow IE to save it to disk then it is nearly impossible for someone else to be able to get that file and use brute force to crack it. Launch Internet Explorer. Select the Tools from the menu bar. Then select Internet Options... from the drop down menu. Once the internet options has loaded click on the advanced tab. Under security find where it says Do not save encrypted pages to disk and check it. Click OK

44. Clear pagefile at shutdown
I only recommend this for people who are paranoid as your pagefile has to be recreated at every boot and has a big hit on performance. Your pagefile could contain passwords etc. This can be useful if you are imaging your computer with drive image or ghost to get your image as small as possible.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement
If value does not exist add the following value
ClearPageFileAtShutdown : 1 (Type Reg_DWord)

45. Make all Desktop Settings Permanent
Make all Desktop Settings Permanent in an window: window size, position, toolbar etc. Run Regedit and go to:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Right-click in the right hand pane, click New, and select DWORD Value. Name it 'NoSaveSettings'
Now right-click on it, choose Modify, and type 1 in the Value data box.
Click OK and exit the Registry Editor.
All future windows settings will be from now on those you specified BEFORE creating the new "NoSaveSettings" Registry value, and can be changed ONLY temporarily. Next time you open that same window, its settings will revert back to the ones you started with, before this Registry change. To reenable permanent settings changes again, goto the same Registry key above, right-click on "NoSaveSettings", choose Modify, and change its Value data to 0.

46. Clear Internet Explorer Typed URL History
Internet Explorer caches any URL's that are typed into the address bar. This could become a privacy issue on a shared computer, or it may become a nuisance if there is a particular URL you want to remove without clearing the whole history. Open your registry and find the key below and delete any value you want to remove.

Registry Settings:
Key: [HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs]

47. Dlls and Exes to Read only
Make all your dll's, exe's and com files read only. If you make all your application files (EXE) and dll's read only it will make your system more secure because normally trojans and viruses don't have any built in routines to change attributes of the files they are designed to modify - they can't modify a read only file without first changing its attributes. There are reasons viruses and trojans don't try to change the attributes
- Virus programmers usually don't think anyone would make all their exe & dll files read only and don't write code to deal with that obstacle.
- Even if they think about it, the goal of all viruses is to keep them as small as possible so they are harder to detect. Adding routines to change attributes increases the size of the programs. When an exe or dll or com file can't be modified the virus can't spread. BUT even better... If something tries to modify a read only file Windows usually pops up a notice and that would tip you that something suspicious was going on. If you try to delete a folder that has read only files you will be prompted with a second confirmation and this extra step helps to avoid mistakes of accidentally deleting the wrong files or folders.

48. Turn off auto-insert notification on all cd drives
Do this from control panels\system\devicemanager - click on each of your cd drives and goto properties\settings and uncheck auto insert notification. I have seen some commercial magazine disks that try to execute a virus automatically when a disc is inserted into your machine. Although a good virus checker would detect this.

In NT you will have to do this through the registry.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDRom]

Change to value of 'Autorun', or create a new DWORD value if it doesn't already exist, and set the data to equal '0' for Autorun disabled. Restart your computer. For example, the setting may look like: Autorun 0x00000000 (0)

49. Stop .reg files from being automatically run
This next registry entry changes the way a .reg file is handled. If a .reg is opened normally it would ask you 'are you sure you want to add details to the registry' and when a .reg is run with the /s switch it wouln't ask you it would just add the details anyway. This reg file changes the behaviour of a reg file, so if it is executed it will only edit the file and not import it into the registry. To merge the Registry file into your Registry, you will need to right-click on it and select Merge.

-----Begin cut & paste here-----
REGEDIT4

[HKEY_CLASSES_ROOT\regfile\shell]
@="edit"
------End cut & paste here------

50. Spyware
Run 'Ad-Aware' program to fight the spying that a least 100 or so programs are known to do. (I do this mainly to save the band width wasted by the data and banner ads that are passing back and forth.) www.lavasoft.de
Also check out SpyBot from http://spybot.safer-networking.de/

51. Create a shortcut to lock computer
This works in XP and probably NT and 2000. Right click on desktop and select new -> shortcut. Then copy and paste this in the program location box "rundll32.exe user32.dll,LockWorkStation" Click next and enter a name for you shortcut and then click finish. Now you can copy and paste that shortcut anywhere you want on your computer.

52. Physically secure and protect your servers and critical workstations
Quite simply lock them up - password protect consoles, lock them away in secure fireproof halon strong rooms which are alarmed and have security cameras inside. Make sure rooms have no windows and no roof or any access of any kind apart from one security door. The secure door must be very strong and protected with multiple entry systems e.g. keycard access with codepunch and/or fingerprint/retina scan recognition systems - you get the idea...

53. XP Permissions
Sharing of files and folders can be managed in two ways. If you chose simplified file sharing, your folders can be shared with everyone on your network or workgroup, or you can make your folders private. (This is how folders are shared in Windows 2000.) However, in Windows XP Professional, you can also set folder permissions for specific users or groups.

To do this, you must first change the default setting, which is simple file sharing. Open Control Panel, click Tools, and then click Folder Options. Click the View tab, and scroll to the bottom of the Advanced Settings list. Clear the Use simple file sharing (Recommended) check box. To manage folder permissions, browse to the folder in Windows Explorer, right-click the folder, and then click Properties. Click the Security tab, and assign permissions, such as Full Control, Modify, Read, and/or Write, to specific

users. You can set file and folder permissions only on drives formatted to use NTFS, and you must be the owner or have been granted permission to do so by the owner.

54. Web Bugs

Web bugs are little images embedded in web pages which refer back to a remote site and thereby cull tracking information about your web surfing. They're often only 1 pixel square and transparent, so for all practical purposes they're invisible. To nullify web bugs you need to stop communications to the ad companies running them. A good way to do this is by using Silencer from the Bloatbusters.
http://radsoft.net/bloatbusters/downloads/silencer.zip

Another process that can track visitors is the feature called "User Data Persistence" appeared in MS IE 5.0 and is not as well known or as easily managed as cookies, but unfortunately can accomplish the same thing. There is no warning flag that can be toggled to tell you when Data Persistence is being used on a web site to store information from your system, but it can be turned off: open IE -> from the File menu click Tools -> Internet Options -> Security -> Custom Level -> Miscellaneous -> disable "User Data persistence". The purpose Data Persistence was developed for was to offer the ability to "persist" information, which also lets you retain style and state beyond a single web page.
You can also IE About Boxes with this registry entry which works for all OS's up to XP.

-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProtocolDefaults]
"about"=dword:00000004
"about:"=dword:00000004
-----Begin cut & paste here-----

UPDATE: "It will kill the use of a blank page as the startup browser page. There's not a lot that can be done as it seems that IE cannot be made to differentiate between the keyword "about" and one of those annoying about: URLs. However, I've had good success with fixing it by adding "about:blank" both under: Control Panel -> Internet Options -> click Security tab -> highlight Trusted sites -> click the Sites... button -> uncheck the "Require server verification (https:) for all sites in this zone" box -> highlight "Add this Web site to the
zone:" box -> type about:blank -> click the Add button -> click OK twice, and this DWORD Value:
"about:blank"=dword:00000003 under the same Registry key above."

55. Forgotten Passwords

This section will give you a basic idea of how to retrieve/workround forgotten passwords for various different elements of the operating system.

Content Advisor
If you have forgotten the Content Advisor password, you can delete it by browsing to this folder in Regedit.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ratings
Select the icon called Key in the right-hand pane and press delete. Close Regedit.
You can now start Internet Explorer and goto View, Internet Options.... Select the Content tab, and click on Disable. When asked for a password, don't enter anything, just click on OK.

Dialup Password and Other Passwords
If you have forgotten your password for dialup accounts and various other items that have asterisks for the password download Snadboys Revelation which will tell you the password. www.snadboy.com/

Outlook Password
HKEY_LOCAL_MACHINE\Software\Microsoft\Protected Storage System Provider*Default*
\Data\89c39569-6841-11d2-9f59-0000f8085266
or to:
HKEY_LOCAL_MACHINE\Software\Microsoft\Protected Storage System Provider\<UserName>
\Data\89c39569-6841-11d2-9f59-0000f8085266

If user profiles are enabled on your computer, go to:
HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider\<UserName>
\Data\89c39569-6841-11d2-9f59-0000f8085266

Then delete its subkey. Now open OE and type in a new identity password.
Note that the subkey name and the CLSID are the same. There is difference of uppercase and lowercase.
If you know your CLSID, go to this Registry key:
HKEY_CURRENT_USER\Identities\{CLSID}
to find out the OE password key name."

Screen Saver
Have you ever forgotten your screen saver password ?
Just fire up Regedit and go to:
HKEY_USERS\.Default\Control Panel\desktop

In the right hand pane look for the "ScreenSave_Data" String value. Highlight it and hit the Delete key.
Exit the Registry Editor when done. Of course, everybody who has been "playing" with personal computers for a while has learned the "easy way" around this: press and hold Ctrl+Alt+Delete simultaneously, followed by/or Ctrl+Esc. This "classic" trick works with all versions of windows (havent tested on XP though).

56. Restrict access to certain executables

Restrict access to certain executables you deem dangerous (possibly CMD.EXE) etc.

57. Temporarily Assign Yourself Administrative Permissions
Many programs require you to have Administrative permissions to be able to install them. Here is an easy way to temporarily assign yourself Administrative permissions while you remain logged in as a normal user.
Hold down the Shift key as you right-click on the program's setup file. Click Run as. Type in a username and password that have Administrative permissions. This will also work on applications in the Start menu.

58. Create a password reset disc in XP
If you're running Windows XP Professional as a local user in a workgroup environment, you can create a password reset disk to log onto your computer when you forget your password. To create the disk: Click Start, click Control Panel, and then click User Accounts. Click your account name. Under Related Tasks, click Prevent a forgotten password. Follow the directions in the Forgotten Password Wizard to create a password reset disk. Store the disk in a secure location, because anyone using it can access your local user account

59. Windows 2000 Baseline Security Checklist
The purpose of this checklist is to give instructions for configuring a baseline level of security on computers running Windows 2000 Professional. Security settings can be configured and applied to locally via the Security Configuration Tool Set. Security policies can be created by using the Security Configuration Tool Set and distributed and applied via Group Policy for those machines in a domain. This guide outlines recommended security settings for Windows 2000. A step-by-step guide to configuring enterprise security policies using the Security Configuration Tool Set is located on the Microsoft TechNet Security Web site.www.microsoft.com/technet/prodtechnol/windows2000serv/howto/entsec.asp

- Verify that all disk partitions are formatted with NTFS
- Verify that the Administrator account has a strong password
- Disable unnecessary services
- Disable or delete unnecessary accounts
- Protect files and directories
- Make sure the Guest account is disabled
- Protect the registry from anonymous access
- Apply appropriate registry ACLs
- Restrict access to public Local Security Authority (LSA) information
- Set stronger password policies
- Set account lockout policy
- Configure the Administrator account
- Remove all unnecessary file shares
- Set appropriate ACLs on all necessary file shares
- Install antivirus software and updates
- Install the latest Service Pack
- Install the appropriate post-Service Pack security hotfixes
- Windows 2000 Professional Configuration Checklist Details

Verify that all disk partitions are formatted with NTFS
NTFS partitions offer access controls and protections that aren't available with the FAT, FAT32, or FAT32x file systems. Make sure that all partitions on your computer are formatted using NTFS. If necessary, use the convert utility to non-destructively convert your FAT partitions to NTFS. Warning If you use the convert utility, it will set the ACLs for the converted drive to Everyone: Full Control. Use the fixacls.exe utility from the Windows NT Server Resource Kit to reset them to more reasonable values.

Verify that the Administrator account has a strong password
Windows 2000 allows passwords of up to 127 characters. In general, longer passwords are stronger than shorter ones, and passwords with several character types (letters, numbers, punctuation marks, and nonprinting ASCII characters generated by using the ALT key and three-digit key codes on the numeric keypad) are stronger than alphabetic or alphanumeric-only passwords. For maximum protection, make sure the Administrator account password is at least nine characters long and that it includes at least one punctuation mark or nonprinting ASCII character in the first seven characters. In addition, the Administrator account password should not be synchronized across multiple computers. Different passwords should be used on each computer to raise the level of security in the workgroup or domain.

Disable unnecessary services
After installing Windows 2000, you should disable any network services not required for the computer. In particular, you should consider whether your computer needs any IIS 5.1 Web services.

Disable or delete unnecessary accounts
You should review the list of active accounts (for both users and applications) on the system in the Computer Management snap-in and disable any non-active accounts and delete accounts which are no longer required.

Protect files and directories
Refer to Default Access Control Settings in Windows 2000 document on the Microsoft TechNet Security Web site for details on the default Windows 2000 file system ACLs and how to make any necessary modifications.

Make sure the Guest account is disabled
By default, the Guest account is disabled on systems running Windows 2000. If Guest account is enabled, disable it.

Protect the registry from anonymous access
The default permissions do not restrict remote access to the registry. Only administrators should have remote access to the registry, because the Windows 2000 registry editing tools support remote access by default. To restrict network access to the registry:

Add the following key to the registry:
Hive HKEY_LOCAL_MACHINE \SYSTEM
Key \CurrentControlSet\Control\SecurePipeServers
Value Name \winreg

Select winreg, click the Security menu, and then click Permissions.
Set the Administrators permission to Full Control, make sure no other users or groups are listed, and then click OK.
The security permissions (ACLs) set on this key define which users or groups can connect to the system for remote registry access. In addition, the AllowedPaths subkey contains a list of keys to which members of the Everyone group have access, notwithstanding the ACLs on the winreg key. This allows specific system functions, such as checking printer status, to work correctly regardless of how access is restricted via the winreg registry key. The default security on the AllowedPaths registry key grants only Administrators the ability to manage these paths. The AllowedPaths key, and its proper use, is documented in Microsoft Knowledge Base article Q155363.

Apply appropriate registry ACLs
Clean-installed Windows 2000 systems have secure default ACLs on the registry. However, upgrades from previous versions (e.g., Windows NT 4) do not modify the previous security settings and should have the default Windows 2000 settings applied. Refer to the to Default Access Control Settings in Windows 2000 document on the Microsoft TechNet Security Web site for details on the Windows 2000 registry ACLs and how to make any necessary modifications.

Restrict access to public Local Security Authority (LSA) information
You need to be able to identify all users on your system, so you should restrict anonymous users so that the amount of public information they can obtain about the LSA component of the Windows NT Security Subsystem is reduced. The LSA handles aspects of security administration on the local computer, including access and permissions. To implement this restriction, create and set the following registry entry:

Hive HKEY_LOCAL_MACHINE \SYSTEM
Key CurrentControlSet\Control\LSA
Value Name RestrictAnonymous
Type REG_DWORD
Value 1

Set stronger password policies
Use the Local Security Policy snap-in to strengthen the system policies for password acceptance. Microsoft suggests that you make the following changes:

- Set the minimum password length to at least 8 characters
- Set a minimum password age appropriate to your network (typically between 1 and 7 days)
- Set a maximum password age appropriate to your network (typically no more than 42 days)
- Set a password history maintenance (using the "Remember passwords" option) of at least 6
- Set account lockout policy

Windows 2000 includes an account lockout feature that will disable an account after an administrator-specified number of logon failures. For maximum security, enable lockout after 3 to 5 failed attempts, reset the count after not less than 30 minutes, and set the lockout duration to "Forever (until admin unlocks)". The Windows NT Server Resource Kit includes a tool that allows you to adjust some account properties that aren't accessible through the normal management tools. This tool, passprop.exe, allows you to lock out the administrator account:
The /adminlockout switch allows the administrator account to be locked out

Configure the Administrator account
Because the Administrator account is built in to every copy of Windows 2000, it presents a well-known objective for attackers. To make it more difficult to attack the Administrator account, do the following both for the local Administrator account on each computer:

- Rename the account to a nonobvious name (e.g., not "admin," "root," etc.)
- Establish a decoy account named "Administrator" with no privileges. Scan the event log regularly looking for attempts to use this account.
- Enable account lockout on the real Administrator accounts by using the passprop utility
- Disable the local computer's Administrator account.
- Remove all unnecessary file shares

All unnecessary file shares on the system should be removed to prevent possible information disclosure and to prevent malicious users from leveraging the shares as an entry to the local system.

Set appropriate ACLs on all necessary file shares
By default all users have Full Control permissions on newly created file shares. All shares that are required on the system should be ACL'd such that users have the appropriate share-level access (e.g., Everyone = Read). < /FONT >
Note The NTFS file system must be used to set ACLs on individual files in addition to share-level permissions.

Install antivirus software and updates
It is imperative to install antivirus software and keep up-to-date on the latest virus signatures on all Internet and intranet systems. More security antivirus information is available on the Microsoft TechNet Security Web site at:
www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/default.asp

Install the latest Service Pack
Each Service Pack for Windows includes all security fixes from previous Service Packs. Microsoft recommends that you keep up-to-date on Service Pack releases and install the correct Service Pack as soon as your operational circumstances allow. The current Service Pack for Windows 2000 is available at:
www.microsoft.com/windows2000/downloads/servicepacks
Service Packs are also available through Microsoft Product Support. Information about contacting Microsoft Product Support is available at http://support.microsoft.com/support/contact/default.asp.

Install the appropriate post-Service Pack security hotfixes. Microsoft issues security bulletins through its Security Notification Service .

Addition security settings
There are additional security features not covered in this document that should be leveraged when securing systems running Windows 2000. Information about these security features such as Encrypting File System (EFS), Kerberos, IPSEC, PKI, and IE security is available on the Microsoft TechNet Security Web site:
www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/wn2ksec.asp

60. Windows 2000 Server Baseline Security Checklist

This checklist outlines the steps you should take to secure computers running Windows 2000 Server either on their own or as part of a Windows NT or Windows 2000 domain. These steps apply to Windows 2000 Server and Windows 2000 Advanced Server.

Important The purpose of this checklist is to give instructions for configuring a baseline level of security with Windows 2000 Server computers. Security settings can be configured and applied to local servers through the Security Configuration Tool Set. Domain security policies can be created by using the Security Configuration Tool Set and distributed and applied through Group Policy. This guide outlines recommended security settings for Windows 2000. A step-by-step guide to configuring enterprise security policies using the Security Configuration Tool Set is located on the Microsoft TechNet Security Web site.

This checklist contains information about editing the registry. Before you edit the registry, make sure you understand how to restore it if a problem occurs. For information about how to do this, view the "Restoring the Registry" Help topic in Regedit.exe or the "Restoring a Registry Key" Help topic in Regedt32.exe.

Verify that all disk partitions are formatted with NTFS
NTFS partitions offer access controls and protections that aren't available with the FAT, FAT32, or FAT32x file systems. Make sure that all partitions on your server are formatted using NTFS. If necessary, use the convert utility to non-destructively convert your FAT partitions to NTFS.
Warning If you use the convert utility, it will set the ACLs for the converted drive to Everyone: Full Control. Use the fixacls.exe utility from the Windows NT Server Resource Kit to reset them to more reasonable values.

Verify that the Administrator account has a strong password
Windows 2000 allows passwords of up to 127 characters. In general, longer passwords are stronger than shorter ones, and passwords with several character types (letters, numbers, punctuation marks, and non-printing ASCII characters generated by using the ALT key and three-digit key codes on the numeric keypad) are stronger than alphabetic or alphanumeric-only passwords. For maximum protection, make sure the Administrator account password is at least nine characters long and that it includes at least one punctuation mark or non-printing ASCII character in the first seven characters. In addition, the Administrator account password should not be synchronized across multiple servers. Different passwords should be used on each server to raise the level of security in the workgroup or domain.

Disable unnecessary services
After installing Windows 2000 Server, you should disable any network services not required for the server role. In particular, you should consider whether your server needs any IIS components and whether it should be running the Server service for file and print sharing. You should also avoid installing applications on the server unless they are absolutely necessary to the server's function. For example, don't install e-mail clients, office productivity tools, or utilities that are not strictly required for the server to do its job.

Disable or delete unnecessary accounts
You should review the list of active accounts (for both users and applications) on the system in the Computer Management snap-in, and disable any non-active accounts, and delete accounts which are no longer required.

Protect files and directories
Clean-installed Windows 2000 systems have secure default ACLs on the file system. However, upgrades from previous versions (e.g., Windows NT 4) do not modify the previous security settings and should have the default Windows 2000 settings applied. Refer to Default Access Control Settings in Windows 2000 document on the Microsoft TechNet Security Web site for details on the default Windows 2000 file system ACLs and how to make any necessary modifications.

Make sure the Guest account is disabled
By default, the Guest account is disabled on systems running Windows 2000 Server. If the Guest account is enabled, disable it.
Protect the registry from anonymous access. The default permissions do not restrict remote access to the registry. Only administrators should have remote access to the registry, because the Windows 2000 registry editing tools support remote access by default. To restrict network access to the registry:

Add the following key to the registry:
HKEY_LOCAL_MACHINE \SYSTEM
Key \CurrentControlSet\Control\SecurePipeServers
Value Name \winreg

Select winreg, click the Security menu, and then click Permissions.
Set the Administrators permission to Full Control, make sure no other users or groups are listed, and then click OK.
The security permissions (ACLs) set on this key define which users or groups can connect to the system for remote registry access. In addition, the AllowedPaths subkey contains a list of keys to which members of the Everyone group have access, notwithstanding the ACLs on the winreg key. This allows specific system functions, such as checking printer status, to work correctly regardless of how access is restricted via the winreg registry key. The default security on the AllowedPaths registry key grants only Administrators the ability to manage these paths. The AllowedPaths key, and its proper use, is documented in Microsoft Knowledge Base article Q155363.

Apply appropriate registry ACLs

Clean-installed Windows 2000 systems have secure default ACLs on the registry. However, upgrades from previous versions (e.g., Windows NT 4) do not modify the previous security settings and should have the default Windows 2000 settings applied. Refer to to Default Access Control Settings in Windows 2000 document on the Microsoft TechNet Security Web site for details on the default Windows 2000 registry ACLs and how to make any necessary modifications.

Restrict access to public Local Security Authority (LSA) information
You need to be able to identify all users on your system, so you should restrict anonymous users so that the amount of public information they can obtain about the LSA component of the Windows NT Security Subsystem is reduced. The LSA handles aspects of security administration on the local computer, including access and permissions. To implement this restriction, create and set the following registry entry:

Hive HKEY_LOCAL_MACHINE \SYSTEM
Key CurrentControlSet\Control\LSA
Value Name RestrictAnonymous
Type REG_DWORD
Value 1

Set stronger password policies
Use the Domain Security Policy (or Local Security Policy) snap-in to strengthen the system policies for password acceptance. Microsoft suggests that you make the following changes:

Set the minimum password length to at least 8 characters
Set a minimum password age appropriate to your network (typically between 1 and 7 days)
Set a maximum password age appropriate to your network (typically no more than 42 days)
Set a password history maintenance (using the "Remember passwords" option) of at least 6
Set account lockout policy

Windows 2000 includes an account lockout feature that will disable an account after an administrator-specified number of logon failures. For maximum security, enable lockout after 3 to 5 failed attempts, reset the count after not less than 30 minutes, and set the lockout duration to "Forever (until admin unlocks)." The Windows NT Server Resource Kit includes a tool that allows you to adjust some account properties that aren't accessible through the normal management tools. This tool, passprop.exe, allows you to lock out the administrator account:
The /adminlockout switch allows the administrator account to be locked out

Configure the Administrator account
Because the Administrator account is built in to every copy of Windows 2000, it presents a well-known objective for attackers. To make it more difficult to attack the Administrator account, do the following both for the domain Administrator account and the local Administrator account on each server:

Rename the account to a nonobvious name (e.g., not "admin," "root," etc.)
Establish a decoy account named "Administrator" with no privileges. Scan the event log regularly looking for attempts to use this account. Enable account lockout on the real Administrator accounts by using the passprop utility
Disable the local computer's Administrator account.

Remove all unnecessary file shares
All unnecessary file shares on the system should be removed to prevent possible information disclosure and to prevent malicious users from using the shares as an entry to the local system.

Set appropriate ACLs on all necessary file shares
By default all users have Full Control permissions on newly created file shares. All shares that are required on the system should be ACL'd such that users have the appropriate share-level access (e.g., Everyone = Read).
Note The NTFS file system must be used to set ACLs on individual files in addition to share-level permissions.

Install antivirus software and updates
It is imperative to install antivirus software and keep up-to-date on the latest virus signatures on all Internet and intranet systems. More security antivirus information is available on the Microsoft TechNet Security Web site.

Install the latest Service Pack
Each Service Pack for Windows includes all security fixes from previous Service Packs. Microsoft recommends that you keep up-to-date on Service Pack releases and install the correct Service Pack for your servers as soon as your operational circumstances allow. The current Service Pack for Windows 2000, SP2, is available on the Microsoft Web site. Service Packs are also available through Microsoft Product Support. Information about contacting Microsoft Product Support is available on the Microsoft Web site.

Install the appropriate post-Service Pack security hotfixes
Microsoft issues security bulletins through its Security Notification Service. When these bulletins recommend installation of a security hotfix, you should immediately download and install the hotfix on your member servers.

Additional security settings
There are additional security features not covered in this document that should be leveraged when securing servers running Windows 2000. Information about these security features such as Encrypting File System (EFS), Kerberos, IPSEC, PKI, and IE security is available on the Microsoft TechNet Security Web site.

61. Windows XP Baseline Security Checklist
Important The purpose of these checklists is to give instructions for configuring a baseline level of security on Windows XP computers. This guide does not provide a complete list of all security features provided in Windows XP, or how to use them. These checklists contain information about editing the registry. Before you edit the registry, make sure you understand how to restore it if a problem occurs. For information about how to do this, see online Help for Registry Editor.

Windows XP Home Edition Configuration Checklist Details
- Verify that all disk partitions are formatted with NTFS
- Protect file shares
- Use Internet Connection Sharing for shared Internet connections
- Enable Internet Connection Firewall
- Use account passwords
- Use the "Make Private" feature
- Install anti-virus software and updates
- Keep up-to-date on the latest security updates

Windows XP Professional Configuration Checklist Details
- Verify that all disk partitions are formatted with NTFS
- Protect file shares
- Use Internet Connection Sharing for shared Internet connections
- Enable Internet Connection Firewall
- Use software restriction policies
- Use account passwords
- Disable unnecessary services
- Disable or delete unnecessary accounts
- Make sure the Guest account is disabled
- Set stronger password policies
- Set account lockout policy
- Install anti-virus software and updates
- Keep up-to-date on the latest security updates

XP HOME EDITION CHECKLIST

Verify that all disk partitions are formatted with NTFS
NTFS partitions offer access controls and protections that aren't available with the FAT, FAT32, or FAT32x file systems. Make sure that all partitions on your computer are formatted using NTFS. If necessary, use the Convert utility to non-destructively convert your FAT partitions to NTFS.

Protect file shares
Windows XP Home Edition uses a network access model called "Simple File Sharing," where all attempts to log on to the computer from across the network will be forced to use the Guest account. This means that network access through Server Message Block (SMB, used for file and print access), as well as Remote Procedure Call (RPC, used by most remote management tools and remote registry access) will only be available to the Guest account.

In the Simple File Sharing model, file shares can be created so that access from the network is read-only, or access from the network is able to read, create, change, and delete files. Simple File Sharing is intended for use on a home network and behind a firewall, such as the one provided by Windows XP. If you are connected to the Internet, and are not operating behind a firewall, you should remember that any file shares you create might be accessible to any user on the Internet.

Use Internet Connection Sharing (ICS) for shared Internet connections
Windows XP provides the ability to share a single Internet connection with multiple computers on a home or small business network through the ICS feature. One computer, called the ICS host, connects directly to the Internet and shares its connection with the rest of the computers on the network. The client computers rely on the ICS host computer to provide access to the Internet. Security is enhanced when ICS is enabled because only the ICS host computer is visible to the Internet.

To enable ICS, right-click an Internet connection in Network Connections, click Properties, click the Advanced tab, and then select the appropriate check box. You can also configure ICS by using the Home Networking Wizard. For more information about ICS, see Help and Support Center in Windows XP.

Enable Internet Connection Firewall (ICF)
Designed for use in the home or small business, Internet Connection Firewall (ICF) provides protection for Windows XP computers that are directly connected to the Internet, or for the computers or devices connected to the Internet Connection Sharing host computer that is running ICF. The Windows XP ICF makes use of active packet filtering, which means that ports on the firewall are dynamically opened only for as long as necessary to enable you to access the services you're interested in.

To enable ICF, right-click an Internet connection in Network Connections, click Properties, click the Advanced tab, and then select the appropriate check box. You can also configure ICF by using the Home Networking Wizard. For more information about ICF, see Help and Support Center in Windows XP.

Use account passwords
Passwords should be assigned to individual accounts on Windows XP Home Edition computers that are accessed by multiple people who want to protect their data from each other. Windows XP home users get separate but accessible file storage by default, with optional password protection. When you create a password for yourself, Windows offers to lock down your "My Documents" folder, as well as any subfolders. That way, if you have a password and want privacy, you will be protected from other non-administrator users of the computer. Assigning account passwords will also prevent anyone from simply walking up to the computer and using it.

Use the "Make Private" feature
In the simple file sharing model, Windows does not directly expose the complexity of managing file access control lists to the user. Instead, the user interface features an option called "make private" which, when selected for a folder, will modify the underlying access control for that folder so that other non-administrative users cannot access it. This feature only works if the file system is NTFS.

Install anti-virus software and updates

One of the most important things for protecting systems is to use anti-virus software, and ensure that it is kept up-to-date. All systems on the Internet, a corporate Intranet, or a home network should have anti-virus software installed. More security anti-virus information is available on the Microsoft TechNet Security Web Site.

Keep up-to-date on the latest security updates
The Auto Update feature in Windows XP can automatically detect and download the latest security fixes from Microsoft. Auto Update can be configured to automatically download fixes in the background and then prompt the user to install them once the download is complete. To configure Auto Update, click System in Control Panel and select the Automatic Updates tab. Choose the first notification setting to download the updates automatically and receive notification when they are ready to be installed. Additionally, Microsoft issues security bulletins through its Security Notification Service. These bulletins are issued for any Microsoft product that is found to have a security issue. When these bulletins recommend installation of a security hotfix, you should immediately download and install the hotfix on your computers.

XP PRO CHECKLIST

Verify that all disk partitions are formatted with NTFS
Verify that all disk partitions are formatted with NTFS. NTFS partitions offer access controls and protections that aren't available with the FAT, FAT32, or FAT32x file systems. Make sure that all partitions on your computer are formatted using NTFS. If necessary, use the Convert utility to non-destructively convert your FAT partitions to NTFS.

Protect file shares
By default, Windows XP Professional systems that are not connected to a domain use a network access model called "Simple File Sharing," where all attempts to log on to the computer from across the network will be forced to use the Guest account. This means that network access through Server Message Block (SMB, used for file and print access), as well as Remote Procedure Call (RPC, used by most remote management tools and remote registry access) will only be available to the Guest account.

In the Simple File Sharing model, file shares can be created so that access from the network is read-only, or access from the network is able to read, create, change, and delete files. Simple File Sharing is intended for use on a home network and behind a firewall, such as the one provided by Windows XP. If you are connected to the Internet, and are not operating behind a firewall, you should remember that any file shares you create might be accessible to any user on the Internet.

The Classic security model is used if your Windows XP computer is joined to a domain, or if Simple File Sharing is disabled. In the Classic security model, users who attempt to log on to the local computer from across the network must authenticate as themselves, and are not mapped to the Guest account. File shares should be created so that access from the network is only granted to the appropriate groups and/or individual users.

Use Internet Connection Sharing (ICS) for shared Internet connections
Windows XP provides the ability to share a single Internet connection with multiple computers on a home or small business network through the ICS feature. One computer, called the ICS host, connects directly to the Internet and shares its connection with the rest of the computers on the network. The client computers rely on the ICS host computer to provide access to the Internet. Security is enhanced when ICS is enabled because only the ICS host computer is visible to the Internet.

To enable ICS, right-click an Internet connection in Network Connections, click Properties, click the Advanced tab, and then select the appropriate check box. You can also configure ICS by using the Home Networking Wizard. For more information about ICS, see Help and Support Center in Windows XP.

Enable Internet Connection Firewall (ICF)
Designed for use in the home or small business, ICF provides protection for Windows XP computers that are directly connected to the Internet, or for the computers or devices connected to the Internet Connection Sharing host computer that is running ICF. The Windows XP ICF makes use of active packet filtering, which means that ports on the firewall are dynamically opened only for as long as necessary to enable you to access the services you're interested in.

To enable ICF, right-click an Internet connection in Network Connections, click Properties, click the Advanced tab, and then select the appropriate check box. You can also configure ICF by using the Home Networking Wizard. For more information about ICF, see Help and Support Center in Windows XP.

Use software restriction policies
Software restriction policies provide administrators with a policy driven mechanism that identifies software running in their domain, and controls the ability of that software to run. Using a software restriction policy, an administrator can prevent unwanted programs from running; this includes viruses and Trojan horses, or other software that is known to cause conflicts when installed. Software restriction policies can be used on a standalone computer by configuring the local security policy. Software restriction policies also integrate with Group Policy and Active Directory.

For details on creating software restriction policies, refer to the What's New in Security for Windows XP Professional and Windows XP Home Edition white paper.

Use account passwords
To protect users who do not password-protect their accounts, Windows XP Professional accounts without passwords can only be used to log on at the physical computer console. By default, accounts with blank passwords can no longer be used to log on to the computer remotely over the network, or for any other logon activity except at the main physical console logon screen. For example, you cannot use the secondary logon service (RunAs) to start a program as a local user with a blank password.

Assigning a password to a local account removes the restriction that prevents logging on over a network. It also permits that account to access any resources it is authorized to access, even over a network connection. As a result, it is better to leave a blank password assigned to an account rather than assigning a weak, easily guessed password. When assigning account passwords, make sure the password is at least nine characters long and that it includes at least one punctuation mark or non-printing ASCII character within the first seven characters.

Caution If your computer is not in a physically secured location, it is recommended that you assign passwords to all local user accounts. Failure to do so allows anyone with physical access to the computer to easily log on using an account that does not have a password. This is especially important for portable computers, which should always have strong passwords on all local user accounts.

Note This restriction does not apply to domain accounts. It also does not apply to the local Guest account. If the Guest account is enabled and has a blank password, it will be permitted to log on and access any resource authorized for access by the Guest account. If you want to disable the restriction against logging on to the network without a password, you can do so through Local Security Policy.

Disable unnecessary services
After installing Windows XP, you should disable any network services not required for the computer. In particular, you should consider whether your computer needs any IIS Web services. By default, IIS is not installed as part of Windows XP and should only be installed if its services are specifically required.

Disable or delete unnecessary accounts
You should review the list of active accounts (for both users and programs) on the system in the Computer Management snap-in. Disable any non-active accounts and delete any accounts which are no longer required.

Make sure the Guest account is disabled
This setting recommendation only applies to Windows XP Professional computers that belong to a domain, or to computers that do not use the Simple File Sharing model.

On Windows XP Professional systems that are not connected to a domain, users who attempt to log on from across the network will be forced to use the Guest account by default. This change is designed to prevent hackers attempting to access a system across the Internet from logging on by using a local Administrator account that has no password. To use this feature, which is part of the Simple File Sharing model, the Guest account must be enabled on all Windows XP computers that are not joined to a domain. For those computers that are joined to a domain, or for unjoined computers that have turned off the Simple File Sharing model, the Guest account should be disabled. This will prevent users attempting to log on to the computer from across the network from using the Guest account.

Set stronger password policies
To protect users who do not password-protect their accounts, Windows XP Professional accounts without passwords can only be used to log on at the physical computer console. By default, accounts with blank passwords can no longer be used to log on to the computer remotely over the network, or for any other logon activity except at the main physical console logon screen. Note This restriction does not apply to domain accounts. It also does not apply to the local Guest account. If the Guest account is enabled and has a blank password, it will be permitted to log on and access any resource authorized for access by the Guest account.

Use the Local Security Policy snap-in to strengthen the system policies for password acceptance. Microsoft suggests that you make the following changes:

- Set the minimum password length to at least 8 characters
- Set a minimum password age appropriate to your network (typically between 1 and 7 days)
- Set a maximum password age appropriate to your network (typically no more than 42 days)
- Set a password history maintenance (using the "Remember passwords" radio button) of at least 6
- Set account lockout policy

Windows XP includes an account lockout feature that will disable an account after an administrator-specified number of logon failures. For example, enable local account lockout after 5-10 failed attempts, reset the count after not less than 30 minutes, and set the lockout duration to "Forever (until admin unlocks)". If that's too aggressive, consider permitting the account to automatically unlock after a certain period of time.

There are two common goals for using account lockout: one is to make it obvious that multiple attempts have been made to log on to a user account with an invalid password; the second is to protect accounts from attempts to guess a password by dictionary attacks, or iterative guessing. There is no one correct setting here that will apply to all environments. Consider reasonable settings for your environment.

Install anti-virus software and updates
One of the most important things for protecting systems is to use anti-virus software, and ensure that it is kept up-to-date. All systems on the Internet, a corporate Intranet, or a home network should have anti-virus software installed. More security anti-virus information is available on the Microsoft TechNet Security Web Site.

Keep up-to-date on the latest security updates
The Auto Update feature in Windows XP can automatically detect and download the latest security fixes from Microsoft. Auto Update can be configured to automatically download fixes in the background and then prompt the user to install them once the download is complete. To configure Auto Update, click System in Control Panel and select the Automatic Updates tab. Choose the first notification setting to download the updates automatically and receive notification when they are ready to be installed.

62. Internet Explorer Security Checklist
This checklist outlines basic security measures for Internet Explorer version 5.01 Service Pack 2 or later.

- Verify that you are running a 128-bit browser
- On the Tools menu, click Internet Options, and then click the Security tab.
  Verify that your security zones are set to their default levels.
- On the Tools menu, click Internet Options, and then click the Advanced tab.
  Verify that your Advanced settings are set to their default levels.
- Be sure to visit Windows Update regularly for new security updates

To configure security zone settings:

- On the Tools menu of Internet Explorer, click Internet Options, and then click the Security tab.
- Click a security zone to select it and view its current settings.
- Change the following settings as necessary:
- Security Level. To change the security level for the selected zone to High, Medium, Medium-low, or Low, move the slider. The on-screen description for each level can help you decide which level to select.
Sites. To add or remove Web sites from the zone, click the Sites button, and then click the Add or Remove button to customize your list of sites for the selected zone.

Custom Level. For more precise control of your security settings, click the Custom Level button, and then select the options you want. For more detailed instructions, please see Setting up Security Zones.

63. Be Paranoid
Don't panic, but be paranoid all the time. Take every security concern or oddball alert seriously.

SECURING INTERNET INFORMATION SERVER (IIS)

1. Get these tools
MS IIS lockdown tool
Microsoft has released a new security tool that makes it simple to secure an IIS 4.0 or 5.0 web server. The tool, known as the IIS Lockdown Tool, allows web servers to quickly and easily be put into the right configuration - in which the server provides all of the services the administrator wants to provide, and no others. Customers can use this tool to instantly protect their systems against security threats that target web servers.

The tool offers two operating modes. The default is Express Lockdown which, with a single mouse click, configures the server in a highly secure way that is appropriate for most basic web servers. For administrators who want to pick and choose the technologies that will be enabled on the server, the tool offers an Advanced Lockdown mode. A comprehensive help system provides information and recommendations for selecting the best configuration, and an undo facility allows the most recent lockdown to be reversed.

Wondering whether it's worth the time to use the tool? Consider this: a web server configured using the Express Lockdown would be completely protected against Code Red and virtually all known security vulnerabilities affecting IIS 4.0 and 5.0 - even without the patches for these vulnerabilities. I do, of course, recommend that all customers, even those running locked-down servers, continue to stay current on all security patches, but this vividly illustrates the value of the tool.
http://search.microsoft.com/

Urlscan Security Tool
Urlscan is a powerful security tool that works in conjunction with the IIS Lockdown Tool to give IIS Web site administrators the ability to turn off unneeded features and restrict the kind of HTTP requests that the server will process. By blocking specific HTTP requests, the Urlscan security tool prevents potentially harmful requests from reaching the server and causing damage.
www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/urlscan.asp

2. Set appropriate ACLs on virtual directories
Although this procedure is somewhat application-dependent, some rules of thumb apply:

File Type	Access Control Lists
CGI (.exe, .dll, .cmd, .pl)	Everyone (X) Administrators (Full Control) System (Full Control)
Script files (.asp)	Everyone (X) Administrators (Full Control) System (Full Control)
Include files (.inc, .shtm, .shtml)	Everyone (X) Administrators (Full Control) System (Full Control)
Static content (.txt, .gif, .jpg, .html)	Everyone (R) Administrators (Full Control) System (Full Control)

3. Recommended default ACLs by file type
Rather than setting ACLs on each file, you are better off creating new directories for each file type, setting ACLs on the directory, and allowing the ACLs to inherit to the files. For example, a directory structure might look like this:

C:\inetpub\wwwroot\myserver\static (.html)
C:\inetpub\wwwroot\myserver\include (.inc)
C:\inetpub\wwwroot\myserver\script (.asp)
C:\inetpub\wwwroot\myserver\executable (.dll)
C:\inetpub\wwwroot\myserver\images (.gif, .jpeg)
Also, be aware that two directories need special attention:

C:\inetpub\ftproot (FTP server)
C:\inetpub\mailroot (SMTP server)
The ACLs on both these directories are Everyone (Full Control) and should be overridden with something tighter, depending on your level of functionality. Place the folder on a different volume than the IIS server if you're going to support Everyone (Write), or use Windows 2000 disk quotas to limit the amount data that can be written to these directories.

4. Set appropriate IIS Log file ACLs
Make sure the ACLs on the IIS-generated log files (%systemroot%\system32\LogFiles) are:

Administrators (Full Control)
System (Full Control)
Everyone (RWC)
This is to help prevent malicious users from deleting the files to cover their tracks.

5. Enable logging
Logging is paramount when you want to determine whether your server is being attacked. You should use W3C Extended Logging format by following this procedure:

Load the Internet Information Services tool.
Right-click the site in question, and choose Properties from the context menu.
Click the Web Site tab.
Check the Enable Logging check box.
Choose W3C Extended Log File Format from the Active Log Format drop-down list.
Click Properties.
Click the Extended Properties tab, and set the following properties:

Client IP Address
User Name
Method
URI Stem
HTTP Status
Win32 Status
User Agent
Server IP Address
Server Port

The latter two properties are useful only if you host multiple Web servers on a single computer. The Win32 Status property is useful for debugging purposes. When you examine the log, look out for error 5, which means access denied. You can find out what other Win32 errors mean by entering net helpmsg err on the command line, where err is the error number you are interested in.

6. Disable or Remove All Sample Applications
Samples are just that, samples; they are not installed by default and should never be installed on a production server. Note that some samples install so that they can be accessed only from http://localhost, or 127.0.0.1; however, they should still be removed. The following lists the default locations for some of the samples.

Sample	Virtual Directory	Location
IIS Samples	\IISSamples	c:\inetpub\iissamples
IIS Documentation	\IISHelp	c:\winnt\help\iishelp
Data Access	\MSADC	c:\program files\common files\system\msadc

- Remove the IISADMPWD Virtual Directory
This directory allows you to reset Windows NT and Windows 2000 passwords. It is designed primarily for intranet scenarios and is not installed as part of IIS 5, but it is not removed when an IIS 4 server is upgraded to IIS 5. It should be removed if you don't use an intranet or if you connect the server to the Web. Refer to Microsoft Knowledge Base article Q184619 for more information about this functionality.

- Remove Unused Script Mappings
IIS is preconfigured to support common filename extensions such as .asp and .shtm files. When IIS receives a request for a file of one of these types, the call is handled by a DLL. If you don't use some of these extensions or functionality, you should remove the mappings by following this procedure:

- Open Internet Services Manager.
- Right-click the Web server, and choose Properties.
- Click Master Properties
- Select WWW Service, click Edit, click HomeDirectory, and then click Configuration
- Remove these references:

If you don't use...	Remove this entry:
Web-based password reset	.htr
Internet Database Connector (all IIS 5 Web sites should use ADO or similar technology)	.idc
Server-side Includes	.stm, .shtm, and .shtml
Internet Printing	.printer
Index Server	.htw, .ida and .idq

Note Internet Printing can be configured through Group Policy as well as via the Internet Services Manager. If there is a conflict between the Group Policy settings and those in the Internet Service Manager, the Group Policy settings take precedence. If you remove Internet Printing via the Internet Services Manager, be sure to verify that it won't be re-enabled by either local or domain group policies. (The default Group Policy neither enables nor disables Internet Printing.) In the MMC Group Policy snap-in, click Computer Configuration, click Administrative Templates, click Printing, and then click Web-based Printing.

Note Unless you have a mission-critical reason to use the .htr functionality, you should remove the .htr extension.

CHAPTER [7]

A FEW USEFUL PROGRAMS I RECOMMEND

Also check out Axcels excellent software essentials at http://members.aol.com/axcel216/toy.htm

3d Mark 2002 **- www.madonion.com**
Quite simply the best benchmarking software for testing out your 3d graphics card

Agent **- www.forteinc.com**
Very good news program. I use it for email also but is limited until V2 comes out that is. Definitely get rid of Outlook from your computer and use this or Eudora or Pegasus for email.

AS Pack **- www.aspack.com**
is an advanced executable file compressor, capable of reducing the file size of 32-bit Windows programs by as much as 70%. ASPack makes Windows 95/98/NT programs and libraries smaller, and hence faster to both load and download.

Boot Log Analyzer **- www.vision4.dial.pipex.com**
For Windows 9x/ME checks/reports on slow loading/failed drivers

Cacheman **- www.outertech.com**
Tunes Windows cache settings - very good and highly recommended.
Also frees up Ram and tunes various system settings. Excellent.

Catch Up **- http://catchup.cnet.com**
Great free service that informs you of latest updates to your programs.

CleanSys **- www.theabsolute.net/sware/index.html#clnsys**
Does an indepth search of your system drive for references to dll's that are not needed.

CloneCD **- www.elby.org/english/corp/index.htm**
Copies many hard to copy CD's

Copernic Pro **- www.copernic.com**
Best search program for the internet there is! - queries multiple search engines at once.

Desktool **- www.metaproducts.com/**
Good toolbar/menu program.

Dreamweaver **- www.macromedia.com**
The best web design software there is.

DriveImage Pro **- www.powerquest.com**
The best program to image and backup many computers.

FileMon **- www.sysinternals.com**
This company does some of the most useful programs there are for the PC. Check out their website ! This program monitors live file changes but at a very low level.

FTP Voyager **- www.rhinosoft.com**
Very powerful FTP program.

Genius **- www.indiesoft.com**
Like a swiss army knife of extremely useful programs. Excellent program.

Icon Packager **- www.stardock.com**
Great program for changing your icons. Also check out Windows Blinds once you're there.

Internet Explorer **- www.microsoft.com/downloads/search.asp**
The latest and the best internet browser from Microsoft.

Irfanview **- http://stud1.tuwien.ac.at/~e9227474/**
The best + fastest Windows graphics viewer, editor + conversion Tool: supports all popular graphic, icon, cursor, audio and video file formats.

MBR Work **- www.terabyteunlimited.com**
Does everything you need to backup etc your Master Boot Record.

Microsoft TweakUI
www.microsoft.com/ntworkstation/downloads/PowerToys/Networking/NTTweakUI.asp
Tweaks various settings that are hidden away in the registry.

Nero **- www.ahead.de**
Good CD/DVD recording package available.

Offline Explorer **- www.metaproducts.com**
Excellent web downloader for downloading whole websites.

Ontrack Data Advisor **- www.ontrack.com/dataadvisor**
Hard disk low level diagnostic and recovery tool.

Opera **- www.opera.com**
Fastest web browser I've seen and very good !

Partition Magic **- www.powerquest.com**
Quite simply the best hard drive partitioning software ever.

Photoshop **- www.adobe.com**
Without doubt the best editing program for for design but expensive.
Also try Photoshop Elements which is a lot better than Paintshop Pro !

Power DVD **- www.cyberlink.com**
Good DVD playback software.

RegGuide **- www.regedit.com**
Excellent guide on the registry, the tweaking of hundreds of various components etc.

RegMon **- www.sysinternals.com**
This program monitors live changes to the registry.

Resource Hacker **- http://rpi.net.au/~ajohnson/resourcehacker**
Great - lets you change virtually anything in programs.

Restorator **- www.bome.com/Restorator**
Like Reource Hacker but not free.

RoboForm **- www.roboform.com**
Fills in boring repetitive forms for you on web pages. Very handy.

RTVReco **- www.clearlight.com/~rtvsoft**
There's nothing more than I hate most and that is the same requester messages flashing up time and time again. This beauty of a program will click them for you!

SecondCopy 2000 **- www.centered.com**
Clones one drive to another at specified times. Very configurable.

SiSoftSandra Pro **- www.sisoftware.co.uk/sandra/**
The best system analyser and benchmark software that I've seen.

Star Office **- www.sun.com/products/staroffice/**
In my view far better than MS Office.

System Mechanic **- www.iolo.com**
Another excellent cleanup program that I highly recommend.

System Restore Remover ME **- http://defsoft.iwarp.com**
Remove system restore from Millennium and gain performance.

System Sentry **- www.easydesksoftware.com**
Comparison of System against OS's original files.

Ultra Edit **- www.ultraedit.com**
Very powerful and easy to use text/html/binary etc edit

VNC **- www.uk.research.att.com/vnc/winvnc.html**
Excellent free program to remotely control another computer. Available on a lot of platforms. Excellent!

Winrar **- www.**
Good compression program.

Winzip **- www.winzip.com**
Good compression program.

Xen, XenTweak etc **- www.x9000.net**
Cleanup, backup, restore and tweaking programs.

XN View **- www.xnview.com/**
Graphics viewer, editor + conversion tool

X-Setup **- www.xteq.com**
Last but certainly not least ! Xteq X-Setup is the mother in ultimate system configuration and tweaking. Highly recommended.

SECURITY PROGRAMS I RECOMMEND

Ad Aware **- www.lavasoft.de**
A good Internet spyware detection and removal program.

Advanced Admin Tools **- www.glocksoft.com**
Good toolkit but not as good as Net Scan Tools.

Analog X Tools **- www.analogx.com/contents/news.htm**
Wide range of tools and utilities and free.

AVG Antivirus **- www.grisoft.com**
Good virus checker and free for personal use !

BigFix **- www.bigfix.com**
Checks your files and notifies of updates and security patches - great and free !

Hook Protect
www.geocities.com/SiliconValley/Hills/8839/hookprot.html
Detects programs that infringe the privacy and confidentiality on personal computers
e.g. keyloggers, interceptors, spys, trojans etc.

NeoTrace **- www.neoworx.com**
Useful to use in conjunction with a firewall program to find hackers etc. Also good diagnostic tool.

NetScanTools **- www.nwpsw.com/index.html**
The best suite of networking and internet tools on the PC.

Pretty Good Privacy **- www.pgp.com**
Excellent suite of programs that will encrypt your data. Author of this program Phil Zimmerman nearly went to prison because PGP was exported outside of the states and anything other a certain bit range on encryption in the states, is classified as a weapon.

Registry Run Guard **- www.geocities.com/SiliconValley/Hills/8839/pcguar.html**
Will inform you if anything has put itself into your startup groups.

SecurityGuide **- www.regedit.com**
Excellent guide on the registry and security.

Webtrend Security Tools **- www.webtrends.com**
Superb analysis Tools for analysing your logfiles etc

I am still updating the above list of programs.

CHAPTER [8]

INTERNET TWEAKING SITES

General

3dSpotlight	http://www.3dspotlight.com/
911networks	www.911networks.com/
98lite	www.98lite.net/
ActiveWin	http://activewin.com/
Ars Technica	www.arstechnica.com/
Axcel	http://members.aol.com/axcel216/
Bill James Tweaks	www.billsway.com/notes_public/
Bob Cerelli	www.onecomputerguy.com/
Cyberwizard Pit	www.cyberwizardpit.com/
Digital Dimensions	www.maxknightx.dd.btinternet.co.uk/ddx.htm
Dougs Tweaks	http://people.ne.mediaone.net/dbknox/
Eshelman	www.aumha.org/

Extreme Tech	www.extremetech.com
Fix It Windows	www.fixwindows.com/
Franks Windows	www.worldowindows.com/
Guru3d	www.guru3d.com/
Langalist	www.langa.com/
Lockergnome	http://virtualgraphicsworld.freeservers.com/lockergnome.htm
NeoWin	www.neowin.net/
NT Compatbile	www.ntcompatible.com/
NV News	www.nvnews.net/
Object Desktop	www.stardock.com/products/odnt/index.html
PC Mechanic	www.pcmech.com/
PCForrest	www.pcforrest.freeserve.co.uk/
Powertools	http://home.att.net/~r.rizun/
PurePerformance.com	www.pureperformance.com/
Reactor Critical	www.reactorcritical.com/
RegEdit	www.regedit.com/downloads/
Shell Extension City	http://shellcity.net/
Speed Demonz	www.rojakpot.com/Speed_Demonz.htm
SpeedGuide.net	www.speedguide.net/index.shtml
Speedy3d	www.speedy3d.com/
The-Ctrl-Alt-Del	www.the-ctrl-alt-del.com/
Tweak3D.net	www.tweak3d.net/
Tweak Central	http://tweakcentral.com/files.htm
TweakTown	www.tweaktown.com/
Virtual Plastic	www.virtualplastic.net/
VR Zone	www.vr-zone.com/
Winguides Support Forums	http://forums.winguides.com/
WinOScentral	www.winoscentral.com/
WinPlanet	www.winplanet.com/winplanet/
WSNine	http://users.bigpond.net.au/thomps/cgmt/
Xteq	www.xteq.com

NT/2000

2000 FAQ	www.windows2000faq.com/
Focuson2000	http://windows2000.about.com/compute/windows2000/mbody.htm
JSI Inc's Reghacks	www.jsiinc.com/reghack.htm
NT Toolbox	www.nttoolbox.com/
Tech Tips	www.ntpro.org/files/techtips.html
Tweak NT	http://arstechnica.com/tweak/nt/index.html
Waynes	http://is-it-true.org/nt/index.shtml
Win2000 Tips	http://win2000tips.home.att.net/
Win2000	http://web.ukonline.co.uk/cook/Win2000.htm
Windows 2000 Hints	www.rojakpot.com/Other_Articles/Win2K_Tips/Win2k_Tips.htm
Zdnet 2000	www.zdnet.com/zdhelp/filters/windows2000/

XP

AccessXP Max Programming	www.maxprogramming.com/windows/
Beta Elite	www.ibelite.com/
Paul Thurrott's SuperSite	www.winsupersite.com/
Microsoft XP HowTo	www.microsoft.com/windowsxp/pro/using/howto/
Microsoft XP Expert Zone	www.microsoft.com/windowsxp/expertzone/default.asp
Tweak XP	www.totalidea.de/
Welcome to WinBeta	http://winbeta.cjb.net/
WinXP Exchange	http://winxp.n3.net/
WinXP World	www.winxpworld.com/downloads.shtml
Wxperience.com	www.wxperience.com/
Xeons Windows XP Centre	http://winxp.descrypt.com/
XP Powered	http://xp.modrica.com/

Benchmarks

3d mark 2001	www.madonion.com/download/
Dslreports.com	www.dslreports.com
High Speed Speedtest	http://speedtest.mybc.com/
Ntlworld Test	http://homepage.ntlworld.com/dgilbert/testpage.htm
Roadrunner Bandwidth	www.houston.rr.com/speed/speed2.asp?total=18.01
SpeedGuide TCP-IP Analyzer	http://forums.speedguide.net
Text Test	http://performance.toast.net/text2.htm?979653416160
Ziff Davis Benchmarks	http://etestinglabs.com/benchmarks/default.asp

INTERNET OVERCLOCKING/HARDWARE/TWEAKING SITES

_Overclock.co.uk	www.overclock.co.uk/
_Overclockers.co.uk	www.overclockers.co.uk/
_Overclockingstore.co.uk	www.theoverclockingstore.co.uk/
_Quietpc.com	www.quietpc.com/

_RipNet UK	www.ripnet-uk.com/
_Virtual Hideout	www.virtualhideout.net/
3d Cool	www.3dcool.com/
AMD Motherboard.com	www.amdmb.com/
Apus Hardware	www.apushardware.com/
Athlon OC	www.athlonoc.com/
Bit Tech UK	www.bit-tech.net/
Blu Screen of Deth	www.bluescreenofdeth.net/
BXBoards	www.bxboards.com/
Club Overclocker	www.cluboverclocker.com/
Dangerous Dog	www.dangerousdog.com/
DreddNews	www.dreddnews.com/
Extreme Overclocking	www.extremeoverclocking.com/
Firing Squad	http://firingsquad.gamers.com/
Geek News	www.geeknews.net/
Hardware Extreme	www.hwextreme.com/
Hardware One	www.hardware-one.com/
Hard OCP	http://hardocp.com/
Heatsink Guide	www.heatsink-guide.com/
Hexus	www.hexus.net/
HighSpeed PC	www.highspeedpc.com/
HotHardware.com	www.hothardware.com/
I am not a geek	www.iamnotageek.com/
Legion	www.legionhardware.com/
M3d Zone	www.m3dzone.com/
Modding Zone	www.moddingzone.com/
Motherboards.org	www.motherboards.org/
OC Addiction	www.ocaddiction.com/
OCtools	www.octools.com/
OCWorkBench	www.ocworkbench.com/
Otheos's site!!!	www.otheos.clara.net/
Overclockers Cafe	www.overclockercafe.com/
Overclockers Shootout	www.ocshoot.com/
Overclockers.com	www.overclockers.com/
Overclockin.com	www.overclockin.com/
Overclocking.dk	www.overclocking.dk/
PC Mechanic	www.pcmech.com/
PC Snoop	www.pcscoop.com/
Savagezone	www.savagezone.net/
Spode's Abode	www.spodesabode.com/
SysOpt.com	www.sysopt.com/
System Internals	www.sysinternals.com/
Tech Extreme	www.techextreme.com/
Tom's Hardware	www.tomshardware.com/
Tweakers Asylum	www.tweakersasylum.com/
TweakMax	www.tweakmax.com/
Via Abit FAQ	www.viahardware.com/faq/kt7/kt7faq.htm]
Via Hardware	www.viahardware.com/
Void Your Warranty	www.voidyourwarranty.net/
Warp2Search	www.warp2search.net
ZZZ Online	http://zzz.com.ru/

Usenet Groups for Overclocking and Hardware Discussion

Usenet FAQ's	www.faqs.org/faqs/
Overclocking	alt.comp.hardware.overclocking
Overclocking AMD	alt.comp.hardware.overclocking.amd
Homebuilt PCs	alt.comp.hardware.homebuilt
Homebuilt PCs	alt.comp.hardware.pc-homebuilt
ABIT Motherboards	alt.comp.periphs.mainboard.abit
ASUS Motherboards	alt.comp.periphs.mainboard.asus
Nvidia Gfx Cards	alt.comp.periphs.videocards.nvidia
Hardware Discussion	comp.sys.ibm.pc.hardware.chips

Customisation

_Customize.org	www.customize.org/
_Dangeruss-Industries	www.dangeruss-industries.com/
_Deskmod	http://deskmod.com/
_Deviant Art	www.deviantart.com/
_End Effect	www.endeffect.com/
_My Skins	www.myskins.com/
_Skinbase.org	www.skinbase.org/
_Skins.org	www.skinz.org/
_Wincustomize.com	http://wincustomize.com/
_Zeroplace.com	www.zeroplace.com/
Dead Dreamer	http://misery.subnet.at/
Desktop Imperium	http://chapter3.net/imperium/
DOT Studio	http://dotstudio.m78.com/DST/
E-Icons	www.ctcom.it/~giovanni/eicons/

IconFactory.com	www.iconfactory.com/
Unofficial Iconpax archive	http://greenfield.fortunecity.com/panthera/299/

OTHER RELATED SITES

News/Latest Apps

_Cnet Catchup	http://catchup.cnet.com/
AnandTech	www.anandtech.com/
Beta Elite	www.ibelite.com/
Betanews	www.betanews.com/
Davecentral - What's hot	www.davecentral.com/hot.html
Download.com - editors picks	www.download.com/pc/fdoor/0,322,0,00.html?st.dl.redir.pick.fd
File Flash	www.fileflash.com/
Internet Magazine	www.internet-magazine.com/
Nhellworld	www.frankw.net/network/nthw/
Paul Thurotts Supersite	www.wininformant.com/
PC Advisor	www.pcadvisor.co.uk/
PC NewsCenter	www.dimensionx.sitehosting.net/
Shareware.com - most pop files	www.download.com/PC/Result/MostPopular/
SlaughterHouse - todays picks	www.slaughterhouse.com/pick.html
The E-List	www.aumha.org/elist.htm
The Inquirer	www.theinquirer.net/
The Register	www.theregister.co.uk/
TracerLock	www.tracerlock.com/
Windows Planet	http://windowplanet.net/
ZD Net	www.hotfiles.com/

Newsletters

Subscribe to some of these newsletters for up to the minute news of tweaks etc

3D Spotlight	www.3dspotlight.com/
Brian Livingstone	www.iwsubscribe.com/newsletters/
CWS Apps	http://e-newsletters.internet.com
InfoWorld	www.iwsubscribe.com/newsletters/
Langa List	www.langa.com/
Lockergnome	www.lockergnome.com/changesub.html
Neat Net Tricks	www.neatnettricks.com/index.html
Opensource - Andover	www.osdn.com/newsletters/
Paul Thurrotts Wininfo	www.wininformant.com/
Slaughterhouse (good)	www.slaughterhouse.com/delivery.html
The E-List	www.aumha.org/elist.htm
The Naked PC	www.TheNakedPC.com/index2.html
The Register	www.theregister.co.uk/
VNUNet	www.vnunet.com/
ZdNet	www.zdnet.com/zdnn/

Companys

Adaptec	www.adaptec.com/
American Megatrends	www.ami.com/
ASUS Home	www.asus.com/
Award Software	www.award.com/
Creative Labs	www.europe.creative.com/
Giga Byte	www.giga-byte.com/
Intel	www.support.intel.com/support/swd
Matrox	www.matrox.com/mga/
Mr Tech	www.mrtech.com/news/
Network Associates	www.nai.com/asp_set/download/upgrade/find.asp

Downloads

32bit.com	www.32bit.com/
CNET.com	http://download.cnet.com/
FilePlanet Game Patches	www.fileplanet.com/
Garbo PC collection	http://garbo.uwasa.fi/pc/
Jumbo	www.jumbo.com/
No Nags	www.nonags.com/
NT Ware	http://home.ntware.com/
PC Advisor	www.pcadvisor.co.uk/
PC Magazine	www.pcmag.com/
Rocket Download	www.rocketdownload.com/
Shareware.com	www.shareware.com/
Simtel.Net	www.simtel.net/
Slaughter House	www.slaughterhouse.com/index.html?ct000en_andanavbar
Stroud	http://cws.internet.com/
TuCows	www.tucows.com/
Utility Geek	www.utilitygeek.com/
WebAttack	www.webattack.com/freeware/index.shtml

ZDNet	www.hotfiles.com/

Drivers

_3D Chipset	www.3dchipset.com/default.asp
_Gfx Bios etc	http://bws.sprintnet.pl/files/files.html
_Maximum Reboot	www.maxreboot.com/
_Nvidia	www.nvidia.com/view.asp?PAGE=drivers
3dFiles	www.3dfiles.com/
Bios	http://sysopt.earthweb.com/bios.html
BusMaster Drivers	www.bmdrivers.com/
Comp Geeks	www.compgeeks.com/drivers.asp
Creative	www.soundblaster.com/liveware//
Driver Guide	www.driverguide.com/
Driver HeadQuarters	www.drivershq.com/
DriverZone	www.driverzone.com/
G-Force FAQ	www.geforcefaq.com/faq.cgi
Help Drivers	www.helpdrivers.com/
IBM HD Utils	www.storage.ibm.com/hdd/support/download.htm
Intel Bus Master Drivers	http://support.intel.com/support/chipsets/driver.htm
Jargons Driver Archive	www.jargon.iki.fi/
LostCircuits BIOS	www.lostcircuits.com/advice/bios2/2.shtml
Motherboards.com	www.motherboards.com/catalog/
Mr Driver	www.mrdriver.com/index.html
Neowin Drivers	www.neowin.net/drivers.shtml
Rivastation Nvidia	www.rivastation.com/
Soundcard Utils	www.3dss.com/drivers/utils.html
TechSetGO	www.techsetgo.com/
VIAhardware.com	www.viahardware.com/
Wims Bios	www.ping.be/bios/
Windrivers.com	www.windrivers.com/

Freeware

_Pricelessware1	www.sover.net/~whoi/Priceless.html
_Pricelessware2	http://home.att.net/~willowbrookemill/pricelessware.html
Acme Freeware	http://acmefreeware.com/
Analog X	www.analogx.com/contents/download.htm
Completely Free	www.completelyfreesoftware.com/index_all.html
Freeware Home	www.freewarehome.org/
Freeware Plus	www.freewareplus.com/
Freeware Posse	www.freewareposse.com
Freeware32	http://freeware32.efront.com/
Moochers	www.moochers.com/
NONAGS Freeware	www.nonags.com/
Shell Extension City	www.shellcity.net/
Son Of Spy Freeware	www.sover.net/~whoi/Index.html
Tiny Apps	www.tinyapps.org/
Top Quality Freeware	www.topqualityfreeware.com/index.shtml
Utility Geek	www.utilitygeek.com/
WebAttack.com	www.webattack.com/

Gadgets

Firebox	www.firebox.com/
Gizmos UK	www.gizmos-uk.com
I want one of those	www.iwantoneofthose.com/
Think Geek	www.thinkgeek.com/

Microsoft

_Corporate Update for XP	http://v4.windowsupdate.microsoft.com/en/default.asp?corporate=true
_Download Hotfixes	http://support.microsoft.com/highlights/default.asp?pr=topsdn&cl=136&SD=TECH
_Download Updates	http://corporate.windowsupdate.microsoft.com/en/default.asp
_Download Page	www.microsoft.com/downloads/search.asp
Direxť X	www.microsoft.com/directx/homeuser/downloads/default.asp
FuckMicrosoft.com	www.fuckmicrosoft.com/
Microsoft Internet Keyboard	www.microsoft.com/hardware/keyboard/intkey.asp
Microsoft Knowledge Base	http://search.support.microsoft.com/kb/c.asp?ln=en-gb
Microsoft Main	www.microsoft.com/
Microsoft Tech Support	http://support.microsoft.com/professional/
Office Update	http://officebeta.microsoft.com/
Windows 2000 Downloads	www.microsoft.com/windows2000/downloads/
Windows 2000	www.microsoft.com/windows2000/library/resources/reskit/tools/
Windows Media	www.windowsmedia.com/
Windows Update	http://windows.microsoft.com/isapi/redir.dll?prd=windowsupdate&pver=&ar=WindowsUpdate
Windows	www.microsoft.com/isapi/redir.dll?prd=ie&ar=windows

Misc

Bootdisk.com	www.bootdisk.com/
Bootdisk Magic	www.bootdiskmagic.com/
BotSpot	www.botspot.com/

Cable Modem Tips	http://homepage.ntlworld.com/robin.d.h.walker/
CD Rom God	www.gankish.net/rumblesoft
Codec Zone	http://codeczone.virtualave.net/fixes.htm
DLL Archive	http://solo.abac.com/dllarchive/index.html
Easy-Files for missing DLLs etc	www.easy-files.com/
Making a Boot Win2k with SP2	www.bink.nu/Bootcd/default.htm
MyHelpdesk.com	www.myhelpdesk.com/Membership/HomeVisitor.asp
PC Computer extensions	www.computerhope.com/dosext.htm
PC Pitstop	www.pcpitstop.com/
Policys	www.elkantler.net/security/security.htm
Ultimate Bootdisk	www.startdisk.com/Web2/ubd/ubd.htm
Windows Shutdown	www.aumha.org/a/shutdown.htm

Scripts/Batch Files

Batch Scripting Site	www.fpschultze.de/batstuff.html
Batfiles	http://home7.inet.tele.dk/batfiles/
DOS Batch Language	www.maem.umr.edu/~batch/batchtoc.htm
Dos Commands	www3.sympatico.ca/rhwatson/dos7/
Dos Utils	www.jason-n3xt.org/dos/
Eric's Webspace	www.ericphelps.com/
Gords World of Batch Files	www.cableyorkton.com/users/gbraun/batch/
Horst Schaeffers Batch Pages	http://home.mnet-online.de/horst.muc/
Rob Woudes Scripting	www.robvanderwoude.com/
Simtel.net	www.simtel.net/pub/msdos/batchutl/
T Lavedas	www.pressroom.com/~tglbatch/
VBScript Tools	www.billsway.com/vbspage/

INTERNET SECURITY SITES

_AntiOnline	www.antionline.com/
_ARIN Whois	www.arin.net/whois/index.html
_DSL Reports	www.dslreports.com/secureme
_Elephants Toolbox	www.cotse.com/refs.htm
_Hacker Tracker	http://onlinescanner.com/cgi-bin/ldtracker
_Hacking Exposed	http://hackingexposed.com/
_Hacker Whacker	www.hackerwhacker.com/
_Hosts File	www.smartin-designs.com/hosts_info.htm
_Ports	www.sans.org/newlook/resources/IDFAQ/oddports.htm
_Secure Me Net	www.secure-me.net/scan
_Security Guide	http://security.winguides.com/
_Security Information	www.kobayashi.cjb.net/
_SecurityFocus	www.securityfocus.com/
_Security Pointer Downloads	www.securitypointer.com/downloads.htm
_Shields UP!	https://grc.com/x/ne.dll?bh0bkyd2
_TL Security	www.tlsecurity.net/main.htm
_Virtual Suicide	http://suicide.netfarmers.net/
Anonimity & Privacy	www.leader.ru/cgi-bin/go?who
Anonymizer	www.anonymizer.com/
BigFix	www.bigfix.com/
BlackIce Ports	www.netice.com/Advice/Exploits/Ports/
Catch Up	www.manageable.com/
Cipher War	www.cipherwar.com/
Computer Security Info	www.alw.nih.gov/Security/security.html
Cotse.com	www.cotse.com/
Crypto Yashy	http://crypto.yashy.com/
Default Password List	www.phenoelit.de/dpl/index.html
DosTest	www.doshelp.com/dostest.htm
Dostest Trojan Ports	www.doshelp.com/trojanports.htm
Hack in the Box	www.hackinthebox.org/
Hack Resource Centre	www.radsoft.net/security/hack/
Hackers Club	http://hackersclub.com/
Hackology	www.hackology.com/
Hacktivist	http://thehacktivist.com
Help Net Security	www.net-security.org/
Hideaway.net	www.hideaway.net/
Internet Sleuthing Resources	http://users.rcn.com/rms2000/sleuth/index.htm
Internet Network Security	http://netsecurity.about.com/compute/netsecurity/
John Doe	www.cix.co.uk/~net-services/jd.htm
L0pht Heavy Industries	www.l0pht.com/
Library of Information	www.hackersclub.com/km/library/
Microsoft Security	www.microsoft.com/security/
Microsoft Security Advisor	www.microsoft.com/technet/mpsa/start.asp
Netbios fact and fiction	http://cable-dsl.home.att.net/netbios.htm
New Order	http://neworder.box.sk/
NMRC	www.nmrc.org/new/index.html

NT Security	www.ntsecurity.net/
Online Privacy Related Software	http://privacy.net/ here
Packet storm	http://packetstorm.securify.com/index.shtml
Privacy Resources	www.epic.org/privacy/privacy_resources_faq.html
Privacy Rights	www.privacyrights.org/
Rewebber - surf in private	www.rewebber.de/
Russian Password Crackers	www.password-crackers.com/crack.html
Safe Hex - Safe Computing	www.claymania.com/safe-hex.html
SecuriTeam	www.securiteam.com/
Security Administrator	www.secadministrator.com/
Security FAQ	www.w3.org/Security/Faq/www-security-faq.html
Security Focus	www.securityfocus.com/
Security Watch	www.securitywatch.com/
Silent Surf	www.silentsurf.com/
Spam Mimic	www.spammimic.com/
Spychecker	www.spychecker.com/
The Happy Hacker	www.happyhacker.org/
Whitehats	http://whitehats.com/
ZDTV CyberCrime	www.zdnet.com/zdtv/cybercrime/

Antivirus

AVP	www.avp.com/
Central Command	http://centralcommand.com/
ICSA Labs Certified	www.icsalabs.com/html/communities/antivirus/certifiedproducts.shtml
Kaspersky (AVP)	www.kaspersky.com/
Mcafee	www.mcafee.com/
Panda ActiveScan	www.pandasoftware.com/activescan/activescan.asp
Symantec	www.sarc.com/avcenter/cgi-bin/navsarc.cgi#nav50

PGP (Pretty Good Privacy)

GNU	www.gnupg.org/gnupg.html
International PGP Home Page	www.stud.ifi.uio.no/pgp/
PGP Home Page	www.pgp.com/
Phil Zimmerman	www.philzimmermann.com/

Security Apps

Access Data Software	www.accessdata.com/
Adaware	www.lavasoftusa.com/downloads.html
AnalogX	www.analogx.com/contents/news.htm
Back Orifice 2000	www.bo2k.com/
BlackIce	http://advice.networkice.com/
Download Software	www.zedz.net/
Hoobienet	www.hoobie.net/index.html
It Toolbox	http://security.ittoolbox.com
Nessus Security Scanner	www.nessus.org/
Password Recovery Software	www.elcomsoft.com/prs.html
Sam Spade	http://samspade.org/ssw/
SecureWin Home Page	www.securewin.com/
Security Software	www.alw.nih.gov/Security/security-prog.html
Son Of Spy's Freeware	www.crosswinds.net/~sonofspy/Security.html
Spychecker	http://spychecker.com/
Tiny Firewall	www.tinysoftware.com/pwall.php
Tiny Firewall Config	http://members.home.net/zyklon/tpf.html
Tiny Firewall FAQ	http://tpffaq.r4f.com/
Tools	www.hoobie.net/security/exploits/
Updates.com	http://updates.zdnet.com/
Webtrends	www.webtrends.net/tools/security/scan.asp
X Corps Tools	http://xcorps.net/
Zone Alarm	www.zonelabs.com/za_download_1.htm
ZoneLog	http://zonelog.co.uk/

Usenet Groups for Security Discussion

alt.2600.hackers
alt.2600.hackerz
alt.computer.security
alt.comp.virus
alt.hacking
alt.security
alt.security.pgp
comp.os.ms-windows.nt.admin.security
comp.security.announce
comp.security.firewalls
comp.security.misc
microsoft.public.inetserver.iis.security
microsoft.public.win2000.security

INTERNET SEARCH SITES

_Google	www.google.com/
_Google Image Search	http://images.google.com/
_Google News	http://groups.google.com
Altavista	www.altavista.com/
Ask Jeeves	www.askjeeves.com/
Dogpile	www.dogpile.com/
Euroseek	www.euroseek.net/page?ifl=uk
Excite News	www.excite.com/
FTP Search V34	http://dalet.belnet.be:8000/ftpsearch
FTP Search	http://ftpsearch.lycos.com/?form=medium
Highway 61	www.highway61.com/
Hotbot	www.hotbot.com/
Infoseek	http://guide-p.infoseek.com/
Look Smart	www.looksmart.com/r?l3p&h1
Lycos	www.lycos.com/
Magellan	www.mckinley.com/
Metacrawler	http://metacrawler.com/
Northern Light	www.nlsearch.com/
Webcrawler	http://webcrawler.com/
Yahoo	www.yahoo.com/

CHAPTER [9]

BIOS TWEAKING

Introduction

By modifying settings in your BIOS you can improve performance, reduce boot time, fix incompatibility problems & many other things. This guide will take you through the BIOS & how to update it, change setting to improve performance, etc. & how to overclock your system using BIOS settings too. Some of these settings are from various sources e.g. motherboard manuals and from my own experience but the majority of these settings are taken from an excellent website called 'Speed Demons' www.rojakpot.com - thankyou Adrian.

BIOS keys

del during boot	AMI, Award
Esc during boot	Toshiba
F1 during boot	Toshiba; Phoenix; Late model PS/1 Value Point and 330s
F2 during boot	NEC
F10 when square in top RH corner of screen	Compaq
Ins during boot	IBM PS/2s w/ Reference Partition
Reset twice Some	Dells
Alt Enter	Dell
Alt ? some	PS/2s
Ctrl-Esc	General
Ctrl Ins some	PS/2s when pointer at top right of screen
Ctrl Alt Esc	AST Advantage, Award, Tandon
Ctrl Alt +	General
Ctrl Alt S	Phoenix
Ctrl Alt Ins	Zenith, Phoenix
Ctrl S	Phoenix
Ctrl Shift Esc	Tandon 386
Shift Ctrl Alt + Num Pad del	Olivetti PC Pro
Setup disk Old	Compaqs, Epson (Gemini), IBM, IBM PS/2, Toshiba, most old 286s

BIOS Passwords

These are useful to know if someone has put a password in your Bios and you need to get into it to change some settings. However if you can boot into windows there are many tools/utilities you can use that will tell you the Bios password or reset it - some of these tools can be found on www.antionline.com and also www.esiea.fr/public_html/Christophe.GRENIER You can however also open up the computer and find the jumper to short the Bios, which will also let you in (look in the manual for the jumper)

AMI BIOS Default Passwords

A.M.I.
AM
AMI
AMI_SW
AMI?SW
BIOS
HEWITT RAND
LKWPETER
PASSWORD

AWARD BIOS Default Passwords
589589
589721
ALLY
ALFAROME
AWARD_SW
AWARD?SW
AWKWARD
BIOSTAR
CONCAT
HLT
J256
J262
LKWPETER
SER
SKY_FOX
SYXZ

BIOS flashing

You should begin by updating your BIOS to the latest version. This can fix issues with certain motherboards, add more features or just improve performance. Although BIOS flashing is a little more dangerous than say, updating drivers as if you do it wrong you may need a new motherboard or BIOS chip. As a result I'd recommend that if you're happy with your PC as it is then you can probably skip this section. Given the potential risks involved with this its highly recommended you backup important data. You can find a list of motherboard manufacturers (& their BIOS updates) at Windrivers.com. Also check out www.amdmb.com for AMD Bios downloads.

Your manufacturers website may also contain instructions on how to flash your BIOS. NOTE - BIOS flashing can only be completed in true DOS mode & not in Windows9x/NT.

What to do

- Begin by downloading the BIOS update & a BIOS flashing utility, e.g. Award Flash utility.

- Make a bootable floppy disk (startup disk), Windows 2000 (& other) users can download one here. A standard Windows 98 bootdisk will suffice.

- Extract the files from the BIOS update & the BIOS Flashing utility & copy them onto the floppy disk (BIOS update will end with the .bin, binary file extension).

- Restart your system & boot from the floppy drive (you may need to make changes in your BIOS to do this, its also recommended that you Load BIOS defaults before doing so).

- Ensure that no memory managers are running by typing in MEM /c or MEM /d at the command prompt. If they are you may need to edit the config.sys file on the disk to remove the references to them (EMM386.EXE & HIMEM.SYS). You'll need to load up Windows to do this. Open A:\config.sys with Notepad & delete those lines. Reboot then using the bootdisk.

- Type A:\ to go into the floppy drive where you can being the Flashing process.

- Update the BIOS via the Flash utility, e.g. To use the Award Flash utility you should enter in AWDFLASH.EXE. Substitute in the appropriate filename if necessary.

- You will be asked for the file name to program, enter in the name of the *.bin file on the disk, e.g. NEW.BIN. Hit Enter to continue.

- You may be prompted to save your current BIOS. Do so at your own discretion, e.g. Save it as BACKUP.BIN. I would advise backing up your BIOS here, just in case anything untoward happens.

- The BIOS update procedure will now begin. Do NOT interupt this procedure in any way. You will be told what to do & when to do it.

Reboot when prompted to finish the update. Enter the BIOS & Load BIOS defaults. Save the changes & exit. Boot Windows as usual now & once all is working fine you can start tweaking the BIOS settings. BIOS settings You can boot up faster & improve your performance by changing settings in your BIOS. First of all need to access it. When you're starting the PC, hit the Delete key. It should bring up the BIOS a few seconds later. Use another key if necessary.

NOTE - Write down all your current settings for future reference in case you do something that you shouldn't have. Either that or want you just want to restore it to your old configuration. Some of the definitions used are taken from my manual. You may need to search under different sections of your BIOS to find these, so be prepared to look. I'll put these into different sub-categories where they generally would appear.

BIOS OPTIONS (last updated February 2003)

BOOTSTRAP MANAGEMENT

Boot other device
This feature determines whether the BIOS will attempt to load an operating system from the Second Boot Device or Third Boot Device if it fails to load one from the First Boot Device. This feature is **enabled** by default and it is recommended that you leave it as such. This will allow the BIOS to check the second and third boot devices for operating systems on failing to find one on the first boot device. Otherwise, the BIOS will just halt the booting process with the error message No Operating System Found even if there's an operating system on the second or third boot device.

Boot sequence
Common Options :
A, C, SCSI
C, A, SCSI
C, CD-ROM, A
CD-ROM, C, A
D, A, SCSI (only when you have at least 2 IDE hard disks)
E, A, SCSI (only when you have at least 3 IDE hard disks)
F, A, SCSI (only when you have 4 IDE hard disks)
SCSI, A, C
SCSI, C, A
A, SCSI, CLS/ZIP, C

This feature enables you to set the sequence in which the BIOS will search for an operating system during the boot-up process. To ensure the shortest booting time possible, select the hard disk that contains your operating system as the first choice. Normally, this would be drive C but if you are using a SCSI hard disk, then select SCSI. Some motherboards have a second IDE controller built-in. In such motherboards, the SCSI option is replaced with an EXT option. This allows the computer to boot from an IDE hard disk connected to the second IDE controller or from a SCSI hard disk. If you want to boot from an IDE hard disk running off the first IDE controller, do not set the Boot Sequence to start with EXT. Please note that this feature works in conjunction with the Boot Sequence EXT Means feature.

Boot sequence ext means
Common Options : IDE, SCSI
This feature will only have an effect if the EXT option had been selected in the Boot Sequence feature. This feature allows you to control whether the system boots from an IDE hard disk that's connected to the second IDE controller found on some motherboards or a SCSI hard disk. To boot from an IDE hard disk that's connected to the second IDE controller, you must first set the Boot Sequence feature to start with the EXT option first. For example, the EXT, C, A setting. Then, you have to set this feature, Boot Sequence EXT Means to IDE. In order to boot from a SCSI hard disk, set the Boot Sequence feature to start with the EXT option first. For example, the EXT, C, A setting. Then, you have to set this feature, Boot Sequence EXT Means to SCSI.

Boot up floppy seek
This feature controls whether the BIOS checks for a floppy drive when the system boots up or not. If enabled, the BIOS will attempt to initialize the floppy drive. If it cannot detect one (either due to improper configuration or physical inavailability), it will flash an error message. However, the system will still be allowed to continue the boot process. If the floppy drive is present, the BIOS will query the drive to find out if it supports 40 or 80 tracks operation. But since all floppy drives in use today only support 80 tracks operation, this check is redundant. If this feature is disabled, the BIOS will skip the floppy drive check. This speeds up the booting process by several seconds. Since the floppy drive check is essentially pointless, it is recommended that you **disable** this feature for a faster booting process.

Boot up numlock status
This feature sets the input mode of the numeric keypad at boot up. If you turn this feature **on,** the numeric keypad will be set to function in the numeric mode (for typing out numbers) when the system boots up. But if you set it to Off, it will function in the cursor control mode (for controlling the cursor). The numeric keypad's input mode can be switched to either numeric or cursor control mode at anytime after boot up. This feature merely sets the inital input mode of the keypad at boot up. The choice of inital keypad input mode is entirely up to your preference.

First boot device
This feature allows you to select the first device from which the BIOS will attempt to load an operating system. If the BIOS finds and loads an operating system from the device selected through this feature, it won't load another operating system, even if you have one on a different device. For example, if you set Floppy as the first boot device, the BIOS will ignore the Windows XP installation on your hard disk and load up the DOS 3.3 boot disk which you have placed in the floppy drive instead. In short, this feature allows you to choose the first device to boot from. This is particularly useful when you need to load a boot disk for troubleshooting purposes or for installing a new operating system.

By default, Floppy is the first boot device in practically all motherboards. But, unless you boot often from the floppy drive, it's better to set your hard disk (usually HDD-0) as the first boot device. This will shorten the booting process because the BIOS no longer needs to check the floppy drive for a bootable operating system. More importantly, doing so prevents the BIOS from loading the wrong operating system in case you forgot to remove the boot disk from the floppy drive! This also indirectly prevents the loading of any virus infected floppy disk that was left in the drive during booting. To install operating systems that come on bootable CD-ROMs (i.e. Microsoft Windows XP) in a new hard disk, you will need to select CDROM as the first boot device. This enables you to boot directly from the CD-ROM and load the operating system's installation routine.

Quick boot
This feature was designed to decrease the time it takes for you to boot up your system. But it's not the same as the Quick Power On Self Test feature because it doesn't merely shorten or skip some system tests just to speed up boot time. It makes use of additional techniques to further shorten the booting process. In fact, the Quick Power On Self Test should be considered as a subset of the Quick Boot feature. In addition to skipping some tests and shortening the others, Quick Boot also performs the following techniques to further speed up the booting process :-

Spin up the hard disks as soon as power is supplied (or as soon as possible)
Initialize only critical parts of the chipset

Read memory size from SPD (Serial Presence Detect) chip on the memory DIMM
Eliminate logo delays (inserted by most manufacturers)
You should **enable** this feature for faster booting. But if you make any hardware changes, it is recommended that you disable this feature so that the BIOS can run full diagnostic tests to detect any problems that may slip through the abbreviated testing scheme offered by this feature. After a few error-free test runs, you can reenable this feature for faster booting without impairing system stability.

Quick power on self test

When enabled, this feature will skip or shorten some of the system tests that are performed during the booting up process. This allows the system to boot up much quicker. You should **enable** this feature for faster booting. But if you make any hardware changes, it is recommended that you disable this feature so that the BIOS can run full diagnostic tests to detect any problems that may slip through the abbreviated testing scheme offered by this feature. After a few error-free test runs, you can reenable this feature for faster booting without impairing system stability.

Second boot device

This feature allows you to select the second device from which the BIOS will attempt to load an operating system. If the BIOS finds and loads an operating system from the device selected through this feature, it won't load another operating system, even if you have one on a different device. For example, if you set Floppy as the first boot device and HDD-0 as the second boot device, the BIOS will boot straight into the Windows 98 installation on your hard disk and ignore the Windows XP installation CD in your CD-ROM drive if there's no bootable disk in the floppy drive. In short, this feature allows you to choose the second device to boot from.

By default, HDD-0 is the second boot device in practically all motherboards. But, unless you boot often from the floppy drive (which is often the first boot device), it is better to set your hard disk (HDD-0) as the first boot device. This will shorten the booting process because the BIOS no longer needs to check the floppy drive for a bootable operating system. More importantly, doing so prevents the BIOS from loading the wrong operating system in case you forgot to remove the boot disk from the floppy drive! This also indirectly prevents the loading of any virus infected floppy disk that was left in the drive during booting.

Third boot device

This feature allows you to select the third device from which the BIOS will attempt to load an operating system. If the BIOS finds and loads an operating system from the device selected through this feature, it won't load another operating system, even if you have one on a different device. For example, if you set Floppy as the first boot device, HDD-0 as the second boot device and SCSI as the third boot device, the BIOS will boot straight into the Windows 98 installation on your SCSI hard disk and ignore the Windows XP installation CD in your CD-ROM drive if there's no bootable IDE hard disk or bootable floppy disk. In short, this feature allows you to choose the third device to boot from.

GRAPHICS SUBSYSTEM

AGP 2x mode

This BIOS feature is found on AGP 2X-capable motherboards. When enabled, it allows the AGP bus to make use of the AGP 2X transfer protocol to boost the AGP bus bandwidth. If it's disabled, then the AGP bus will only use the standard AGP1X transfer protocol. The baseline AGP 1X protocol only makes use of the rising edge of the AGP signal for data transfer. This translates into a bandwidth of 264MB/s. But **enabling** AGP 2X Mode doubles that bandwidth by transferring data on both the rising and falling edges of the signal. Through this method, the effective bandwidth of the AGP bus is doubled even though the AGP clock speed remains at the standard 66MHz. This is the same method by which UltraDMA/33 derives its performance boost.

The AGP 2X protocol must be supported by both the motherboard and graphics card for this feature to work. Of course, this feature will only appear in your BIOS if your motherboard supports the AGP 2X transfer protocol! So, all you need to do is make sure your graphics card supports AGP 2X transfers. If it does, enable AGP 2X Mode to take advantage of the faster transfer mode. Disable it only if you are facing stability issues or if you intend to overclock the AGP bus beyond 75MHz with sidebanding support enabled. Please note that doubling the AGP bus bandwidth through the AGP 2X transfer protocol won't double the performance of your AGP graphics card. The performance of the graphics card relies on far more than the bandwidth of the AGP bus. The performance boost is most apparent when the AGP bus is really stressed (i.e. during a texture-intensive game).

AGP 4x drive strength

This BIOS feature is similar to AGP Driving Control. It allows you to set whether to allow the AGP controller to dynamically adjust the AGP driving strength or to allow manual configuration by the BIOS. Due to the tighter tolerances of the AGP 4X bus, the AGP 4X controller features auto-compensation circuitry that compensate for the motherboard's impedance on the AGP bus. It does this by dynamically adjusting the drive strength of the I/O pads over a range of temperature and voltages when AGP 4X mode is selected.

The auto-compensation circuitry has two operating modes. By default, it is set to automatically compensate for the impedance once or at regular intervals by dynamically adjusting the AGP drive strength. The circuitry can also be disabled or bypassed. In this case, it is up to the user (through the BIOS) to write the desired drive strength value to the AGP I/O pads. When you set this BIOS feature to **Auto**, the AGP drive strength values are obtained from the auto-compensation circuitry. Normally, this is the recommended setting as it allows the AGP controller to dynamically adjust for motherboard impedance changes. However, manual configuration of the AGP drive strength may be necessary.

Some AGP 4X cards were not designed according to published AGP 4X signal impedance and routing guidelines. Therefore, these cards may not work reliably with the default drive strengths issued by the compensation circuit. To correct this problem, you can bypass the compensation circuit and force the AGP I/O pads to use a particular drive strength. Usually, this will be a higher than normal drive strength. You can also make use of this feature for overclocking purposes. Increasing the drive strength increases the stability of the AGP bus by reducing the impedance from the motherboard and boosting the signal strength. But be very, very circumspect when you increase the AGP drive strength on an overclocked AGP bus as your AGP card may be irreversibly damaged in the process!

Therefore, for troubleshooting or overclocking purposes, you should set the AGP 4X Drive Strength to **Manual**. This allows you to manually set the AGP Drive Strength value via the AGP Drive Strength P Ctrl and AGP Drive Strength N Ctrl options. Note that this

feature is a little different from AGP Driving Control because it usually comes with two to four different drive strength controls. The AGP Driving Control feature only comes with a single drive strength control.

AGP 4x mode

This BIOS feature is only found on AGP 4X-capable motherboards. When enabled, it allows the AGP bus to make use of the AGP 4X transfer protocol to boost the AGP bus bandwidth. If it's disabled, then the AGP bus is only allowed to use the AGP 1X or AGP 2X transfer protocol. The baseline AGP 1X protocol only makes use of the rising edge of the AGP signal for data transfer. This translates into a bandwidth of 264MB/s. The AGP 2X protocol doubles that by utilizing the falling edge of the AGP signal for data transfer as well. However, the AGP 4X protocol uses four strobe signals to further double the bandwidth to just over 1GB/s. The four strobes can either be used as four separate signals (with data transferred only on the falling edge) or they can be used as two differential pairs, transferring data on both edges of the signals. Either way, the AGP bandwidth is quadrupled over that of the AGP 1X transfer protocol.

The AGP 4X protocol must be supported by both the motherboard and graphics card for this feature to work. Of course, this feature will only appear in your BIOS if your motherboard supports the AGP 4X transfer protocol! So, all you need to do is make sure your graphics card supports AGP 4X transfers. If it does, enable AGP 4X Mode to take advantage of the faster transfer mode. You must disable it if your graphics card doesn't support AGP 4X transfers. The BIOS will then report that the maximum supported transfer mode is AGP 2X. By default, many motherboards come with the AGP 4X transfer mode disabled. This is because not everyone will be using AGP 4X-capable graphic cards. When cards capable of only AGP 1X or 2X operation are installed, this feature must be disabled for the cards to properly. To prevent complications with uninformed users, most manufacturers simply disable AGP 4X mode by default.

However, this means that users of AGP 4X cards will unnecessarily lose out on the greater amount of bandwidth available through the AGP 4X transfer mode. So, if you are using an AGP 4X-capable graphics card, it's recommended that you **enable** this feature for better AGP bus performance. Please note that quadrupling the AGP bus bandwidth through the AGP 4X transfer protocol won't really quadruple the performance of your AGP graphics card. The performance of the graphics card relies on far more than the bandwidth of the AGP bus. The performance boost is most apparent when the AGP bus is really stressed (i.e. during a texture-intensive game).

AGP aperture size

This BIOS feature allows you to select the size of the AGP aperture. The aperture is a portion of the PCI memory address range that is to be dedicated for use as AGP memory address space. Host cycles that hit the aperture range are forwarded to the AGP bus without need for translation. The aperture size also determines the maximum amount of system RAM that can be allocated to the AGP graphics card for texture storage. The AGP aperture size should be calculated using this formula : maximum usable AGP memory size x 2 plus 12MB. The actual usable AGP memory space is less than half the AGP aperture size set in the BIOS. This is because the AGP controller needs a write combined memory area equal in size to the actual AGP memory area (uncached) plus an additional 12MB for virtual addressing. Therefore, it isn't simply a matter of determining how much AGP memory space you need. You also need to calculate the final aperture size by doubling the amount of AGP memory space desired and adding 12MB to the total.

Note that the AGP aperture is merely address space, not physical memory in use. The physical memory is allocated and released as needed only when Direct3D makes a "create non-local surface" call. Windows 95 (with VGARTD.VXD) and later versions of Microsoft Windows use a waterfall method of memory allocation. Surfaces are first created in the graphics card's local memory. When that memory is full, surface creation spills over into AGP memory and then system memory. So, memory usage is automatically optimized for each application. AGP and system memory are not used unless absolutely necessary.

It's quite common to hear many people recommending that the AGP aperture size should be exactly half the amount of system RAM. However, this is wrong for the same reason why swapfile size shouldn't always be 1/4 of system RAM. Like the swapfile, the size of the AGP memory space shrinks as the graphics card's local memory increases in size. This is because the graphics card will have more local memory to dedicate to texture storage. This reduces the need for AGP memory. So, if you upgrade to a graphics card with more memory, you shouldn't be "deceived" into thinking that it will therefore require even more AGP memory! On the contrary, a smaller AGP memory space will required.

If your graphics card has very little graphics memory (4MB - 16MB), you may need to create a large AGP aperture, up to half the size of the system RAM. The graphics card's local memory and the AGP aperture size combined should be roughly around 64MB. For cards with more local memory, you needn't create quite so big an aperture. Note that the size of the aperture does not correspond to performance so increasing it to gargantuan proportions will not improve performance. Still, it is recommended that you keep the AGP aperture around **64MB to 128MB** in size. Now, why is such a large aperture size recommended despite the fact that most graphics cards now come with large amounts of local memory? Shouldn't we just set it to the absolute minimum to save system RAM?

Well, in the first place, many graphics cards require an AGP aperture of at least 16MB in size to work properly. This is probably because the virtual addressing space is already 12MB in size! In addition, many software have AGP aperture size requirements that are mostly unspecified. Some games actually use so much textures that a large AGP aperture is needed even with graphics cards with large memory buffers. And if you remember the formula above, the AGP aperture must be more than twice the size of the desired AGP memory space. So, if you want 15MB of AGP memory for texture storage purposes, then the AGP aperture has to be at least 42MB in size. Therefore, it makes sense to set a large AGP aperture size in order to cater for all eventualities.

Please note that reducing the AGP aperture size won't save you any RAM. Again, what setting the AGP aperture size does is limit the amount of system memory the AGP bus can appropriate when it needs to. It is not used unless absolutely necessary. So, setting a 64MB AGP aperture doesn't mean that 64MB of your system memory will be appropriated. It will only limit the maximum amount of system memory that can be used by the AGP bus to 64MB (with a usable AGP memory space of only 26MB).

Now, while increasing the AGP aperture size beyond 128MB won't take up system RAM, it would still be best to keep the aperture size in the 64MB-128MB range so that the GART (Graphics Address Relocation Table) won't become too big. As the amount of local memory on graphics cards increases and texture compression becomes commonplace, there's less of a need for the AGP aperture size to grow beyond 64MB. Therefore, it is recommended that you set the AGP Aperture Size to 64MB or at most, 128MB.

AGP clock / CPU FSB clock

The AGP bus clock speed is referenced from the CPU bus clock speed. However, the AGP bus was only designed to run at 66MHz while the CPU bus runs anywhere from 66MHz to 133MHz. Therefore, a suitable AGP bus to CPU bus clock speed ratio or divider must be selected to ensure that the AGP bus won't run way beyond 66MHz. When the ratio is set to 1/1, the AGP bus will run at the same speed as the CPU bus. This is meant for processors that use the 66MHz bus speed, like the older Intel Celeron processors.

The 2/3 divider is used when you use a processor running with a bus speed of 100MHz. This divider will cut the AGP bus speed down to 66MHz. The 1/2 divider was recently introduced with motherboards that provide 133MHz bus speed support. Such motherboards need the 1/2 divider to make the AGP bus run at the standard 66MHz. Without this divider, the AGP bus would have to run at 89MHz, which is more than what most AGP cards can withstand.

Generally, you should **set this feature according to the CPU bus speed** you are using. This means using the 1/1 divider for 66MHz bus speed CPUs, the 2/3 divider for 100MHz bus speed CPUs and the 1/2 divider for 133MHz CPUs.
If you are overclocking the CPU bus, you are supposed to reduce the divider to ensure that the AGP bus speed remains within specifications. However, most AGP cards can run with the AGP bus overclocked to 75MHz. Some would even happily run at 83MHz! However, anything above 83MHz would be a little iffy. In most cases, you can still stick with the original AGP bus / CPU bus clock divider when you overclock the CPU. This means that the AGP bus will be overclocked as well. But as long as the AGP card can work at the higher clock speed, it shouldn't be a problem. In fact, you can expect a linear increase in AGP bus performance. Be warned though - overclocking the AGP bus can potentially damage your AGP card. So, be circumspect when you overclock the AGP bus. 75MHz is normally the safe limit for most AGP cards.

AGP drive strength N ctrl

This is one of the functions slaved to the AGP 4X Drive Strength feature. If you set the AGP 4X Drive Strength to Auto, then the value you choose won't have any effect. In order for this function to have any effect, you need to set AGP 4X Drive Strength to Manual. This function determines the N transistor drive strength of the AGP bus. The drive strength is represented by Hex values from 0 to F (0 to 15 in decimal). The default N transistor drive strength differs from motherboard to motherboard. But the higher the drive strength, the greater the compensation for the motherboard's impedance on the AGP bus.

In conjunction with AGP 4X Drive Strength and AGP Drive Strength P Ctrl, this function is used to bypass AGP dynamic compensation in cases where the auto-compensation circuitry cannot provide adequate compensation. This is mainly seen when the AGP graphics card was not designed according to the AGP 4X impedance and routing guidelines. Please check with your graphics card manufacturer if your card requires the N transistor drive strength to be manually set. Due to the nature of this BIOS function, it is possible to use it as an aid in overclocking the AGP bus. The AGP bus is sensitive to overclocking, especially in AGP 4X mode, with sideband and Fast Write support enabled. A higher N (and P) transistor drive strength may just be what you need to overclock the AGP bus higher than is normally possible. By raising the drive strength of the AGP bus, you can improve its stability at overclocked speeds.

Please be very, very circumspect when you increase the AGP drive strength on an overclocked AGP bus as your AGP card may be irreversibly damaged in the process! Also, contrary to popular opinion, increasing the AGP drive strength will not improve the performance of the AGP bus. It is not a performance enhancing feature so you **shouldn't** increase the N transistor drive strength unless you need to.

AGP drive strength P ctrl

This is one of the functions slaved to the AGP 4X Drive Strength feature. If you set the AGP 4X Drive Strength to Auto, then the value you choose won't have any effect. In order for this function to have any effect, you need to set AGP 4X Drive Strength to Manual. This function determines the P transistor drive strength of the AGP bus. The drive strength is represented by Hex values from 0 to F (0 to 15 in decimal). The default P transistor drive strength differs from motherboard to motherboard. But the higher the drive strength, the greater the compensation for the motherboard's impedance on the AGP bus.

In conjunction with AGP 4X Drive Strength and AGP Drive Strength N Ctrl, this function is used to bypass AGP dynamic compensation in cases where the auto-compensation circuitry cannot provide adequate compensation. This is mainly seen when the AGP graphics card was not designed according to the AGP 4X impedance and routing guidelines. Please check with your graphics card manufacturer if your card requires the P transistor drive strength to be manually set. Due to the nature of this BIOS function, it is possible to use it as an aid in overclocking the AGP bus. The AGP bus is sensitive to overclocking, especially in AGP 4X mode, with sideband and Fast Write support enabled. A higher P (and N) transistor drive strength may just be what you need to overclock the AGP bus higher than is normally possible. By raising the drive strength of the AGP bus, you can improve its stability at overclocked speeds.

Please be very, very circumspect when you increase the AGP drive strength on an overclocked AGP bus as your AGP card may be irreversibly damaged in the process! Also, contrary to popular opinion, increasing the AGP drive strength will not improve the performance of the AGP bus. It is not a performance-enhancing feature so you **shouldn't** increase the P transistor drive strength unless you need to.

AGP driving control

This feature is similar to AGP 4X Drive Strength. It allows you to set whether to allow the AGP controller to dynamically adjust the AGP driving strength or to allow manual configuration by the BIOS. Due to the tighter tolerances of the AGP 4X bus, the AGP 4X controller features auto-compensation circuitry that compensate for the motherboard's impedance on the AGP bus. It does this by dynamically adjusting the drive strength of the I/O pads over a range of temperature and voltages when AGP 4X mode is selected. The auto-compensation circuitry has two operating modes. By default, it is set to automatically compensate for the impedance once or at regular intervals by dynamically adjusting the AGP drive strength. The circuitry can also be disabled or bypassed. In this case, it is up to the user (through the BIOS) to write the desired drive strength value to the AGP I/O pads.

When you set this BIOS feature to **Auto**, the AGP drive strength values are obtained from the auto-compensation circuitry. Normally, this is the recommended setting as it allows the AGP controller to dynamically adjust for motherboard impedance changes. However, manual configuration of the AGP drive strength may be necessary.

Some AGP 4X cards were not designed according to published AGP 4X signal impedance and routing guidelines. Therefore, these cards may not work reliably with the default drive strengths issued by the compensation circuit. To correct this problem, you can

bypass the compensation circuit and force the AGP I/O pads to use a particular drive strength. Usually, this will be a higher than normal drive strength. You can also make use of this feature for overclocking purposes. Increasing the drive strength increases the stability of the AGP bus by reducing the impedance from the motherboard and boosting the signal strength. But be very, very circumspect when you increase the AGP drive strength on an overclocked AGP bus as your AGP card may be irreversibly damaged in the process!

Therefore, for troubleshooting or overclocking purposes, you should set the AGP Driving Control to Manual. This allows you to manually set the AGP drive strength value via the AGP Driving Value function. Note that this feature is a little different from AGP 4X Drive Strength because it usually comes with a single drive strength control. The AGP 4X Drive Strength feature comes with two to four drive strength controls.

AGP driving value
This function is slaved to AGP Driving Control. If you set the AGP Driving Control to Auto, then the value you set here won't have any effect. In order for this function to have any effect, you need to set the AGP Driving Control to Manual. This function determines the overall drive strength of the AGP bus. The drive strength is represented by Hex values from 00 to FF (0 to 255 in decimal). The default AGP drive strength differs from motherboard to motherboard. But the higher the drive strength, the greater the compensation for the motherboard's impedance on the AGP bus. On the reference motherboard, the default drive strength was C5 (197).

In conjunction with AGP Driving Control, this function is used to bypass AGP dynamic compensation in cases where the auto-compensation circuitry cannot provide adequate compensation. This is mainly seen when the AGP graphics card was not designed according to the AGP 4X impedance and routing guidelines. If you are using an AGP card built around the **NVIDIA GeForce 2 line of GPUs, then it is recommended that you put AGP Driving Control into Manual mode and set AGP Driving Value to EA (234).** For other cards, please check with the manufacturer if your card requires the AGP driving strength to be manually set.

Due to the nature of this BIOS function, it is possible to use it as an aid in overclocking the AGP bus. The AGP bus is sensitive to overclocking, especially in AGP 4X mode, with sideband and Fast Write support enabled. A higher AGP drive strength may just be what you need to overclock the AGP bus higher than is normally possible. By raising the drive strength of the AGP bus, you can improve its stability at overclocked speeds. Please be very, very circumspect when you increase the AGP drive strength on an overclocked AGP bus as your AGP card may be irreversibly damaged in the process! Also, contrary to popular opinion, increasing the AGP drive strength will not improve the performance of the AGP bus. It is not a performance enhancing feature so you shouldn't increase the AGP drive strength unless you need to.

AGP master 1WS read
In most motherboards, the AGP bus-mastering device has to wait for at least two wait states (AGP clock cycles) before it can initiate a read command. This BIOS feature allows you to reduce that delay to only one wait state. This speeds up all reads that the AGP bus-master makes from the system memory. So, for better AGP read performance, **enable** this feature. **Disable** it only if you notice visual anomalies like wireframe effects and pixel artifacts or if your system hangs on running software that make use of AGP texturing.

Curiously, some motherboards apparently come with a default AGP master read latency of 0! Enabling the AGP Master 1WS Read in such cases will actually increase the latency by one wait state and reduce AGP read performance. Although it's quite unlikely that the default AGP master read latency would be zero, that's what their manuals say. So, check your motherboard manual to see if your motherboard's manufacturer implemented the first (and more common) interpretation of the AGP Master 1WS Read feature or the second one. Either way, the lower the AGP master read latency, the higher the read performance of the AGP bus.

AGP master 1WS write
In most motherboards, the AGP bus-mastering device has to wait for at least two wait states (AGP clock cycles) before it can initiate a write command. This BIOS feature allows you to reduce that delay to only one wait state. This speeds up all writes that the AGP bus-master makes to the system memory. So, for better AGP write performance, **enable** this feature. **Disable** it only if you notice visual anomalies like wireframe effects and pixel artifacts or if your system hangs on running software that make use of AGP texturing.

Curiously, some motherboards apparently come with a default AGP master write latency of 0! Enabling the AGP Master 1WS Write in such cases will actually increase the latency by one wait state and reduce AGP write performance. Although it's quite unlikely that the default AGP master write latency would be zero, that's what their manuals say. So, check your motherboard manual to see if your motherboard's manufacturer implemented the first (and more common) interpretation of the AGP Master 1WS Write feature or the second one. Either way, the lower the AGP master write latency, the higher the write performance of the AGP bus.

AGPCLK / CPUCLK
The AGP bus clock speed is referenced from the CPU bus clock speed. However, the AGP bus was only designed to run at 66MHz while the CPU bus runs anywhere from 66MHz to 133MHz. Therefore, a suitable AGP bus to CPU bus clock speed ratio or divider must be selected to ensure that the AGP bus won't run way beyond 66MHz. When the ratio is set to 1/1, the AGP bus will run at the same speed as the CPU bus. This is meant for processors that use the 66MHz bus speed, like the older Intel Celeron processors.

The 2/3 divider is used when you use a processor running with a bus speed of 100MHz. This divider will cut the AGP bus speed down to 66MHz. The 1/2 divider was recently introduced with motherboards that provide 133MHz bus speed support. Such motherboards need the 1/2 divider to make the AGP bus run at the standard 66MHz. Without this divider, the AGP bus would have to run at 89MHz, which is more than what most AGP cards can withstand.

Generally, you should **set this feature according to the CPU bus speed you are using.** This means using the 1/1 divider for 66MHz bus speed CPUs, the 2/3 divider for 100MHz bus speed CPUs and the 1/2 divider for 133MHz CPUs.

If you are overclocking the CPU bus, you are supposed to reduce the divider to ensure that the AGP bus speed remains within specifications. However, most AGP cards can run with the AGP bus overclocked to 75MHz. Some would even happily run at 83MHz! However, anything above 83MHz would be a little iffy. In most cases, you can still stick with the original AGP bus / CPU bus clock divider when you overclock the CPU. This means that the AGP bus will be overclocked as well. But as long as the AGP card can work at the higher clock speed, it shouldn't be a problem. In fact, you can expect a linear increase in AGP bus performance. Be warned

though - overclocking the AGP bus can potentially damage your AGP card. So, be circumspect when you overclock the AGP bus. 75MHz is normally the safe limit for most AGP cards.

Init display first

Although the AGP bus was designed exclusively for the graphics subsystem, some users still have to use PCI graphics cards for multi-monitor support. This is because there can be only one AGP port! So, if you want to use multiple monitors. you must either get an AGP card that provides multi-monitor support or use PCI graphics cards. For those who upgraded from a PCI graphics card to an AGP one, it's certainly enticing to use the old PCI graphics card to support a second monitor. The PCI card would certainly do the job just fine as it merely sends display data to the second monitor. You don't need a powerful graphics card to run the second monitor as Microsoft Windows 2000/XP does not support 3D graphics acceleration on the second monitor.

In such cases of an AGP graphics card working in tandem with a PCI graphics card, the BIOS has to determine which graphics card is the primary graphics card. Naturally, the default would be the AGP graphics card since in most cases, it would be the faster card. However, a BIOS switch that allows you to manually select the graphics card to boot the system with is required. This is particularly important if you have AGP and PCI graphics cards but only one monitor. There's where the Init Display First feature comes in. It allows you to select whether to boot the system using the AGP graphics card or the PCI graphics card.

If you are only using a single graphics card, then the BIOS will detect it as such and boot it up, irrespective of what you set the feature to. However, there may be a slight reduction in initialization time if you set this feature to its proper setting. For example, if you only use an AGP graphics card, then setting Init Display First to **AGP** may speed up your system's booting-up process. Therefore, if you are only using a single graphics card, it is recommended that you set the Init Display First feature to the proper setting for your system (AGP for a single AGP card and PCI for a single PCI card). But if you are using multiple graphics cards, it's up to you which card you want to use as your primary display card. It is recommended that you select the fastest graphics card as the primary display card.

Video bios cacheable

This feature is only valid when the video BIOS is shadowed. Enabling this feature forces the processor's Level 2 cache to cache the video BIOS ROM from C0000h-C7FFFh. This greatly speeds up accesses to the video BIOS. However, this does not translate into better system performance because modern operating systems like Microsoft Windows XP do not need to access the video BIOS. Everything can be done much quicker by using drivers to access the hardware directly.

As such, it would be a waste of Level 2 cache bandwidth if the video BIOS is cached instead of data that are more critical to the system's performance. In addition, if any errant program writes into this memory area, it will result in a system crash. So, it is highly recommended that you **disable** this feature for better system performance.

Video bios shadowing

When this feature is enabled, the video BIOS is copied to the system RAM for quicker access. Shadowing improves the BIOS' performance because the BIOS can now be read by the CPU through the 64-bit memory bus as opposed to the 8-bit XT bus. This appears quite attractive since this results in at least a 100-fold increase in transfer rate and the only price is the loss of some system RAM which is used to mirror the ROM contents. However, modern operating systems bypass the BIOS completely and access the graphics card's hardware directly using drivers. No BIOS calls are made so absolutely no benefit from BIOS shadowing can be realized. In light of this, there's no point in wasting RAM shadowing the video BIOS so **disable**.

Ryu Connor confirmed this by sending me a link to a Microsoft article about Shadowing BIOS under WinNT 4.0. According to this article, shadowing the BIOS (irrespective of what BIOS it is) does not bring about any performance enhancements because it is not used by Windows NT. It will just waste memory. Although the article did not say anything about other versions of Microsoft Windows, this is true for all versions of Microsoft Windows from Windows 95 onwards. In addition, there's a risk of certain software accessing the RAM region that has already been used to shadow the video BIOS. When this happens, the system will crash. Fortunately, this is no longer an issue as the shadowed RAM region has now been moved far from the reach of programs.

Finally, most graphics cards now use Flash ROM (EEPROM) which is much faster than the old ROM and even faster than DRAM. Thus, there's no longer a need for video BIOS shadowing and there may even be a performance advantage in not shadowing the BIOS! Another reason why shadowing is contraindicated in graphics cards with Flash ROM is because it prevents you from updating the contents of the Flash ROM. Any attempt in updating the BIOS that has been shadowed will most likely result in a system crash. On the other hand, there may still be a use for this feature. Some real-mode DOS games still make use of the video BIOS because they don't directly access the graphics processor (although the more graphics-intensive ones do). So, if you still play old real-mode DOS games, you can try enabling Video BIOS Shadowing for better performance. This tip is courtesy of Ivan Warren.

New video cards, the ones that have accelerated functions, fall into a different category. They actually have a processor built into the card. In the same way that the system BIOS tells your processor how to start your computer, your video BIOS tells your video processor how to display images. The reason new cards have flash ROMs on them is they allow manufacturers tofix any bugs that exist in the code. Any operating system that uses the accelerated features of a video card will communicate directly with the video processor. This is the job of the video driver. The idea is, the driver presents the operating system with a documented set of function calls. When one of these calls is made, the driver sends the appropriate command to the video processor. The video processor then carries out the commands as its programming (the video BIOS) dictates.

As far as shadowing the video BIOS goes, it doesn't matter. Windows, Linux or any other operating system that uses the accelerated functions never directly communicates with the video BIOS. Good 'ole DOS, however, does; and the same functions that existed in the original VGA cards still exist in the new 3D cards. Depending on how the video interfaces of the DOS programs are written, they may benefit from having the video BIOS shadowed. So, apparently you are 100% correct in assuming that modern video cards do not use the 'DOS addressable' BIOS for anything except driverless VGA/EGA/text modes... Now, that's not to say 'BIOS updates' are useless, as the actual BIOS of the card includes far more than the little table DOS can see. It can include micro-code with patches for problems (just like how motherboard BIOS updates can fix certain processor problems).

BIOS shadowing can cause SERIOUS and permanent harm to the video card itself... After the failed 'shadowed' flash, the card was never again able to render DOS video modes or text; and further BIOS updates would not work since they 'failed to detect current BIOS revision'. If you are wondering why you should still update the video BIOS even though it appears to be useless, the video BIOS doesn't only contain DOS video functions. The video BIOS these days also contain code for 2D, 3D and video acceleration.

Therefore, using the latest video BIOS is likely to boost performance and cut down on bugs. In addition, the latest drivers may not work with older versions of the video BIOS. So, it's advisable to keep updating the video BIOS whether you use real-mode DOS or not. This tip is courtesy of Adam Nellemann.

Video ram cacheable

This feature enables or disables the caching of the video RAM at A0000h-AFFFFh using the processor's Level 2 cache. This is supposed to speed up accesses to the video RAM. However, this actually does not translate into better system performance. Many graphics cards now have a RAM bandwidth of 5.3GB/s (128bit x 166MHz DDR) and that number is climbing rapidly. Meanwhile, most system only have SDRAM bandwidth of around 1.06GB/s (64bit x 133MHz) or 2.13GB/s (64bit x 133MHz x 2) with DDR SDRAM. As you can see, the average graphics cards' memory subsystem is at least 2.5 to 5 times faster than system memory. Therefore, it makes more sense to cache the slower system SDRAM instead of the graphics card's RAM.

But even if you want to maximize the performance of the graphics card, caching the video RAM using the processor's L2 cache is actually quite pointless. This is because the video RAM communicates with the L2 cache via the AGP bus which has a maximum bandwidth of only 1.06GB/s using the AGP4X protocol. And that bandwidth is halved in this case because the data has to pass in two directions. So what it means in the end is that the caching of the video RAM has to be done via a 533MB/s-wide bottleneck!

In addition, if any program writes into this memory area, it will result in a system crash. So, there's very little benefit in caching the video card's RAM. It would be much better to use the processor's L2 cache to cache the system memory instead. It is recommended that you **disable** Video RAM Cacheable for better performance. For more detailed information, take a look at the Video RAM Caching guide.

MEMORY SUBSYSTEM

Act bank a to b cmd delay

Act Bank A to B CMD Delay (short for Activate Bank A to Activate Bank B Command Delay) or tRRD is a DDR timing parameter. It specifies the minimum amount of time between successive ACTIVATE commands to the same DDR device, even to different internal banks. The shorter the delay, the faster the next bank can be activated for read or write operations. However, because row activation requires a lot of current, using a short delay may cause excessive current surges.

Because this timing parameter is DDR device-specific, it may differ from one DDR device to another. DDR DRAM manufacturers typically specify the tRRD parameter based on the row ACTIVATE activity to limit current surges within the device. If you let the BIOS automatically configure your DRAM parameters, it will retrieve the manufacturer-set tRRD value from the SPD (Serial Presence Detect) chip. However, you may want to manually set the tRRD parameter to suit your requirements.

For desktop PCs, a delay of 2 cycles is recommended as current surges aren't really important. This is because the desktop PC essentially has an unlimited power supply and even the most basic desktop cooling solution is sufficient to dispel any extra thermal load that the current surges may impose. The performance benefit of using the shorter 2 cycles delay is of far greater interest. The shorter delay means every back-to-back bank activation will take one clock cycle less to perform. This improves the DDR device's read and write performance.

Note that the shorter delay of 2 cycles works with most DDR DIMMs, even at 133MHz (266MHz DDR). However, DDR DIMMs running beyond 133MHz (266MHz DDR) may need to introduce a delay of 3 cycles between each successive bank activation. Select **2 cycles** whenever possible for optimal DDR DRAM performance. Switch to **3 cycles** only when there are stability problems with the 2 cycles setting. In mobile devices like laptops however, it would be advisable to use the longer delay of 3 cycles. Doing so limits the current surges that accompany row activations. This reduces the DDR device's power consumption and thermal output, both of which should be of great interest to the road warrior.

Delay DRAM read latch

This feature is similar to DRAM Read Latch Delay. It fine-tunes the DRAM timing parameters to adjust for different DRAM loadings. The DRAM load changes with the number as well as the type of DIMMs installed. DRAM loading increases as the number of DIMMs increases. It also increases if you use double-sided DIMMs instead of single-sided ones. In short, the more DRAM devices you use, the greater the DRAM loading. As such, a single single-sided DIMM provides the lowest DRAM load possible.

With heavier DRAM loads, you may need to delay the moment when the memory controller latches onto the DRAM device during reads. Otherwise, the memory controller may fail to latch properly onto the desired DRAM device and read from it. Normally, you should let the BIOS select the optimal amount of delay from values preset by the manufacturer (using the Auto option). But if you notice that your system has become unstable upon installation of additional DIMMs, you should try setting the DRAM read latch delay yourself.

The longer the delay, the poorer the read performance of your memory modules. However, the stability of your memory modules won't increase together with the length of the delay. Remember, the purpose of the feature is only to ensure that the memory controller will be able to latch onto the DRAM device with all sorts of DRAM loadings.
The amount of delay should just be enough to allow the memory controller to latch onto the DRAM device in your particular situation. Don't unnecessarily increase the delay. It isn't going to increase stability. In fact, it may just make things worse! So, **start with 0.5ns and work your way up until your system stabilizes.**

If you have a light DRAM load, you can ensure optimal performance by manually using the No Delay option. This forces the memory controller to latch onto the DIMMs without delay, even if the BIOS presets indicate that a delay is needed. Naturally, this can potentially cause stability problems if you actually have a heavy DRAM load. Therefore, if you find that your system has become unstable after using the No Delay option, simply revert back to the default value of Auto so that the BIOS can adjust the read latch delay to suit the DRAM load.

DRAM act to prechrg cmd

Like SDRAM Tras Timing Value, this feature controls the memory bank's minimum row active time (tRAS). This constitutes the length of time from the activate command to the precharge command of the same bank. Hence, the name DRAM Act to PreChrg CMD which is short for DRAM Activate Command to Precharge Command. Now, tRAS is important because it determines how soon

after a row activation can the same row be precharged for another cycle. If an exceedingly long tRAS is chosen, the row may be unnecessarily delayed from precharging for another cycle. But if you set it for too short a period, there may not be enough time to complete the read/write cycle. When that happens, data may be lost or corrupted.

For optimal performance, **use the lowest value you can** (5T in this case). But if you start getting memory errors or system crashes, increase the value one clock cycle at a time until you get a stable system. Please note that because the bank cycle time (tRC) = minimum row active time (tRAS) + row precharge time (tRP), you should take into account the values for tRC and tRP before selecting the tRAS value.

DRAM data integrity mode

ECC, which stands for Error Checking and Correction, enables the memory controller to detect and correct single-bit soft memory errors. The memory controller will also be able to detect double-bit errors although it will not be able to correct them. This provides increased data integrity and system stability. However, this feature can only be enabled if you are using special ECC memory modules. Now, this type of memory module is special (and more expensive!) as it comes extra memory chips and a wider path. This is because the chipset needs to append a certain number of extra ECC bits (called ECC code) to each data word that's written to the memory module. When the data word is read back, the memory controller will recalculate the ECC code of the read data word and compare it to the original ECC code that was written to memory earlier. If the codes are identical, then the data is valid.

But if there's a single-bit error in the data word, the memory controller can identify the defective bit by analyzing the differences in the two ECC codes. That bit can then be corrected by simply flipping it to the opposite state (from 0 to 1 and vice versa). Just for general information, here's a list of ECC code length required for various data path widths using the current Hamming code algorithm standard :-

Data Path Width	ECC Code Length
8-bit	5 ECC bits
16-bit	6 ECC bits
32-bit	7 ECC bits
64-bit	8 ECC bits
128-bit	9 ECC bits

Because present day processors use 64-bit wide data paths, 72-bit (64-bit data + 8-bit ECC) ECC memory modules are required to implement ECC. Please note that the maximum data transfer rate of the 72-bit ECC memory module is the same as the 64-bit memory module. The extra 8-bits are only for the ECC code and do not carry any data. So, using 72-bit memory modules will not give you any boost in performance. In fact, because the memory controller has to calculate the ECC code for every data word that is read or written, there will be some performance degradation, roughly in the region of 3-5%. This is one of the reasons why ECC memory modules aren't that popular. Throw in the fact that ECC memory modules are both expensive and hard to come by; and you have the top three reasons why ECC memory modules will never be mainstream solutions.

But if data integrity is of utmost importance to you and you can't afford to have your system down due to errant cosmic rays or radiation from the DRAM packaging, ECC memory is the only way to go. The loss of 3-5% in memory performance is really nothing, compared to the peace of mind that ECC can give.

In any case, the matter of this BIOS feature is much easier to settle. **If you are using standard 64-bit memory modules, you must select the Non-ECC option**. **But if you already spent the extra dollar to get 72-bit ECC memory modules, you should enable the ECC feature**, no matter what people say about losing some memory performance. It doesn't make sense to buy expensive ECC memory modules and then disable ECC! Remember, you are not really losing performance. You are just trading it for greater stability and data integrity.

DRAM interleave time

This BIOS feature determines the amount of additional delay between successive bank accesses when the SDRAM Bank Interleave feature has been enabled. Naturally, the shorter the delay, the faster the memory module can switch between banks and consequently perform better. Therefore, it is recommended that you **set the DRAM Interleave Time as low as possible** for better memory performance. In this case, it would be 0ms which introduces no additional delay between bank accesses. Increase the DRAM Interleave Time to 0.5ms only if you experience stability problems.

DRAM prechrg to act cmd

Like SDRAM Trp Timing Value, this feature controls the memory bank's precharge time (tRP). This constitutes the time it takes for the Precharge command to complete and the row to be available for activation. Hence the name DRAM PreChrg to Act CMD which is short for DRAM Precharge Command to Activate Command. Now, tRP is important because it determines how soon a row can be activated after a Precharge command has been issued. If an exceedingly long tRP is chosen, that may unnecessarily reduce performance by preventing the row from being activated earlier. But if you set it for too short a period, the row may not be sufficiently precharged and that may cause data loss or corruption when the memory controller attempts to read from that row.

For optimal performance, **use the lowest value you can** (2T in this case). **But if you start getting memory errors or system crashes, increase the value.** Note that because the bank cycle time (tRC) = minimum row active time (tRAS) + row precharge time (tRP), you should take into account the values for tRC and tRAS before selecting the tRP value.

DRAM read latch delay

This BIOS feature is similar to Delay DRAM Read Latch. It fine-tunes the DRAM timing parameters to adjust for different DRAM loadings. The DRAM load changes with the number as well as the type of DIMMs installed. DRAM loading increases as the number of DIMMs increases. It also increases if you use double-sided DIMMs instead of single-sided ones. In short, the more DRAM devices you use, the greater the DRAM loading. As such, a single single-sided DIMM provides the lowest DRAM load possible.

With heavier DRAM loads, you may need to delay the moment when the memory controller latches onto the DRAM device during reads. Otherwise, the memory controller may fail to latch properly onto the desired DRAM device and read from it. The longer the delay, the poorer the read performance of your memory modules. However, the stability of your memory modules won't necessarily improve if you enable this feature. Remember, the purpose of the feature is only to ensure that the memory controller will be able to latch onto the DRAM device with all sorts of DRAM loadings.

So, for optimal performance, you should **disable** this feature. This prevents the BIOS from delaying the latching of the DRAM devices which produces the best read performance possible. However, if **you notice that your system has become unstable upon installation of additional DIMMs, enable this feature.** The BIOS will then automatically select the optimal amount of delay from values preset by the manufacturer.

Fast R/W turn around

When the memory controller receives a write command right after a read command, an additional period of delay is normally introduced before the write command is actually initiated. This extra delay is only introduced when there's a switch from reads to writes. Switching from writes to reads will not suffer from such a delay. As its name suggests, this BIOS feature allows you to skip that delay so that the memory controller can switch or "turn around" from reads to writes faster than normal. This improves the write performance of the memory subsystem. Therefore, it's recommended that you **enable** this feature for faster read-to-write turnarounds.

However, not all memory modules can work with the tighter read-to-write turnaround. If your memory modules cannot handle the faster read-to-write turnaround, data may be lost or become corrupted. When that happens, **disable** this feature to correct the problem.

Force 4 way interleave

This feature allows you to force the memory controller to use the 4-bank SDRAM interleave mode which provides better performance than the 2-bank interleave mode. However, you must have at least 4 banks of memory in the system for this feature to work properly. Please note that we are talking about memory banks here, not number of DIMMs. A SDRAM DIMM is internally made up of one or more memory banks that can be accessed simultaneously.

Normally, SDRAM DIMMs that use 16Mbit memory chips (usually 32MB or smaller in size) have only two memory banks. So, if you are using such a small capacity DIMM, you should disable Force 4-Way Interleave unless you use two or more DIMMs. SDRAM DIMMs that use 64Mbit or larger memory chips are four-banked in nature. These DIMMs are at least 64MB in size. If you are using such four-banked DIMMs, it doesn't matter if you are using just one DIMM or several of them. You should **enable Force 4-Way Interleave for better performance**. For more information on bank interleaving, you should check out the details of the SDRAM Bank Interleave BIOS feature.

MD driving strength

There's no auto-compensation mechanism for the memory bus. So, it's up to the motherboard designer to determine the amount of driving strength needed to compensate for the motherboard's impedance on the memory bus. The BIOS will then load up the preset driving strength value whenever it boots up the motherboard. The default driving strength is usually sufficient for normal DRAM loads. It is kept low in order to reduce EMI (Electromagnetic Interference) and power consumption. However, this means that the default driving strength may not be sufficient for heavy DRAM loads (multiple double sided DIMMs).

This is where the MD Driving Strength feature comes in. It offers simplified control of the driving strength of the memory data bus. The default value is Lo or Low. With heavy DRAM loads, you might want to set this feature to Hi or High. Due to the nature of this BIOS feature, it is possible to use it as an aid in overclocking the memory bus. Your SDRAM DIMM may not overclock as well as you want it to. But by raising the driving strength of the memory bus, it is possible to improve its stability at overclocked speeds.

However, this is not a surefire way of overclocking the memory bus. All you may get at the end of the day is increased EMI and power consumption. In addition, increasing the memory bus drive strength will not improve the performance of your memory subsystem. Therefore, it is recommended that you leave the MD Driving Strength at its **default Lo or Low setting** unless you have a heavy DRAM load or if you are trying to stabilize an overclocked DIMM.

Memory hole at 15M-16M

Certain ISA cards require exclusive access to the 1MB block of memory from the 15th to the 16th megabyte to work properly. Enabling this feature reserves that memory area for the card's use. If this feature is not enabled, that memory area will be made available to the operating system and this may prevent the ISA card from working properly. When you enable this feature, 1MB of RAM (the 15th MB) will be reserved exclusively for the ISA card's use. This effectively reduces the total amount of memory available to the operating system by 1MB. Therefore, if you have 256MB of RAM, the usable amount of RAM will be reduced to 255MB.

Please note that in certain motherboards, this feature may actually render all RAM above the 15th MB unavailable to the operating system! In such cases, you will end up with only 14MB of usable RAM, irrespective of how much RAM your system actually has. Since ISA cards are a thing of the past, you should **disable** this feature. Even if you have an ISA card that you absolutely have to use, that doesn't mean you actually need to enable this feature. Most ISA cards do not need exclusive access to this memory area. Make sure that your ISA card requires this memory area before enabling this feature. This feature should only be considered as a final resort in getting a stubborn ISA card to work.

OS select for DRAM > 64mb

When there's more than 64MB of RAM in a computer, older versions of IBM's OS/2 operating system differ from other operating systems in the way it manages memory. Please note that this is only true for older versions of OS/2 that haven't been upgraded using IBM's FixPaks. If you are running an old, non-updated version of OS/2, you will need to select the OS/2 option. Starting with OS/2 Warp v3.0, the memory management system had been changed to the more conventional method. Therefore, if you are using OS/2 Warp v3.0 or higher, you should select Non-OS/2 instead. You should also select Non-OS/2 if you have upgraded an older version of OS/2 with the FixPaks that IBM have been releasing over the years.

If you select the OS/2 option with a newer or updated version (v3.0 or higher) of OS/2, it will cause erroneous memory detection. For example, if you have 64MB of RAM, it may only register as 16MB. Or if you have more than 64MB of RAM, it may register as only 64MB of RAM. So, if you are running OS/2 Warp v3.0 or higher; or if you have already installed all the relevant IBM FixPaks, you should select Non-OS/2. Users of non-OS/2 operating systems (like Microsoft Windows XP) should select the **Non-OS/2 option**. Doing otherwise will cause memory errors if you have more than 64MB of RAM in your system.

Read wait state

This feature determines how long the memory controller should wait before sending the read data to the data requester (i.e. processor, graphics card, etc..). By default, a wait state is added before the data is sent to the requester. Therefore, read performance is reduced because the memory controller has to wait one cycle before sending any data. In addition, to prevent overlapping of a read and a write request when the Read Wait State is set to 1 Cycle, an additional delay cycle is inserted between every read cycle that is followed immediately by a write cycle. This is similar to disabling the Fast R-W Turn Around feature. This effectively reduces the memory write performance.

Therefore, it is recommended that you **set the Read Wait State to 0 Cycle for better memory read and write performance**. **Note that this may cause system instabilities in certain situations. When that happens, just reset the value to 1 Cycle.**

Read around write

This BIOS feature allows the processor to execute read commands out of order, as if they are independent from the write commands. It does this by using a Read-Around-Write buffer. Writes are accumulated in this buffer and then written to memory as a burst transfer. This reduces the number of writes to memory and boosts the memory subsystem's read performance.

In addition, the Read-Around-Write buffer serves as a cache of the most up-to-date data that hasn't been written to memory yet. So, if a read command points to a memory address whose latest write (content) is still in the Read-Around-Write buffer (waiting to be copied into memory), the read command will be satisfied by the cache contents instead. In short, if the Read-Around-Write buffer has the data, the processor can directly read from it, without waiting to access the memory (which will take more time). This further improves the memory's read performance. Therefore, it is highly recommended that you **enable** this feature for better memory read performance.

Refresh interval

Memory cells normally need to be refreshed every 64 msec. However, simultaneously refreshing all the rows in a typical memory chip will cause a big surge in power requirements. In addition, a simultaneous refresh causes all data requests to stall, which greatly impacts performance. To avoid both problems, refreshes are normally staggered according to the number of rows. Since a typical memory chip contains 4096 rows, the memory controller usually refreshes a different row every 15.6 µsec (64,000 µsec / 4096 rows = 15.6 µsec). This reduces the amount of current used during each refresh and it allows data to be accessed from the other rows.

Usually, DIMMs that use 128Mbit or smaller memory chips have 4096 rows while memory chips with higher capacity (256Mbit and above) will have 8192 rows. For memory chips that come with 8192 rows, the refresh interval will need to be halved to 7.8 µsec because there are now twice as many rows to serviced within the stipulated 64 msec for the entire chip. Therefore, the typical refresh interval for 128Mbit (not MB!) or smaller memory chips would be 15.6 µsec while those for 256Mbit or larger memory chips would be 7.8 µsec. Please note that if you are using a mix of 128Mbit or smaller DIMMs with 256Mbit or larger DIMMs, the fail-safe Refresh Interval would be 7.8 µsec, not 15.6 µsec.

Although JEDEC standards call for a 64 msec refresh cycle, memory chips these days can actually hold data for longer than that. So, using a longer refresh cycle is quite possible. With a longer refresh cycle, the memory chips are refreshed less often, reducing both the amount of bandwidth wasted on refreshes and the amount of power consumed (which is great for laptops and other portable devices). For better performance, you should consider increasing the Refresh Interval from the default values (15.6 µsec for 128Mbit or smaller memory chips and 7.8 µsec for 256Mbit or larger memory chips) up to 128 µsec. Please note that **if you increase the Refresh Interval too much, the memory cells may lose their contents**. Therefore, you should start with small increases in the Refresh Interval and test your system after each hike before increasing it further. If you face stability problems upon increasing the Refresh Interval, reduce the Refresh Interval step by step until the system is stable.

Refresh mode select

Memory cells normally need to be refreshed every 64 msec. However, simultaneously refreshing all the rows in a typical memory chip will cause a big surge in power requirements. In addition, a simultaneous refresh causes all data requests to stall, which greatly impacts performance. To avoid both problems, refreshes are normally staggered according to the number of rows. Since a typical memory chip contains 4096 rows, the memory controller usually refreshes a different row every 15.6 µsec (64,000 µsec / 4096 rows = 15.6 µsec). This reduces the amount of current used during each refresh and it allows data to be accessed from the other rows.

Usually, DIMMs that use 128Mbit or smaller memory chips have 4096 rows while memory chips with higher capacity (256Mbit and above) will have 8192 rows. For memory chips that come with 8192 rows, the refresh interval will need to be halved to 7.8 µsec because there are now twice as many rows to serviced within the stipulated 64 msec for the entire chip. Therefore, the typical refresh interval for 128Mbit (not MB!) or smaller memory chips would be 15.6 µsec while those for 256Mbit or larger memory chips would be 7.8 µsec. Please note that if you are using a mix of 128Mbit or smaller DIMMs with 256Mbit or larger DIMMs, the fail-safe refresh interval would be 7.8 µsec, not 15.6 µsec.

Although JEDEC standards call for a 64 msec refresh cycle, memory chips these days can actually hold data for longer than that. So, using a longer refresh cycle is quite possible. With a longer refresh cycle, the memory chips are refreshed less often, reducing both the amount of bandwidth wasted on refreshes and the amount of power consumed (which is great for laptops and other portable devices). For better performance, you should consider increasing the Refresh Mode Select from the default values (15.6 µsec for 128Mbit or smaller memory chips and 7.8 µsec for 256Mbit or larger memory chips) up to 128 µsec. Please note that **if you increase the Refresh Mode Select too much, the memory cells may lose their contents**. Therefore, you should start with small increases in the Refresh Mode Select and test your system after each hike before increasing it further. If you face stability problems upon increasing the Refresh Mode Select, reduce it step by step until the system is stable.

SDRam Bank Interleave

This feature enables you to set the interleave mode of the SDRAM interface. Interleaving allows banks of SDRAM to alternate their refresh and access cycles. One bank will undergo its refresh cycle while another is being accessed. This improves performance of the SDRAM by masking the refresh time of each bank. A closer examination of interleaving will reveal that since the refresh cycles of all the SDRAM banks are staggered, this produces a kind of pipelining effect.

If there are 4 banks in the system, the CPU can ideally send one data request to each of the SDRAM banks in consecutive clock cycles. This means in the first clock cycle, the CPU will send an address to Bank 0 and then send the next address to Bank 1 in the

second clock cycle before sending the third and fourth addresses to Banks 2 and 3 in the third and fourth clock cycles respectively. The sequence would be something like this :- As a result, the data from all four requests will arrive consecutively from the SDRAM without any delay in between. But if interleaving was not enabled.

With interleaving, the first bank starts transferring data to the CPU in the same cycle that the second bank receives an address from the CPU. Without interleaving, the CPU would send the address to the SDRAM, receive the data requested and then wait for the SDRAM to refresh before initiating the second data transaction. This wastes a lot of clock cycles. That's why the memory bandwidth increases when interleaving is enabled. However, bank interleaving only works if the addresses requested consecutively are not in the same bank. If they are, then the data transactions behave as if the banks were not interleaved. The CPU will have to wait until the first data transaction clears and that SDRAM bank refreshes before it can send another address to that bank.

Each SDRAM DIMM consists of either 2 banks or 4 banks of memory. 2-banked SDRAM DIMMs use 16Mbit SDRAM chips and are usually 32MB or less in size. 4-banked SDRAM DIMMs, on the other hand, usually use 64Mbit SDRAM chips though the SDRAM density may be up to 256Mbit per chip. All SDRAM DIMMs of at least 64MB in size or greater are 4-banked in nature.

If you are using a single 2-banked SDRAM DIMM, set this feature to 2-Bank. But if you are using two 2-banked SDRAM DIMMs, you can use the 4-Bank option as well. With 4-banked SDRAM DIMMs, you can use either interleave options.

Naturally, 4-bank interleave is better than 2-bank interleave so if possible, **set it to 4-Bank**. Use the 2-Bank option only if you are using a single 2-banked SDRAM DIMM. Please note, however, that Award (now part of Phoenix Technologies) recommends that SDRAM bank interleaving be disabled if 16Mbit SDRAM DIMMs are used. This is because early 16Mbit SDRAM DIMMs used to have stability problems with bank interleaving. All current SDRAM modules can use bank interleaving without stability problems though.

SDRam cas latency time

This BIOS feature controls the time delay (in clock cycles) that passes before the SDRAM module starts to carry out a read command after receiving it. It also determines the number of clock cycles required for the completion of the first part of a burst transfer. In other words, the lower the latency, the faster memory reads can occur. Please note that some SDRAM modules may not be able to handle the lower latency and may lose data. Therefore, **set the SDRAM CAS Latency Time to 2 for better memory read performance but increase it to 3 (2.5 in DDR memory) if your system becomes unstable.** Interestingly, increasing the CAS latency time does have an advantage in that it will often allow the SDRAM module to run at a higher clock speed. So, if you hit a snag while overclocking your SDRAM module(s), try increasing the CAS latency time.

SDRam cycle length

This feature is same as the SDRAM CAS Latency Time feature. This BIOS feature controls the time delay (in clock cycles) that passes before the SDRAM module starts to carry out a read command after receiving it. It also determines the number of clock cycles required for the completion of the first part of a burst transfer. In other words, the lower the latency, the faster memory reads can occur.

Please note that some SDRAM modules may not be able to handle the lower latency and may lose data. Therefore, **set the SDRAM Cycle Length to 2 for better memory read performance but increase it to 3 (2.5 in DDR memory) if your system becomes unstable.** Interestingly, increasing the cycle length does have an advantage in that it will often allow the SDRAM module to run at a higher clock speed. So, if you hit a snag while overclocking your SDRAM module(s), try increasing the cycle length.

SDRam cycle time tras/trc

This feature determines the minimum number of clock cycles required for the Tras and the Trc of the SDRAM. Tras refers to the SDRAM's Row Active Time, which is the length of time the row will remain open for data transfers. It is also known as Minimum RAS Pulse Width. Trc, on the other hand, refers to the SDRAM's Row Cycle Time, which determines the length of time for the entire row-open to row-refresh cycle to complete.

The **default setting is 6/8 which is more stable and slower than 5/6.** The 5/6 setting cycles the SDRAM faster but may not leave the row open long enough for data transactions to complete. When this happens, the contents of the memory cells may be corrupted. This is especially true at SDRAM clockspeeds above 100MHz.

Therefore, you should try 5/6 for better SDRAM performance and only increase it to 6/8 if your system becomes unstable. You can also use the slower 6/8 setting if you are trying to overclock your SDRAM modules as it may allow the modules to run at a higher clockspeed.

SDRam idle limit

This feature sets the number of idle cycles a SDRAM bank has to wait before recharging. It allows you to improve the efficiency of the SDRAM read and write cycles by adjusting the amount of time that the bank is allowed to remain idle before it is recharged. Increasing the SDRAM Idle Limit to more than the default of 8 cycles allows the SDRAM bank to delay recharging longer during times of no activity so that if a read or write command comes along, it can be instantly satisfied. However, this is limited by the refresh cycle already set by the BIOS. That means the SDRAM bank will refresh when it needs to be recharged whether the number of idle cycles have reached the SDRAM Idle Limit or not. So, the SDRAM Idle Limit setting can only be used to force the refreshing of the SDRAM bank before the set refresh cycle but not to actually delay the refresh cycle.

Reducing the number of cycles from the default of 8 cycles to 0 cycles forces the SDRAM bank to initiate a refresh cycle once no valid requests are sent to the memory controller. In short, the SDRAM bank is refreshed as soon as it is idle. Theoretically, this may increase the efficiency of the SDRAM as the effects of refreshing the banks are masked because they are done during idle cycles. However, if there are any data requests after the bank starts its refresh cycle, they will have to wait until the bank is completely refreshed and activated before they can be satisfied.

Because refreshes do not occur that often (usually only about once every 64 msec), the impact of refreshes on SDRAM performance is really quite minimal and the benefits of masking the SDRAM's refreshes during idle cycles will not be noticeable. In fact, there's a high risk that data requests will get stalled more often, especially with the idle limit of 0 cycle. As such, you are more likely to see reduced performance with the 0 cycles setting, especially since even a single idle cycle will cause the bank to go into a bandwidth-expensive refresh cycle. On the plus side, the contents of the memory cells will be refreshed more often and there will be little chance of losing data due to insufficiently refreshed memory cells. For best performance, this feature should be disabled so that

refreshing can be delayed for as long as possible. This reduces the number of refreshes and increases the effective memory bandwidth.

An alternative method would be to greatly increase the value of the Refresh Interval or Refresh Mode Select feature to boost bandwidth and use this feature to maintain the data integrity of the memory cells. As ultra long refresh intervals (i.e. 64 or 128 µsec) can cause memory cells to lose their contents, setting a low SDRAM Idle Limit like 0 or 8 cycles allows the memory cells to be refreshed more often, with a high chance of those refreshes being done during idle cycles. This appears to combine the best of both worlds - a long bank active period when the memory controller is being stressed and more refreshes when the memory controller is idle.

In reality though, this is a really unreliable way of ensuring sufficient refresh cycles since it depends on the vagaries of memory usage to provide sufficient idle cycles to trigger the refreshes. If your memory subsystem is constantly in heavy use, there may not be any idle cycles to trigger an early refresh. This will cause the memory cells to lose their contents because they are not being refreshed enough. Therefore, it is recommended that you maintain a proper refresh interval and **disable** this feature. This will allow you to boost memory bandwidth by delaying refreshes for as long as possible and still maintain the data integrity of the memory cells via regular and reliable refresh cycles.

SDRam leadoff command
This option allows you to adjust the leadoff time needed before the data stored in the SDRAM can be accessed. In most cases, it is the access time for the first data element in a burst. The shorter the leadoff time, the faster read operations can start. Therefore, it is recommended that you set the SDRAM Leadoff Command value to **3** for faster SDRAM reads. Please note, however, that not all SDRAM modules can work properly with the shorter leadoff time. **So, if your system becomes unstable after using the Leadoff Command value of 3 clock cycles, revert back to the slower default leadoff time of 4 clock cycles.**

SDRam page closing policy
The memory controller allows up to four pages to be opened at any one time. These pages have to be in separate memory banks and only one page may be open in each memory bank. If a processor cycle to the SDRAM falls within those open pages, it can be satisfied without delay. This naturally improves performance. But if it does not, then either one page must be closed and the correct page opened, resulting in the full latency penalty... or all open pages are closed and new pages opened up. This feature basically determines if the chipset should try to leave the pages open (by closing only one open page) or try to keep them closed (by closing all open pages) whenever there's a page miss.

The One Bank setting forces the memory controller to only close one page whenever a page miss occurs. This allows the other pages to be accessed at the cost of only 1 clock cycle. However, when a page miss occurs, there's a chance that subsequent data requests will result in page misses as well. In long memory reads that cannot be satisfied by any of the open pages, this may cause up to four full latency reads to occur, which reduces performance. Fortunately, after the four full latency reads, the memory controller can often predict what pages will be needed next and open them for minimum latency reads. Thus, the effect of consecutive page misses will be somewhat limited.

The All Banks setting, on the other hand, forces the memory controller to send an All Banks Precharge Command to the SDRAM interface whenever there's a page miss. This causes all the open pages to close (precharge). Therefore, subsequent reads only need to activate the necessary memory bank. This is useful in cases where subsequent data requests will result in page misses as there's no need to wait for the memory banks to precharge before they can be activated. However, it also means that you won't be able to benefit from data accesses that could have been satisfied by the open pages.

As you can see, both settings have their advantages and disadvantages. But you should see better performance with the One Bank setting as the open pages allow very fast accesses. The All Banks setting, however, has the advantage of keeping the memory contents refreshed more often. This improves stability although this is only useful if you have chosen a SDRAM refresh interval that is longer than the standard 64 msec. Therefore, it is recommended that you **use the One Bank setting for better performance**. **The All Banks setting can be used to improve stability but if you are keeping the refresh interval within specification, then it is of little use.**

SDRam precharge control
The memory controller allows up to four pages to be opened at any one time. These pages have to be in separate memory banks and only one page may be open in each memory bank. If a processor cycle to the SDRAM falls within those open pages, it can be satisfied without delay. This naturally improves performance. But if it does not, then either one page must be closed and the correct page opened, resulting in the full latency penalty... or all open pages are closed and new pages opened up.

This feature basically determines if the chipset should try to leave the pages open (by closing only one open page) or try to keep them closed (by closing all open pages) whenever there's a page miss. When enabled, the memory controller will only close one page whenever a page miss occurs. This allows the other pages to be accessed at the cost of only 1 clock cycle. However, when a page miss occurs, there's a chance that subsequent data requests will result in page misses as well. In long memory reads that cannot be satisfied by any of the open pages, this may cause up to four full latency reads to occur, which reduces performance. Fortunately, after the four full latency reads, the memory controller can often predict what pages will be needed next and open them for minimum latency reads. Thus, the effect of consecutive page misses will be somewhat limited.

When disabled, however, the memory controller will send an All Banks Precharge Command to the SDRAM interface whenever there's a page miss. This causes all the open pages to close (precharge). Therefore, subsequent reads only need to activate the necessary memory bank. This is useful in cases where subsequent data requests will result in page misses as there's no need to wait for the memory banks to precharge before they can be activated. However, it also means that you won't be able to benefit from data accesses that could have been satisfied by the open pages.

As you can see, both settings have their advantages and disadvantages. But you should see better performance with this feature enabled as the open pages allow very fast accesses. The disabled setting, however, has the advantage of keeping the memory contents refreshed more often. This improves stability although this is only useful if you have chosen a SDRAM refresh interval that is longer than the standard 64 msec. Therefore, it is recommended that you **enable this feature for better performance.** You can **disable this feature to improve stability but if you are keeping the refresh interval within specification, then it is of little use.**

SDRam RAS precharge time
This feature sets the number of cycles required for the RAS (Row Address Strobe) to accumulate its charge before the SDRAM refreshes. Reducing the precharge time to 2 improves SDRAM performance. However, the precharge time of 2 may be insufficient for some SDRAM modules. In such cases, the module may not be refreshed properly and it may fail to retain data. So, it is recommended that you **set the SDRAM RAS Precharge Time to 2 for better performance but increase it to 3 if you experience system stability issues after reducing the precharge time.**

SDRam RAS to CAS delay
This feature allows you to insert a delay between the RAS (Row Address Strobe) and CAS (Column Address Strobe) signals. This delay occurs when the SDRAM is written to, read from or refreshed. Naturally, reducing the delay improves the performance of the SDRAM module while increasing it reduces performance. Therefore, it is recommended that you **reduce the delay from the default value of 3 to 2 for better SDRAM performance**. However, **if you experience system stability issues after reducing the delay, reset the value back to 3.**

SDRam tras timing value
Like DRAM Act to PreChrg CMD, this feature controls the memory bank's minimum row active time (tRAS). This constitutes the length of time from the activate command to the precharge command of the same bank. Now, tRAS is important because it determines how soon after a row activation can the same row be precharged for another cycle. If an exceedingly long tRAS is chosen, the row may be unnecessarily delayed from precharging for another cycle. But if you set it for too short a period, there may not be enough time to complete the read/write cycle. When that happens, data may be lost or corrupted.

For optimal performance, **use the lowest value you can (usually 5 clock cycles). But if you start getting memory errors or system crashes, increase the value one clock cycle at a time until you get a stable system.** Please note that because the bank cycle time (tRC) = minimum row active time (tRAS) + row precharge time (tRP), you should take into account the values for tRC and tRP before selecting the tRAS value.

SDRam trc timing value
This feature controls the memory bank's cycle time (tRC). This constitutes the time it takes for the bank to cycle from one activation to another. Now, tRC is important because it determines the minimum number of clock cycles it takes for the bank to be activated, precharged and activated again. The shorter the tRC, the faster the memory bank can cycle and this improves performance. However, if you set it for too short a period, the row may not be sufficiently precharged or remain activated long enough; and that may cause data loss or corruption. But if an exceedingly long tRC is chosen, this may unnecessarily reduce performance by preventing the bank from being cycled faster and thus allowing data accesses to occur faster.

For optimal performance, **use the lowest value you can** (usually 7 clock cycles). But **if you start getting memory errors or system crashes, increase the value**. Note that because the bank cycle time (tRC) = minimum row active time (tRAS) + row precharge time (tRP), you should take into account the values for tRAS and tRP before selecting the tRC value.

SDRam trcd timing value
This feature controls the memory bank's RAS to CAS delay (tRCD). Formula-wise, tRCD = RAS to CAS latency + read or write command delay. This constitutes the time it takes before a read or write command can be issued to the memory bank after it is activated. Now, tRC is important because it determines the length of the delay that takes place after activation of a bank to the issuing of a read or write command to that bank. The shorter the delay, the earlier the read or write command can be issued and this improves performance. However, if the delay is too short, the bank may not be properly activated when the read or write command is received. This may cause data loss or corruption. On the other hand, an exceedingly long tRCD reduces performance.

For optimal performance, use the lowest value you can (usually 3 clock cycles). **But if you start getting memory errors or system crashes, increase the value**.

SDRam trp timing value
Like DRAM PreChrg to Act CMD, this feature controls the memory bank's precharge time (tRP). This constitutes the time it takes for the Precharge command to complete and the row to be available for activation. Now, tRP is important because it determines how soon a row can be activated after a Precharge command has been issued. If an exceedingly long tRP is chosen, that may unnecessarily reduce performance by preventing the row from being activated earlier. But if you set it for too short a period, the row may not be sufficiently precharged and that may cause data loss or corruption when the memory controller attempts to read from that row.

For optimal performance, **use the lowest value you can** (usually 2 clock cycles). But **if you start getting memory errors or system crashes, increase the value.** Note that because the bank cycle time (tRC) = minimum row active time (tRAS) + row precharge time (tRP), you should take into account the values for tRC and tRAS before selecting the tRP value.

SDRam trrd timing value
tRRD is a DDR timing parameter which specifies the minimum amount of time between successive ACTIVATE commands to the same DDR device, even to different internal banks. The shorter the delay, the faster the next bank can be activated for read or write operations. However, because row activation requires a lot of current, using a short delay may cause excessive current surges. Because this timing parameter is DDR device-specific, it may differ from one DDR device to another. DDR DRAM manufacturers typically specify the tRRD parameter based on the row ACTIVATE activity to limit current surges within the device. If you let the BIOS automatically configure your DRAM parameters, it will retrieve the manufacturer-set tRRD value from the SPD (Serial Presence Detect) chip. However, you may want to manually set the tRRD parameter to suit your requirements.

For desktop PCs, a delay of 2 cycles is recommended as current surges aren't really important. This is because the desktop PC essentially has an unlimited power supply and even the most basic desktop cooling solution is sufficient to dispel any extra thermal load that the current surges may impose. The performance benefit of using the shorter 2 cycles delay is of far greater interest. The shorter delay means every back-to-back bank activation will take one clock cycle less to perform. This improves the DDR device's read and write performance.

Note that the shorter delay of 2 cycles works with most DDR DIMMs, even at 133MHz (266MHz DDR). However, DDR DIMMs running beyond 133MHz (266MHz DDR) may need to introduce a delay of 3 cycles between each successive bank activation. **Select 2 cycles whenever possible for optimal DDR DRAM performance. Switch to 3 cycles only when there are stability problems with the 2 cycles setting.** In mobile devices like laptops however, it would be advisable to use the longer delay of 3 cycles. Doing so limits the current surges that accompany row activations. This reduces the DDR device's power consumption and thermal output, both of which should be of great interest to the road warrior.

Shadowing address ranges

This feature allows you to cordon off specific memory blocks (xxxx-xxxx) to shadow the BIOS of certain add-on cards. This may improve performance of the card if the BIOS is used to control its functions. Such applications are mostly limited to bootable network cards. In most cases, there's no need for this feature as modern operating systems directly access hardware through drivers. Shadowing will just waste memory. Therefore, it is recommended that you **disable** this feature.

Ryu Connor confirmed this by directing me to the Microsoft article, Shadowing BIOS under WinNT 4.0. According to this article, shadowing the BIOS (irrespective of what BIOS it is) will not bring about any performance enhancements because it is not used by Windows NT. It will only waste memory. Although the article did not say anything about other versions of Microsoft Windows, this is true for all version of Microsoft Windows from Windows 95 onwards. In addition, Ivan Warren warns that if you are using an add-on card which is using the CXXXX-EFFFF area for I/O, shadowing that memory block may prevent the card from working because read or write requests might not be passed to the ISA bus.

Super bypass mode

This feature basically enables the memory request organizer (MRO) of the memory controller to skip certain pipeline stages when transferring data to and from the memory subsystem. This improves memory performance by allowing low latency accesses to the memory subsystem. However, this feature can only be safely enabled if the following conditions are true :-

- The system only has a single processor present. Systems with dual-processor motherboards can also enable this feature if only one processor is present.
- The processor clock speed multiplier must be 4 or greater. This means the processor must be running at least four times faster than its bus speed.

For better memory performance, it is recommended that you enable this feature. However, you must make sure that you are only using a single processor that is running at least four times faster than the processor bus. You should **disable this feature if your system does not meet the two requirements stated above.**

Super bypass wait state

This feature is used to fine-tune the Super Bypass feature to correct for internal timing variations. When enabled, the memory controller forces a wait state delay for all super bypass requests. Official documents recommend that a wait state be added for a 133MHz memory bus (266MHz in DDR SDRAM systems). Systems using a 100MHz memory bus (200MHz in DDR SDRAM systems) do not need this delay. Of course, those are just the safe, official recommendations for this feature. As forcing a wait state on all super bypass requests reduces the effectiveness of the Super Bypass feature, **it is recommended that you try using the 0 Cycle setting.** It should work even at memory clock speeds greater than 133MHz. But **if you start experiencing system stability issues after using this 0 Cycle setting**, set this feature to 1 Cycle. This slows down the super bypass transactions but will allow your system to use the Super Bypass feature at higher clock speeds.

System bios cacheable

This feature is only valid when the motherboard BIOS is shadowed. Since most motherboard manufacturer hardwire the shadowing of the motherboard BIOS, this is really a moot point. Enabling this feature forces the processor's Level 2 cache to cache the motherboard BIOS ROM from F0000h to FFFFFh. This greatly speeds up accesses to the BIOS. However, this does not translate into better system performance because modern operating systems like Microsoft Windows XP do not need to access the motherboard BIOS. Everything can be done much quicker by using drivers to access the hardware directly.

As such, it would be a waste of Level 2 cache bandwidth if the motherboard BIOS is cached instead of data that are more critical to the system's performance. In addition, if any errant program writes into this memory area, it will result in a system crash. So, it is highly recommended that you **disable** this feature for better system performance.

Write date in read delay

This feature controls the Write Data In to Read Command Delay (tWTR) memory timing. This constitutes the minimum number of clock cycles that must occur between the last valid write operation and the next read command to the same internal bank of the DDR device. Note that this is only applicable for read commands that follow a write operation. Consecutive read operations or writes that follow reads are not affected. With a 1 Cycle delay, a read command that follows a valid write operation will be delayed one clock cycle after the completion of that write command before it is issued. The 2 Cycles option increases the delay to two clock cycles.

Generally speaking, the 1 Cycle delay offers faster switching from writes to reads and consequently better read performance. The 2 Cycles delay reduces read performance slightly but it will improve stability, especially at higher clock speeds. It may also allow the memory chips to clock higher. In other words, increasing this delay (as well as other memory timings) may allow you to overclock the module higher than is normally possible.

The default is 2 Cycles but **it is recommended that you use the 1 Cycle delay if possible for better memory read performance.** But **if you face stability issues, increasing this delay to 2 Cycles** is one of the steps you should try.

Write recovery time

This feature controls the tWR memory timing which determines the minimum number of clock cycles that must occur before a precharge command can be asserted to the bank after the completion of a valid write operation to the same bank. In other words, it specifies the amount of delay (in clock cycles) that must occur between a write command and a subsequent precharge command to the same internal bank. Please note that it does not determine the time it takes for the bank to precharge. This feature only controls how soon the bank can start precharging right after a write operation to the same internal bank.

The shorter the delay, the earlier the bank can be precharged for another read/write operation. This improves performance and allows faster cycling times. Contrary to other memory timings, a shorter delay here may improve the overclockability of the memory module as it allows faster cycling times. The default value is 2 Cycles but **it is recommended that you use the 1 Cycle delay for better memory read performance** as well as increased overclockability.

MISCELLANEOUS

Anti virus protection

The Anti-Virus Protection feature is actually an enhanced version of the Virus Warning feature. Besides the standard boot sector or partition table protection, this BIOS feature also offers more comprehensive anti-virus protection via built-in rule-based anti-virus code like ChipAway. When you enable this feature, the BIOS will halt the system and flash a warning message whenever there's an attempt to write to the boot sector or the partition table. Note that this only protects the boot sector and the partition table, not the entire hard disk.

This feature can cause problems with software that need to access the boot sector. One good example is the installation routine of all versions of Microsoft Windows from Windows 95 onwards. When enabled, this feature causes the installation routine to fail. Also, many disk diagnostic utilities that access the boot sector can also trigger the system halt and error message as well. Therefore, you should disable this feature before running such software.
Alternatively, you can select the internal rule-based anti-virus code. The software used in the reference motherboard is called ChipAway. Enabling ChipAway provides better anti-virus protection by scanning for and detecting boot viruses before they have a chance to infect the boot sector of any hard disk.

Note that this feature is useless for hard disks that run on external controllers with their own BIOS. Boot sector viruses will bypass the system BIOS with its anti-virus protection features and write directly to the hard disks. Such controllers include additional IDE or SCSI controllers that are either built into the motherboard or available via add-on cards. I recommend **disabling** this.

Flash bios protection

One frustrating problem faced by many users and motherboard manufacturers is the corruption of the BIOS by viruses or failed BIOS updates. This has been a problem since motherboards started shipping with Flash BIOS ROMs instead of static BIOS ROMs. Because such an issue could potentially mean high numbers of really needless RMAs, many manufacturers now write-protect the BIOS code and only allow write access to the Flash ROM when the user specifically toggles a switch. The switch can be physical like a jumper or DIP switch or it can be a software toggle like a BIOS feature.

The Flash BIOS Protection feature is a software toggle that controls write access to the BIOS. When it is enabled, the BIOS code is write-protected and cannot be changed. This protects it from any attempt to modify it, including BIOS updates and virus attacks. Therefore, if you intend to update the BIOS, you'll need to disable this feature first. It is highly recommended that you **enable** this feature at all times. You should only disable it when you intend to update the BIOS. After updating the BIOS, you should immediately re-enable it to protect the BIOS against viruses.

Hardware reset protect

This BIOS feature is very useful for file servers and routers that need to be running 24 hours a day, 365 days a year. When it is enabled, the hardware reset button will be disabled. This prevents the possibility of any accidental resets. When disabled, the reset button will function as normal. If you are running a mission-critical server or have kids who just love to press little red buttons, it is highly recommended that you enable this feature. Otherwise, it is really up to your preference. Naturally, people using buggy operating systems or applications are advised to keep this feature **disabled** for more convenient reboots. Heheh...

KBC input clock protect

The PS/2 keyboard communicates with the keyboard controller on the motherboard via a serial data link. The speed of the data link depends on the clock signal generated by the keyboard controller. The higher the clock speed, the faster the keyboard interface. This translates into a more responsive keyboard although not all keyboards can be overclocked. This feature allows you to adjust the keyboard interface clock for better response or to fix a keyboard problem. It is recommended that you select the **16MHz** option for a better keyboard response. **But if the keyboard performs erratically or fails to initialize, try a lower clock speed** to fix the problem.

Onboard IR function

This feature is usually found under the Onboard Serial Port 2 option. It will only appear if the second serial port is enabled. This is because it is slaved to the second serial port. There are two different IR (Infra-Red) modes - IrDA and ASK IR. Select the IR mode that is supported by the external IR device. Choosing the wrong IR mode will prevent your computer from communicating with the external IR device.

Please note that this feature requires an IR beam kit to be plugged into the IR header on the motherboard. Without the IR beam kit, enabling this feature won't have any effect. Also, enabling the IR function prevents the second serial port from being used by normal serial devices. So, **if you do not need to use the onboard IR function, disable this feature to allow the second serial port to be used** for other purposes.

Power on function

This feature allows you to set the method by which your system can be turned on. Normally, it is set as Button Only so that your system will only start up if you press the casing's power button or switch. Other options including starting up the system using the keyboard (if it supports the Keyboard 98 standard), a keyboard hot key (for other standard keyboards) or the mouse.

Please note that only PS/2 mice support the Mouse Left or Mouse Right options. Mice using serial or USB connections do not support this power on function. However, some PS/2 mice may not be able to support this function due to compatibility problems (read : bugs, design flaws). If you select, the Mouse Left option, the left button of the mouse will be used to start up the system. The Mouse Right option selects the right mouse button as the power on button instead. The Keyboard 98 option will only work if you have installed Windows 98 (or better) and you have the appropriate keyboard. Then you can use the keyboard's wake-up key to start up the system.

Older keyboards that do not conform to the Keyboard 98 standard and therefore do not have the special wake-up key can use the Hot Key option instead. There are twelve hot keys available : **Ctrl-F1** to Ctrl-F12. Select the hot key you want and you will be able to start up the computer using that hot key. There is **no performance advantage in choosing any one of the options** above so choose the option that you are most comfortable with.

Reset configuration data

The ESCD (Extended System Configuration Data) is a feature of the Plug and Play BIOS that stores the IRQ, DMA, I/O and memory configurations of all ISA, PCI and AGP cards in the system (Plug and Play-capable or otherwise). The data is stored in a special area of the BIOS ROM so that the BIOS can reuse the configuration data when it boots up the system. As long as there are no hardware changes, the BIOS does not need to reconfigure the ESCD. If you install a new piece of hardware or modify your computer's hardware configuration, the BIOS will automatically detect the changes and reconfigure the ESCD. Therefore, there's no need to manually force the BIOS to reconfigure the ESCD.

However, sometimes, the BIOS may not be able to detect the hardware changes and the a serious conflict of resources may occur. The operating system may not even boot as a result. This is where the Reset Configuration Data feature comes in. This feature **allows you to manually force the BIOS to clear the previously saved ESCD data and reconfigure the settings.** Just enable the feature and reboot your computer. The new ESCD should resolve the conflicts and allow the operating system to load normally. There's no need for you to manually disable this feature yourself as the BIOS will automatically reset it to the default setting of Disabled after reconfiguring the ESCD.

Security setup

This feature will only work once you have created a password through the PASSWORD SETTING option in the main BIOS screen. Selecting the System option will force the BIOS to ask for the password everytime the system boots up. If you **choose Setup, then the password is only required for access to the BIOS**. This option is useful for system adminstrators or computer resellers who need to keep novice users from messing around with the BIOS. :-)

Typematic rate

This feature determines the rate at which the keyboard will repeat the keystroke if you press it continuously. This feature will only work if the Typematic Rate Setting feature has been enabled. The available settings are all in characters per second. Therefore, a typematic rate of 30 will mean that if you press a particular key continuously, the keyboard will repeat the keystroke at the rate of 30 characters per second. The higher the typematic rate, the faster the keyboard will repeat the keystroke. The choice of what setting to use is entirely up to personal preference. **Disable.**

Typematic rate delay

This setting will only work if the Typematic Rate Setting option has been enabled. This is the delay, in milliseconds (thousandths of a second), before the keyboard automatically repeats the keystroke that you have pressed continuously. The longer the delay, the longer the keyboard will wait before it starts repeating the keystroke. As such, using a short delay is useful for people who type quickly and don't like to wait long for a keystroke to be repeated. In contrast, a long delay is useful for users who tend to press the keystroke for long periods. This prevents the keyboard from wrongly repeating keystrokes with such users.

Virus warning

This BIOS feature provides rudimentary anti-virus protection by watching over writes to the boot sector and partition table. When you enable this feature, the BIOS will halt the system and flash a warning message whenever there's an attempt to write to the boot sector or the partition table. Note that this only protects the boot sector and the partition table, not the entire hard disk. This feature can cause problems with software that need to access the boot sector. One good example is the installation routine of all versions of Microsoft Windows from Windows 95 onwards. When enabled, this feature causes the installation routine to fail. Also, many disk diagnostic utilities that access the boot sector can also trigger the system halt and error message as well. Therefore, you should disable this feature before running such software.

Note that this feature is useless for hard disks that run on external controllers with their own BIOS. Boot sector viruses will bypass the system BIOS with its anti-virus protection features and write directly to the hard disks. Such controllers include additional IDE or SCSI controllers that are either built into the motherboard or available via add-on cards.

PROCESSOR

CPU level 2 cache ECC checking

This feature enables or disables the L2 (Level 2 or Secondary) cache's ECC (Error Checking and Correction) function, if available. Enabling this feature is recommended because it will detect and correct single-bit errors in data stored in the L2 cache. As most data reads will be satisfied by the L2 cache, the L2 cache's ECC function should catch and correct almost all single-bit errors in the memory subsystem. It will also detect double-bit errors but not correct them. But this isn't such a big deal since double-bit errors are extremely rare. For all practical purposes, the ECC check should be able to catch virtually all data errors. This is especially useful at overclocked speeds when errors are most likely to creep in.

There are those who advocate disabling ECC checking because it reduces performance. True, ECC checking doesn't come free. You can expect some performance degradation with ECC checking enabled. However, unlike ECC checking of DRAM modules, the performance degradation associated with L2 cache ECC checking is comparatively small. Balance that against the increased stability and reliability achieved via L2 cache ECC checking and the minimal reduction in performance seems rather cheap, doesn't it? Of course, if you don't do any serious work with your system and want a little speed boost for your games, disable CPU L2 Cache ECC Checking by all means.

But if you are overclocking your processor, ECC checking may enable you to overclock higher than was originally possible. This is because any single-bit errors that occur as a result of overclocking will be corrected by the L2 cache's ECC function. So, for most intents and purposes, I recommend that you **enable** this feature for greater system stability and reliability. Note that the presence of this feature in the BIOS doesn't necessarily mean that your processor's L2 cache actually supports ECC checking. Many processors don't ship with ECC-capable L2 cache. In such cases, you can still enable this feature in the BIOS but it will have no effect.

CPU level 1 cache

The modern processor is a very fast piece of silicon. Unfortunately, RAM development is so far behind that the processor would be fatally stalled by the slow memory accesses had it been forced to rely on current RAM technology alone. To alleviate this problem, designers have integrated a small amount of ultra-fast RAM within the processor core. This small amount of RAM is used to cache instructions and data for the processor's instantaneous access. Hence, it is known as the primary or level 1 or L1 cache. In current processor design, the L1 cache can range from 32K to 128KB in size.

Only if the data required is not found in the L1 cache, is the processor required to retrieve it from the L2 cache or the RAM itself. When it does so, the processor incurs the penalties of accessing much slower memory. Fortunately, the L1 cache is often able to satisfy the processor's data requirements. In fact, it's so efficient that it makes the entire memory subsystem appear to be almost as fast as it is. This BIOS feature is used to enable or disable the processor's L1 cache. Naturally, the default and recommended setting is **Enabled**.

This feature is useful for overclockers who want to pinpoint the cause of an unsuccessful overclocking attempt. For example, if your processor cannot reach 1GHz with the L1 cache enabled but can do so when the L1 cache's disabled; then the L1 cache is what's stopping the processor from running at 1GHz stably. But if the processor still can't reach 1GHz, then the problem lies elsewhere. However, disabling the L1 cache in order to increase the overclockability of the CPU is a very bad idea. The lack of L1 cache will cause the processor to stall because the memory subsystem won't be fast enough to continuously feed data to the processor. Therefore, except for troubleshooting purposes, this feature should be left enabled.

CPU level 2 cache

The modern processor is a very fast piece of silicon. Unfortunately, RAM development is so far behind that the processor would be fatally stalled by the slow memory accesses had it been forced to rely on current RAM technology alone. To alleviate this problem, designers have integrated a small amount of ultra-fast RAM within the processor core. This small amount of RAM is used to cache instructions and data for the processor's instantaneous access. Hence, it is known as the primary or level 1 or L1 cache. In current processor design, the L1 cache can range from 32K to 128KB in size.

Only if the data required is not found in the L1 cache, is the processor required to retrieve it from the RAM itself. When it does so, the processor incurs the penalties of accessing much slower memory. Fortunately, the L1 cache is often able to satisfy the processor's data requirements. In fact, it's so efficient that it makes the entire memory subsystem appear to be almost as fast as it is.

However, as the disparity between processor speed and RAM speed widens, the penalties incurred whenever there's a L1 cache miss becomes more significant. This is compounded by the fact that while the size of the L1 cache only doubled or quadrupled in recent years, the system will often have 16 times to 32 times more RAM! The small L1 cache size is inadequate in most cases and will not be able to satisfy many of the data requests. If the processor has to retrieve the data directly from the RAM, it will suffer a significant drop in performance.

As such, designers often include a secondary or level 2 or L2 cache. This cache is designed to meet data requests that the L1 cache cannot satisfy. Although slower than the L1 cache, the L2 cache compensates by being much larger in size. This allows it to cache a lot more data compared to the L1 cache. As the two caches working together are able to satisfy over 95% of data reads, the need to access the much slower RAM is reduced to the minimum. This BIOS feature is used to enable or disable the processor's L2 cache. Naturally, the default and recommended setting is **Enabled**.

This feature is useful for overclockers who want to pinpoint the cause of an unsuccessful overclocking attempt. For example, if your processor cannot reach 1GHz with the L2 cache enabled but can do so when the L2 cache's disabled; then the L2 cache is what's stopping the processor from running at 1GHz stably. But if the processor still can't reach 1GHz, then the problem lies elsewhere. However, disabling the L2 cache in order to increase the overclockability of the CPU is a very bad idea. The lack of L2 cache will cause the processor to stall because the memory subsystem won't be fast enough to continuously feed data to the processor. Therefore, except for troubleshooting purposes, this feature should be left enabled.

Gate A20 option

The A20 address line is a relic from the past. It came about because the father of x86 processors - the Intel 8088 only had 20 address lines! That meant that it could only address 1MB of memory. When the Intel 80286 processor was introduced, it had 24 address lines. To maintain 100% software compatibility with the 8088, the 80286 had a real mode that would truncate addresses to 20-bits. Unfortunately, a design bug prevented it from truncating the addresses properly. This prevented the 80286 from running many 8088-compatible software.

To solve this problem, IBM designed an AND gate switch to control the 20th address bit. This switch was henceforth known as the Gate A20. When enabled, all available address lines would be used by the processor for access to memory above the first megabyte. In the 8088-compatible real mode, the Gate A20 would be used to clear the 20th bit of all addresses. This allows the 80286 to function like a superfast 8088 processor with access only to the first megabyte of memory. Even in modern systems, Gate A20 is still important. This is because the processor needs to turn A20 on and off in order to switch between real mode and protected mode. Since operating systems like Microsoft Windows 98 switch a lot between real mode and protected mode, relying on the understandably slow keyboard controller is no longer acceptable.

The motherboard chipset's I/O port 0x92 (System Control Port A) was therefore recruited to take over the job. A lot faster than the keyboard controller, the 0x92 port allows the processor to switch much faster between real mode and protected mode. This translates into faster memory access and better system performance. This BIOS feature is used to determine the method by which Gate A20 is controlled. The Normal option forces the chipset to use the slow keyboard controller to do the switching. The Fast option, on the other hand, allows the chipset to use its own 0x92 port for faster switching. No candy for guessing which is the recommended setting!

Please note this feature is only important for operating systems that switch a lot between real mode and protected mode. These operating systems include 16-bit operating systems like MS-DOS and 16-bit/32-bit hybrid operating systems like Microsoft Windows 98. This feature has no effect if the operating system only runs in real mode (no operating system currently in use does that, as far as I know) or if the operating system operates entirely in protected mode (i.e. Microsoft Windows XP). This is because if no A20

mode switching is required, then it doesn't matter at all if the switching was done by the slow keyboard controller or the faster 0x92 port.

With all is said and done, however, the recommended setting for this BIOS feature is still **Fast** even with operating systems that don't do much mode switching. Except for very rare instances in which using the 0x92 port to control Gate A20 causes spontaneous reboots, there's no reason why you should keep using the slow keyboard controller to turn A20 or or off.

In order queue depth

For greater performance at high clock speeds, motherboard chipset designs now feature a pipelined processor bus. The multiple stages in this pipeline can further be used to queue up multiple commands to the processor. This command queuing greatly improves performance because it effectively masks the latency of the processor bus. In optimal situations, the amount of latency between each succeeding command can be reduced to only a single clock cycle! This BIOS feature controls the use of the processor bus' command queue. Normally, there are only two options available. Depending on the motherboard chipset, the options could be (1 and 4), (1 and 8) or (1 and 12). This is because this BIOS feature actually only allows you to disable or enable the command queuing capability of the processor bus pipeline.

It does not allow you to control the number of commands that can be queued. This is because the number of commands that can be queued depends entirely on the number of stages in the pipeline. As such, you can expect to see this feature associated with options like Enabled and Disabled in some motherboards.

The first queue depth option is always 1, which prevents the processor bus pipeline from queuing any outstanding commands. If selected, each command will only be issued after the processor has finished with the previous one. Therefore, every command will incur the maximum amount of latency. This varies from 4 clock cycles for a 4-stage pipeline to 12 clock cycles for pipelines with 12 stages. As you can see, this reduces performance as the processor has to wait for each command to filter down the pipeline. The severity of the effect depends greatly on the depth of the pipeline. The deeper the pipeline, the greater the effect.

If the second queue depth option is 4, this means that the processor bus pipeline has 4 stages in it. Selecting this option allows the queuing of up to 4 commands in the pipeline. Each command can then be processed successively with a latency of only 1 clock cycle.

If the second queue depth option is 8, this means that the processor bus pipeline has 8 stages in it. Selecting this option allows the queuing of up to 8 commands in the pipeline. Each command can then be processed successively with a latency of only 1 clock cycle.

If the second queue depth option is 12, this means that the processor bus pipeline has 12 stages in it. Selecting this option allows the queuing of up to 12 commands in the pipeline. Each command can then be processed successively with a latency of only 1 clock cycle.

Please note that the latency of only 1 clock cycle is only possible if the pipeline is completely filled up. If the pipeline is only partially filled up, then the latency affecting one or more of the commands will be more than 1 clock cycle. Still, the average latency for each command will be much lower than it would be with command queuing disabled.

In most cases, it is highly recommended that you enable command queuing by selecting the options of 4 / 8 / 12 or in some cases, Enabled. This allows the processor bus pipeline to mask its latency by queuing outstanding commands. You can expect a significant boost in performance with this feature enabled.

Interestingly, this feature can also be used as an aid in overclocking the processor. Although the queuing of commands brings with it a big boost in performance, it may also make the processor unstable at overclocked speeds. To overclock beyond what's normally possible, you can try disabling command queuing. This may reduce performance but it will make the processor more stable and may allow it to be further overclocked.

But please note that the performance deficit associated with deeper pipelines (8 or 12 stages) may not be worth the increase in processor overclockability. This is because the deep processor bus pipelines have very long latencies. If they are not masked by command queuing, the processor may be stalled so badly that you may end up with poorer performance even if you are able to further overclock the processor. So, it is **recommended that you enable command queuing for deep pipelines,** even if it means reduced overclockability.

Level 2 cache latency

Whenever the processor's Level 2 cache receives a read/write command, a certain period of time passes before the cache can actually process the command. This delay is called latency and the shorter the latency, the faster the Level 2 cache can service data reads/writes. This BIOS feature enables you to change the latency of the processor's Level 2 cache. By default, this feature is set to **Auto** which means that the processor's Level 2 cache will be left to its default latency setting. This is the **safest option.**

You can also manually select the latency of the cache. For this purpose, this BIOS feature provides options ranging from 1 clock cycle to 15 clock cycles. Please note that setting too low a latency can cause the Level 2 cache to lose data integrity or fail altogether. This will manifest as a system crash or an inability to boot-up at all. Therefore, it is recommended that you start with a high latency and work your way down until you start to encounter stability issues. This allows you to figure out what's the lowest latency your processor's Level 2 cache can support. Select that latency for optimal performance without stability issues.

Please note that this is a processor-dependent feature. Not all processors support BIOS manipulation of the Level 2 cache latency. If the processor does not support the manipulation of its Level 2 cache latency, then this BIOS feature will not have any effect, irrespective of what you select.

MPS control version for OS

This feature is **only applicable to multiprocessor motherboards** as it specifies the version of the Multi-Processor Specification (MPS) that the motherboard will use. The MPS is a specification by which PC manufacturers design and build Intel architecture systems with two or more processors.

MPS 1.1 was the original specification. MPS version 1.4 adds extended configuration tables for improved support of multiple PCI bus configurations and greater expandability in the future. In addition, MPS 1.4 introduces support for a secondary PCI bus without requiring a PCI bridge. Please note that MPS version 1.4 is required for a motherboard to support a secondary PCI bus without the need for a PCI bridge.

If your operating system comes with support for MPS 1.4, you should change the setting from the default of 1.1 to **1.4**. You also need to enable MPS 1.4 support if you need to make use of the secondary PCI bus on a motherboard that doesn't come with a PCI bridge. This is because only MPS 1.4 supports a bridgeless secondary PCI bus.
You should only leave it as 1.1 only if you are running an older operating system that only supports MPS 1.1.

According to Eugene Tan, Windows NT already supports MPS 1.4. Therefore, newer operating systems like Windows 2000 and Windows XP shouldn't have any problem supporting MPS 1.4. However, users of the ABIT BP6 motherboard and Windows 2000 should take note of a possible problem with the MPS version set to 1.4. Dan Isaacs reported that when you set the MPS version to 1.4 in the ABIT BP6, Windows 2000 will not use the second processor. So, if you encounter this problem, set the MPS Version Control For OS to 1.1.

Processor number feature

This feature is only valid if you are using a processor that features an embedded unique identification number. This infamous "feature" debuted in the Intel Pentium III processor and is mainly found only in that processor. If the BIOS of my notebook is correct, the Transmeta Crusoe processor may also support this feature. But most manufacturers have refrained from integrating such a "feature" in their processors. Even Intel has declined to add this feature to the Intel Pentium 4 processor.

This feature will most probably not appear unless you are using an Intel Pentium III or Transmeta Crusoe processor. It gives you the ability to control whether the embedded identification number can be read by external programs or not. Enable this if your secure transactions require you to use such a feature. Otherwise, I would recommend that you **disable** this feature to safeguard your privacy. This is because the embedded identification number can be misused to track your online activities.

Speed error hold

This feature was designed to prevent accidental overclocking. This is very useful for novice users who want nothing to do with overclocking and yet may have inadvertently set the wrong processor speed in the BIOS. When enabled, this feature will check the processor clock speed at boot up and halt the booting process if the clock speed is different from the speed stated in the processor ID. It will also display an error message to warn you that the processor is running at the wrong speed. To correct the situation, you will have to enter the BIOS and correct the processor speed. Most BIOSes, however, will automatically reset the processor to the correct speed. All you have to do then is enter the BIOS, verify it and save the change.

If you are thinking of overclocking the processor, you must **disable** this feature as it prevents the motherboard from booting up with an overclocked processor. Although this may seem really obvious, I have seen countless overclocking initiates puzzling over the error message whenever they try to overclock their processors. So, before you start pulling your hair and screaming hysterically that Intel or AMD has finally implemented a clock speed lock on their processors, try disabling this feature. ;-)

Spread spectrum

When the motherboard's clock generator pulses, the extreme values (spikes) of the pulses create EMI (Electromagnetic Interference). The Spead Spectrum feature reduces the EMI by modulating the pulses so that the spikes of the pulses are reduced to flatter curves. It does so by varying the frequency slightly so that the signal doesn't use any particular frequency for more than a moment. This reduces the amount of interference that will affect the other electronics in the area. The BIOS usually offers two different levels of modulation - 0.25% or 0.5%. That's the amount of modulation (or jitter) from the baseline signal. The greater the modulation, the greater the reduction of EMI. Therefore, if you need to significantly reduce EMI in the surrounding area, a modulation of 0.5% is recommended.

In most conditions, frequency modulation via this feature shouldn't cause any problems. However, system stability may be slightly compromised in certain situations. For example, enabling Spread Spectrum may cause improper functioning of timing-critical devices like clock-sensitive SCSI devices. Spread Spectrum can also cause problems with overclocked systems, especially those that have been taken to extremes. The slight modulation of frequency may cause the processor or any other overclocked components of the system to fail, leading to very predictable consequences. Of course, this depends on the amount of modulation, the extent of overclocking and other factors like temperature variation, etc... As such, the problem may not readily manifest itself instantly.

Therefore, it is recommended that you **disable** this feature if you are overclocking your system. The risk of crashing your system isn't worth the reduction in EMI. Of course, if EMI reduction is important to you, enable this feature by all means but reduce the clock speed a little to give this feature some "space" to modulate safely. If you are not overclocking, the decision to enable or disable this feature is really up to you. But if you ask me, unless you have EMI problems, it's best to disable this feature to remove the possibility of stability issues.

Some BIOSes also offer a Smart Clock option. Instead of modulating the frequency of the pulses over time, Smart Clock turns off the AGP, PCI and SDRAM clock signals that are not in use. Thus, EMI can be reduced without compromising system stability. As a bonus, using Smart Clock also help to reduce power consumption. The degree of EMI and power reduction will depend on the number of free (empty) AGP, PCI and SDRAM slots. But generally, Smart Clock won't be able to reduce EMI as effectively as simple frequency modulation. Still, if your BIOS comes with this Smart Clock option, you should select it over the 0.25% or 0.5% options if you need some EMI reduction. It will allow you to reduce EMI without any risk of compromising stability.

STORAGE SUBSYSTEM

32 bit disk access

The name 32-bit Disk Access is actually a misnomer because it doesn't really allow 32-bit access to the hard disk. The IDE interface is always 16-bits in width even when the IDE controller is on the 32-bit PCI bus. What this feature actually does is command the IDE controller to combine two 16-bit reads from the hard disk into a single 32-bit double word transfer to the processor. This allows the PCI bus to be more efficiently used as the number of transactions required for a particular amount of data is effectively halved!

However, according to a Microsoft article (Enhanced IDE operation under Windows NT 4.0), 32-bit disk access can cause data corruption under Windows NT in some cases. Therefore, Microsoft recommends that Windows NT 4.0 users disable 32-bit Disk Access.

Lord Mike asked 'someone in the know' about this matter and he was told that the data corruption issue was taken very seriously at Microsoft and that it had been corrected through the Windows NT 4.0 Service Pack 2. Although he couldn't get an official statement from Microsoft, it's probably safe enough to enable 32-bit Disk Access on a Windows NT 4.0 system, just as long as it has been upgraded with Service Pack 2.

Because it realizes the performance potential of the 32-bit IDE controller and improves the efficiency of the PCI bus, it is highly advisable to enable 32-bit Disk Access. If you disable it, data transfers from the IDE controller to the processor will only occur in 16-bits chunks. Naturally, this degrades the performance of the IDE controller as well as the PCI bus. As such, you should disable this feature only if you actually face the possibility of data corruption (with an unpatched version of Windows NT 4.0). You can also find more information on the Windows NT issue in the details of the IDE HDD Block Mode feature! **Enable**.

ATA100 RAID / IDE controller

This feature is only found on certain motherboards that come with an extra UltraDMA/100 IDE controller with RAID support. It allows you to enable or disable the function of that controller. Please note that the IDE controller covered by this BIOS feature is different from the chipset's built-in IDE controller. This extra UltraDMA/100 IDE controller is often added to provide UltraDMA/100 and RAID support in motherboards whose chipset does not offer UltraDMA/100 or RAID support. Even if the chipset's built-in IDE controller supports UltraDMA/100 as well as RAID, it is not controlled by this BIOS feature. This feature is only used for the extra IDE controller.

For the purpose of avoiding confusion, I shall hence refer to the built-in IDE controller as an internal IDE controller while add-on IDE controller will be known as an external IDE controller. If you want to attach one or more IDE devices to the external UltraDMA/100 RAID controller, you should enable this feature. You should only disable it for the following reasons :-

- if you don't have any IDE device attached to the external UltraDMA/100 RAID controller
- for troubleshooting purposes
- Disabling the external IDE controller will free up two IRQs and speed up system booting. This is because the IDE controller's BIOS doesn't have to be loaded and the external controller's often long boot-up check and initialization sequence will be skipped. So, **if you don't use the external IDE controller, it is recommended that you disable it.**

Delay IDE initial

Regardless of its shortcomings, the IDE standard is remarkably backward compatible. Every upgrade of the standard was designed with compatibility with older IDE devices in mind. So, you can actually use the old 40MB hard disk that came with your ancient 386 system in your spanking new Athlon XP system! However, the slower motors used in the older drives may still cause some problems. Because motherboards boot up and initialize the IDE devices much faster now, they may not be able to detect IDE devices that cannot spin up in time. So, your older IDE devices may not be accessible even though they are working just fine.

This BIOS feature allows you to force the BIOS to delay the initialization of IDE devices for up to 15 seconds. This gives your IDE devices more time to spin up before the BIOS initializes them. You should leave the delay at the **default value of 0 if possible** for the shortest possible booting time. Most IDE devices manufactured in the last few years have no problem spinning up in time for initialization. But if one or more of your IDE devices fail to initialize during the boot up process, start with a delay of 1 second and increase the delay until all your IDE devices initialize properly.

Floppy 3 mode support

For reasons best known to the Japanese, their computers come with special 3 mode 3.5" floppy drives. While physically similar to the standard 3.5" floppy drives used by the rest of the world, these 3 mode floppy drives differ in the disk formats they support. Unlike normal floppy drives, 3 mode floppy drives support three different floppy disk formats - 1.44MB, 1.2MB and 720KB, hence their name. They allow the system to support the Japanese 1.2MB floppy disk format as well as the standard 1.44MB and 720KB (obsolete) disk formats.

If you own a 3 mode floppy drive and need to use the Japanese 1.2MB disk format, you must enable this feature by selecting either Drive A, Drive B or Both (if you have two 3 mode floppy drives). Otherwise, your 3 mode floppy drive won't be able to read the special 1.2MB format properly. However, if you only have a standard floppy drive, **disable** this feature or your floppy drive may not function properly.

HDD smart capability

This feature enables or disables support for the hard disk's S.M.A.R.T. capability. S.M.A.R.T. (Self Monitoring Analysis And Reporting Technology) is supported by all current hard disks and it allows the early prediction and warning of impending hard disk disasters. You should enable it if you want to use S.M.A.R.T.-aware utilities to monitor the hard disk's condition. Enabling it also allows the monitoring of the hard disk's condition over a network.

However, there's a possibility that enabling S.M.A.R.T. may cause spontaneous reboots with networked computers. Johnathan P. Dinan reported encountering such an issue. Apparently, S.M.A.R.T. continuously sends packets of data through the network even when there's actually nothing monitoring those data packets. This may have caused the spontaneous reboots that he had experienced. Therefore, if you experience spontaneous reboots or crashes with a networked computer, try disabling this feature.

While S.M.A.R.T., at first glance, looks like a really great safety feature, it isn't really useful or necessary for most users. For S.M.A.R.T. to work, it isn't simply a matter of enabling it in the BIOS. You actually have to keep a S.M.A.R.T.-aware hardware monitoring utility running in the background all the time. This means using up some memory and processor time just to monitor S.M.A.R.T. data from the hard disk. That's quite alright if the hard disk you are using is highly unreliable and you need advanced warning of any impending failure. However, hard disks these days are reliable enough to make S.M.A.R.T. redundant in most cases. Unless you are running mission-critical applications, it's very unlikely that S.M.A.R.T. will be of any use at all.

Please note that even if you don't use any S.M.A.R.T.-aware utility, enabling S.M.A.R.T. in the BIOS uses up some bandwidth because the hard disk will be constantly sending out data packets. So, if you do not use S.M.A.R.T.-aware utilities or if you don't need that level of real-time reporting, **disable** HDD S.M.A.R.T. Capability for better overall performance.

IDE hdd block mode

The IDE HDD Block Mode feature speeds up hard disk access by transferring multiple sectors of data per interrupt instead of using the usual single-sector transfer mode. When you enable this feature, the BIOS will automatically detect if your hard disk supports block transfers and set the proper block transfer settings for it. Depending on the motherboard chipset, up to 64KB of data can be transferred per interrupt with IDE HDD Block Mode enabled. Since all current hard disks support block transfers, there is usually no reason why IDE HDD Block Mode cannot be enabled.

However, Microsoft Windows NT may have a problem with block transfers. According to Chris Bope, Windows NT does not support IDE HDD Block Mode and enabling this feature can cause data to be corrupted. Ryu Connor confirmed this by sending me a link to a Microsoft article (Enhanced IDE operation under Windows NT 4.0). According to this article, IDE HDD Block Mode and 32-bit Disk Access have been found to cause data corruption in some cases. Therefore, Microsoft recommends that Windows NT 4.0 users disable IDE HDD Block Mode.

Lord Mike asked 'someone in the know' about this matter and he was told that the data corruption issue was taken very seriously at Microsoft and that it had been corrected through the Windows NT 4.0 Service Pack 2. Although he couldn't get an official statement from Microsoft, it's probably safe enough to enable IDE HDD Block Mode on a Windows NT 4.0 system, just as long as it has been upgraded with Service Pack 2.

Please note that if you disable IDE HDD Block Mode, only 512 bytes of data can transferred per interrupt. Needless to say, this significantly degrades performance. So, disable IDE HDD Block Mode only if you actually face the possibility of data corruption (with an unpatched version of Windows NT 4.0). Otherwise, it is highly recommended that you **enable** this feature for significantly better hard disk performance

Master drive PIO mode

This feature is usually found under the Onboard IDE-1 Controller or Onboard IDE-2 Controller feature. It is linked to one of the IDE channels so if you disable one, the corresponding Master Drive PIO Mode option for that IDE channel either disappears or becomes grayed out. This feature allows you to set the PIO (Programmed Input/Output) mode for the Master IDE drive attached to that particular IDE channel. Normally, you should leave it as **Auto** and let the BIOS auto-detect the IDE drive's PIO mode. You should only set it manually for the following reasons :-

- if the BIOS cannot detect the correct PIO mode.
- if you want to try to run the IDE device using a faster PIO mode than it was designed for.
- if you have overclocked the PCI bus and one or more of your IDE devices cannot function properly (the problem may be corrected by forcing the IDE devices to use a slower PIO mode).

Please note that forcing an IDE device to use a PIO transfer rate that's faster than what it's rated for can potentially cause data corruption. Here is a table of the different PIO transfer rates and their corresponding maximum throughputs.

PIO Data Transfer Mode	Maximum Throughput
PIO Mode 0	3.3 MB/s
PIO Mode 1	5.2 MB/s
PIO Mode 2	8.3 MB/s
PIO Mode 3	11.1 MB/s
PIO Mode 4	16.6 MB/s

Master drive ultra DMA

This feature is usually found under the Onboard IDE-1 Controller or Onboard IDE-2 Controller feature. It's linked to one of the IDE channels so if you disable one, the corresponding Master Drive UltraDMA function for that IDE channel either disappears or is greyed out. This feature allows you to enable or disable UltraDMA support (if available) for the Master IDE device attached to that particular IDE channel. Normally, you should leave it as **Auto** and let the BIOS auto-detect if the drive supports UltraDMA. If it does, the proper UltraDMA transfer mode will be enabled for that drive, allowing it to burst data at anywhere from 33MB/s to 133MB/s (depending on the transfer mode supported).

You should only disable it for troubleshooting purposes. For example, certain IDE devices may not run properly using DMA transfers when the PCI bus is overclocked. Disabling UltraDMA support will force the drive to use the slower PIO transfer mode. This may allow the drive to work properly with the higher PCI bus speed.

Please note that setting this to Auto will not enable UltraDMA or any of the slower DMA modes for IDE devices that do not support UltraDMA or DMA transfers. If your drive does not support any DMA modes, then it will automatically set the drive to do PIO transfers.

In addition, for any of the DMA transfer modes to work (including UltraDMA modes), you have to enable DMA transfer support in the operating system you are using. In Windows 9x, this can be accomplished by ticking the DMA checkbox in the properties sheet of the IDE drive in question. In Windows 2000/XP, you have to set the transfer mode of the IDE device to DMA If Available in the Advanced Settings tab of the associated IDE channel's properties page. For easy reference, here's a table of the different DMA transfer rates and their corresponding maximum throughputs.

DMA Transfer Mode	Maximum Throughput
DMA Mode 0	4.16 MB/s
DMA Mode 1	13.3 MB/s
DMA Mode 2	16.6 MB/s
UltraDMA 33	33.3 MB/s
UltraDMA 66	66.7 MB/s
UltraDMA 100	100.0 MB/s

UltraDMA 133 133.3 MB/s

Onboard FDD controller
This feature allows you to enable or disable the onboard floppy drive controller. If you are using a floppy drive connected to the motherboard's built-in floppy drive controller, leave it at the default setting of **Enabled**. But if you are using an add-on floppy drive controller card or if you are not using any floppy drives at all, set it to Disabled to save an IRQ. The free IRQ can then be used by other devices.

Onboard IDE 1 controller
This feature is a misnomer because there is actually only one IDE controller present on the motherboards. The single IDE controller comes with two IDE channels, each of which supports up to two IDE drives. Therefore, the single IDE controller supports a total of 4 IDE devices through its two IDE channels. It has become common practice, unfortunately, to label these IDE channels as "IDE controllers". So, while this BIOS feature's name suggests that it controls the functionality of the 'first' IDE controller, it actually controls only the first IDE channel of the motherboard's single built-in IDE controller. You should leave this **enabled** if you are using this IDE channel. Disabling it will prevent any IDE devices attached to this channel from functioning at all.

If you are not attaching any IDE devices to this channel (or if you are using a SCSI / an add-on IDE card), **you can disable this IDE channel to free an IRQ.** The IRQ can then be used by other devices. Disabling this IDE channel will also speed up boot-time a little as the BIOS will not need to query this channel for IDE devices when it boots up the motherboard.

Onboard IDE 2 controller
This feature is a misnomer because there is actually only one IDE controller present on the motherboards. The single IDE controller comes with two IDE channels, each of which supports up to two IDE drives. Therefore, the single IDE controller supports a total of 4 IDE devices through its two IDE channels. It has become common practice, unfortunately, to label these IDE channels as "IDE controllers". So, while this BIOS feature's name suggests that it controls the functionality of the 'second' IDE controller, it actually controls only the second IDE channel of the motherboard's single built-in IDE controller. You should leave this **enabled** if you are using this IDE channel. Disabling it will prevent any IDE devices attached to this channel from functioning at all.

If you are not attaching any IDE devices to this channel (or if you are using a SCSI / an add-on IDE card), you **can disable this IDE channel to free an IRQ.** The IRQ can then be used by other devices. Disabling this IDE channel will also speed up boot-time a little as the BIOS will not need to query this channel for IDE devices when it boots up the motherboard.

Report no FDD for win95
If you are using Windows 95 without a floppy disk drive, you have to enable this feature to release IRQ6. This is required to meet Windows 95's logo certification. Otherwise, you will get an error message. For other operating systems, this feature has no relevance. Therefore, it doesn't matter what you set with other operating systems.

Slave drive PIO mode
This feature is usually found under the Onboard IDE-1 Controller or Onboard IDE-2 Controller feature. It is linked to one of the IDE channels so if you disable one, the corresponding Slave Drive PIO Mode option for that IDE channel either disappears or becomes grayed out. This feature allows you to set the PIO (Programmed Input/Output) mode for the Slave IDE drive attached to that particular IDE channel. Normally, you should leave it as **Auto** and let the BIOS auto-detect the IDE drive's PIO mode. You should only set it manually for the following reasons :-

- if the BIOS cannot detect the correct PIO mode.
- if you want to try to run the IDE device using a faster PIO mode than it was designed for.
- if you have overclocked the PCI bus and one or more of your IDE devices cannot function properly (the problem may be corrected by forcing the IDE devices to use a slower PIO mode).

Please note that forcing an IDE device to use a PIO transfer rate that's faster than what it's rated for can potentially cause data corruption. Here is a table of the different PIO transfer rates and their corresponding maximum throughputs.

PIO Data Transfer Mode	Maximum Throughput
PIO Mode 0	3.3 MB/s
PIO Mode 1	5.2 MB/s
PIO Mode 2	8.3 MB/s
PIO Mode 3	11.1 MB/s
PIO Mode 4	16.6 MB/s

Slave drive ultra DMA
This feature is usually found under the Onboard IDE-1 Controller or Onboard IDE-2 Controller feature. It's linked to one of the IDE channels so if you disable one, the corresponding Slave Drive UltraDMA function for that IDE channel either disappears or is greyed out. This feature allows you to enable or disable UltraDMA support (if available) for the Slave IDE device attached to that particular IDE channel. Normally, you should leave it as **Auto** and let the BIOS auto-detect if the drive supports UltraDMA. If it does, the proper UltraDMA transfer mode will be enabled for that drive, allowing it to burst data at anywhere from 33MB/s to 133MB/s (depending on the transfer mode supported).

You should only disable it for troubleshooting purposes. For example, certain IDE devices may not run properly using DMA transfers when the PCI bus is overclocked. Disabling UltraDMA support will force the drive to use the slower PIO transfer mode. This may allow the drive to work properly with the higher PCI bus speed.

Please note that setting this to Auto will not enable UltraDMA or any of the slower DMA modes for IDE devices that do not support UltraDMA or DMA transfers. If your drive does not support any DMA modes, then it will automatically set the drive to do PIO transfers.

In addition, for any of the DMA transfer modes to work (including UltraDMA modes), you have to enable DMA transfer support in the operating system you are using. In Windows 9x, this can be accomplished by ticking the DMA checkbox in the properties sheet of the IDE drive in question. In Windows 2000/XP, you have to set the transfer mode of the IDE device to DMA If Available in the

Advanced Settings tab of the associated IDE channel's properties page. For easy reference, here's a table of the different DMA transfer rates and their corresponding maximum throughputs.

DMA Transfer Mode	Maximum Throughput
DMA Mode 0	4.16 MB/s
DMA Mode 1	13.3 MB/s
DMA Mode 2	16.6 MB/s
UltraDMA 33	33.3 MB/s
UltraDMA 66	66.7 MB/s
UltraDMA 100	100.0 MB/s
UltraDMA 133	133.3 MB/s

Swap floppy drive

This feature used to logically swap the mapping of drives A: and B:. Therefore, it is only useful if you have two floppy drives. Normally, the sequence by which you connect the floppy drives to the cable determines which drive is drive A: and which is drive B:. If you attach the floppy drives wrongly and obtain a drive mapping that isn't to your satisfaction, there normally wasn't any way to correct this except to physically swap the floppy cable connections. However, with this feature, you can swap the logical arrangement of the floppy drives without opening up the case. When it is enabled, the floppy drive that originally was mapped to drive A: would be remapped to drive B: and the reverse goes for the drive that was originally set as drive B:.

Although this appears to be merely a feature of convenience, it can be quite important if you are using two floppy drives of different form factors (3.5" and 5.25") and you need to boot from the second drive. Because the BIOS can only boot from drive A:, you will have to physically swap the drive connections or use this feature to do it logically. If your floppy drive mapping is correct or if you only have a single floppy drive, there's no need to enable this feature. Leave it at the default setting of **disabled.**

UltraDMA 100 IDE controller

This feature is only found on certain motherboards that come with an extra IDE controller. It allows you to enable or disable the function of that controller. Please note that the IDE controller covered by this BIOS feature is different from the chipset's built-in IDE controller. This extra UltraDMA/100 IDE controller is often added to provide UltraDMA/100 support in motherboards whose chipset does not offer UltraDMA/100 support. Even if the chipset's built-in IDE controller supports UltraDMA/100, it is not controlled by this BIOS feature. This feature is only used for the extra IDE controller.

For the purpose of avoiding confusion, I shall hence refer to the built-in IDE controller as an internal IDE controller while add-on IDE controller will be known as an external IDE controller. If you want to attach one or more IDE devices to the external UltraDMA/100 controller, you should **enable** this feature. You should only disable it for the following reasons :-

- if you don't have any IDE device attached to the external UltraDMA/100 controller
- for troubleshooting purposes
- **disabling** the external IDE controller will **free up two IRQs and speed up system booting.**

This is because the IDE controller's BIOS doesn't have to be loaded and the external controller's often long boot-up check and initialization sequence will be skipped. So, if you don't use the external IDE controller, it is recommended that you disable it.

UltraDMA 66 IDE controller

This feature is only found on certain motherboards that come with an extra IDE controller. It allows you to enable or disable the function of that controller. Please note that the IDE controller covered by this BIOS feature is different from the chipset's built-in IDE controller. This extra UltraDMA/66 IDE controller is often added to provide UltraDMA/66 support in motherboards whose chipset does not offer UltraDMA/66 support. Even if the chipset's built-in IDE controller supports UltraDMA/66, it is not controlled by this BIOS feature. This feature is only used for the extra IDE controller.

For the purpose of avoiding confusion, I shall hence refer to the built-in IDE controller as an internal IDE controller while add-on IDE controller will be known as an external IDE controller. If you want to attach one or more IDE devices to the external UltraDMA/66 controller, you should enable this feature. You should only disable it for the following reasons :-

if you don't have any IDE device attached to the external UltraDMA/66 controller for troubleshooting purposes
Disabling the external IDE controller will **free up two IRQs and speed up system booting.** This is because the IDE controller's BIOS doesn't have to be loaded and the external controller's often long boot-up check and initialization sequence will be skipped. So, if you don't use the external IDE controller, it is recommended that you disable it.

SYSTEM BUS

16 bit recovery time

The PCI bus runs at a much higher clock speed than the ISA bus. So, for ISA cards to work properly with I/O cycles from the PCI bus, additional bus clock cycles must be inserted between each consecutive PCI-originated I/O cycles to the ISA bus. By default, the bus recovery mechanism inserts 3.5 clock cycles between each consecutive 16-bit I/O cycle to the ISA bus. This feature enables you to insert even more clock cycles between each consecutive 16-bit I/O cycle to the ISA bus. For example, if you choose 3 cycles, the bus recovery mechanism inserts a total of 3.5 cycles + 3 cycles = 6.5 cycles between each consecutive 16-bit I/O cycle. Choosing NA sets the number of delay cycles to the minimum 3.5 clock cycles.

Most 16-bit ISA cards will work fine with the minimum 3.5 delay cycles. However, some ISA cards may require additional delay cycles. Keep increasing the number of additional delay cycles until the card works properly. You might also need to increase the number of delay cycles if you are overclocking the PCI bus. But if possible, set the 16-bit I/O Recovery Time to **NA** for optimal ISA bus performance. Increase the I/O Recovery Time only if you are having problems with your 16-bit ISA cards. Note that this feature is **only valid if you are using 16-bit ISA cards**. It has no effect if there are no 16-bit ISA devices in the system.

8 bit recovery time

The PCI bus runs at a much higher clock speed than the ISA bus. So, for ISA cards to work properly with I/O cycles from the PCI bus, additional bus clock cycles must be inserted between each consecutive PCI-originated I/O cycles to the ISA bus. By default,

the bus recovery mechanism inserts 3.5 clock cycles between each consecutive 8-bit I/O cycle to the ISA bus. This feature enables you to insert even more clock cycles between each consecutive 8-bit I/O cycle to the ISA bus. For example, if you choose 3 cycles, the bus recovery mechanism inserts a total of 3.5 cycles + 3 cycles = 6.5 cycles between each consecutive 8-bit I/O cycle. Choosing NA sets the number of delay cycles to the minimum 3.5 clock cycles.

Most 8-bit ISA cards will work fine with the minimum 3.5 delay cycles. However, some ISA cards may require additional delay cycles. Keep increasing the number of additional delay cycles until the card works properly. You might also need to increase the number of delay cycles if you are overclocking the PCI bus. But if possible, set the 8-bit I/O Recovery Time to **NA** for optimal ISA bus performance. Increase the I/O Recovery Time only if you are having problems with your 8-bit ISA cards. Note that this feature is **only valid if you are using 8-bit ISA cards.** It has no effect if there are no 8-bit ISA devices in the system.

Autodetect DIMM/PCI clk

When the motherboard's clock generator pulses, the extreme values (spikes) of the pulses creates EMI (Electromagnetic Interference). This causes interference with other electronics in the area. To reduce this problem, the BIOS can either modulate the pulses (to make them flatter) or turn off unused AGP, PCI or SDRAM clock signals. This feature is similar to the Smart Clock option of the Spread Spectrum feature, which acts by the second method. If you enable it, the BIOS will monitor the AGP, PCI and SDRAM DIMM slots. The clock signals of unoccupied slots are automatically turned off.. The clock signals to occupied AGP, PCI or SDRAM slots will also be turned off whenever there's no activity.

Theoretically, EMI (Electromagnetic Interference) can be reduced this way without compromising system stability. This also allows the computer to reduce power consumption because only components that are running will use power and then only when they are actually doing work. The choice of whether to enable or disable this feature is really up to your personal preference. But since this feature reduces EMI and power consumption without compromising system stability, it's recommended that you **enable** it.

Byte Merge

This BIOS feature is similar to the PCI Dynamic Bursting feature. If you have already read about the CPU to PCI Write Buffer feature, you should know that the chipset has an integrated write buffer which allows the CPU to immediately write up to four words of PCI writes to it, thus freeing it quickly and allowing it to work on other tasks. However, the CPU doesn't always write 32-bit data to the PCI bus. 8-bit and 16-bit writes can also take place. But while the CPU may write 8-bits of data to the PCI bus, it is considered as a single PCI transaction, equivalent to a 16-bit or 32-bit write. This reduces the effective PCI bandwidth, especially if there are many 8-bit or 16-bit CPU-to-PCI writes.

To solve this problem, the write buffer can be programmed to accumulate and merge 8-bit and 16-bit writes into 32-bit writes. The buffer then writes the merged data to the PCI bus. As you can see, merging the smaller 8-bit or 16-bit writes into a few large 32-bit writes reduces the number of PCI transactions required. This increases the efficiency of the PCI bus and improves its bandwidth. This feature controls the byte merging capability of the PCI write buffer. If it is enabled, every write transaction will go straight to the write buffer. They are accumulated until enough data is available to be written to the PCI bus in a single burst. This improves the PCI bus' performance so it's recommended that you **enable** this feature.

If you disable byte merging, all writes will still go to the PCI write buffer (if CPU to PCI Write Buffer has been enabled). But the buffer won't accumulate and merge the data. The data is written to the PCI bus as soon as it is free. As such, there may be a loss of PCI bus efficiency, particularly when 8-bit or 16-bit data is written to the bus. However, please note that Byte Merge may be incompatible with certain PCI network interface cards (also known as NICs). Boar-Ral explains :-

I noticed that some PCI cards really despise Byte Merge, in particular the 3Com 3C905 series of NICs. While this may only apply to certain motherboards, in my case the P3V4X, I feel that this is probably not the case and it is a rather widespread problem. Issues I have encountered with Byte Merge enabled range from Windows 98 SE freezing at the boot screen to my NIC not functioning at all. This issue has been confirmed with others using the same NIC and is what alerted me to the issue in the first place.

I wanted to confirm the observation posted by Boar-Ral concerning the "Byte Merge" BIOS setting. After enabling "Byte Merge" and making other recommended BIOS setting changes, I suddenly lost all network I/O from my system. And yes, I happen to be using a 3Com 3C905B-TX NIC (with an Asus A7V motherboard). After a great deal of trial and error troubleshooting, I found that disabling "Byte Merge" would let everything work again.

On the other hand, Cprall discovered that he was able to use the NIC in Windows 98 SE but not in Windows 2000. Check out what he has to say :-
I'll even third this to say I was recently bitten by the same (A7V motherboard at BIOS 1009 and 3C905B-TX network card). I did have one slight addition to what was seen here. With Byte Merge enabled, I was able to access the network under Windows 98 SE, but not Windows 2000. With Byte Merge disabled, the network card works under both. **In conclusion, if your NIC (Network Interface Card) won't work properly, try disabling Byte Merge.** That will take a bite out of the PCI bus' performance but that can't be helped if you want the NIC to work. Other than this exception, you should enable Byte Merge for better performance.

CPU drive strength

The system controller has auto-compensation circuitry that compensates for impedance variations in motherboard designs. But since the motherboard impedance is more or less fixed for each motherboard design, the manufacturer will sometimes determine the optimal drive strength for that particular design and use it instead of relying on the auto-compensation circuitry. Either way, the motherboard's impedance on the processor bus will be compensated for.

However, when the auto-compensation logic is bypassed and a fixed drive strength is used, the amount of impedance compensation may not be sufficient sometimes. Hence the need for this BIOS feature. It allows you to manually set the processor bus drive strength. The higher the value, the stronger the drive strength.

Due to the nature of this BIOS feature, it is possible to use it as an aid in overclocking the CPU. Your CPU may not overclock as well as you wanted it to. But by raising the CPU Drive Strength, it is possible to improve its stability at overclocked speeds. So, try the higher values of 2 or 3 if your CPU just won't go the extra mile.

However, this is not a surefire way of overclocking the CPU. Increasing it to the highest value will not necessarily mean that you can overclock the CPU more than you already can. In addition, it is important to note that increasing the CPU drive strength will not improve its performance. Contrary to popular opinion, it is not a performance enhancing feature.

Although little else is known about this feature, the downsides to a high CPU drive strength would probably be increased EMI (Electromagnetic Interference), power consumption and thermal output. Therefore, unless you need to boost the processor bus drive strength (for troubleshooting or overclocking purposes), it is recommended that you leave it at the **default setting**.

CPU to PCI post write

This feature controls the CPU-to-PCI write buffer. If this buffer is disabled, the processor writes directly to the PCI bus. Although it may seem like the faster and better method, that isn't really true. Because the processor bus (which runs from 100MHz to 266MHz and beyond) is many times faster than the PCI bus (33MHz), any CPU writes to the PCI bus will have to wait until the PCI bus is ready to receive data. This prevents the processor from doing anything else until it has completed the transaction.

Enabling this feature allows the processor to immediately write up to four words of data to the CPU-to-PCI write buffer so that it can move onto another task without waiting for those four words of data to be written to the PCI bus.
Now, the data in the write buffer won't reach the PCI bus any faster than usual. This is because they will only be written to the PCI bus when the next available PCI cycle starts. But the difference here is that the entire operation can now occur without tying up the processor.

To sum it all up, enabling the CPU to PCI write buffer frees up CPU cycles that would normally be wasted waiting for the PCI bus. Therefore, it is recommended that you **enable** the CPU to PCI write buffer.

CPU to PCI write buffer

This feature controls the CPU-to-PCI write buffer. If this buffer is disabled, the processor writes directly to the PCI bus. Although it may seem like the faster and better method, that isn't really true. Because the processor bus (which runs from 100MHz to 266MHz and beyond) is many times faster than the PCI bus (33MHz), any CPU writes to the PCI bus will have to wait until the PCI bus is ready to receive data. This prevents the processor from doing anything else until it has completed the transaction.

Enabling this feature allows the processor to immediately write up to four words of data to the CPU-to-PCI write buffer so that it can move onto another task without waiting for those four words of data to be written to the PCI bus.
Now, the data in the write buffer won't reach the PCI bus any faster than usual. This is because they will only be written to the PCI bus when the next available PCI cycle starts. But the difference here is that the entire operation can now occur without tying up the processor.

To sum it all up, enabling the CPU to PCI write buffer frees up CPU cycles that would normally be wasted waiting for the PCI bus. Therefore, it is recommended that you **enable** the CPU to PCI write buffer.

Delayed transaction

The ISA bus is slower than the PCI bus. So, when the PCI bus wants to write to the ISA bus, it has to wait until the ISA bus is ready. Because the ISA bus is many, many times slower than the PCI bus, the PCI bus is normally stalled for a long time whenever a PCI cycle to the ISA bus is initiated. This prevents other devices from accessing the PCI bus and can cause problems for time-critical applications that need constant access to the PCI bus.

To prevent the PCI bus from stalling every time it tries to write to the ISA bus, many chipsets now come with an embedded 32-bit posted write buffer. This buffer is designed to store PCI-to-ISA writes and thus allows delayed transaction cycles to be generated. When enabled, the PCI bus immediately writes up to two 16-bit or four 8-bit data to the write buffer. The PCI bus can then be freed to perform other transactions. The buffer contents are independently written to the ISA bus when it's ready. Now, the data in the write buffer won't reach the ISA bus any faster than usual. This is because they will only be written to the ISA bus when the next available ISA cycle starts. But the difference here is that the entire operation can now occur without tying up the PCI bus.

This BIOS feature controls the operation of that embedded 32-bit posted write buffer. If enabled, up to four bytes of PCI-to-ISA writes are buffered and the PCI bus is released after writing to the buffer. If Delayed Transaction is disabled, the PCI bus will bypass the write buffer and write directly to the ISA bus.

It's highly recommended that you **enable** this feature for better PCI performance and to meet PCI 2.1 specifications. Disable it only if your PCI cards cannot work properly with this feature enabled or if you are using an ISA card that is not PCI 2.1 compliant. Note that Delayed Transaction is only important if you are actually using ISA devices. It is of no consequence at all if you are not using any ISA devices or if your motherboard doesn't even come with ISA slots!

Duplex selection

The Duplex Select option is usually found under the Onboard Serial Port 2 BIOS feature. It is slaved to the second serial port so if you disable that serial port, this option will disappear from the screen or appear grayed out.
This feature allows you to determine the transmission mode of the IR port. Selecting Full-Duplex permits simultaneous two-way transmission, like a conversation over the phone. On the other hand, selecting Half-Duplex only permits transmission in one direction at any one time, which is more like a conversation over the walkie-talkie.

Naturally, the Full-Duplex mode is the faster and more desirable choice. You should use **Full-Duplex** if possible. Consult your IR peripheral's manual to determine if it supports Full-Duplex transmission or not. The IR peripheral must support Full-Duplex for this option to work.

ECP mode use DMA

This feature is usually found under the Parallel Port Mode feature. It's slaved to the ECP (Extended Capabilities Port) options of the Parallel Port Mode feature so if you do not enable either ECP or ECP+EPP, this feature will disappear from the screen or appear grayed out. The ECP mode uses the DMA protocol to achieve data transfer rates of up to 2.5Mbits/s and provides symmetric bidirectional communication. This means it requires the use of a DMA channel.

By default, the parallel port uses DMA Channel 3 when in ECP mode. This works just fine in most situations so you shouldn't need to change it. This feature was provided just in case one of your add-on cards requires the use of DMA Channel 3. In that case, you can use this BIOS feature to force the parallel port to use the alternative DMA Channel 1. Otherwise, stick with the **default setting of Channel 3**.

ECP mode select

This feature is usually found under the Parallel Port Mode feature. It's slaved to the EPP (Enhanced Parallel Port) options of the Parallel Port Mode feature so if you do not enable either EPP or ECP+EPP, this feature will disappear from the screen or appear grayed out. There are two versions of the EPP transfer protocol - EPP 1.7 and EPP 1.9. This feature allows you to select the version of EPP that the parallel port should use.

Generally, **EPP 1.9** is the preferred setting because it supports the newer EPP 1.9 devices and most EPP 1.7 devices; and offers advantages like support for longer cables. However, because certain EPP 1.7 devices cannot work properly with an EPP 1.9 port, this BIOS feature was implemented to allow you to set the EPP mode to EPP 1.7 when such an issue crops up.

For more information, check out KasperPedersen's explanation :-
In the EPP protocol, the port asserts a request strobe (I want to read/write). The attached device reads the data, and asserts an acknowledge strobe (I have taken/provided the data). The port then negates the strobe (operation done). Finally the attached device negates its acknowledgement (I'm ready for another operation). The difference between 1.7 and 1.9 is the last state where the attached device removes the acknowledge strobe. 1.7 ports don't check that the device has negated the acknowledge strobe, but presumes that the device will have removed it when 125ns have passed. This can be a problem if cables are long.

This was fixed in 1.9: Before it starts a cycle, it waits for the attached device to negate the acknowledge strobe from the last cycle. This allows for a cleaner hardware design at the device end; and longer cables (50m possible if IEEE1284 is used, even though that's outside the specs.) It sums down to that setting the port for 1.9 is compatible with previous 1.7 devices, but setting the port for 1.7 will cause problems with 1.9 devices or long cables. The reason it's an option at all is that "some" 1.7 devices won't cope with a new cycle less than 125 ns after the port has negated the request strobe. This is to be considered a hardware bug in the device.

ISA 14.318mhz clock

The ISA bus only runs at a clock speed of 8.33MHz. Because each ISA data transfer takes anywhere from two to eight clock cycles to complete, this yields a maximum bandwidth of only 4.77MB/s for 8-bit cards and 8.33MB/s for 16-bit cards. Maximum bandwidth for the 8-bit ISA bus = 8.33MHz x 1 byte (8-bits) ÷ 2 clock cycles per transfer = 4.77MB/s Maximum bandwidth for the 16-bit ISA bus = 8.33MHz x 2 bytes (16-bits) ÷ 2 clock cycles per transfer = 8.33MB/s

This BIOS feature allows you to overclock the ISA bus using the reference clock generator speed of 14.318MHz. This improves the ISA bus bandwidth by 72%! 8-bit cards will thus have a bandwidth of 7.16MB/s while 16-bit cards will have a bandwidth of 14.32MB/s.

Naturally, it is recommended that you enable this feature to give the ISA bus a performance boost. Of course, this is only useful if you have ISA devices in your system. Otherwise, this feature is redundant. Please note that while newer ISA cards are capable of running at this 'out-of-spec' speed, older ones may not work properly at this speed. Therefore, if your ISA card fails to function properly, **disable** this feature.

Master priority rotation

This feature controls the processor's access to the PCI bus. If you choose 1 PCI, the processor will always be granted access right after the current PCI bus master transaction completes, irrespective of how many other PCI bus masters are on the queue. This affords the quickest processor access to the PCI bus but it also means poorer performance for PCI devices.

If you choose 2 PCI, the processor will be granted access after the current and the next PCI transaction completes. In other words, the processor is guaranteed access after two PCI bus master transactions, irrespective of how many other PCI bus masters are also on the queue. This means the processor has to wait a little longer than with the 1 PCI option but PCI devices will have more access to the PCI bus.

If you choose 3 PCI, the processor will only be granted access to the PCI bus after the current PCI bus master transaction and the following two PCI bus master transactions on the queue have been completed. Therefore, the processor has to wait for three PCI bus masters to complete their transactions on the PCI bus before it can gain access to the PCI bus itself. This means poorer processor-to-PCI performance but PCI bus masters will enjoy better performance.

But no matter what you choose, the processor is guaranteed access to the PCI bus after a certain number of PCI bus master grants. It doesn't matter if there are numerous PCI bus masters on the queue or when the processor requested access to the PCI bus. The processor will always be granted access after one PCI bus master transaction (1 PCI), two transactions (2 PCI) or three transactions (3 PCI).

For better overall performance, it is recommended that you select the **1 PCI** option as this allows the processor to access the PCI bus with minimal delay. However, if you wish to improve the performance of your PCI devices, you can try the 2 PCI or 3 PCI options. They allocate more PCI bus resources to your PCI cards.

Onboard parallel port

This feature allows you to select the I/O address and IRQ for the onboard parallel port. The default I/O address of 378h and IRQ of 7 should work well in most cases. Unless you have a problem with the parallel port, you should leave it at the **default** settings. Only select an alternative I/O address or IRQ if the parallel port settings are conflicting with other devices.

You can also **disable the onboard parallel port if you do not need to use it.** Doing so frees up the I/O port and IRQ used by the parallel port. Those resources can then be reallocated for other devices to use.

Onboard serial port 1

This feature allows you to manually select the I/O address and IRQ for the first serial port. It is recommended that you leave it as **Auto** so that the BIOS can select the best settings for it. But if you need a particular I/O port or IRQ that's been taken up by this serial port, you can manually select an alternative I/O port or IRQ for it. You can also **disable this serial port if you do not need to use it.** Doing so frees up the I/O port and IRQ used by this serial port. Those resources can then be reallocated for other devices to use.

Onboard serial port 2

This feature allows you to manually select the I/O address and IRQ for the second serial port. It is recommended that you leave it as **Auto** so that the BIOS can select the best settings for it. But if you need a particular I/O port or IRQ that's been taken up by this serial port, you can manually select an alternative I/O port or IRQ for it. You can also **disable this serial port if you do not need to use it.** Doing so frees up the I/O port and IRQ used by this serial port. Those resources can then be reallocated for other devices to use.

Onboard USB controller

This BIOS feature is somewhat similar to Assign IRQ For USB. But instead of controlling the assignment of an IRQ to the motherboard's onboard USB controller, this feature directly controls the function of the onboard USB controller. Enable this feature if you want to attach your USB devices to the onboard USB controller. If you disable this feature, the USB controller will be disabled and you won't be able to connect any USB devices to it. But **if you don't use any USB devices, this frees up an IRQ for other devices to use.** This is particularly useful when you have many devices that can't share IRQs. Disabling this feature may not be necessary with APIC-capable motherboards because they come with more IRQs.

P2C/C2P concurrency

P2C/C2P Concurrency enables the PCI-to-CPU and CPU-to-PCI traffic to occur concurrently (simultaneously). This prevents the CPU from being "locked up" during PCI transfers. It also allows PCI traffic to the processor to occur without delay even when the processor is writing to the PCI bus. This may prevent performance issues with certain PCI cards. Therefore, it is recommended that you **enable** this feature for better performance.

Parallel port mode

This function is usually found under the Onboard Parallel Port feature. It's linked to the parallel port so if you disable the parallel port, this function will not appear or will appear greyed out. There are four options. By default, the parallel port is usually set to the Normal (SPP) mode. SPP stands for Standard Parallel Port and it is the original transfer protocol for the parallel port. Therefore, it will work with all parallel port devices.

Originally a unidirectional port, the SPP was eventually adapted to work bidirectionally. So, contrary to popular opinion, the SPP mode is capable of bidirectional transfers. However, it can only receive 4-bits of data in this bidirectional mode. Its output, fortunately, remains at 8-bits. This gives the parallel port in SPP mode an output rate of 150KB/s and an input rate of 50KB/s. The ECP (Extended Capabilities Port) transfer mode was introduced by Microsoft and Hewlett-Packard to provide fast, bidirectional communication between the computer and high-performance printers and scanners. It uses the DMA protocol to achieve data transfer rates of up to 2MB/s and provides symmetric bidirectional communication.

On the other hand, EPP (Enhanced Parallel Port), now known as IEEE 1284, uses existing parallel port signals to provide asymmetric bidirectional communication. It was also designed for high-speed communications, offering transfer rates of up to 2MB/s. As you can see, SPP is a very slow transfer mode. It should only be selected when faster transfer modes cannot be used (i.e. with old printers or scanners). With modern parallel port devices, the ECP and EPP modes are the transfer modes of choice.

Generally, because of its FIFOs and the DMA channel it uses, ECP is good at large data transfers. Therefore, it is the transfer mode that works best with scanners and printers. EPP is better with devices that switch between reads and writes frequently (like ZIP drives and hard disks). This tip was obtained from Jan Axelson's Parallel Port FAQ so check it out if you require more information on parallel ports.

However, **before you set the transfer mode, please check your parallel port device's documentation.** The manufacturer of your parallel port peripheral may have designated a preferred parallel port mode for the device in question. In that case, it is best to follow their recommendation. If the device documentation did not state any preferred transfer mode and you still do not know what mode to select, you can select the ECP+EPP mode. If you select this mode, the BIOS will automatically determine the transfer mode to use for your device.

However, this should be considered as a last resort as you may be needlessly tying up a DMA for nothing if your device does not use ECP at all. Or the BIOS may not select the best parallel port mode for the device. If possible, **set the parallel port to the transfer mode that best suits your parallel port device.**

Passive release

If you have already read about the CPU to PCI Write Buffer feature, you should know that the chipset has an integrated write buffer that allows the CPU to immediately write up to four words of PCI writes to it, thus freeing it quickly and allowing it to work on other tasks. This BIOS feature controls the passive release function of the CPU to PCI Write Buffer. So, if the write buffer is disabled, this function will not have any effect. However, the reverse isn't true. The CPU to PCI Write Buffer feature will still work even if Passive Release is disabled.

What Passive Release does is allow the write buffer to independently write the data to the PCI bus at the first available opportunity. It can do so even when the processor is busy doing something else. Without Passive Release, the write buffer waits till the CPU reasserts the write request before it writes to the PCI bus. This still saves time (and improves performance) because the CPU doesn't actually need to resend the data. The write buffer is ready to offload the data the moment the PCI bus arbiter releases control of the bus to the CPU. However, because the write buffer has to wait for the CPU to retry the transaction, this reduces its effectiveness.

This is a particularly big problem when an ISA device engages the ISA bus. Because the ISA bus is very slow, this ties up the PCI bus and prevents the CPU from accessing it for a very long time. If the CPU-to-PCI write buffer had been enabled, the CPU immediately writes to the buffer. This frees the CPU to engage in other tasks but the write buffer cannot write to the PCI bus until both the CPU is free to retry the write and the PCI bus is free to receive.

Passive Release helps by allowing the write buffer to "passively write" to the PCI bus without CPU intervention and while the ISA device is engaging the PCI bus. This essentially allows the CPU to indirectly write to the PCI bus even when the ISA device has control over it. Without this feature, the PCI bus arbiter will only allow other (non-CPU) PCI masters to access the PCI bus. For best performance, enable Passive Release. This will dramatically reduce the hogging effect of slow ISA devices on the PCI bus. However, some ISA cards may not work well with Passive Release. In such cases, disable Passive Release or better yet, throw the card away and get a PCI version!

If you don't use any ISA device, this feature should still be enabled because it will allow the write buffer to offload its data to the PCI bus without waiting for the CPU to retry the transaction. This improves the CPU and PCI bus performance. Please note that if you do not enable the CPU to PCI Write Buffer, this feature will have no effect.

PCI 2.1 compliance

This is the same thing as Delayed Transaction. The ISA bus is slower than the PCI bus. So, when the PCI bus wants to write to the ISA bus, it has to wait until the ISA bus is ready. Because the ISA bus is many, many times slower than the PCI bus, the PCI bus is normally stalled for a long time whenever a PCI cycle to the ISA bus is initiated. This prevents other devices from accessing the PCI bus and can cause problems for time-critical applications that need constant access to the PCI bus.

To prevent the PCI bus from stalling every time it tries to write to the ISA bus, many chipsets now come with an embedded 32-bit posted write buffer. This buffer is designed to store PCI-to-ISA writes and thus allows delayed transaction cycles to be generated. When enabled, the PCI bus immediately writes up to two 16-bit or four 8-bit data to the write buffer. The PCI bus can then be freed to perform other transactions. The buffer contents are independently written to the ISA bus when it's ready. Now, the data in the write buffer won't reach the ISA bus any faster than usual. This is because they will only be written to the ISA bus when the next available ISA cycle starts. But the difference here is that the entire operation can now occur without tying up the PCI bus.

This BIOS feature controls the operation of that embedded 32-bit posted write buffer. If enabled, up to four bytes of PCI-to-ISA writes are buffered and the PCI bus is released after writing to the buffer. If PCI 2.1 Compliance is disabled, the PCI bus will bypass the write buffer and write directly to the ISA bus.

It's highly recommended that you **enable** this feature for better PCI performance and to meet PCI 2.1 specifications. Disable it only if your PCI cards cannot work properly with this feature enabled or if you are using an ISA card that is not PCI 2.1 compliant. Note that PCI 2.1 Compliance is only important if you are actually using ISA devices. It is of no consequence at all if you are not using any ISA devices or if your motherboard doesn't even come with ISA slots!

PCI chaining

PCI chaining feature is designed to speed up writes from the processor to the PCI bus by allowing write combining to occur at the PCI interface. Essentially, when PCI chaining is enabled, up to four quadwords of CPU writes to contiguous PCI addresses will be chained together and written to the PCI bus as a single PCI burst write. When this feature is disabled, each CPU write to the PCI bus will be handled as separate non-burst writes. Needless to say, bursting four quadwords of CPU write in a single PCI write is much faster than separate non-burst writes. It will also reduce the amount of time the CPU has to wait while writing to the PCI bus. Therefore, it is recommended that you **enable** this feature for better CPU to PCI write performance.

PCI clock / CPU FSB clock

The PCI bus is specified to run at a maximum clock speed of 33MHz. The processor bus, on the other hand, has a much higher clock speed. Most processors run on a 100MHz processor bus. Newer processors utilize an even faster 133MHz processor bus. Of course, there are reports of overclockers reaching bus speeds in excess of 166MHz! The PCI bus speed is derived from the processor's bus speed. It does this with the use of clock speed dividers.

This BIOS feature enables you to manually select the PCI bus / CPU bus clock divider. As this divider determines the speed that the PCI bus will run at, the manipulation of this feature allows you some control over the PCI bus speed. As such, you can use it to overclock the PCI bus. With that said, you should keep in mind that while some PCI cards can run at speeds beyond 41.5MHz, the recommended safe limit for an overclocked PCI bus is 37.5MHz. This is the speed at which practically all new PCI cards can run at without breaking a sweat.

Of course, running at a higher speed is definitely possible. But there's a risk of data corruption which is particularly worrisome with the IDE controller which runs off the PCI bus. So, if you intend to overclock beyond 37.5MHz, test and make sure that your IDE devices are running fine before you do any serious work!

Selecting the clock divider of 1/2 makes the PCI bus run at half the processor bus speed. If your processor bus is set to 100MHz, the PCI bus speed will be 50MHz. As such, this clock divider is useful for processor bus speeds of 66MHz to 75MHz. Within that range, the PCI bus will run from 33MHz to 37.5MHz.

Selecting the clock divider of 1/3 makes the PCI bus run at a third of the processor bus speed. If your processor bus is set to 100MHz, the PCI bus speed will be 33MHz. As such, this clock divider is useful for processor bus speeds of 100MHz to 112.5MHz. Within that range, the PCI bus will run from 33MHz to 37.5MHz.

Selecting the clock divider of 1/4 makes the PCI bus run at a quarter of the processor bus speed. If your processor bus is set to 100MHz, the PCI bus speed will be 25MHz. As such, this clock divider is useful for processor bus speeds of 133MHz to 150MHz. Within that range, the PCI bus will run from 33MHz to 37.5MHz.

You will probably be wondering about the gaps in the covered processor bus speeds above. Well, only processor bus speeds that will produce PCI clock speeds that are within the range of optimal PCI clock speeds (33MHz to 37.5MHz) are shown above. The other processor bus speeds will either produce a slow PCI bus or an excessively overclocked one. Therefore, for optimal PCI bus performance, **try to strike for one of the processor bus speed-divider combinations shown above.**

Please note that motherboards that claim 200-266MHz processor bus speeds are actually only running at 100-133MHz. The 200-266MHz claim is based on the fact that in these motherboards, data is transferred on both edges of the clock signal, thereby

doubling the bandwidth of the processor bus. Therefore, as far as this feature is concerned, such motherboards are only running at 100-133MHz.

PCI delay transaction

This is the same thing as Delayed Transaction. The ISA bus is slower than the PCI bus. So, when the PCI bus wants to write to the ISA bus, it has to wait until the ISA bus is ready. Because the ISA bus is many, many times slower than the PCI bus, the PCI bus is normally stalled for a long time whenever a PCI cycle to the ISA bus is initiated. This prevents other devices from accessing the PCI bus and can cause problems for time-critical applications that need constant access to the PCI bus.

To prevent the PCI bus from stalling every time it tries to write to the ISA bus, many chipsets now come with an embedded 32-bit posted write buffer. This buffer is designed to store PCI-to-ISA writes and thus allows delayed transaction cycles to be generated. When enabled, the PCI bus immediately writes up to two 16-bit or four 8-bit data to the write buffer. The PCI bus can then be freed to perform other transactions. The buffer contents are independently written to the ISA bus when it's ready.

Now, the data in the write buffer won't reach the ISA bus any faster than usual. This is because they will only be written to the ISA bus when the next available ISA cycle starts. But the difference here is that the entire operation can now occur without tying up the PCI bus. This BIOS feature controls the operation of that embedded 32-bit posted write buffer. If enabled, up to four bytes of PCI-to-ISA writes are buffered and the PCI bus is released after writing to the buffer. If PCI Delay Transaction is disabled, the PCI bus will bypass the write buffer and write directly to the ISA bus.

It's highly recommended that you **enable** this feature for better PCI performance and to meet PCI 2.1 specifications. Disable it only if your PCI cards cannot work properly with this feature enabled or if you are using an ISA card that is not PCI 2.1 compliant. Note that PCI Delay Transaction is only important if you are actually using ISA devices. It is of no consequence at all if you are not using any ISA devices or if your motherboard doesn't even come with ISA slots!

PCI dynamic bursting

This is similar to the Byte Merge feature. If you have already read about the CPU to PCI Write Buffer feature, you should know that the chipset has an integrated write buffer which allows the CPU to immediately write up to four words of PCI writes to it, thus freeing it quickly and allowing it to work on other tasks. However, the CPU doesn't always write 32-bit data to the PCI bus. 8-bit and 16-bit writes can also take place. But while the CPU may write 8-bits of data to the PCI bus, it is considered as a single PCI transaction, equivalent to a 16-bit or 32-bit write. This reduces the effective PCI bandwidth, especially if there are many 8-bit or 16-bit CPU-to-PCI writes.

To solve this problem, the write buffer can be programmed to accumulate and merge 8-bit and 16-bit writes into 32-bit writes. The buffer then writes the merged data to the PCI bus. As you can see, merging the smaller 8-bit or 16-bit writes into a few large 32-bit writes reduces the number of PCI transactions required. This increases the efficiency of the PCI bus and improves its bandwidth. This feature controls the dynamic bursting capability of the PCI write buffer. If it is enabled, every write transaction will go straight to the write buffer. They are accumulated until enough data is available to be written to the PCI bus in a single burst. This improves the PCI bus' performance so it's recommended that you enable this feature.

If you disable PCI dynamic bursting, all writes will still go to the PCI write buffer (if CPU to PCI Write Buffer has been enabled). But the buffer won't accumulate and merge the data. The data is written to the PCI bus as soon as it is free. As such, there may be a loss of PCI bus efficiency, particularly when 8-bit or 16-bit data is written to the bus.
Note that like Byte Merge, this feature **may not be compatible with certain PCI network interface cards.** For more details, please check out the Byte Merge feature.

PCI IRQ activated by

This BIOS feature allows you to set the method by which the IRQs for your PCI devices are activated or triggered. ISA and old PCI devices are edge-triggered (using a single voltage level) while newer PCI and AGP devices are level-triggered (using multiple voltage levels). This is important mainly because PCI devices must be level-triggered to share IRQs. The multiple voltage levels supported by level-triggered cards are used to activate the proper device among multiple devices sharing the same IRQ. Edge-triggered devices only support a single voltage level which can only be used to activate or deactivate their IRQs. Therefore, IRQs allocated to edge-triggered devices cannot be shared with other devices.

When PCI devices were initially introduced, they were almost always edge-triggered and therefore didn't support IRQ sharing. That's why the default and recommended setting for older PCI devices was invariably Edge. Unfortunately, that misled people into thinking that it would be the same for newer PCI devices.

Current PCI devices are all level-triggered and so support IRQ sharing. This is critical in allowing the use of the numerous PCI devices in present day computers. Without IRQ sharing, IRQ conflicts would have posed serious configuration problems. Of course, the introduction of the Advanced Programmable Interrupt Controller or APIC solves this problem completely by providing anywhere from 24 to 512 IRQ lines! But until all motherboards come with APIC, IRQ sharing will continue to play an important role in allowing multiple PCI devices to work in harmony.

Because every PCI device currently in the market is level-triggered, it makes sense to set this BIOS feature to Level so that your PCI devices can share IRQs. However, if you are **still using old edge-triggered devices, select Edge to force the chipset to allow only edge-triggering of PCI devices.** This may cause configuration problems if there are IRQ conflicts but it will prevent system crashes or lockups that can occur if the chipset erroneously attempts to level-trigger an edge-triggered PCI device.

PCI latency timer

This feature controls how long a PCI device can hold the PCI bus before another takes over. The larger the value, the longer the PCI device can retain control of the bus. As each access to the bus comes with an initial delay before any transaction can be made, a short PCI latency time will actually reduce the effective PCI bandwidth while longer latencies improve it. On the other hand, while increasing the PCI latency time lets each PCI device access the bus longer, the response time of all PCI devices suffers in return. In other words, a long PCI latency will allow active PCI device to use the PCI bus longer albeit at the expense of other PCI devices queuing up to use the bus. All PCI devices will therefore have to wait longer before gaining access to the bus.

Normally, the PCI Latency Timer is set to 32 cycles. For better PCI performance, a larger value should be used. Try increasing it to **64 cycles** or even 128 cycles. The optimal value for every system is different. So, benchmark your PCI cards' performance after each change to determine the optimal PCI latency time for your system.

Note that a longer PCI latency isn't necessarily better. Too long a latency can reduce performance as too much time may be allocated to each PCI device to the disadvantage of the other devices on the bus. This is especially true with systems that have many PCI devices. Also, some time-critical PCI devices may not agree with a long latency **so if you start facing problems with one or more of your PCI devices, reduce** the latency.

PCI master 0 WS read
This feature determines whether the chipset inserts a delay before any reads from the PCI bus. If this is enabled, then read requests to the PCI bus are executed immediately (with zero wait states), if the PCI bus is ready to send data. But if it is disabled, then every read request to the PCI bus is delayed by one wait state. Normally, it is recommended that you **enable this feature for faster PCI performance.** However, **disabling it may be useful when attempting to stabilize an overclocked PCI bus.** The delay will generally improve the overclockability and stability of the PCI bus.

PCI master 0 WS write
This feature determines whether the chipset inserts a delay before any writes to the PCI bus. If this is enabled, then writes to the PCI bus are executed immediately (with zero wait states), if the PCI bus is ready to receive data. But if it is disabled, then every write transaction to the PCI bus is delayed by one wait state. Normally, it is recommended that you **enable this feature for faster PCI performance.** However, **disabling it may be useful when attempting to stabilize an overclocked PCI bus.** The delay will generally improve the overclockability and stability of the PCI bus.

PCI master read caching
Just like Video RAM Cacheable, this feature may actually hinder performance although it was designed to improve it. How is that so? If this feature is enabled, the processor's L2 cache will be used to cache PCI bus master reads. This was designed to boost the performance of PCI bus masters. However, this reduces the processor's performance since it uses up some of the precious L2 cache.

That's why ASUS recommends that only those using AMD Athlons should enable this feature. Duron users should disable this feature because its small L2 cache will not be able to cache the PCI reads without a massive hit to memory bandwidth. However, it is questionable that even Athlon systems will really benefit from this feature. For one thing, the Athlon doesn't have so much L2 cache that using it to boost PCI bus masters' performance won't detrimentally affect its performance. And just like the Video RAM Cacheable feature, it involves two-way use of the processor bus (the EV6 bus in this case), which reduces its efficiency and the processor's performance as well.

So, does the boost in PCI bus master performance justify the loss in processor and memory performance? Although the final word is still in the air, I recommend **disabling** this feature. IMHO, **the use of precious L2 cache to cache PCI bus masters is just not worth the potential benefit** in PCI bus performance.

PCI pipelining
This BIOS feature determines if PCI transactions to the memory subsystem will be pipelined. If enabled, the memory controller allows PCI transactions to be pipelined. This masks the latency of the PCI bus which greatly improves the efficiency of the bus. However, this is only true for multiple transactions in the same direction. Pipelining won't help with PCI devices that switch between reads and writes often. This feature is different from a burst transfer in which multiple data are transferred consecutively with only a single command. In PCI pipelining, different transactions are preprocessed in the pipeline without waiting for the current transaction to finish. Normally, outstanding transactions have to wait for the current one to complete before they are initiated.

Please note that because the transactions are pipelined and flagged as performed (even though they have not actually been completed), data coherency problems may occur. This is because other devices may be writing to the same block of memory as the PCI device. This may cause valid data to be overwritten by outdated or expired data, causing problems like data corruption or hard system locks.

If the PCI pipeline is disabled, the memory controller is forced to check for outstanding transactions from other devices to the same block address that each PCI transaction is targeting. If there's a match, then the PCI transaction is stalled until the other transaction has completed. This essentially forces the memory controller to hold the PCI bus until the PCI transaction is cleared to occur. It also prevents PCI transactions from being pipelined. Both factors greatly reduce performance.

Therefore, for better performance, the PCI pipeline should be **enabled**. This allows the latency of the bus to be masked for consecutive transactions. However, **if your system constantly locks up for no apparent reason**, try **disabling** this feature. **Disabling PCI Pipelining reduces performance but ensures that data coherency is strictly maintained for maximum reliability.**

PCI prefetch
This feature controls the system controller's PCI prefetch capability. When enabled, the system controller will prefetch eight quadwords (or one cache line) of data from the SDRAM when a PCI device reads from the main memory. This is done on the assumption that PCI device will request the next cache line of data. This allows subsequent contiguous memory accesses by the same PCI device to occur with minimal delay. So, it is recommended that you **enable** this feature for better PCI read performance

PCI target latency
This feature determines if the system controller conforms to the PCI maximum target latency rule. According to the PCI maximum target latency rule, the PCI device must service a read request within 32 PCI clock cycles for the initial read and 8 PCI clock cycles for each subsequent read. Note that this only applies to the PCI bus. It does not apply to the AGP bus. When this feature is disabled, the PCI bus master will not be disconnected when it cannot service a read request within the stipulated 32 PCI clock cycles for the initial read and 8 PCI clock cycles for subsequent reads.

When this feature is enabled, the system controller will disconnect the PCI bus master and force a retry when it cannot service a read request within 32 PCI clock cycles for the initial read and 8 PCI clock cycles for subsequent reads. It is recommended that you **enable** this feature to prevent potential deadlocks when there's PCI to AGP traffic.

PCI to DRAM prefetch

This feature controls the system controller's PCI prefetch capability. When enabled, the system controller will prefetch eight quadwords (or one cache line) of data from the SDRAM when a PCI device reads from the main memory. This is done on the assumption that PCI device will request the next cache line of data. This allows subsequent contiguous memory accesses by the same PCI device to occur with minimal delay. So, it is recommended that you **enable** this feature for better PCI read performance.

PCI / VGA palatte snoop

This feature is only useful if you use a fixed-function add-on display card like a MPEG decoder card that requires a VGA-compatible graphics card to be present. Such fixed-function display cards generally do not have their own VGA palette. So, they will have to "snoop" the VGA palette data from the PCI graphics card to generate the proper colours. Normally, the PCI graphics card's Feature Connector is used for this purpose.

When enabled, the PCI graphics card will not respond to the framebuffer writes. It will forward them to the add-on card via its Feature Connector. The fixed-function display card can then snoop the palette data and generate the proper colours. This ensures accurate colour reproduction as well as prevent the monitor from displaying a blank screen after using the add-on card. It is recommended that you **disable** this feature **unless you are using a fixed-function add-on display card** which requires palette snooping.

PCI#2 Access #1 retry

This BIOS feature is linked to CPU to PCI Write Buffer. When the buffer is enabled, the CPU writes straightaway to the buffer instead of the PCI bus. The buffer then attempts to write the data to the PCI bus via Passive Release. This frees the CPU from waiting until the PCI bus is free before it writes the data. However, the attempted buffer write to the PCI bus may fail because the PCI bus may still be busy. When that happens, this BIOS feature determines if the buffer write should be reattempted or sent back for arbitration. If this BIOS feature is enabled, then the buffer will attempt to write to the PCI bus until successful. If disabled, the buffer will flush its contents and register the transaction as failed. The CPU will then have to write again to the write buffer.

Generally, it is highly recommended that you **enable** this feature as this will improve the CPU's performance. However, **if you have many PCI devices and their performance is more important than the CPU's, you might want to disable** this feature to prevent the generation of too many retries which may severely tax the PCI bus. Disabling this feature will improve the PCI bus performance especially when you have slow PCI devices that hog the PCI bus for long periods at a stretch. Please note that if you do not enable CPU to PCI Write Buffer, this feature will have no effect.

RxD, TxD active

This feature is usually found under the Onboard Serial Port 2 option. It's linked to the second serial port so if you disable that port, this feature will disappear from the screen or appear grayed out. This feature enables you to set the IR reception/transmission polarity as High or Low. You'll need to **consult your IR peripheral's documentation** to determine the correct polarity. Choosing the wrong polarity will prevent a proper IR connection from being established with the IR peripheral.

S2K bus driving strength

The S2K bus refers to the Athlon processor bus. This BIOS feature determines if the chipset should automatically adjust the drive strength of the Athlon processor bus or allow manual configuration. The default value of **Auto** allows the chipset to dynamically adjust the Athlon bus strength or use values already preset by the manufacturer. Normally, this is the recommended setting. However, there may be occasions when manual configuration of the S2K bus driving strength may be desirable.

It is possible to make use of this feature for overclocking purposes. Increasing the drive strength increases the stability of the S2K bus by reducing the impedance from the motherboard and boosting the signal strength. But be very, very circumspect when you increase the S2K bus drive strength with an overclocked processor as you may be irreversibly damage the processor!

If you wish to manually configure the S2K bus driving strength, you must set the S2K Bus Driving Strength to Manual. This allows you to manually set the S2K bus driving strength value via the S2K Strobe P Control and S2K Strobe N Control options.

S2K strobe N control

This is one of the functions slaved to the S2K Bus Driving Strength feature. If you set the S2K Bus Driving Strength to **Auto**, then the value you choose won't have any effect. In order for this function to have any effect, you need to set S2K Bus Driving Strength to Manual. This function determines the N transistor drive strength of the S2K bus. The drive strength is represented by Hex values from 0 to F (0 to 15 in decimal). The default N transistor drive strength differs from motherboard to motherboard. But the higher the drive strength, the greater the compensation for the motherboard's impedance on the S2K bus. This function is used in conjunction with S2K Bus Driving Strength and S2K Strobe P Control to bypass the dynamic compensation.

Due to the nature of this BIOS function, it is possible to use it as an aid in overclocking the S2K bus. A higher N (and P) transistor drive strength may just be what you need to overclock the S2K bus higher than is normally possible. By raising the drive strength of the S2K bus, you can improve its stability at overclocked speeds.

Please be very, very circumspect when you increase the S2K drive strength with an overclocked processor as you may be irreversibly damage the processor! Also, contrary to popular opinion, increasing the S2K drive strength will not improve the performance of your AMD processor. It is not a performance enhancing feature so you shouldn't increase the N transistor drive strength unless you need to.

S2K strobe P control

This is one of the functions slaved to the S2K Bus Driving Strength feature. If you set the S2K Bus Driving Strength to **Auto**, then the value you choose won't have any effect. In order for this function to have any effect, you need to set S2K Bus Driving Strength to Manual. This function determines the P transistor drive strength of the S2K bus. The drive strength is represented by Hex values from 0 to F (0 to 15 in decimal). The default P transistor drive strength differs from motherboard to motherboard. But the higher

the drive strength, the greater the compensation for the motherboard's impedance on the S2K bus. This function is used in conjunction with S2K Bus Driving Strength and S2K Strobe N Control to bypass the dynamic compensation.

Due to the nature of this BIOS function, it is possible to use it as an aid in overclocking the S2K bus. A higher P (and N) transistor drive strength may just be what you need to overclock the S2K bus higher than is normally possible. By raising the drive strength of the S2K bus, you can improve its stability at overclocked speeds.

Please be very, very circumspect when you increase the S2K drive strength with an overclocked processor as you may be irreversibly damage the processor! Also, contrary to popular opinion, increasing the S2K drive strength will not improve the performance of your AMD processor. It is not a performance enhancing feature so you shouldn't increase the P transistor drive strength unless you need to.

TX, RX inverting enable
This feature is usually found under the Onboard Serial Port 2 option. It's linked to the second serial port so if you disable that port, this feature will disappear from the screen or appear grayed out. This feature enables you to set the IR transmission/reception polarity as Yes (read as Hi) or No (read as Low). You'll need to **consult your IR peripheral's documentation** to determine the correct polarity. Choosing the wrong polarity will prevent a proper IR connection from being established with the IR peripheral.

USB controller
This BIOS feature is somewhat similar to Assign IRQ For USB. But instead of controlling the assignment of an IRQ to the motherboard's onboard USB controller, this feature directly controls the function of the onboard USB controller. **Enable** this feature if you want to attach your USB devices to the onboard USB controller.

If you disable this feature, the USB controller will be disabled and you won't be able to connect any USB devices to it. But **if you don't use any USB devices, this frees up an IRQ** for other devices to use. This is particularly useful when you have many devices that can't share IRQs. Disabling this feature may not be necessary with APIC-capable motherboards because they come with more IRQs.

USB keyboard support
This feature determines whether support for the USB keyboard is provided by the operating system or the BIOS. Therefore, it will only affect those who are using USB keyboards. If your operating system offers native support for USB keyboards, you **should select the OS option as it will provide much greater functionality**. However, if you are using DOS or other operating systems that do not offer support for USB keyboards, then using the OS option will essentially disable the keyboard as such operating systems cannot 'detect' or work with USB keyboards.

This is where the BIOS option comes in. When enabled, the BIOS will provide support for the USB keyboard. So, you will be able to use the keyboard with both operating systems that don't support USB keyboards and those that do. However, the BIOS option only offers rudimentary support for the USB keyboard so using it will strip the keyboard of all except the most basic functions. As such, it is not recommended that you select this option if you are using an operating system that supports USB keyboards.

Don't forget to switch from the OS option to the BIOS option whenever you want to boot up using a DOS boot disk.
Even if the boot disk was created by a USB-aware operating system like Windows XP, it will not support the USB keyboard.

USB mouse support
This feature determines whether support for the USB mouse is provided by the operating system or the BIOS. Therefore, it will only affect those who are using USB mice. If your operating system offers native support for USB mice, you **should select the OS option as it will provide much greater functionality.** However, if you are using DOS or other operating systems that do not offer support for USB mice, then using the OS option will essentially disable the mouse as such operating systems cannot 'detect' or work with USB mice.

This is where the BIOS option comes in. When enabled, the BIOS will provide support for the USB mouse. So, you will be able to use the mouse with both operating systems that don't support USB miceand those that do. However, the BIOS option only offers rudimentary support for the USB mouse so using it will strip the mouse of all except the most basic functions. As such, it is not recommended that you select this option if you are using an operating system that supports USB mice.

Don't forget to switch from the OS option to the BIOS option whenever you want to boot up using a DOS boot disk.
Even if the boot disk was created by a USB-aware operating system like Windows XP, it will not support the USB mouse.

USWC write posting
The USWC or Uncacheable Speculative Write Combination feature is found in Intel P6 processors (i.e. Pentium Pro, Pentium II, Pentium III, etc...). When used with graphic cards that support linear framebuffers (which all current graphics cards support), it can improve performance by combining smaller data writes into 64-bit writes. This reduces the number of transactions required for a particular amount of data to be transferred into the linear framebuffer of the graphics card. This improves the efficiency of the bus to which the graphics card is attached. Therefore, it is recommended that you **enable** this feature for better performance.

However, **it may cause a host of problems like graphics corruption, system crashes and booting problems if your graphics card does not support such a feature. When that happens, disable** this feature.

Video memory cache mode
The USWC or Uncacheable Speculative Write Combination feature is found in Intel P6 processors (i.e. Pentium Pro, Pentium II, Pentium III, etc...). When used with graphic cards that support linear framebuffers (which all current graphics cards support), it can improve performance by combining smaller data writes into 64-bit writes.
This reduces the number of transactions required for a particular amount of data to be transferred into the linear framebuffer of the graphics card. This improves the efficiency of the bus to which the graphics card is attached. Therefore, it is **recommended** that you select the USWC option for better performance.

However, **it may cause a host of problems like graphics corruption, system crashes and booting problems if your graphics card does not support such a feature. When that happens, select the UC (Uncacheable)** option.

VLink 8X support

V-Link refers to VIA's proprietary interchip bus. Previously, VIA used the PCI bus for connecting the North Bridge and the South Bridge. However, with high-speed PCI devices already saturating the PCI bus, VIA had to turn to an alternative bus for chipset's interchip communication. So, they designed their own bus to link the North Bridge with the South Bridge of their chipsets. The initial version used a quad-pumped 8-bit bus running at 66MHz to provide 266MB/s of interchip bandwidth. This gave them a dedicated bus with twice the bandwidth of the PCI bus (which incidentally has to be shared with other PCI devices). The V-Link debuted in the VIA Apollo KT266 chipset.

VIA has recently enhanced their V-Link technology to provide even more bandwidth for interchip communication. Starting with the Apollo KT400 and P4X400 chipsets, the clock speed of the V-Link bus will be doubled to 133MHz. This doubles the bandwidth of the V-Link bus to 533MB/s. Although the new bus is only four times faster than the PCI bus, VIA chose to call the new bus 8X V-Link.

The VLink 8X Support BIOS feature is used to toggle the doubling of the V-Link bus' clock speed. When enabled, the quad-pumped 8-bit V-Link bus will run at 133MHz, thereby delivering a bandwidth of 533MB/s. When disabled, the V-Link bus will use a clock speed of 66MHz, essentially reverting to the original V-Link standard. This BIOS feature was most likely included for troubleshooting purposes. It is recommended that you **enable** it for better performance.

SYSTEM RESOURCE MANAGEMENT

AGP anti-aliasing

The origin of this feature can be traced back all the way to the original IBM PC. When the IBM PC was designed, it only used ten address lines (10-bits) for IO space allocation. Therefore, the IO space back in those days was only 1KB or 1024 bytes in size. It was also maintained that the first 256 addresses would be exclusively reserved for the motherboard's use, leaving the last 768 addresses for use by add-in devices. This would become a critical factor later on.

Later, motherboards began to utilize 16 available address lines for IO space allocation. This was supposed to create a contiguous IO space of 64KB in size. Unfortunately, many ISA devices by then would only do 10-bit decodes. As such, they fragmented the 64KB IO space into 1KB chunks. To make things worse, the rule that the first 256 addresses is exclusively reserved for the motherboard meant that the first (or lower) 256 bytes of each 1KB chunk would be decoded in full 16-bits. This automatically restricted the 10-bits-decoding ISA devices to the last (or top) 768 bytes of the 1KB chunk of IO space.

Therefore, those ISA devices only had 768 IO locations to use. Because there are so many ISA devices in those days, this limitation created a lot of compatibility problems because the chances of two ISA cards using the same IO space were high. When that happened, one or both of the cards would not work. Although standardizing the IO locations used by various classes of ISA devices ameliorated the situation, it was still not good enough.

A workaround was eventually designed in which the ISA device would first take up a smaller number of IO locations in the 10-bit range. It would then extend its IO space by using 16-bit aliases of the few 10-bit IO locations that it allocated to itself. Because each IO location in the 10-bit decode area have sixty-three16-bit aliases, the total number of IO locations expanded from just 768 locations to a maximum of 49,152 locations! More importantly, each ISA card will now require very few IO locations in the 10-bit range. This drastically reduced the chances of two ISA cards conflicting each other in the limited 10-bit IO space. This workaround became known as ISA Aliasing.

Now, that's all well and good for ISA devices. Unfortunately, the 10-bit limitation of ISA devices is a liability when there are devices that require 16-bit addressing. AGP and PCI devices come to mind. As noted earlier, only the first 256 addresses of the 1KB chunks support 16-bit addressing. As such, all 16-bit addressing devices are limited to only 256 bytes of contiguous IO space! When a16-bit addressing device requires a larger contiguous IO space, it will be have to encroach on ISA IO space. If, for example, an AGP card r equires 8KB of contiguous IO space, it will cover eight of the 1KB IO chunks. Because ISA devices are using ISA Aliasing to extend their IO space, this brings about a high chance of IO space conflicts between ISA devices and the AGP card. Again, when that happens, the affected cards may fail to work.

There are two ways out of this mess. First method would be to limit the AGP card to a maximum of 256 bytes of contiguous IO space. The second, and naturally the preferred method, would be to throw away the restriction and provide the AGP card with all the contiguous IO space it wants. Here's where the AGP ISA Aliasing BIOS feature comes in. The default setting of Enabled forces the system controller to alias ISA addresses using address bits [15:10]. Only the first 10-bits (address bits 0 to 9) are used for decoding. As mentioned above, this restricts all 16-bit addressing devices to a maximum contiguous IO space of 256 bytes.

When disabled, the system controller will not perform any ISA aliasing and all 16 address lines can be used for IO address space decoding. This gives 16-bit addressing devices access to the full 64KB IO space.

It is recommended that you **disable** AGP ISA Aliasing for optimal AGP (and PCI) performance. Enable it only if you have ISA devices that are conflicting with your AGP or PCI cards.

APIC function

The APIC Function BIOS feature is used to enable or disable the motherboard's APIC (Advanced Programmable Interrupt Controller). The APIC is a new distributed set of devices that make up an interrupt controller. In current implementations, it consists of three parts - a local APIC, an I/O APIC and an APIC bus. The local APIC delivers interrupts to a specific processor so each processor in a system has to have its own local APIC. Therefore, a dual processor system must have two local APICs. Because a local APIC has been integrated into every processor since the debut of the original Intel Pentium P54C processor, there's no need to worry about the number of local APICs.

The I/O APIC is the replacement for the old chained 8259 PIC (Programmable Interrupt Controller) still in use in many motherboards. It collects interrupt signals from I/O devices and send messages to the local APICs via the APIC bus which connects it to the local APICs. There can be up to eight I/O APICs in a system, each supporting anywhere from 24 (usually) to 64 interrupt lines. As you can see, this allows a lot more IRQs than is currently possible with the 8259 PIC. Note that without at least one I/O APIC, the local APIC is useless and the system functions as if it's based on the 8259 PIC.

To sum it all up, APIC provides multiprocessor support, more IRQs and faster interrupt handling which are not possible with the old 8259 PIC. Although they can be used in single-processor boards, you are more likely to find them in multi-processor motherboards. This is because APIC is only supported in Windows NT, 2000 and XP. It is not supported in operating systems that are required to support MS-DOS device drivers, i.e. Windows 95/98. But as users transition to Windows XP, you can expect more manufacturers to ship single-processor boards with I/O APICs.

If your single-processor motherboard supports APIC and you are using a Win32 operating system **(Windows NT, 2000 and XP), it's recommended that you enable** this feature to allow faster and better IRQ handling. If you are using a multiprocessor motherboard, you must enable this feature because it's required for IRQ handling in multiprocessor systems.

However, **if you are running Windows 95/98 or a DOS-based operating system on a single-processor motherboard, you must disable** this feature. This is because MS-DOS drivers assume they can write directly to the 8259 PIC (APIC did not exist yet in those days!) and its associated IDT entries. Disabling this feature forces the APIC to revert to the legacy 8259 PIC mode.

Assign IRQ for USB

This BIOS feature is somewhat similar to Onboard USB Controller. It enables or disables the motherboard's onboard USB controller by determining whether it should be assigned an IRQ. **Enable** this feature if you want to attach your USB devices to the onboard USB controller.

If you disable this feature, the USB controller will not be assigned an IRQ. This disables the controller and therefore you won't be able to connect any USB devices to it. But if you don't use any USB devices, this frees up an IRQ for other devices to use. This is particularly useful when you have many devices that can't share IRQs. Disabling this feature may not be necessary with APIC-capable motherboards because they come with more IRQs.

Assign IRQ for VGA

Many graphic cards require an IRQ to function properly. Disabling IRQ assignment for such cards will cause improper operation and/or poor performance. Therefore, it is recommended that you **enable** this feature. Doing so allows the BIOS to assign an IRQ to the graphics card. Some graphics cards may not need an IRQ to work. These cards are usually the low-end cards that provide basic video functions. Check your graphics card's documentation to confirm if it requires an IRQ to work.

If your graphics card doesn't require an IRQ, then you can disable this feature to release an IRQ for other devices to use. This is particularly useful when you have many devices that can't share IRQs. Disabling this feature may not be necessary with APIC-capable motherboards because they come with more IRQs. When in doubt, it's often best to leave it enabled as graphics cards generally function better with an IRQ. This is true even for cards that don't require IRQs.

Force update ESCD

The ESCD (Extended System Configuration Data) is a feature of the Plug and Play BIOS that stores the IRQ, DMA, I/O and memory configurations of all ISA, PCI and AGP cards in the system (Plug and Play-capable or otherwise). The data is stored in a special area of the BIOS ROM so that the BIOS can reuse the configuration data when it boots up the system. As long as there are no hardware changes, the BIOS does not need to reconfigure the ESCD.

If you install a new piece of hardware or modify your computer's hardware configuration, the BIOS will automatically detect the changes and reconfigure the ESCD. Therefore, there's no need to manually force the BIOS to reconfigure the ESCD. However, sometimes, the BIOS may not be able to detect the hardware changes and the a serious conflict of resources may occur. The operating system may not even boot as a result. This is where the Force Update ESCD BIOS feature comes in.

This feature allows you to manually force the BIOS to clear the previously saved ESCD data and reconfigure the settings. Just enable the feature and reboot your computer. The new ESCD should resolve the conflicts and allow the operating system to load normally. There's no need for you to manually disable this feature yourself as the BIOS will automatically reset it to the default setting of Disabled after reconfiguring the ESCD.

PIRQ x Use IRQ No.

This feature allows you to manually set the IRQ for a particular device installed on the AGP and PCI buses. This is especially useful when you are transferring a hard disk from one computer to another; and you don't want to reinstall your operating system to redetect the IRQ settings. By specifying the IRQ for the devices to fit the original settings, you can circumvent a lot of configuration problems after installing the hard disk in a new system. However, this is only required for non-ACPI systems.

Notes (these may differ from motherboard to motherboard) :-

- If you specify a particular IRQ here, you can't specify the same IRQ for the ISA bus.
  If you do, you will cause a hardware conflict.
- Each PCI slot is capable of activating up to 4 interrupts - INT A, INT B, INT C and INT D.
- The AGP slot is capable of activating up to 2 interrupts - INT A and INT B.
- Normally, each slot is allocated INT A. The other interrupts are there as reserves in case the PCI/AGP device requires more than one IRQ or if the IRQ requested has been used up.
- The AGP slot and PCI slot #1 share the same IRQ.
- PCI slot #4 and #5 share the same IRQs.
- USB uses PIRQ_4.

Below is a table showing the relations between PIRQ and INT in the reference motherboard :-

Signals	AGP Slot PCI Slot 1	PCI Slot 2	PCI Slot 3	PCI Slot 4 PCI Slot 5
PIRQ_0	INT A	INT D	INT C	INT B
PIRQ_1	INT B	INT A	INT D	INT C
PIRQ_2	INT C	INT B	INT A	INT D
PIRQ_3	INT D	INT C	INT B	INT A

You will notice that the interrupts are staggered so that conflicts do not happen easily. Still, because the AGP slot and PCI slot 1 share the same set of IRQs, it's best to only use either one of those two slots unless you don't have any other slots to use. The same goes for PCI slots 4 and 5.

Normally, you should just leave it as **Auto.** But if you need to assign a particular IRQ to a device on the AGP or PCI bus, here's how you can make use of this BIOS feature. First of all, determine the slot that the device is located in. Then, check your motherboard's PIRQ table (in the manual) to determine the slot's primary PIRQ. For example, if you have a PCI network card in PCI slot 3, the table above shows that the slot's primary PIRQ is PIRQ_2. Remember, all slots are first allocated INT A if possible.

After that, select the IRQ you want to use for that slot by assigning it to the appropriate PIRQ. If the network card (in the example above) requires IRQ 7, set PIRQ_2 to use IRQ 7. The BIOS will then allocate IRQ 7 to PCI slot 3. It's that easy! :)

Just remember that the BIOS will try to allocate the PIRQ linked to INT A for each slot. So, the primary PIRQ for the AGP slot and PCI slot 1 is PIRQ_0 while the primary PIRQ for PCI slot 2 is PIRQ_1 and so on. It's just a matter of linking the IRQ you want to the correct PIRQ for that slot. Note that Intel i8xx chipsets have 8 interrupt lines (INT A to INT H). So, the AGP slot will always have its own IRQ in motherboards using those chipsets. Thanks to alex-the-cat for that info!

PNP OS installed

This BIOS feature is quite misleading because it alludes that you should set it to Yes if you have an operating system that supports plug and play (PNP) functionality. It isn't quite so simple, unfortunately. What it actually does is determine what devices are configured by the BIOS when the computer boots up and what are left to the operating system. This is rather different from what the name hints, right?

Before you can determine the appropriate setting for this feature, you should determine what kind of BIOS you have. For the purpose of this BIOS feature, the BIOS can be divided into two types - ACPI BIOS and Non-ACPI BIOS. You should also find out if your operating system supports and is currently running in ACPI mode. Please note that while an operating system may tout ACPI support, it's possible to force the operating system to use the older PNP mode. So, find out if your operating system is actually running in ACPI mode. Of course, this is only possible if you have a motherboard with an ACPI BIOS. With a Non-ACPI BIOS, all ACPI-compliant operating systems automatically revert to PNP mode.

Non-ACPI BIOSes are found in older motherboards that do not support the new ACPI (Advanced Configuration and Power Interface) initiative. This can be either the ancient non-PNP BIOS (or Legacy BIOS) or the newer PNP BIOS. With such BIOSes, setting the PNP OS Installed feature to No allows the BIOS to configure all devices under the assumption that the operating system cannot do so. Therefore, all hardware settings are fixed by the BIOS at boot up and will not be changed by the operating system.

On the other hand, if you set the feature to Yes, the BIOS will only configure critical devices like the graphics card and hard disk. The other motherboard devices are then configured by the operating system. This allows the operating system some flexibility in shuffling system resources like IRQs and IO ports to avoid conflicts. It also gives you some degree of freedom in manually shuffling system resources. While all this flexibility in hardware configuration sounds like a good idea, shuffling resources can sometimes cause problems, especially with a buggy BIOS. Therefore, it is recommended that you set this feature to No, to allow the BIOS to configure all devices. You should only set this feature to Yes if the BIOS cannot configure the devices properly or if you need to manually reallocate hardware resources in the operating system.

Now, all current motherboards ship with the new ACPI BIOS. If you are using an ACPI-compliant operating system (i.e. Windows 98 and above) with an ACPI BIOS, then this PNP OS Installed feature is irrelevant. It doesn't matter what setting you use. This is because the operating system will use the ACPI BIOS interface to configure all devices as well as retrieve system information. There's no longer a need to specifically split the job up between the BIOS and the operating system. But if you are using an operating system that does not support ACPI, then the BIOS will fall back to PNP mode. In this situation, consider the BIOS as you would a Non-ACPI BIOS. If there's no need to configure any hardware manually, it's recommended that you set this feature to No.

Please note that bugs in some ACPI BIOS can cause even an ACPI-compliant operating system to disable ACPI. This reverts the BIOS to PNP mode. However, there's an additional catch to it. Certain operating systems (i.e. Windows 98 and above) will only access the buggy BIOS in read-only mode. This means the operating system will rely entirely on the BIOS to configure all devices and provide it with all the hardware configuration. As such, you must set the feature to No if you have a buggy ACPI BIOS.

For Linux users, Jonathan has the following advice -

Although Linux is not really PnP-compatible, most distributions use a piece of software called ISAPNPTOOLS to setup ISA cards. If you have PnP OS set to No, the BIOS will attempt to configure ISA cards itself. This does not make them work with Linux, though, you still need to use something like ISAPNPTOOLS. However, having both the BIOS and ISAPNPTOOLS attempting to configure ISA cards can lead to problems where the two don't agree.

The solution? Set PnP OS to Yes, and let ISAPNPTOOLS take care of ISA cards in Linux, as BIOS configuration of ISA cards doesn't work for Linux anyway (with the current stable and development kernels). Most times, it probably won't make a difference, but someone somewhere will have problems, and Linux will always work with PnP OS set to Yes.

Britt Turnbull recommends disabling this feature if you are running the OS/2 operating system, especially in a multi-boot system. This is because booting another OS can update the BIOS which may later cause problems when you boot up OS/2. In addition, if you add or change hardware, you should enable full hardware detection during the initial boot sequence of OS/2 (ALT-F1 at boot screen -> F5, etc...) so that the new hardware can be registered correctly.

Thomas McGuire of 3D Spotlight sent me this e-mail from Robert Kirk at IBM :-

"Actually, the setting "PnP OS" is really misnamed. A better thing would be to say "do you want the system to attempt to resolve resource conflicts, or do you want the OS to resolve system conflict?". Setting the system to PnP OS says that even if the machine determines some kind of resource problem, it should not attempt to handle it... Rather, it should pass it on to the OS to resolve the issue. Unfortunately, the OS can't resolve some issues.... which sometimes results in a lock or other problems.

For stability reasons, it is better to set EVERY motherboard's PnP OS option to No, regardless of manufacturer but still allow the BIOS to auto configure PnP devices. Just leave the PnP OS to No. It won't hurt a thing, you lose nothing, your machine will still autoconfigure PnP devices and it will make your system more stable."

To sum it all up, except for certain cases, it is highly recommended that you to set this BIOS feature to **No**, irrespective of whatever operating system you actually use. Exceptions to this would be the inability of the BIOS to configure the devices properly in PNP mode and a specific need to manually configure one or more of the devices.

Resources controlled by
The BIOS has the capability to automatically configure all of the boot and Plug & Play compatible devices. Normally, you should set it as **Auto**, so that the BIOS can automatically assign the IRQs and DMA channels. All the IRQ and DMA assignment fields should disappear as a result. But if you are facing problems assigning the resources automatically via the BIOS, you can select Manual to reveal the IRQ and DMA assignment fields. Then you can assign each IRQ or DMA channel to either Legacy ISA or PCI/ISA PnP devices.

Legacy ISA devices are compliant with the original PC AT bus specification and require a specific interrupt / DMA channel to function properly. PCI/ISA PnP devices, on the other hand, adhere to the Plug & Play standard and can use any interrupt / DMA channel.

CONCLUSION
Hopefully your PC will now be performing better &/or more stabily by modifying BIOS settings.
With a bit of luck you may even have managed to overclock your system as well, which would give even greater performance gains.

CHAPTER [10]

OVERCLOCKING TIPS

INDEX

AMD OVERCLOCKING
- changing the multiplier on amd chips
- fsb and multiplier combinations

GFX CARD OVERCLOCKING
- general
- why should I overclock my gforce?
- cooling
- tools you need
- lets start
- add coolbits entry to your registry and overclock
- other programs for gfx card overclocking
- benchmarking for gfx cards etc

SYSTEM STABILITY TESTING

RELATED SOFTWARE

TROUBLESHOOTING
- operating system crashes immediately after a certain intensive program is run:
- your pc doesn't even turn on

INTRODUCTION

Want the power of a new processor--for free? Would you care for a more muscular graphics card--without upgrading? You just might have them: all you have to do is learn how to overclock. Overclocking generally refers to forcing a CPU, front-side bus, graphics chip, or graphics card memory to perform faster than it's supposed to perform. Done successfully, it can increase the performance of your system without new components. There's risk, of course--for instance, you can age your PC's components prematurely and void their warranties--but as with any worthwhile risk, there's plenty of reward. Overclocking can damage your components if done incorrectly. It will void virtually all warranties and it WILL reduce the life of your components.

It's wise to avoid overclocking or otherwise experimenting with a system that you use for mission-critical tasks and data. Don't overclock your main workstation. Do your experimenting on a system that, should something go awry, you can live without for a few days. And if there's anything on the hard drive that you care about, back it up on removable media before you tweak the system.

No matter what component you're planning on pushing to lofty new frequency heights, the preferred methodology, especially for novice overclockers, is the same. Sometimes called progressive overclocking, the basic philosophy is to take speed increases in small doses. Knowing the default clock speed of the component, you should attempt to overclock it in very small increments--perhaps one to two percent at a time.

There are people who spend hundreds, sometimes thousands of dollards for an extra handful of clock-speed. In the past, overclocking was simply changing your motherboard's settings for the next higher CPU Multiplier. It's not as simple anymore, since both Intel and AMD have locked the multipliers in their CPU's. As a result, in today's world the bus speed is usually the only easy way to overclock and achieve CPU speeds that don't officially exist. Bus speed, as opposed to CPU overclocking changes your whole motherboard's BUS, affecting PCI, AGP (with all the components attached to them) as well as Memory speed, so in effect you are overclocking everything! Because of the fact you are overclocking your whole system and every component connected to it, one of the necessary requirements is to have good quality components. You have a better chance of reaching higher speeds and still running a stable system with good quality brand name components instead of cheap off the wall hardware. Some brands/models of hardware overclock better then others, some don't overclock very well at all, so it's a good idea to already have a rock stable system with good quality hardware before you attempt overclocking, since overclocking essentially pushes your system beyond the manufacturer's specs, adding heat to the equation.

The thing to remember is that ALL processors are the same and are merely "rated" to run at a specified speed. A single wafer (a wafer contains about 35 chips) will yield many different speeds. The Mhz rating of the chip is not known until it has been assembled and tested in one of Intel's many assembly plants. A single wafer could have Pentium III processors ranging from the 500e all the way to the 1Ghz Coppermine, as well as some chips that don't work at all and are thrown out. It is during this 'validation' process that overclocking becomes a reality. A small wafer comprised of many individual ICs.

The speed at which a CPU operates has less to do with the internal workings of the CPU itself than the settings of the computer's motherboard. Often, the only factor separating one CPU from another is how they are marketed. For instance, an AMD Duron 700 and an AMD Duron 800 are, for all practical purposes, likely identical parts generated in the fabrication process; except that AMD has decreed that one's clock should run faster than the other's. We know that a process called "binning" often occurs in CPU manufacturing, where the CPUs are tested for the highest possible safe frequency, and placed in a particular "speed-bin", but again it's very likely a processor ranked for 700 MHz came off the same fabrication line as one ranked at 800MHz, and can very likely run very safely at 800MHz.

Manufacturers like AMD Inc. and Intel Corp. want their components to be stable. If a user's system crashes or hangs, they want the user to be confident it was, say, a Windows error. Processors and other components, therefore, are often marketed below their fastest possible operating frequencies: if the Duron from the above example tests stable to 700MHz but fails at a faster speed, selling it as a 600MHz processor all but guarantees that it won't fail under normal use. This is often referred to as manufacturer overspec. In addition, the 'rated' speed is guaranteed to work even under extreme environmental conditions such as poorly cooled cases and poorly regulated voltages for at least 10 years. The goal of the overclocker is to maximize this headroom by keeping the chip as cool as possible, giving it sufficient voltage and maximizing the available "headroom" that Intel and AMD have so generously left in their chips. Overclockers also are willing to accept the fact that their chips will probably not last 10 years. In some cases, chipmakers also sell a faster chip which has been re-labeled as a slower chip, simply due to economic reasons. In the past, both AMD and Intel have done this and these chips are highly sought after. The Duron 800 is a great example of this right now. Both

AMD's and Intel's chips generally run much faster than this speed but they are in such a heated price war that it serves them economically to sell some chips at these slower speeds. If you can find one for yourself, you could run it at a faster speed and save yourself the expense of buying the faster chip.

Why would you do it ?

As a PC owner, you've probably lamented over the fact that the second you bought your shiny new system with all its state of the art components, even faster ones became available as if the guys at the store had them hidden in back and were just waiting for you to leave. If you've owned your system for a few years, you've also most likely been irritated that some of the newest games, apps and other software goodies have minimum system requirements that prevent them from running on your machine properly--if at all. Sometimes, even the applications that your system should handle won't run quite as well as the glowing reviews lead you to believe.

The most obvious benefit of successfully overclocking a CPU is simple: it runs faster. By running faster, the processor is able to perform its tasks more quickly, resulting in faster application execution. That's not the only reason why overclockers do their thing. The very act of overclocking is embraced by the most passionate PC gearheads--the computer society equivalent of auto enthusiasts who craft holes in their hoods for modified engine blocks. As such, successfully overclocking a processor is sort of a cottage industry hobby to the world of PC power users. The rush and satisfaction that results from successfully pushing a processor beyond what should have been its very limits is often more rewarding than any performance gain. Overclocking may appeal even to those who aren't well versed in the intricacies of their PCs, but who are interested in hands-on learning. In fact, there are few performance tweaks that will cause users to learn more about their equipment and its limits than overclocking.

Basics of overclocking

There are several ways of going about increasing the core speed of your processor. First you must understand how the speed of the CPU is determined. Many years ago, processors such as the 486 ran the same speed as the majority of the components in the system. When you increased the bus speed of the motherboard, the memory, PCI slots and processor were all scaled by the exact same amount. Since the 486 DX2, however, the CPU speed has been set as a multiple of the front side bus speed (FSB) which is the speed the motherboard is running. The DX2 ran at twice the speed of the motherboard (2x) and thus, a 486 DX2 66MHz has a motherboard that runs only 33MHz..

Starting with the 486 DX2 and continuing onto the original Pentium and early Pentium II chips, it was much easier to overclock your processor. You could change both the FSB and the bus multiplier. The Pentium 75 was a great example of this. It ran with a 50MHz FSB and a 1.5x multiplier. Many people had success changing the multiplier to 2x, resulting in a 25MHz overclock to 100MHz. Those more sure of their system components might change their system to a 66MHz FSB with a 1.5x multiplier (also 200MHz). Keep in mind that running a faster FSB (and thus faster memory and other components) results in higher performance. Some of the better chips were able to run 120MHz with a 60MHz FSB and a 2x multiplier. You can see the flexibility offered by being able to change the multiplier and the FSB speeds.

Chip examples

Since late 1998, starting with the PII-333 and 350, all Intel processors (except engineering samples) have their multiplier internally locked. AMD used to preach strongly against multiplier locking back in the days of the K6-2 (which is unlocked), however upon releasing their hugely successful Athlon, AMD decided the problems they were having with Re-markers warranted instituting a multiplier lock. (Re-markers are people who sell overclocked CPUs that are actually "re-marked" at the higher speed for a profit). While there is nothing illegal about overclocking, nor is there anything illegal about selling overclocked chips, you must mention that they are overclocked.

With these "locked" chips, there are two ways to overclock. The first is to "unlock" them. This can be tricky and may require some experience but is generally the method of choice for AMD chips. We will cover this in the 'advanced overclocking' section. The easiest way to overclock a processor is simply to increase the FSB speed and as such, this is generally the method of choice for Intel CPUs. This is controlled by the motherboard. You will have to check your motherboard documentation to see exactly how to change this speed, however I will go over several common methods.

Historically, CPU's such as the P2-350 and P2-400 came multiplier locked at 3.5x and 4x limiting our overclocking potential somewhat. This is why the old P2-333 was so popular - it used the same core (more or less) than its faster brothers, but had a multiplier (which could be changed by the user) of up to 5.5x, offering us lots of potential for MHz. for free :) Like I said, since around 19th August 1998, all new Intel CPU's were supplied locked with ONE multiplier only. ANY new Intel etc. made after that date, will not step down a multiplier. That means the old trick of reducing the multiplier and increasing the bus speed no longer works!!

The Celeron 266, was also extremely popular because its multiplier was a low multiplier; 4 x 100 seemed almost guaranteed, with many running successfully at 4 x 112! However, this CPU was plagued by its lack of L2 cache. Its successor, the Celeron 300a included 128KB of on-die L2 cache, improving performance while maintaining the overclockability of its predecessor. The Celeron 300a is generally considered the most 'famous' overclocking chip ever and is still found in a great number of systems. Virtually every 300a chip made was capable of running 4.5x100MHz and some even ran 4.5x112=504MHz. At the time, this $100 CPU was beating Intel's flagship, the PII-450, which cost a hefty £450. The P2-300 SL2W8 was another CPU's of choice for those seeking to simply increase their 66MHz FSB to 100MHz and leave it at that. The P2-333 SL2TV also produced good results at 5 x 100 or beyond!

Shortly later, the Celeron 366 found its way into the limelight. A new stepping on the Celeron core allowed greater clock speeds and the majority of Celeron 366 CPUs manufactured during 1999 could run 5x5x100=550MHz. Nowadays, the world has moved on, and the battleground has been drawn between Intel and AMD. In one corner sits the AMD Duron and Thunderbird chips, which are currently doing battle with Intel's flagship "Coppermine" line. Right now unlocked Duron 600 CPUs are doing 900MHz-1.1Ghz very nicely, with the Intel P3-750e sometimes running quite happily at 1Ghz also.

As it stands now (Dec 2000) in the ThunderBird vs Coppermine battle, Intel is taking a beating. The Coppermine can almost never run faster than 1.1GHz without extreme measures whereas the ThunderBird Athlon is shipping with factory marked 1.2GHz units, often able to run near 1.3GHz. Athlon 1Ghz parts often run 1.1Ghz or 1.2Ghz and even lower clocked Athlons can sometimes cross the 1GHz threshold. Intel's Celeron can often run above 900MHz, however it is plagued by poor performance. Current consensus is that a Duron 1Ghz can equal or match a Pentium III running at 1Ghz.

Examples of terminology used

You will encounter terms like "multiplier" and "bus-speed". If you have an Intel CPU, you do not need to worry too much about "multiplier" as you cannot alter this on any CPU manufactured after August 1998. Chances are your Intel CPU was made after that date. You are more interested in "bus-speed". A Celeron 400 runs at a multiplier of 6x, and a bus speed of 66Mhz. So multiply 6 by 66 and you have 400Mhz. The "multiplier" in this case is 6x and the "bus speed" in this case is 66Mhz. Easy!

Ok, lets try another - a Pentium III 700e runs at 7x multiplier and 100Mhz bus speed. Yep - that rights - times 7 x 100 = 700Mhz. In this case you have a "multiplier" of 7 and a "bus speed" of 100Mhz. OK try one yourself - a Celeron 300 runs with a multiplier of 4.5. What is the "bus speed" of that CPU?. If you did the math and divided 300 by 4.5 (300 / 4.5) and got 66Mhz then award yourself a gold star!

Here's one for you AMD fanatics - the water is slightly muddied here as internally AMD chipsets run at 200Mhz. However you don't really need to worry about that since the clock itself is running at 100MHz. What you see as the end user is the 100Mhz. So a Duron 650 runs at 6.5 x 100 as far as you - the overclocker - is concerned. So to get 715Mhz out of a Duron 650, you'd set the bus speed to 110Mhz and Presto! Your Duron 650 is now running at 715Mhz or 6.5 x 110.

From initial reports, it appears that the Pentium 4 uses a similar method to the Athlon, running its Front Side Bus clock at 100MHz while actually transferring data at 400MHz. For our purposes, you can assume that the clock is actually 100MHz. So the 1.5Ghz unit will be running 15x100=1500MHz. Initial reports indicate that the FSB can be pushed to about 125MHz without too much difficulty, yeilding a 500MHz effective FSB speed and reasonable overclocking potential. Note that the DRDRAM speed is derived from the FSB speed using a 4x Multipler. PC800 DRDRAM runs at 400MHz so this is perfect for it. 500MHz may be beyond the capabilities of some DRDRAM so we might begin to see motherboards that allow adjustment of this DRDRAM multiplier. Armed with this knowledge you will attempt to increase the bus speed on your motherboard to increase the speed of your CPU! For instance, if you can increase the bus speed of your Celeron 566 up to 75 Mhz, your new speed will be 8.5 x 75 = 638MHz!

Is overclocking dangerous?

Several times you've probably heard people say that CPU overclocking is dangerous. Usually it seems like newbies, PC retailers, and CPU manufacturers say these things. Is overclocking really dangerous? Well, yes and no. And keep in mind, it's "dangerous" for your CPU; not for you, personally. If you truly know what you're doing, it really isn't that dangerous. But even an experienced overclocker can kill a CPU if they aren't careful or overlook certain things like voltage. For the average PC user, overclocking is more dangerous. The safety precautions that an overclocking veteran would take may be overlooked by a newbie. So, when Intel (for example) declares that overclocking is risky and can be dangerous, they are usually saying so for all the newbies out there that are new or unfamiliar to overclocking. It's simply for liability.

Overclocked processor lifetime

Worst case scenario for the lifetime of a non-burned out overclocked processor is over two years, while most processors will continue to function after five or six years. Unless you don't upgrade your system except when it breaks (this is very uncommon among overclockers and tweakers alike), you should never run into a problem with your processor's lifetime.

Electromigration

If you strip everything down to its most basic function, a processor conducts electricity through a series of transistors to perform its various functions. Electrical currents generate heat. Heat assists in the breakdown of metal. Since transistors are made of conductive metals, heat is a danger to them. When you force them to work faster, they consume more power per unit time, and generate even more heat. Each transistor within the chip's core develops an electrostatic charge over time, much like the way iron can develop a magnetic charge that will linger after any electric current has subsided.

CPUs and other processors are subject to electromigration, which is the gradual breakdown of the very components that carry the circuit's electricity. The actual circuit paths may form shorts or create open circuits through electromigration. Due mainly to this phenomenon, every component in a PC has a one hundred percent failure rate--provided it's operated long enough, any computer processor will eventually fail. Heat accelerates electromigration. Keeping a processor in an overclocked state for a long time will hasten its demise. Overclocking has the equivalent effect on a component as running a car engine over the redline for extended periods: it shortens their life expectancy. Considering that modern processors are designed to have a life of at least 10 years, even if you shorten your CPU's life by half, it would still be obsolete much faster than it will fail.

Even if a system keeps its processor at a relatively cool temperature, pushing it beyond its limits can still result in unpredictable--and risky--behavior. Simply cooling at the surface of the chip doesn't necessarily dissipate all the heat generated inside the CPU itself. Overclocked systems can exhibit symptoms ranging from graphical glitches to data loss. Electrostatic migration shouldn't be a problem for most overclocked processors unless you exceed the company's maximum core frequency for that particular model of core.

If you are exceeding the maximum frequency for a particular model of core, you need to be careful as to how long you have your computer running and how many consecutive hours a day you have it turned off. The longer you have your computer turned off at one time, the longer it will take for electrostatic migration to affect your system. You can't stop electrostatic migration from occurring, but depending on how you use your computer will determine how fast it will begin to take hold. Don't worry about it too much though, because even in the worst cases, it still takes a few years before it starts causing problems.

Safety precautions

There are a couple of very important things to keep in mind when you are attempting to overclock a computer, so that you don't damage your equipment. The first of these things is to make sure you have adequate cooling to take on the project you are planning. As will be discussed later, cooling can make or break an overclock - but that isn't its only benefit. It also helps prevent damage being done to the chips due to excessive heat.

Ok, now that I have taken care of explaining the importance of cooling to you, on to the (second) most important safety precaution - which has to do with progressive overclocking. I know, I know, that isn't a term most people have ever heard of - and that's because I just coined the term. Progressive overclocking has to do with the process of slowly clocking your system faster and faster until it reaches its peak stable speed. The process with a CPU is more difficult - mainly because it is hastlesome to go back into the BIOS for every clock change. With bus clocks, bus multipliers, and chip voltages to contend with, things aren't always hunky-dory.

IMPORTANT FACTORS FOR SUCCESSFUL OVERCLOCKING

Cpu cooling
(discussed in detail further down)
Your CPU Heatsink/Fan might do the trick, but it's very likely you'll need a top quality combo. Another, often overlooked fact is that a simple Thermal Compound (from www.overclockers.co.uk) applied between the heatsink and the CPU can provide for much better heat transfer and cooler Processor.
Tip: A thermal compound called "Arctic Grease", although somewhat pricey seems to be very popular among overclockers these days.

Case cooling
The temperature inside the case will also increase, as a result of overclocking, heating all of the devices and possibly increasing the chance of a crash. For ATX cases, I'd recommend an additional intake fan and exhaust fan. The size of the case as well as the placement of the cables inside will also affect its cooling, get rounded cables if you can for best air flow in the case and use air filters in front of the intake fans and vents, keep your case cover on for correct airflow and to reduce dust buildup (dust is an important enemy, it acts as an insulator keeping your hardware even warmer). For proper airflow, a simple rule might help reduce heat in your case even further, just install one more exhaust fan than your intake fans - it's more important to remove warm air from the case, than to blow cold air in... Something learned from experience.

Quality components
RAM, Hard Disks, Video Cards all can stop functioning at higher bus speeds, quality components are of course less susceptible to failure under stress. Also, well built, brand name motherboards can definitely make the difference between success and failure. Abit and Asus are two well known very overclockable, easy and friendly motherboards.

Monitoring software
There are certain software packages out there that help you monitor CPU & motherboard temperature, as well as fan speed. These software utilities can either show readings on demand, or they can be left running in your system tray, displaying temperatures and warnings... These utilities rely on new motherboards with Temperature sensors built into the motherboard. Most high-end motherboards manufactured in the last few years have this capability, some even have the temperature and fan speed readings in the BIOS as well.

Motherboard Monitor - is a tool that will display information from the sensor chip on your motherboard in your Windows system tray. MBM supports a wide range of Chipsets & Sensor Chip combinations.

WCPUID - is a program that displays detailed information about the CPU in your system. Shows Internal / External Clock, Multiplier, Cache info., AGP Info. etc ... It's very detailed and can help you see and confirm what your computer's current settings are. It's a good overclocking tool in the sense that you can confirm what you are actually doing.

THE OVERCLOCKING PROCESS
For an Intel based system, the first thing to check is whether or not you can configure the processor speed and internal voltage within the BIOS. Most newer motherboards, as well as most older ABIT boards, support "jumperless" configuring. If you are lucky enough to have such a system, your job is simple. All you need to do is raise the processor speed to what you want, change the voltage if necessary, and you're gold. If you have to deal with the jumpers, however, you've got a chore for yourself.

To change the computer's settings using jumpers, you are going to need your motherboard manual, or a copy of a jumper map for the particular model of motherboard. Using the jumper maps, determine the proper settings for the wanted processor speed and core voltage. Then move the jumpers on the motherboard so that they match the jumper map. To do this, you may need a pair of tweezers and a pen light. Woo-hoo, congratulations, now your system is overclocked. But wait, that was too simple - what gives? Why did I write this huge guide about overclocking if the steps were easy as 1-2-3? Well, we aren't quite done yet.

The next step in this process is to attempt to start up your computer. The first test is seeing whether or not the computer will post. Posting is the process of the computer initializing the BIOS and loading up the system settings. If your computer won't even do this, there is almost no chance you will ever get it to run at the configured speed. Go back and lower the processor speed and try again. If the computer did post, however, but it won't boot up Windows, you may want to try going back and upping the chip's core voltage. Take this as a word of advice though, make sure that you don't raise the core voltage too much - generally no higher than 0.3 V above default. If you go much higher than this, you run a serious chance of permanently damaging your computer.

Assuming your computer starts to boot Windows, but crashes before the system begins to settle down, you have two options as to how to deal with the crash. You can either go back and change the system's core voltage or you can add more cooling. That may include adding more case fans, installing a larger and more powerful fan/heatsink combo, or both. At this point, if you are able to do both, you may even be able to reach a higher speed. Ok, your computer boots. Great! But you aren't out of the dark yet, because you still have to check and see if the system is completely stable.

BUS, CPU, MEMORY & AGP SPEEDS
First, in order to figure out what all this means lets define a few terms. The internal CPU speed refers to the actual speed that the CPU is operating at. When you go to the store or look up system specs you will see, for example, Pentium III 800Mhz. The 800Mhz part refers to the internal operating frequency of the CPU in question. To make this easy just know that is the speed of the processor, 800 Mega-Hertz in this case. The higher the speed (internal CPU clock) of the processor the faster it processes information and the more you can do with your computer in every CPU intensive task.

Most newer motherboards have a FSB (Front Side Bus, which will also be referred to as "bus speed") control setting in their BIOS. Abit was the first to popularize this feature with their "SoftMenu" BIOS (see below) that allows bus as well as voltage and other tweaking options to be changed without ever opening the computer's case. With systems like Abit's, there is generally a whole menu devoted to speed and tweaking options designed for overclocking. Menus such as these are increasing in popularity as they

are much easier to use. No matter who makes your mainboard, be it Abit, Asus, Soyo, MSI, most BIOS do offer overclocking features - look out for them :)

The bus speed refers to the actual motherboard and it's components. They also run in Mega-Hertz (Mhz) and they all run together at different dividers, or fractions of the CPU speed. Your motherboard has traces on it, if you look down at a motherboard and you see all those long lines running all through it to different components that is the bus of the motherboard, data paths to all the components. The Front Side Bus (FSB) by definition is the bus that connects the processor (CPU) and the main Memory (RAM). The PCI bus is the bus that connects all the PCI devices (connected to the PCI expansion slots), as well as the I/O Controller for your Hard Drive and CD-ROM. The AGP bus is the bus that your AGP video card runs on from the AGP slot. These are the main buses you have to worry about when overclocking. Other types of buses, such as SCSI are also affected by overclocking, but they're beyond the scope of this article, besides they are generally affected by the PCI/ISA bus.

How this all fits together: It takes the FSB speed (which is also the RAM speed don't forget) multiplied by the CPU Multiplier to create the CPU Internal Clock speed. For example a FSB speed of 100Mhz times a multiplier of 8 will equal 800Mhz, that is expressed like this: 100 x 8 = 800. Simple as that. The 3 Official FSB speeds currently are 66Mhz, 100Mhz, and 133Mhz. In order to get other bus speeds and try to get different Internal CPU speeds, your motherboard needs to have more FSB option settings, we will go into more detail a little later. Keep in mind when you do overclock the FSB you are overclocking your memory (RAM) so if you have some modules of some slow cheap pieces of memory they may not like to be overclocked at all. If you buy good brand name memory like Corsair, Mushkin, Micron, Infeneon or Samsung, you will have a much better chance at overclocking your FSB.

You also need to know the speed in Mhz of the other buses in your PC. This is because when you raise the Front Side Bus (FSB) you are also raising all the other bus speeds. The PCI bus officially runs at 33Mhz, you need to keep it as close to that spec as you can, because overclocking it to high might cause one of your PCI components not to operate correctly. It works like this, in order to get the PCI bus at 33Mhz at a 100Mhz FSB you would use a divider of 1/3 It's expressed like this 100 x 1/3 = 33.3 which is 33Mhz. These divider settings are set in your BIOS, or by jumpers on your motherboard, if at all possible (you might want to check your motherboard's manual for additional info). Now lets say we wanted to raise the FSB to 133Mhz if we kept a divider of 1/3 the PCI bus would be running at 133 x 1/3 = 44.3Mhz this is way too high and devices attached to your PCI bus may not work at this setting. So what do you do? Change the divider setting, most new motherboards that officially support the 133Mhz FSB have a divider setting of 1/4 you can use, 133 x 1/4 = 33.25 or rounded to 33Mhz which is back on spec.

The next bus you have to worry about is the AGP bus. The AGP bus, as you recall, is the bus that your AGP Video Card runs off of, so the only device you have to worry about overclocking is the bus that the video card is plugged into. The AGP bus runs at 66Mhz, so no matter what you do when you overclock try to keep it as close to 66Mhz as you can and you won't have any problems with your video card. Now most newer video cards can take a high AGP bus setting, I've seen some go as high as 100Mhz and most make it to 88Mhz but for first time overclockers I recommend that you try to keep it as close to 66Mhz as you can. The AGP bus uses dividers just like the PCI bus.
At a 100FSB you have to use a divider of 2/3 it's expressed like this 100 x 2/3 = 66.6 or 66Mhz. If you were to raise the FSB to 133 and keep the 2/3 divider you would have an AGP bus of 133 x 2/3 = 88Mhz. In order for it to get back to normal you would have to use a divider of 1/2 now this is a problem on all Intel BX chipset motherboards because they only go up to a 2/3 divider, there is no 1/2 divider, and anything over the 100Mhz FSB speed will mean overclocking the AGP bus speed as well.

Again, when increasing your FSB speed, you'll also have to consider all the other devices in your system. Just because the CPU runs stable at the higher speed settings doesn't mean you have overclocked successfully. Any of the other devices can stop functioning or start causing problems. You might need to edit your CMOS and lower some of the settings for the RAM and/or Hard Drives to get your system functioning without problems. It is a fact that by overclocking you increase the chances of system faults, crashes and overall instability, so if avoiding a crash is crucial, consider buying faster Processor or components, rather than overclocking.

Just remember for reference:

PCI Bus	= 33Mhz
AGP Bus	= 66Mhz
FSB x Multiplier	= CPU Internal Clock Speed
FSB x Divider	= PCI or AGP Bus Speed

Effect of non-standard bus speeds

Non-standard bus speeds can have a variety of effects on various types of computer hardware. Hard drives can miswrite data, CD writers can create even more coasters than usual, CD-ROM drives can refuse to function, RAM can refuse to work properly, etc., etc., etc. Some of these problems can be fixed by adding some rudimentary cooling, but many of them are simple limitations of the hardware which will limit a system's overclockability. Keep an eye out for these things because they can cause serious problems with a system. Most of these problems occur when using bus speeds that exceed the PCI bus frequency. PCI is intended to run at 33 MHz. If you set it to ove 40 MHz or so (using 83, 124, or 133+ MHz bus), there is a fair chance your hard drive will lose everything. See page 3 of the Hard Drive Tweak Guide for more information.

FSB limitations and agp clock speeds

As processor quality increases overclockability, overclockers are finding themselves running Front Side Bus(FSB) speeds that are farther and farther above spec. Ironically, the "old" BX chipset is often the platform of choice for many because it still offers the highest clock-for-clock performance of any other chipset. Often, processors such as the PIII-550e are able to run at speeds in excess of 800MHz. Running at this speed results in an FSB speed often greater than 145MHz. The BX chipset is only designed to run with a 100MHz FSB or lower. When running at its maximum rating of 100MHz, the BX chip only has to divide the FSB by 2/3 to achieve the proper 66MHz operation in the AGP slot. As the FSB increases, this 2/3 multiplier results in higher and higher AGP bus speeds, creating more strain on the video subsystem. At 145MHz FSB, the AGP slot is running at 97MHz!!! That is nearly 150% of the 'rated' speed. Most video cards cannot tolerate this increased speed and will not run.

Some of the newest cards, notably the GeForce line from nVidia and the Radeon from ATI, have been able to tolerate this speed on occasion. While running significantly over 90MHz on the AGP bus is still a stretch, a majority of these cards will run the 89MHz bus required to support a 133MHz FSB on the BX platform. This is a much more common overclocked speed, as the BX *does* support a 1/4 PCI divider, leaving the PCI perfectly in spec (33MHz) while the FSB is at 133MHz. If the AGP card only shows mild instability at the overclocked speed, a small increase in the IO voltage (only supported by some motherboards) *can* increase stability. If you are having extreme difficulty finding an AGP card to run with a high FSB, or if you want to use a greater than 150MHz FSB, you have

two options. Either you can use a PCI video card or a different chipset. At 160MHz, the AGP bus is running 107MHz, 62% over spec, however the PCI bus is running at 40MHz (only 21% over spec). You can also look at motherboards which are designed for the 133MHz FSB and thus support a 1/2 AGP divider. These include boards based around the Intel i815 chipset, the VIA Apollo Pro 133 and 133a chipsets, or the i820 (uses DRDRAM). With a 1/2 AGP divider, the AGP is running only 80MHz while the FSB runs at 160MHz and should be well within the tolerances of most cards. There has been good success at 166MHz FSB with the i815 chipset, which is probably your best bet for high FSB settings. There are reports of both the BX chipset and the i815 chipset reaching 220MHz FSB using special cooling and modified motherboards.

In addition, certain FSB speeds are harder to reach than others. For example, the 83MHz FSB speed will not run reliably on many systems, even where the same system might be able to run a 95 or 100MHz setting. This all depends on what speed the motherboard is set to change the AGP and PCI dividers and how sensitive the system is to the higher bus speeds. PCI Speeds of greater than 40-42MHz generally cause problems. Timing sensitive devices such as network cards, SCSI cards and video input devices sometimes have trouble at even lower speeds. AGP speeds of 80MHz and above cause problems on many older cards, however newer cards can often run up to around 90MHz. Another measure to stabilize a card is to reduce the bus interface to AGP 1x, disable sidebanding or disable fast writes these will help you get a little higher speed, but it is best to just accept the speed that your system runs with these features enable. One other extreme method of squeezing out a few more MHz is to decrease the "AGP Aperture" to minimum (usually 4MB). By basically cutting off 95% of the communication between the main memory and AGP card, this method will cause your card to run EXTREMELY poorly in 3D applications, however will allow you to brag to your friends that you have the highest MHz rating!! *big grin* Exact dividing points depend on your motherboard and are sometimes adjustable.

Pushing the limits of agp and pci clock

How does overclocking or adjusting the FSB effect other components, such as video cards, sound cards, and hard drives? Greatly. Make sure if you're running at 100 MHz FSB, you try to set the PCI clock to 1/3. For anything significantly higher, try to set the PCI clock to 1/4 (if available). If the PCI bus clock reaches about 43 MHz or higher (remember, 33 MHz default), it could possibly fry the contents of your hard drive (the data, that is). Also it could make items such as sound cards and network cards not function properly.

On the same note, AGP clock shouldn't be set much higher than 66 MHz (default). If you set the bus speed to 100 or higher, set the multiplier to 2/3 or lower (if available). Higher AGP clocks will not help performance, but can harm stability, and possibly kill an AGP card over long periods of time.

FSB speedagp divider pci divider

50-79MHz1/11/279-83MHz1/1 or 2/31/2 or 1/383-117MHz2/31/3117-124MHz2/3 or 1/21/3 or 1/4124MHz+2/3 or 1/2*1/4*Depending on chipset **Note:** many motherboards depend on the CPU's request for either 100 or 133 FSB to determine the AGP divider. Thus, on a CPU that normally runs at 100MHz the AGP divider will be 2/3, regardless of the support for a 1/2 AGP divider. In this case, check your manual for a "FSB override", "sel 100/133" or "AGP divider" jumper or switch, or use a Slocket that has such a jumper (such as Iwill's Slocket II).

Memory speed considerations

Today, the great majority of people run SDRAM memory. Old 72-pin SIMMS with an EDO or FP format are now very outdated and never found in 'modern' systems. The newest Direct Rambus DRAM is is too expensive for the normal desktop system. Standard SDRAM is found in three varieties, separated by their maximum speed capability. Original SDRAM runs at 66MHz and is sometimes called PC66. Newer memory speeds are PC100 and PC133. There are also companies that sell a PC150 memory, however this is not an officially recognized format. DDR (double data rate) SDRAM is just beginning to enter the mainstream as a SDRAM 'replacement'. It has been used for several years on graphics cards and in specialized applications however this is the first it will be available for commercial, all purpose use. The AMD 760 was the first chipset to introduce DDR SDRAM support. It was announced October 30th, 2000 and represents the next step in the evolution of the x86 architecture. It may very well replace the failing DRDRAM standard being pushed by Rambus. Generally, if you are running over 100MHz FSB it is best to use PC133 memory. While some of the highest quality PC100 memory has been shown to run over 145MHz, you will have much more consistent results with PC133 memory. SDRAM chip speed is measured by its refresh rate and is expressed in nanoseconds (ns). Standard (PC66) SDRAM is usually rated at 12ns. PC100 memory must be rated with 10ns or faster speed, however most modern, high quality PC100 memory is rated at 8ns. PC133 memory must be rated at 7.5ns or faster and has stricter tolerances than PC100 for layout and signal interference in the module itself. When aiming at 133MHz or above, you should always try to use PC133. While some of the best PC100 memory has been tested beyond 145MHz, most modules will not run much above 124-133MHz and some will barely do 112MHz. PC133 modules are guaranteed to run *at least* 133MHz and thus most will run faster.

Cas, ras and memory timings

SDRAM is physically organized in rows and columns of memory addresses. CAS stands for "column access strobe" and refers to the speed the column strobe can be flashed. There are generally two other timings which can be adjusted, called RAS (row access strobe) and CAS-to-RAS delay. Decreasing the timings leads to higher performance, however increased timings can result in higher a tolerance for overclocking. A CAS delay of 2 cycles is generally referred to as CAS2 and is the fastest rating of current generation memory. A CAS3 rating is about 2-3% slower and memory that is only rated to CAS3 timings should be avoided while overclocking because it offers slightly less leeway in overclocking. The CAS timing is the most critical of the group, however RAS and CAS to RAS can also be adjusted. Often these memory timings are given together, written as 2-2-2 or 3-3-3 or any other combination of timings. Generally, 2-2-2 yields the highest performance and 3-3-3 the slowest. A timing of 3-2-2 is a common setting for systems where CAS2 is slightly unstable as it is a good compromise between performance and clock speed. Read the PC133 SDRAM Article for more info on which memory is best at what speeds and how you can determine ns ratings on your memory. The newest chipsets from both Intel and VIA, including the VIA Apollo 133(a) series and the i815 support "asynchronous" memory operation. This simply means that the memory clock can be adjusted independently from the FSB speed. The speed is generally adjusted in coarse increments of around 33MHz. It is often expressed as FSB+33 and FSB-33 or FSB+PCI and FSB-PCI. The FSB+/-PCI is a more accurate description because the memory clock is usually set using the PCI speed. Basically it means that you take the FSB speed and subtract/add the PCI speed. This comes in handy in several situations. First, when running extremely high FSB settings such as 155-166MHz FSB memory can be difficult if not impossible to find. Adjusting the memory to a slower speed can allow slower memory to run on a very high FSB. Also, it can be useful to increase system performance by running a higher memory speed while still using a slower FSB speed. Running a 100MHz FSB, you could set your memory to run at 133MHz, thus increasing system performance by 1-3%.

Hard drive limitations

Overclocking to high FSB speeds can greatly improve system performance, however, just as your CPU, motherboard, memory, AGP and PCI must be able to tolerate the speed, so must your hard drive. The IDE controller is placed on the PCI bus and is affected by overclocking the same as any other PCI device. It is important to choose a hard drive which can tolerate the increased speed. Many older drives will cause data corruption (sometimes extreme) when the PCI speed breaks 40MHz. Most notorious for this are 'older' Maxtor, Fujitsu and Western Digital drives and 'original' UDMA drives. The current generation Western Digital, Maxtor Diamondmax Plus and IBM GXP75 drives have shown to be the *most* tolerant to overclocking.

CPU CORE VOLTAGE

Most CPU's have some sort of way to change the voltage of the chip. Raising (and in some rare cases, lowering) the chip's voltage can create a much stabler chip, at the cost of more heat. Heat, of course, alternately lowers the overclockability of a chip, but it doesn't lower the chip's overclockability as much as upping the voltage raises it. And besides, there is always cooling. But more on that later. Tweaking the core voltage is by far one of the best techniques to achieving a higher clock speed. If you are finding that your are getting a black screen after attempting a new speed, or if Windows will only boot part way, it is likely the solution lies here. Start off at the CPU default and if everything is working, leave it be. If you find things are unstable at your overclocked speed, increase the voltage by 1 notch at a time.

The basic theory on chip voltage and how it affects the processor is this: a higher chip voltage increases the signal strength between transistors within the chip, allowing the signal to ignore greater discrepancies within the silicon core itself. You see, the silicon wafers used to make the chips aren't always pure, and they definitely aren't all of the same quality. A chip with a higher clock rate is generally going to have a core made of a higher quality silicon wafer.

Now, the processor signal has two choices as to how to deal with a chip impurity. It can either jump the gap, or go around it. When the processor frequency is lower, the signal has the time to go around the defect if need be, but if the frequency is too high and the signal must go around, the signal doesn't get to its destination in time or at all causing a miscalculation that usually will cause some form of software error (commonly it causes a crash). However, upping the core voltage is like giving the signal a running start, it allows the signal to jump gaps within the chip with relative ease and the signal gets to it's destination in time.

Default voltages of common computers

Intel CPUs	CPU Speed	Process Stepping Volts
Pentium	60-66	0.8u P5 5.0V
Pentium	75-200	0.6/0.5/0.35u P54 3.3V
Pentium MMX	166-233	0.35u P55C 2.8V
Pentium II*	233-333	0.35u/0.25u all 2.8V/2.0v
Pentium II	300-450	0.25u all 2.0V
Pentium III	450-550	0.25u kA0,kB0 2.0V
Pentium III	600,600B	0.25u kB0 2.05V
Celeron	266-533	0.25u 2.0V
Pentium III	500e-866**	0.18u cA2,cB0 1.65V
Pentium III	600e-1Ghz	0.18u cC0 1.7V
Pentium III	933-1Ghz	0.18u cB0 1.7V
Pentium III	1.0-1.13Ghz	0.18u cC0 1.8V; 1.85V
Celeron II	533a-600	0.18u mB0 1.5V
Celeron II	633-700	0.18u mB0 1.65V
Celeron II	533a-700	0.18u mC0 1.7V

*later CPU's stepped down to 0.25u - i.e. P2-300 SL2W8
**early FC-PGA Coppermines ran at 1.6v

AMD CPUs	CPU Speed	Process Stepping Volts
K6-2	266-400	0.25u - 2.2V
K6-2	450-550	0.25u - 2.2V or 2.4V
K6-III	350-500	0.25u - 2.2V or 2.4V
Athlon	500-700	0.25u Rev 1 1.6V
Athlon	550-750	0.18u r2/K75 1.6V
Athlon	800-850	0.18u r2/K75 1.7V
Athlon	900-1000	0.18u r2/K75 1.8V
Athlon	650-850	0.18u r4/K75.1 1.7V
Athlon	900-1Ghz	0.18u r4/K75.1 1.8V
Athlon	650-1.2Ghz	0.18u TBird 1.7V
Duron	600-800Ghz	0.18u - 1.6V (1.5V)

How important is voltage to overclocking?

Well, since this varies on every system, I'll use my last CPU as an example. It was a Celeron II 566 (8.5 x 66 MHz bus default) that ran at 1.5 volts. When I first received this CPU, I immediately put it into my Abit BF6 motherboard and proceeded to overclock it. With the default 1.5 volts, the CPU could not make it over 620 MHz without crashing. So I put the voltage up to 1.6. Now it ran all the way up to 706 MHz without crashing. However, at 1.6 volts it would crash if I set it higher. So I put it to 1.7 volts and hoped for the best. Sure enough, I managed to hit 808 MHz without problems. I had heard that many people with Celeron II 566 CPUs could hit 850 no problem. So I tried 1.75 volts. Sure enough, it hit 850 without problems. At 1.75 volts it refused to go farther, though. At 1.8 volts I managed 876 MHz. I dropped it back to 1.75v @ 850, however, because of heat issues.

When a company such as AMD or Intel bins its chips (the process or dividing out the speed grades is known as 'binning'), it rates them for a specified voltage. If that voltage is increased, the speed tolerance of the chip is also increased. This is a limited effect which begins to degrade after a 10-20% voltage increase, but it can significantly improve overclockability. Intel lists absolute maximum voltage on the Coppermine at 2.1V (meaning you shouldn't even approach that voltage). AMD lists the same as +0.5V from Vcore. Generally, +0.3V is within acceptable limits. When running a chip with a higher than 'spec' voltage, always ensure it is

adequately cooled as an increased voltage results in an increased heat output. See "cooling review" for some tips. In addition, the colder the CPU temperature is maintained, the greater tolerance it will have for overclocking.

Couple of simple rules I abide by when tweaking the voltage of a cpu:

1. Voltage = Heat - Higher voltage obviously means more heat. Higher voltage may allow you to overclock a CPU higher, but without proper cooling, the PC will freeze or have other problems farther down the road.

2. .3 Volts over Default; MAXIMUM! - It's a bit conservative for some users, but I rarely push a CPU higher than .3 volts over the default setting. Not only will it create more heat, but it could possibly damage the CPU. If you want to push your CPU higher, go for it. Just remember, I don't recommend it. Also, make sure you don't accidently jumper a slocket or a motherboard for something like two volts over the default value. This could result in instant death for your CPU.

How to change the voltage

What do you do if you get a board without voltage adjustments? Well, there are not many options. If you have an Intel Socket 370 CPU, you can mount your CPU in a socket to slot converter card. This only works if your CPU is a socketed chip and your motherboard is able to take a Slot 1 chip. Many of today's converters, such as the Asus Slocket II, Abit Slocket III and the MSI Slocket v2.x are compatible with both PPGA and FC-PGA Intel processors and include jumpers to adjust the voltage of your CPU.

If you use an AMD Athlon with a Slot A interface, you can also use, what many people call a "Golden Fingers Device" (GFD). This is a device which fits onto a special connector on the top of the CPU and allows both multiplier and voltage adjustments to be made via a series of switches mounted on the GFD itself. These are fairly simple devices to use, however, remember that the plastic housing on the back of the CPU must be removed to expose the Golden Fingers attachment. Also keep in mind that a GFD needs to be powered and most have a plug for a standard 4-pin molex connector (hard drive power plug). More extreme measures can be taken to change the voltage where it would not ordinarily be supported, such as physically modifying the CPU, however those are beyond the scope of this article.

Sockets and cpu softMenu II or III voltage

If you're using a slocket (for an FC-PGA based Celeron II), there are a couple tricks you can do with the voltage and FSB settings to achieve better performance and stability. If you want to set the voltage to what is on the slocket, set the SoftMenu settings to use Auto or Default for voltage. This allows you to use 1.8 volts or higher on the slocket itself, regardless of what the BIOS supports. This is especially useful on older Abit motherboards where the voltage can only be set up to 1.7 volts for the Celermine CPUs. For stability at 100 MHz or higher, set the slocket to 100 MHz FSB, even if you're planning on setting it differently within the BIOS setup. This seems to make the CPU more stable, at higher speeds (at least, on the Abit Slocket !!! it does).

BUMPING UP THE CLOCK SPEED/USING SOFTFSB

Now that you've nailed the problems, tweaked the voltage, and dealt with the heat, you probably want to overclock your CPU a bit higher. Instead of using the typical jumpers or the BIOS' CPU clock speed software, consider SoftFSB. SoftFSB is a nifty little program that allows you to change the clock speed of your CPU (on-the-fly) from within Windows. This has obvious benefits... and it can often times lead to higher clock speeds than you thought possible before. When you decide to use SoftFSB to overclock your computer, take the following precautions:

- Save before attempting anything
- Progressively overclock system - go up one speed step at a time to make sure you don't damage the processor.
- Run the stability tests to make sure the overclock was completely successful.
- Want to run your 66 Celeron etc at 100 mhz - have a look at www6.tomshardware.com/cpu/98q2/980514/index.html

Check to see if your motherboard is supported before you start playing around with this program, as it can alter some pretty serious stuff. Once you're sure it supports your system, run the program and choose your motherboard from the drop-down list. Hit "Get FSB". Now it should show all the supported FSB speeds. Change the speed of the FSB to the desired clock. Click "Set FSB" and the new speed should be set. You should probably test stability before deciding on a good speed.

Remember: On most new CPUs, you can't change the multiplier. All overclocking must be done in the FSB (front side bus). To test to see if you've hit the limits of your L2 cache, try disabling the L2 cache in the BIOS setup and setting the clock speed to something that was previously unstable. If the option works and the CPU is stable at the new speed, there is a good chance that your L2 cache is too hot or it's not able to reach the speed you're striving to hit. This is often the limitation on older Pentium II systems.

Good clock speed and stability

There's no doubt that a higher clock speed is better than a lower clock speed. But you must not sacrifice stability to reach that clock speed, or the PC will become basically useless. There are various ways to test the stability of a system at a given clock speed, but in my opinion, the best method is to use the CPU Stability Test. This program simply rules for testing stability. Crank the priority all the way up and run this program overnight. If the system crashes, you've got a problem.

Recommended settings

There are no unique best settings for every system, however I'll try to give you a basic guideline for overclocking. I'll cover settings for motherboards with the following range of bus speeds: 100, 112, 124, 133 MHz. If your Motherboard doesn't support the higher bus speeds, or has some other, not listed here setting, you can still try the rest, get a calculator and figure out the possible combinations yourself remember it's Multiplier x FSB = Internal CPU speed. WARNING: Please keep in mind that the more aggressive settings can damage your CPU over time, increase system instability and don't work on all motherboards/CPUs. Just the fact that the settings appear in this table doesn't mean they are safe for your system and devices, use them at your own risk.

Multiplier	**Common CPU/FSB Speeds**			
	100Mhz	**112Mhz**	**124Mhz**	**133Mhz**
3.0x	300Mhz	336Mhz	372Mhz	399Mhz
3.5x	350Mhz	392Mhz	434Mhz	465Mhz
4.0x	400Mhz	448Mhz	496Mhz	532Mhz
4.5x	450Mhz	504Mhz	558Mhz	598Mhz

5.0x	500Mhz	560Mhz	620Mhz	665Mhz
5.5x	550Mhz	616Mhz	682Mhz	731Mhz
6.0x	600Mhz	672Mhz	744Mhz	798Mhz
6.5x	650Mhz	728Mhz	806Mhz	865Mhz
7.0x	700Mhz	784Mhz	868Mhz	931Mhz
7.5x	750Mhz	840Mhz	930Mhz	997Mhz
8.0x	800Mhz	896Mhz	992Mhz	1.06Ghz
8.5x	850Mhz	952Mhz	1.05Ghz	1.13Ghz
9.0x	900Mhz	1.008Ghz	1.11Ghz	1.19Ghz
9.5x	950Mhz	1.06Ghz	1.17Ghz	1.26Ghz
10.0x	1Ghz	1.12Ghz	1.24Ghz	1.33Ghz
10.5x	1.05Ghz	1.17Ghz	1.30Ghz	1.39Ghz
11.0x	1.10Ghz	1.23Ghz	1.36Ghz	1.46Ghz

COOLING

is the MOST important factor in successful overclocking, running a stable system and keeping your CPU in good shape. If your overclocked CPU operates at a higher than specs temperature, it will shorten its life and electro migration will eventually occur. Other side effects of overheating can be random crashes and unstable system. Generally, today's processors are designed to work between 25 and 100 degrees Celsius (77 to 212 Fahrenheit) and anything outside the temperature range would result in more unstable system and possible damaging of the CPU. Keep this in mind, cooler is better, try to cool your CPU as much as you can, put a big fat heatsink on it with a big fan to help. Other, somewhat more extreme cooling options are using a Peltier (drains a lot of power, active cooling solution), or water cooling kit. Just remember the better cooling solution you choose, the better chances for successful overclocking you have.

There are many types of cooling systems out there for your CPU. They are usually purchased in the form of Heatsink/Fan combos. There are combos for Socket A platforms, FCPGA platforms and the regular SECC1 and SECC2 Slot 1 and Slot 2 platforms. They range in types of huge golden orbs to big square copper or aluminum heatsinks and fans.

One of the most publicized issues with overclocking is the heat. Increasing the clock speed of a CPU will just about always result in more heat. And increasing the voltage does the same... so increasing the clock speed and voltage can lead to insane heat levels, far beyond what the CPU is normally used to dealing with. But that shouldn't be too much of an issue for mild overclocking, since generally, CPUs run at far below their maximum stable temperature. In general, a CPU should be relatively stable so long as the temperature is below 115ºF. Anything over that could lead to instability on certain CPUs. Some systems can be fine way up to 140 or even 160ºF, but for the most part, try to keep the CPU below 115ºF.

Cool room = cool pc technique

If you live in a house with air conditioning that's constantly being run or your room temperature is far lower than your system's temperature, you can probably rid most of your heat problems by removing the side panels to your case. If your room is 70ºF, the air outside your case is probably much cooler than the air inside your case. So remove the panels and you can probably drop the temperature signficantly. Also, try to keep the PC's area well ventilated. No matter how good your CPU fan, or fans are, the air they blow onto your CPU can only be as cold as the air in your case. This might sound obvious, but the heat dissipation from your cooler can be severely disrupted by rising temperatures inside your case. The ATX specification states that air must be drawn into the case, circulated and then expelled. Although fine in principle, in reality the single fan solutions to be found in most cases means that the hot air is not exhausted properly and the case temperature continues to rise. You can reduce your case temperature considerably by simply reversing the direction that your fan works in. In my case I disassembled my power supply, unscrewed the fan,reversed the direction so that the fan "pointed" outwards, and reassembled. In this way the hot air is drawn out of the case by the PSU fan, to be replace by cooler air. You can help this process by installing an extra fan to the front or rear of the case, drawing cool air in. It is well worth installing a secondary fan to draw air in. Positioned near the bottom of the case this will get a nice air rotation going, and will avoid "hot spots" from building up in the corners! Fans stripped from old PSU's are particularly useful for this purpose.

Expel **hot** air at the top **------>**
<------ Draw **cold** air in from the bottom

Software cooling

Some people are skeptical of software cooling's effectiveness, but I have seen very good results. CPUIdle has always been my favorite software cooling utility. On my Celeron 566@850 system, the temperature dropped from 110ºF to 95ºF in a 30 minute period. Only use software cooling on win9x systems

More fans / cooling

It's cost effective to buy fans to cool your PC if you've got a highly overclocked CPU. Consider something that will cool your whole PC, such as The Card Cooler XT. Make sure to have exhaust and intake (hot air going out and cool air coming in) in effective locations. Usually you'll want exhaust near the top of your PC since the heat will rise in a tower case. The intake should probably be near the bottom of the case, since the coolest air in the room is probably close to the floor, especially if it isn't carpeted. :) Consider a better CPU cooler as well if you think the price is worth the overclocked speed you've achieved. Alphas, and typical "big ass fan/heatsink" combos work very well to remove heat from CPUs.

Two of the parts of the overclocking process up the heat produced by the processor - upping the frequency (the actual overclock) and upping the core voltage. Excessive heat within the core creates more of those gaps that I was discussing above for the signal to cross, and too many of these gaps will weaken the signal to the point where it becomes non-existent and creates some more of those wonderful software errors. Here's the lowdown for you physically inclined folks - the extra heat energizes the particles within the silicon wafer. The pathways within the silicon wafer are approaching the size of light rays (read very small), so if the particles move too much, they break their connection with the other particles within the pathway. These temporary breaks do the same thing as the impurities mentioned above. Got it? Good.

Ok, now that you know all about why cooling is so important, here's the skinny on what kind of stuff is available to you hobbyist overclockers out there, and then maybe I'll do a little of the honorable mention thing to the more expensive cooling systems of the

world. The simplest way to cool your chip is called passive air-cooling. Passive air-cooling is basically the use of the surrounding, cooler air to cool the chip, using some sort of ball bearing fan. This is the cheapest, easiest, and most common way to cool your processor - all it entails is attaching a fan/heatsink combo to the processor to cool the thing down.

Hard-core hobbyists, however, are never satisfied with simple 'air' cooling, oh no. Heck, I've even seen some guys go so far as immerse their systems into super-cooled glycerin (a non-conductive liquid) to cool their processors There are two 'reasonable' types of active chip cooling. One, a Peltier system, basically uses a heat-transfer plate (called a Peltier) to conduct heat away from the processor, where it is then carried off by a standard fan/heatsink combo. The only extra stuff you need for this type of system is some form of insulation for the exposed portion of the cold side of the Peltier, because otherwise you will get condensation, and even frost (Peltiers are extremely efficient). Peltiers' distinct disadvantages are that they consume a vast amount of power and that they actually pose a direct danger to your components if used improperly. You should consider upgrading to 400W or higher power supply before installing one that runs off your internal power supply; some Peltiers even require separate 24-volt power supplies. If they're not properly cooled, Peltiers can actually damage the processor they're connected to and melt their own power leads. Never power up a Peltier without also firing up the attached heat sink/fan!

The other 'standard' form of active cooling is using some form of water cooling device. Water cooling systems are gaining popularity over Peltiers. They pump water or another liquid through a channel that takes it through a waterblock that's affixed to the CPU (to cool the chip), and then through a radiator outside of the case (to cool the water). Leufken Technologies www.leufkentechnologies.com sells a number of ready-made water-cooling kits. Even more impressive are the water cooling-ready systems available from Koolance www.koolance.com
In either case, judicious use of thermal compound is necessary to ensure proper thermal contact between the CPU and its cooler. Anyhow, if you've got the cash, their systems are something you might want to look into.

In spite of their ability to keep overclocked processors frigid, both Peltier and water coolers have several disadvantages. For one, they're considerably more expensive than heat sink/fan units. A bigger problem is condensation: Peltiers and water coolers are so efficient that the difference in a case's ambient air temperature and the pocket of cool air generated by the cooler can result in distilled water or even ice forming around the CPU. Should the moisture dribble onto a charged circuit board, or form between the CPU and the socket or slot contacts, it could cause considerable damage. The de facto defenses for this is to waterproof slots and/or sockets with a silicone sealing compound, or to monitor the cooler and attempt to keep its temperature close to the case's ambient temperature, thus preventing condensation from forming in the first place.

To install a cooling device, first you need to remove the old fan/heatsink combo from your processor. This should be a fairly simple operation. Don't be afraid to use a little force to break the seal that was created by the thermal compound. You will then need to use a flat razor to remove the remainder of the thermal compound from the top of the processor. Once this is complete, apply either some more thermal compound or thermal tape (FragTape) to the top of the processor and attach the new heatsink on top of that. Simple enough, huh? Some setups may have other necessary steps to attach the cooling device (thermally insulating silicon caulking compound, etc.) to prevent condensation - but that won't be a problem with a standard fan/heatsink combo.

Regardless of how many case fans you install, you should either install dust filters in each fan situated to pull air into the system, or check your system's internals every week or two for dust buildup. Increased, unfiltered airflow pushes more dust through the case. Dust can stunt the life of case and component fans by building up on their fins and drive shafts, and it can coat--and therefore insulate--various chips and components in your system. If you encounter dust buildup, purchase a can of compressed air at a computer or photography shop and, with the computer powered off, blow the components clean. If you filter your fans, you should clean the filters occasionally. Clogged filters can impede the flow of air through their fans.

No matter how much air you push through your system, you'll need more direct cooling for your overclocked components. The cooling industry is ready, with heat sink/fan coolers available for every shape, size and brand of CPU. Among the most popular are manufacturers are Global WIN www.globalwinusa.com maker of the legendary FOP38 Athlon/Duron cooler, and Thermaltake www.thermaltake.com

Lapping

If you can't afford a Peltier or a water-cooling system, you can increase the thermal transfer of your components by performing a process known as lapping. Heat sinks work by transferring the heat away from a component to a more easily cooled area. Unfortunately, both heat sinks and processors contain irregularities in their surfaces that prohibit contact in some areas. Lapping is the act of removing any irregularities in the surface of a component and a heat sink, rendering them completely flat and therefore able to come into greater contact with each other. As rewarding as it can be in allowing you to push clock frequency envelope even farther, the process of lapping borders on the insane.

The best way to lap a CPU and its heat sink is to first acquire a pane of glass at least eight inches by eight inches, three or four sheets of sandpaper of varying coarseness (perhaps 400, 600 and 800), and plenty of tape. Remove the CPU and separate it from its heat sink. Lay the glass flat on a table and tape the coarsest sandpaper, grit side up, to the glass. As recently as the Pentium, the surface of the CPU that was actually visible was the metal or ceramic package enclosing the actual silicon chip. However, current generation CPUs now have a metal layer, called a heat slug, over the top of the CPU, which helps dissipate the heat generated by today's very hot CPUs. However, the heat slug often has some minor irregularities that prevent a perfect mating between the surface of the slug and the contact area of the active cooler.

Before lapping this Celeron A, you should cover its exposed metal parts with tape. You'll want to sand the heat slug that comes into contact with the heat sink without damaging any other electronic components, such as discrete power regulation devices on the surface of some CPU packages or other metallic parts nearby. For example, on a Celeron CPU, the side that touches the heat sink is surrounded by the backs of the CPU's pins. You should tape over the pins' backs to prevent them from becoming damaged.

Wet the sandpaper slightly--a few well-spread drops of water will do. Place the area of the CPU you wish to lap on the sandpaper. With firm but gentle pressure, stroke the CPU in a circular or figure eight motion on the sandpaper for a few seconds. Then remove the CPU from the sandpaper and inspect it. You'll see scratches on the surface of the heat slug or package. Make sure that "only" the heat slug was sanded, and repeat the process. You should continue this until any etching on the CPU has been nearly removed. Switch to the next smoothest sandpaper, and remove the rest of the etching. Switch to the smoothest sandpaper and sand until any noticeable scratches are gone and the surface is completely smooth.

If you see copper, you've gone too far. Hurl the processor into the nearest trash receptacle and start over!

Repeat the entire procedure on the surface of the heat sink that makes contact with the sandpaper. When you've lapped both surfaces, blow them off with a can of compressed air and visually inspect each to ensure that there aren't any stray metal shavings on them. Check both sides of the processor. Then, since the surface of the sandpaper was wet, allow the heat sink and processor to dry completely before placing them back into the system--but remember to apply a drop of thermal paste between the heatsink and the contact point on the CPU.

Some overclockers have reported shaving one to two degrees Celsius from their CPU temperatures simply through lapping. Others have reported that they accidentally destroyed their processors. Lap at your own risk.

Default temperatures of cpu's

Here are the maximum temperatures for the most popular CPUs. Note that these values are for CPUs that are not overclocked. Overclocked CPUs may run unstable even if their temperature is way below the maximal specified temperature.

AMD Athlon and Duron

Socket A CPUs (Athlon, Duron) up to 1GHz	90°C	
Socket A CPUs (Athlon) 1.1GHz or more		95°C
All Slot A CPUs (Athlon classic, Athlon Thunderbird)	70°C	

AMD K6 series

All K6 CPUs (166-300MHz) and most K6-2/K6-III CPUs	70°C
K6-2/K6-III CPUs, model name ending with X (e.g. K6-2-450AFX)	65°C
K6-2-400AFQ (uncommon)	60°C
K6-2+, K6-III+, most mobile K6/K6-2 CPUs	85°C
mobile K6/K6-2 model ending with K (e.g. mobile K6-2-P-400AFK)	80°C

The temperatures specified for AMD CPUs max case surface temperatures. These CPUs do not have an internal diode to measure CPU temperature. The accuracy of the CPU temperature measurement depends on the motherboard; therefore, it is possible that the CPU overheats even though the CPU temperature reported by the motherboard is below the specified maximal temperature.

Intel Pentium III

Pentium III Socket 370 500-866MHz,		80-85°C
Pentium III Slot 1 (first generation, OLGA) 550-600MHz,		80-85°C
Pentium III Slot 1 ('Coppermine') 500-866MHz		80-85°C
Pentium III Socket 370 and Slot 1, 933MHz		75°C
Pentium III Slot 1 933MHz		60°C
Pentium III Slot 1 1GHz for newer versions	70°C	
for older version	60°C	
Pentium III Slot 1 1.13GHz (first version)	62°C	

Pentium III max temperatures are the maximum temperatures reported by the thermal junction inside the CPU.

Intel Celeron / Celeron

Celeron 266-433MHz (max. CPU case temperature)	85°C	
Celeron 466-533MHz (0.25µ) (max. CPU case temperature)	70°C	
Celeron 533-600MHz ('Coppermine)		90°C
Celeron 633 and 667MHz	82°C	
Celeron 700MHz and more		80°C

Celeron max temperatures are the maximum temperatures reported by the thermal junction inside the CPU, unless otherwise specified.

Intel Pentium II

Pentium II (1st generation, 'Klamath') depending on MHz		72°-75°C
Pentium II (2nd generation, 2.0V core), 266-333MHz		65°C
Pentium II (350-400MHz)	75°C	
Pentium II (450MHz)		70°C

Pentium II temperatures are the maximum temperatures of the thermal transfer plate
(on which the heatsink is installed).

Intel Pentium 4 (Willamette)

Pentium 4 1.3GHz	69°C
Pentium 4 1.4GHz	70°C
Pentium 4 1.5GHz	72°C

Intel Pentium Pro

Pentium Pro, 256 or 512K L2 cache	85°C
Pentium Pro, 1MB L2 cache	80°C

Pentium Pro temperatures are maximum surface temperatures.

AMD OVERCLOCKING (concentrating on socket a processors)

AMD Athlon and Duron CPU's run hotter than Intel CPU's are require greater cooling to run at the same speeds, however this doesn't deter the clocking ability of the AMD K7 Family of CPU. When you overclock the CPU you cause the core of the CPU to run faster than it was originally designed to do and this causes more heat, ergo, you need more cooling, the cooler you can get your CPU to run at, the more change you have of overclocking it. The reason we cool CPU so much is that heat is what causes the CPU to crash and not respond. Heat gets between the components in the CPU and prevents a good electrical currant from flowing and intern causes the CPU to breakdown and stop responding. If we are able to use a larger cooler to extract more heat then the components of the CPU can then receive the currant more efficiently and overclock even more. When you have reached the limit of what you can overclock the CPU to on the default voltage this doesn't signal the end of the overclock for only the components are

having a hard time but the core can still handle more speed so how to we get a clearer electrical signal? Increase the voltage supplied to the core of the CPU. Voltage is one of the most important features that will determine a successful overclock. When you increase the voltage you also increase the amount of heat that the CPU produces and more cooling is again required. When the CPU is made they are given a default core voltage. Slot A AMD Athlon Classics work on a 1.6v core. Socket A and Slot A AMD Athlon Thunderbirds use a 1.7v core. AMD Duron CPU work on a 1.5 or 1.6v core. When changing the voltage to help your overclock you must use common sense and know when enough is enough.

AMD Athlon 2 in PGA or Socket A form is a little different with overclocking as it requires no Goldfinger Device. Overclocking on the Athlon 2 in Socket A has 4 aditional Pins in its Grid Array that when certain voltage signals are sent to the CPU it sets itself to the appropriate multiplier. Unlike Intel CPU's where the CPU tells the motherboard what multiplier to use in a 1 way direction (Information is sent to the board only) AMD Athlon 2 Socket A sends information to the motherboard but also allows information to be sent to the CPU to change its multiplier. With these added features the AMD Athlons are a lot easier to overclock than Intel CPU's as Intel CPU's require you to set the Front Side Bus higher than recommended and as many people know when you overclock the FSB you also overclock the PCI, ISA, AGP and Memory bus. So in order to get the maximum out of your Pentium 3 or Celeron system first you have to get the right CPU, then make sure your memory can handle the excess speeds. Then you have to make sure that your PCI cards can handle the overclocked bus speeds. Then you have the AGP Overclock dilemma. Will your card be able to stand the increased AGP speed. Most cards now a days have been built to handle the increased speeds but not everything can be guaranteed. When you add all this up if only 1 of these can't handle the increased speeds then your overclocking potential is reduced greatly. Say for an example trying to overclock your CPU from 100MHz to 124Mhz FSB. Sure you say my CPU can handle it I placed a bigger heatsink onto it. There is plenty of air getting to it. But then you find out your AGP card can't handle the increased speeds. So now you are left with wondering what is the limiting factor, is it the Video Card or the CPU. With overclocking of the AMD Athlon and Athlon 2 there is no more worry about the perferables. Since all that is being changed is the CPU's multiplier only the CPU is being overclocked beyond limits, therefore you will know if it freezes its not one of the perferables is the CPU itself.

For the Socket A Athlon 2 users overclocking is more easy, you have the L2 cache on the CPU Die meaning no cache control needed and AMD have added 4 extra pins that as stated before when given certain signals allow the CPU multiplier to be set, meaning all you need to buy is an Socket A motherboard that states it has multiplier adjustments.

Case cooling is also something that should not be overlooked because with air cooling your heatsink will be drawing in the air from inside the case and if your case temp is 30deg then your CPU is already doomed. ASUS has a habit of putting the case temp sensor too close to the CPU and Chipset Heatsink so this doesn't give and accurate temp, anywhere from 26deg to 40 deg on the ASUS K7V or K7M are well within overclocking specs but the cooler the case the more likely you are to overclock. If you are planning to overclock you have probably been told to get a good sized Midi Tower or Full Tower... I prefer full tower as the saying goes, "If there is more space inside it takes longer to heat up the air inside". So full towers with at least a good 250w or 300w are well advised. A good Full tower case will have a area at the front of the case for a 80MM 12v DC Fan, this one is used to draw air into the case, some really good ones have 2 at the front for more intake. At the back there should be at least a slot for a 60mm or 80mm case fan. This is used to draw the hot air from the heatsink out of the case. On most Full Towers above the power supply here should be another slot for another 80mm case fan to draw any hot air generated by the CD Drivers and/or Hard Disk Drives. This is good air cooling, Slot Coolers are another idea, if you have a spare PCI or ISA slot you can put a Slot cooler into it. Preferably underneath the AGP Display card.

Changing the multiplier on amd chips

Right now, the most practical way to overclock your ThunderBird (officially the "Athlon with performance enhancing cache memory") or Duron you must have a motherboard that supports multiplier adjustment and you must be sure the L1 bridges are closed. While many chips ship with their L1 bridges intact, some do not and you will have to do that yourself. The most effective way to close these bridges is to use find solder or conductive ink, however a pencil will work adequately. Simply draw a line between the disconnected parts of each bridge. Be sure it is VERY thick since graphite is not a great conductor you need to ensure an adaquate connection.

A 0.5mm or smaller mechanical pencil with soft lead (BB or 2B hardness) is recommended. At first it was thought that this method might not be a long term solution, however many users have reported no problems after 6 months of use so it should not cause any serious problems. If you are worried about the graphite rubbing off and wanting to find a more permanent method, a conductive pen or "rear window defogger kit" pen will lay down a more permanent, metallic line between the two bridge points. You will have to disassemble the pen and use a needle since the bridges themselves are much too small for the tip of the pen to connect.

Be careful that you don't short the bridges by connecting one set to another. After looking over the schematic for the bridge layout, I can say with some confidence that shorting the bridges will not damage the CPU but they will produce undesired multiplier settings, leaving you unable to properly set the multiplier and causing system instability.

FSB and multiplier combinations

You can also use the FSB to increase the speed, however, the VIA KT133 chipset which is the most common Socket A chipset to date (the AMD760 is brand new) cannot often run higher than 110MHz-115MHz. These increases are relatively small but they can help you to hit your maximum speed. For example, my Duron 700 is not quite stable at 10x100Mhz. I know it will work just fine at 9.5x100MHz but I think the 10x100 setting is RIGHT on the edge of stability. I can keep this 9.5x multiplier and increase the FSB speed to 104MHz to get a total CPU speed of 989MHz. In my case, my chip is 100% stable at 989MHz. But don't stop there!! Increasing the FSB provides a greater performance benefit than increasing the multiplier since it increases the speed of the rest of the system as well. My Duron 700 runs great at about 990MHz, so why don't I use the 9x multiplier but increase the FSB to 110MHz? This yields about a 2% performance increase over the old 104MHz FSB. Sometimes it can be even more substantial.

Keep your eye out for the AMD760 chipset. This chipset introduced official support for the 133MHz (266DDR) FSB for the Athlon. It also introduces DDR memory. This 133MHz FSB is a great tool for overclockers. Remember talking about my Duron 700? What if you don't want to open up the box and mess with the multiplier settings? The AMD760 will allow you to get into FSB overclocking, just like you can with Intel chipsets. Leaving the multiplier of the Duron 700 at 7.0x and increasing the FSB to 133MHz will result in the Duron running 933MHz. It is likely that this 933MHz setting would actually be faster than our 989MHz setting because it is using a 31MHz faster FSB speed. It will also decrease heat production and strain on your CPU.

As you can see- the Athlon offers lots of options. With DDR memory offering a 10%-20% improvement in speed over PC133 SDRAM, keep your eyes open for lots of demand in their first few months. For your information: DDR memory continue to use the

"PC" specification that SDRAM uses but it won't be based on MHz speed, but based on transfer rate. 100MHz DDR SDRAM transmits at 200MHz. With a 64bit wide data path, this memory can transmit 1600MB/sec. 100MHz DDR (200MHz) RAM will be known as PC1600. Along these same lines, 266MHz (133DDR) memory will be known as PC2100. Micron is currently working on the PC2600 specification which runs at 333MHz (166DDR). The Athlon's EV6 bus is capable of running 200MHzDDR (400MHz). Once these L1 bridges are closed, the motherboard should be able to assert full control over the multiplier via whatever method it chooses. The Abit KT7 uses Abit's Softmenu III to adjust the multiplier, while other boards such as the Asus A7V and Epox 8KTA+ uses DIP switches placed on the motherboard.

GFX CARD OVERCLOCKING

First off, what exactly is video card overclocking? Well, it is simply running a video card faster than the manufacturer's stated specifications, allowing it to move more data than it did previously. Basically, we "soup it up" a bit. Nifty, eh? It is possible, depending on the type of card, that you may see a nice performance increase from doing this - possibly even a 5% to 20% better frame rate in some of your favorite games. This, in turn, should allow a smoother-moving image on an older machine as well as to help you achieve a lightning-fast frame rate on a box built by a power user. Really, we all know deep down inside that overclocking can be just plain fun, and at the very least we can laugh at our buddies who are not on the cutting edge of "tweakness"!

While this idea will appeal to many of you, there are some of you that this will not be of much use. If all you do is run an Excel Spreadsheet all day or simply surf the Net, this is most likely not something that you will want to embrace or need to embrace. If you want some bragging rights about your "box" then this might be a good starter lesson. Also, your results will of course vary. Overclocking your Vid Card is highly subject to the components used in building it. As a rule of thumb, some of the brand name cards tend to OC better than some of the generic cards, but this is not always the case.

General

NVIDIA makes what is probably the most widely used "performance" graphics card that is out right now. Their GeForce and GeForce2 line of cards are pretty speedy to begin with, but we can make them even a little faster. Of course, let's not leave out ANY of them including 3dfx, Matrox, ATI, and S3. Now keep in mind that you can OverClock just about any Vid Card, and we will show you how to do a few here quickly.

First, remember this, OverClocking your Vid Card technically voids the warranty and also could damage it permanently. The chances of a Vid Card being damaged due to OCing is VERY RARE, but can become a real issue depending how far you want to push the envelope. I have overclocked many Vid Cards in the last three years and I have never had one fail because I OverClocked it. And we have done some pretty strenuous things to cards in the past. For the easy tricks we will show you here, you are most likely to be all right. Usually the worst thing that will happen is that your system will lock up if you are pushing the card beyond its physical limitations. The utilities that we are going to use have safeguards built in to reset your card speeds back to the defaults.

nVidia have made our task much easier, let me explain... The GF2 is manufactured on a .18 micron which means less heat is produced from the card thus making it easier to overclock. The GeForce256 graphics card are manufactured on a .22 micron which makes them quite a bit hotter (harder to overclock) then GF2's. Just by physically touching the GPU (Graphics Processing Unit) on the GF2 you can easily notice how much cooler the GPU is compared to the standard GeForce256 GPUs'. I knew from that stage, all GF2's manufactured on a .18 micron would be excellent to overclock. As we all know, heat is the enemy of overclockers, the cooler something (in this case a GF2) operates at the better overclocking potential we'll have... Simple theory, but true. As far as I know, most GF2's will be shipped with 6ns (166MHz) RAM, our ASUS GF2 v7700 was shipped with high quality 6ns Infineon SGRAM... Like SDRAM RAM (Random Access Memory) the higher quality branded RAM you can find the better, since the memory will be operating at a higher speed then it is designed to be... When considering buying a GF2, always check to see if it has decent branded ram which is no higher then 6ns.

Why should I overclock my gforce/gfx card?

Why should you overclock your nvidia card... It's like asking why should I overclock my CPU. Simple, overclocking something the faster it will perform at. Testing and benchmarking shows that overclocking DOES increase system performance. Anyway back to the subject, the faster you can clock a GF2's memory clock and core engine clock the better.

To measure the temperature of the card we used a excellent piece of software from ASUS, called SmartDoctor which was provided with our GF2. With both the fans we mentioned above working in tandem we managed to have our ASUS v7700 GF2 running @ 20 degrees Celsius (68 degrees Fahrenheit). When overclocking, aim to have your GF2 running no higher then 30 degrees Celsius (78 degrees Fahrenheit). Aim to cool your g-force card eg The Card Cooler or Global Win CAF12. With The Card Cooler and the Global Win CAF12 turned OFF the GPU temperature was 26 degrees Celsius (74 degrees Fahrenheit) remember ASUS SmartDoctor has built in software cooling (similar to CPU Cooling Software) where when the card is not in use, SmartDoctor halts the card thus cooling it down. As I said earlier in this GF2 Over-clocking Guide - the cooler you can run your GF2 at the better you'll be able to overclock it.

Cooling

Now this can be where Vid Card OverClocking can really get to be time consuming, but it can also be a ton of fun! When we push up the MHz levels of the core and memory, they are doing more work than they were before. This also means that they might possibly be generating more heat. By removing some of the heat efficiently, we will sometimes produce an environment that will allow us to OverClock our card higher or maybe give an artifact free image. The cooling part is something that is being taken into account by major players in the graphics board market. I think they have followed the hardware community's lead on cooling. Some of them are doing it while making it look good also! A cooler card is generally going to mean that you will have a more stable card and possibly a card that you can OverClock even further successfully than you could in its stock state. Good coolers are the Card Cooler or Global Win CAF12. Fitting a blueorb fan in replacement of your old video card fan will also make a difference. The cooler you can run your GF2 at the better you'll be able to overclock it.

Tools you need

Instead of using the ASUS Tweaking utilities which was provided with our card, we will use either some simple registry settings and/or an industry standard program called PowerStrip. Here is a list of the stuff you'll need to successfully overclock your GF2.

- Ensure GF2 has a working heatsink fan w/ thermal paste
- Consider extra cooling - eg The Card Cooler or Global Win CAF12 and a BlueOrb
- Common sense - Don't push the GF2 too far

Lets start

Now the first thing you are going to want to do is download and install the most recent drivers off Nvidias website
www.nvidia.com/Products.nsf/htmlmedia/detonator3.html
These drivers are backwards compatible and work with just about any Nvidia card. You also want to make sure that you have the very latest DirectX installed on your system - at the time of writing the latest version was DirectX 8a and I have personally seen a 5/10% increase when using DirectX 9.
www.microsoft.com/directx/homeuser/downloads/default.asp
(I have ommitted 3dfx from this article now because Nvidia cards have took over the reign and are a superb chipset. You can overclock them using Powerstrip software though).

Add coolbits entry to your registry and overclock

copy & paste the text below in Notepad to create a REG file, and save it for example as GeForce.REG, making sure when you goto save in notepad you change the save as type to all files and then run it. Remember to restart Windows after each change.

```
-----Begin cut & paste here-----
REGEDIT4

[HKEY_LOCAL_MACHINE\Software\NVIDIA Corporation\Global\NVTweak]
"CoolBits"=dword:00000003
------End cut & paste here------
```

When we run the above files below to edit the registry, they are going to change the values of certain keys that will allow us to use the factory OverClocking Utilities that come from nvidia. Funny thing is that overclocking and tweaking have gotten so popular that both companies include the utilities to overclock in their driver set. They are just hidden "Easter Eggs" though. Once you learn the secret to the eggs, all is unlocked.

Now once we have rebooted our box, we will want to put our new tools to work. First off, right click the desktop and select "Properties" from the menu. Then select the "Settings" tab. At that point you will see a button labeled "Advanced..." appear. With a nvidia card we have a couple of extra steps along the way. After the "Advanced" button, you will now select the icon tab with the name of your card on it. You should then be faced with a spinning nvidia logo. Now click on the "Additional Properties" button and then the "Hardware Options" tab. Whew! We are finally here. With either type of card you will now be faced with a slider type menu. The nvidia will have two different sliders. If you have an nvidia card you will notice an extra tab called 'Hardware Options' has appeared if the registry entries above have been entered into the registry. If you have not got this tab then you have an Nvidia driver that has the coolbit switched off and is not a problem - just download and install Powerstrip (link further below) and use the same method as explained next but in Powerstrip.

Now at this point all overClocking your Vid Card requires is moving the sliders to a higher number. This is where the fun really comes in, as some folks can move their sliders farther than others and this builds a whole community based on the competition of seeing who can do it faster. Now is the fun part, using the bar drag the Memory Clock bar to the right in 5MHz increments. Progressive overclocking has to do with the process of slowly clocking your system faster and faster until it reaches its peak stable speed. This is frequently done with video card overclocks, because it is very easy to over do it and fry the card. The process with video cards is very easy - you simply overclock in 5 MHz increments until you reach an unstable speed, and then downclock the card in 1 MHz increments until you reach a stable speed.

Then of course comes the obligatory testing to determine whether or not the card is stable even during system strain - and if it passes, you're gold. Once you have dragged the bar over so it is 5MHz higher, click Apply, then ok. If everything looks fine (eg no weird lines, colors, appearances on screen) Click Ok to confirm changes. Congratulations! You have overclocked a GF2... If you only have stock cooling (eg no new cooling gear) don't push the Memory Clock any higher then **350MHz** or CPU Engine Clock any higher then **230MHz**.

If you have extra cooling you can try to push your card a little higher. If your card is running fine (no crashes) at 350MHz Memory Clock try increase to MHz by 20 to 370MHz. Now trying pushing the Engine Clock to 250MHz. After you have applied those settings, and everything is fine (eg no weird lines, colors, appearances on screen) feel free to keep those overclocked settings. Although I'd suggest that you don't have your GF2 overclocked all the time, especially on hot days. Give it a break now and then...

OTHER PROGRAMS FOR GFX CARD OVERCLOCKING

Asus tweaking utility

was suprising to see that manufactures are actually including programs to overclock their products, I thought I'd never see this. I find this program easier and more reassuring to use because the maker of the GF2 made the program. This program uses the same principal as all you need to do is drag the bars left or right, although with this program you can change in 1MHz increments...

DXdiag

One of the cool things that some people don't know about is dxdiag. From the start menu, choose the 'run' option and type in dxdiag. You can troubleshoot almost everything with this applet. Also, most importantly, you can adjust the refresh rate at which DX runs. So you can play those DX games at 80Hz+.

Powerstrip

Powerstrip is a very good program and basically lets you overclock your gfx card. Its basically the same way as the coolbits tweak above. The advantage of Powerstrip is that it will let you overclock all Nvidia cards whilst some drivers from Nvidia do not enable the overclocking option with the coolbits tweak.
http://www.entechtaiwan.com/ps.htm

BENCHMARKING FOR GFX CARDS ETC

Benchmarks allow you to measure your performance increases. By changing my GPU engline clock from 200mhz to 220 mhz and my memory clock from 333mhz to 364mhz I achieved an extra 3 frames per second on Quake 3 timedemo which was in a high resolution. This is only a slight overclock and it is indeed faster. The faster you clock the GPU and memory clock the faster your card will perform.

3dmark 2001
3dmark allows you to not only score the performance of your card and entire system, but you can also upload your scores to a worldwide database so that you can show your scores off. Really fun stuff for tweakers. Benchmarking your system can also be done with simply applying games that you might already own.
www.madonion.com/download/

Nvnews
NVnews site has a great guide that explains how to accomplish some of this benchmarking with specific games.
www.nvnews.net/articles/benchmarking.shtml

Quake 3 test
Quake 3 is probably the most widely used OpenGL benchmark in the world.
www.3dfiles.com

Ziff Davis benchmarking utilities
Other good benchmarking programs such as Winstone, Winbench, 3d Winbench etc, etc -
www.zdnet.com/etestinglabs/filters/benchmarks/

SYSTEM STABILITY TESTING

If you're an overclocking vet, you've probably heard of this process called "burning in", or perhaps you've even burned in a CPU yourself. But does it do anything?
Some may disagree with me here, but I have yet to see a benefit from burning in a CPU. So what is burning in?
Well, my understanding of the process is:
- Find the highest rock solid speed for the CPU.
- Set the voltage slightly higher than needed.
- Run the system as you normally would (at this solid speed) for a given period of time (2 days to a week).
- Try to set the CPU at a higher speed.

CPU 'Burn-in' is an ideal utility for burn-in tests; it's available here: http://users.bigpond.net.au/cpuburn/
Some people claim to gain several MHz using this method. There are generally two types of testing that I perform on a newly overclocked system. One is an intensive integer/FPU test which keeps processor utilization up between 95 & 100% for upwards of a half an hour. If the CPU passes this test, the overclock on the CPU itself is stable. However, even if the system passes that test, I still run a gaming test. The gaming test determines how well the rest of the system responded to the overclock (this is particularly important when dealing with non-standard bus speeds and out-of-spec RAM. Another test that I recommend, if you own the software, is the SiSoft Sandra benchmarks, or alternatively, WinBench 2000. Both pieces of software do subsystem specific testing - something that can be very important, particularly if you are trying to determine which pieces of hardware within your system are causing a failed overclock.

The intensive integer/FPU test is aptly named Stability Test and can be downloaded at www.tweakfiles.com. To use this test, you need to configure it before you overclock. This test will not only keep CPU utilization up at 100%, it will also make sure that the system isn't making any mistakes. This test only takes about a half an hour to complete and is definitely worth the time. If your computer doesn't pass this test, first try to either add more cooling or up the chip voltage a little bit and see if it works - otherwise drop down to the troubleshooting section for a few tips. The second test consists of either using Unreal in Flyby mode with everything turned on (OpenGL), or using 3Dmark 2000 in loop mode (D3D). You really should only use 3Dmark 2000 if your system's OpenGL drivers are less than satisfactory. If you don't have a copy of Unreal, but your computer has a robust OpenGL driver, another alternative would be to use the Q3 demo with xero's 'monkeycrusher' demo. If your system passes both the integer and gaming tests, you have got yourself a stable system. Congrats.

RELATED SOFTWARE

I would not advise you run any cpu cooling software on Windows NT. 2000 or XP as it is not needed - you can however run Motherboard Monitor and Hardware Monitor. There are some CPU cooling programs (CpuIdle, Rain, Waterfall) that claim to lower CPU temperature by up to 30°. These programs can tell when the processor is not busy and put it in sleep mode during the idle time. While using the programs, the processor draws a lot less power and runs much cooler, however they are not very useful in CPU intensive environment, like playing games or defragmenting your HD. Another drawback is the fact that temperature fluctuates much more, based on CPU use. If you'd like more info on the performance of the "cool" programs, try The TX Board at
www.angelfire.com/va/txboard/index.html

Motherboard Monitor - www.euronet.nl/users/darkside/mbmonitor/
Hardware Monitor - www.hmonitor.com/

TROUBLESHOOTING

To do this kind of troubleshooting, your computer has to be booted into Windows. If it isn't, take the steps outlined above to increase the stability of your system. Once you are in Windows, you will need to either install a copy of SiSoft Sandra or Winbench 2000. Then take each of the subsystem tests and run them separately from each other. Make note of which subsystem tests cause the system to crash, and focus on those parts of the system. That may mean adding a hard drive fan, some RAM cooling, etc. Once you have focused on all of the parts of the system that cause a crash (this may include the processor itself as well), go back and go through the system stability tests once again. If you can't get the system to pass the tests now, you may need to go back and lower the speed of the processor.

If you still refuse to give up on your 'golden' speed, however, you may want to try the following things:
- Leave your computer's case open
- Put your computer closer to your air conditioner
- Move your computer farther away from any heating ducts
- Make sure the computer has at least 6" of breathing room (15 cm) between it and anything else.
- Put the computer closer to the floor and farther away from anything that creates heat
  (your subwoofer, monitor, etc)

Now that I've addressed a few issues, let's get into the gist of things. Since you are in fact reading this guide, I'm guessing you are looking for a solution to an overclocking problem you're having. You can't get into Windows? Your PC flashes up random BSODs (Blue Screens of Death)? Your PC can't get past the BIOS? Your PC doesn't turn on when you overclock? I'm simply going to try to help you solve the some of the most common problems. Once you've decided on the problem, read on into the guide for tips on that specific issue. Your operating system (Windows, usually) crashes after a period of time (several minutes or more), without running any extremely intensive programs: If you didn't run any intensive programs, this is most likely a heat issue. Consider lowering the voltage (unless it means sacrificing stability) or better cooling. Read on...

Operating system crashes immediately after a certain intensive program is run:
If a single game or program crashes your PC immediately after it has been launched, this is usually a sign of a few possible problems. The issue is most likely the CPU itself, but it could be the memory. The CPU is overclocked beyond its limit with the supplied voltage, or the CPU simply cannot go that fast (eek!). Try increasing the voltage as long as it's in the "safe" range. Generally a CPU can withstand a .2 or .3 volt increase (over default) for long periods of time. I generally don't recommend going higher than .3 over the default voltage.

If you're sure it's not the CPU, check to see the speed rating of the RAM in your system. 10 ns SDRAM (PC66) should be good up to around 100 MHz FSB. 8 ns SDRAM (most PC100) should be good up to around 125 MHz FSB. 7 ns SDRAM or faster should be good beyond 133 MHz FSB. Anything beyond those values could result in problems from the memory. Another thing to try would be to set the CAS latency in the BIOS setup to 3 instead of 2 (CAS latency determines how much time the computer allows the RAM to recover between 'column' access). This could solve the problem.

Your pc doesn't even turn on
(maybe it turns on, but the monitor doesn't receive a signal) once it's been overclocked, or it can't get past BIOS:
This is one of the most frustrating problems for newbies, because they seem to think their PC is toast when it won't respond to the keyboard or it won't even display video. But hey, we all learn the hard way when it comes to these sorts of problems. To recover the original clock speed, you'll need to do one of the following:
1. Find the jumper on your motherboard that resets the CMOS configuration
2. Find the key on the keyboard that resets the clock speed, or
3. Re-jumper the CPU for a more stable speed on the motherboard or slocket. If you need to find the key or the jumper that resets the clock speed (usually for software CPU configuration), consult the manual. This is different on just about every motherboard.

Now that you know how to fix the problem by returning to default values, you probably want to know how to make the old value stable, right? Well, if it doesn't even receive a video signal, it could be either the CPU is not getting enough voltage (remember, .2 or .3 volts over the default is about the maximum I recommend), or the memory may not be up to it. Make sure your memory can handle such a high FSB speed on another PC if possible. Heat probably isn't an issue at this point since this is immediately after you start the PC.

CHAPTER [11]

CONCLUSION

By now you should have successfully optimised your system. You should notice less hard drive accessing, improved memory subsystem performance and a major speed increase overall ! I've seen some people spend hours and days fine tuning their hardware but their operating system is a mess. They have unnecessary utilities and monitoring tools running in the background. These utilities take a toll on CPU cycles and ultimately slow down your souped up computer.

Spreading knowledge of overclocking techniques requires a group effort. If you want to learn as much as you possibly can, you should certainly read articles and books on PC architecture and optimization, but beyond that you should frequent the forums which are listed in the tweaking and overclocking sites. Overclockers have created a strong and welcoming community. Its members take even the greenest newbies seriously. If you ask an intelligent question you'll often not only receive a bevy of answers and suggestions, but you'll also spawn an insightful discussion of the matter.

Hope you've learned a few things along the way. Email me new tips if you want...

Best Regards,

Paul Brown
x9000@techie.com

--