Windows XP:
Basic Configuration & FAQ

Central Services IT (CS-IT)

UNIVERSITY OF CAMBRIDGE

Department of Physics

E-mail: itdept@phy.cam.ac.uk

Last updated: 21 March 2002
Revision: 1

Introduction

At the time this document is being drafted, Windows XP is a fairly new and exciting operating system. It offers a new style of interface, new accessory software (Internet Explorer 6) and greater scope for functionality (The ability to co-operate and coexist with Unix systems on the network)
It also, however, introduces new security and administrative problems for the inexperienced administrators unless you are aware of what they are, where to find them and how to switch them off.

Purpose

This document is not a "how to use …", but it contains basic administration guidelines for how to disable services that make the machine potentially insecure and reduce the effect your new machines have on others in the same domain or workgroup within the Cavendish Laboratory.

Scope

Anyone that is or has become a Windows 2000 workstation administrator should be aware of basic requirements to ensure the most basic security and ease of use. These skills will be invaluable to you when administering and using Windows XP.
In order to help with that this document is separated into three basic sections;

- Configuration for inexperienced administrators,
- Configuration for more experienced administrators,
- Frequently Asked Questions / concerns demonstrated by new users

This document does assume that you are using Windows XP professional and not Windows XP home edition.
Although the majority of this document refers to a windows XP machine connected to a domain, occasionally it will provide assistance to those machines that are standalone (only connected to the network for internet access.

Overview

Windows XP installations may come with certain services / operations switched on. The combination of these can make the machine potentially unsafe in the Cavendish Network environment, with regard to security and the functionality of the network itself. These services may inc lude (tick those you think you may require):-

■ Found in Service Manager (see below)
□ DHCP Client
□ FTP Publishing Services
□ IIS administration
□ Remote Registry Management
□ RIP Listener
□ SNMP Services
□ Telnet
□
■ Found within other parts of the system
□ IPSEC (Section 3)
□ Master Browsing (Section 1)

Note: If you don't know what they are or don't specifically use them … don't run them, if you *do* then use them with care as they differ from other Windows implementations.

Turning off unnecessary services will increase the speed at which your machine runs. Less load is being put on the system to run unused products.

As Microsoft bring out service packs and security hotfixes, and implement these on their default installations of the operating systems, you may notice that some of the listed services are not there or not active. Do not fret. It is just one less thing for you to have to secure.

However, if you are in any doubt as to whether or not a service should be running, consulting a member of the IT support team before you proceed would not be frowned upon.

Starting up as an administrator
When you install Windows XP (Win XP from now on), or remove your brand new company built machine and turn it on for the first time, you will be asked to put in a password for the Administrator. Obviously *do not forget this password!*
You will be prompted to add a user. If you add one username at this time, Win XP will automatically log that username in every time by default.
If however, you add a second username at this time, it will prompt you to choose a user to log in as.

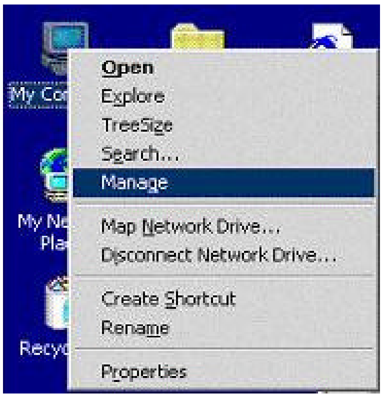
The first local user created *is* a member of the administrators group, any other users created are un the user group by default

If you are making the machine part of a domain, then you will be prompted for a logon name and password.

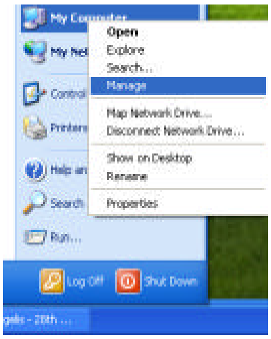
No matter which way you configure your machine; if you try and perform a procedure that requires administrator privileges you will be prompted to supply an administrator user name and password, should you not have the necessary rights.

Computer Management / Administration tools

As opposed to Windows 2K where the administration tools were placed on a Single-right-click on "My Computer" to get the following dialog box; which allows you to open the management console.



Windows XP is similar to this, but "My computer" is no longer on the desktop by default. Now you have my computer on the "start menu".



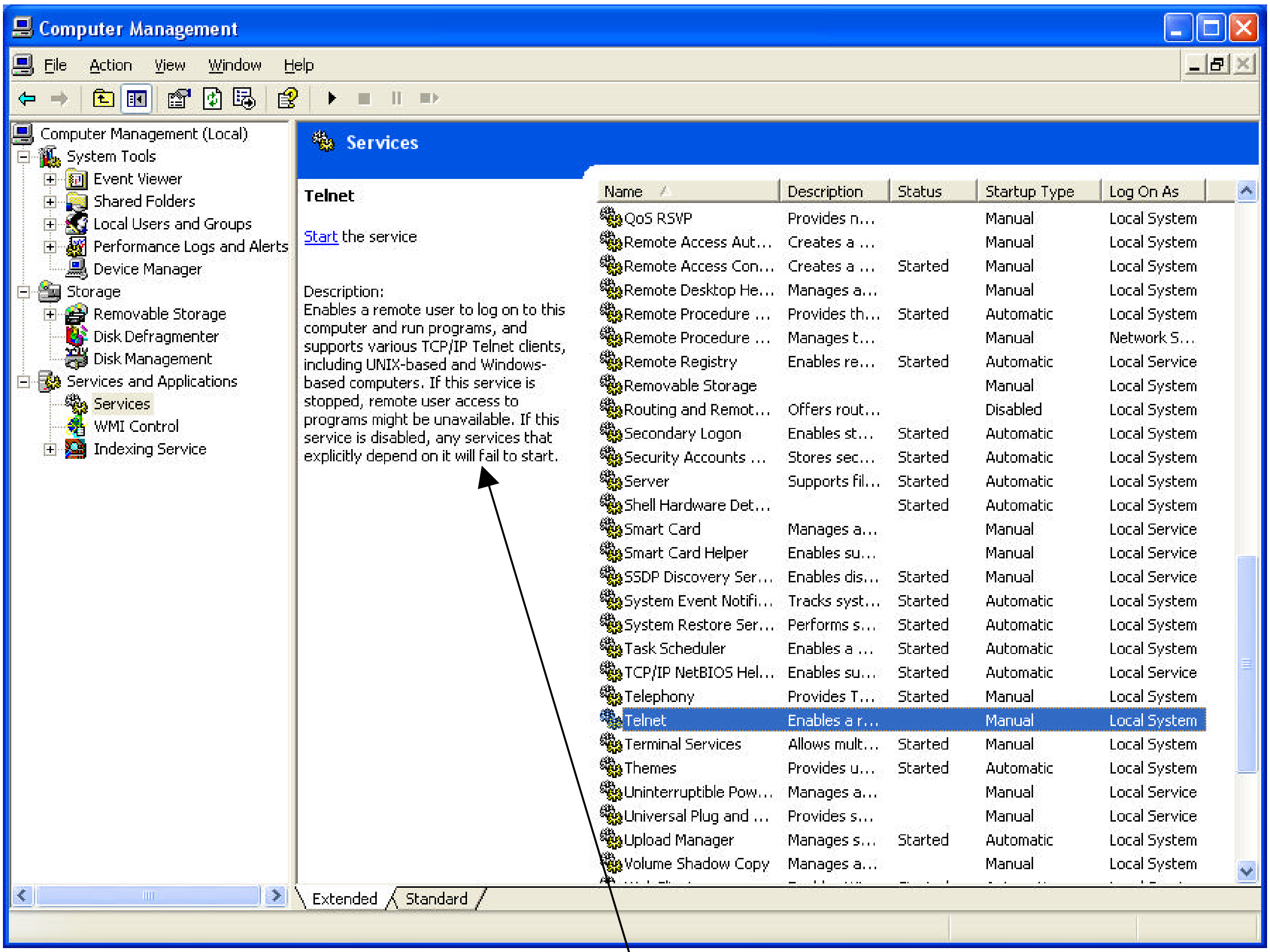
Those of you familiar to Win 2K will recognize the familiar console.
Aside from some minor cosmetics, the console is and works identically.

From here you can control all general administration of your machine. Probably the most important are the "Services" and "Event Viewer". All others are *interesting viewing* but not necessary to administration. If you are running an Internet Information Server (a WEB server or IIS) you will see the bottom option "Internet Information Services" aka **IIS version 5**. Handle this with extreme care. Rules of thumb;

- inspect your logs on a regular basis
- ensure you are up-to-date on service packs and "Hotfixes"
- "if you don't need it switch it off"

Services

From the "Computer Manager" single-click on "Services" and you will be presented with the following screen. From here you can control the services (including those mentioned above as those lending themselves to potential vulnerabilities).



Telnet

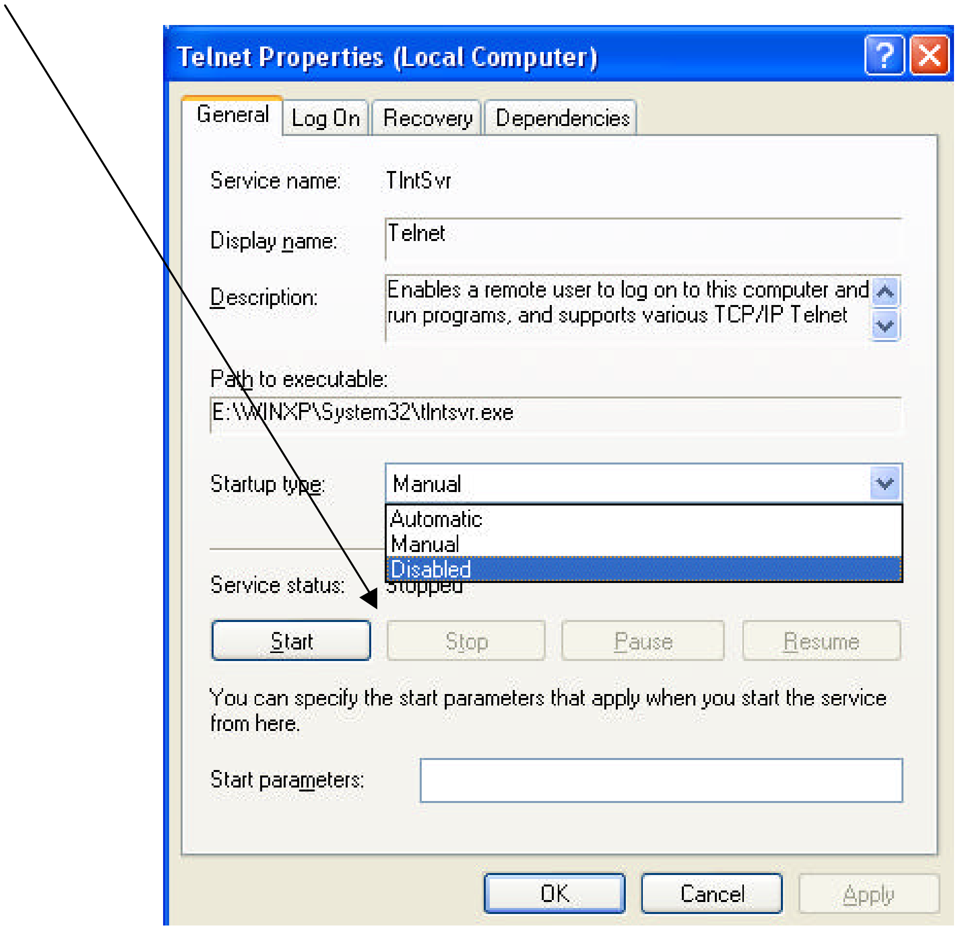
Start the service

Description:
Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet clients, including UNIX-based and Windows-based computers. If this service is stopped, remote user access to programs might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
QoS RSVP	Provides n...		Manual	Local System
Remote Access Aut...	Creates a ...		Manual	Local System
Remote Access Con...	Creates a ...	Started	Manual	Local System
Remote Desktop He...	Manages a...		Manual	Local System
Remote Procedure ...	Provides th...	Started	Automatic	Local System
Remote Procedure ...	Manages t...		Manual	Network S...
Remote Registry	Enables re...	Started	Automatic	Local Service
Removable Storage			Manual	Local System
Routing and Remot...	Offers rout...		Disabled	Local System
Secondary Logon	Enables st...	Started	Automatic	Local System
Security Accounts ...	Stores sec...	Started	Automatic	Local System
Server	Supports fil...	Started	Automatic	Local System
Shell Hardware Det...		Started	Automatic	Local System
Smart Card	Manages a...		Manual	Local Service
Smart Card Helper	Enables su...		Manual	Local Service
SSDP Discovery Ser...	Enables dis...	Started	Manual	Local Service
System Event Notifi...	Tracks syst...	Started	Automatic	Local System
System Restore Ser...	Performs s...	Started	Automatic	Local System
Task Scheduler	Enables a ...	Started	Automatic	Local System
TCP/IP NetBIOS Hel...	Enables su...	Started	Automatic	Local Service
Telephony	Provides T...	Started	Manual	Local System
Telnet	Enables a r...		Manual	Local System
Terminal Services	Allows mult...	Started	Manual	Local System
Themes	Provides u...	Started	Automatic	Local System
Uninterruptible Pow...	Manages a...		Manual	Local Service
Universal Plug and ...	Provides s...		Manual	Local Service
Upload Manager	Manages s...	Started	Automatic	Local System
Volume Shadow Copy	Manages a...		Manual	Local System

Notice that in the "extended" view, a brief description appears to the left of the "services" window. You may also make use of a convenient link to start, pause or stop the service.

A rule-of-thumb recommendation would be to disable all the aforementioned services. Single-right-click on the service and select “Properties”. When presented with the following dialog box.
Select “Disabled” from the “Startup type:” drop-down list then click on “OK”
If the service is already started, you will need to stop it, even if you have just disabled it. Clicking on the “Stop” button contained within this window can do this.



Telnet Properties (Local Computer)

Service name: TlntSvr

Display name: Telnet

Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet

Path to executable:
E:\WINXP\System32\tlntsvr.exe

Startup type: Manual

Automatic
Manual
Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

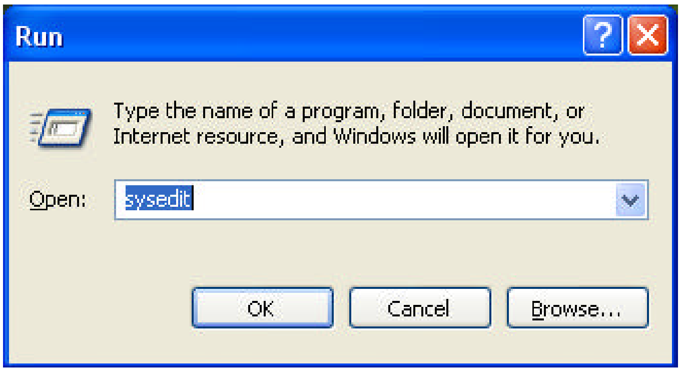
Basic administration: potential mis-configurations

Switch off “Master Browsing”

1. For the inexperienced administrator:

1.a. Click “Start” then select “Run” from the menu.

1.b. In the text-box type “SYSEDIT” and then click on “OK” or press “Enter”[1].



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: sysedit

1.c. Click on the window entitled “`C:\WINNT\SYSTEM.INI`” (this title may– but should not – differ, as long you select the “SYSTEM.INI” file).

1.d. At the top of the file add the following line:

```
MaintainServerList=No
```

If the line already exists make sure it reads as above.

1.e. Close the file and click on “`Yes`” when prompted to save the changes to the SYSTEM.INI file. If prompted to save changes to other files select “No” – unless you are aware of deliberately making changes.

You will need to re-boot the machine for the changes to take effect.

[1] You may get a popup error saying there is no CONFIG.SYS or AUTOEXEC.BAT ; these can be ignored so click “O.K.”

2. For the experienced administrator:

2.a. Go to the registry hive

```
HKEY_LOCAL_MACHINE
    \SYSTEM
            \CurrentControlSet
                    \Services
                            \Browser
                                    \Parameters
```

2.b. Alter (or add) the key value[2] of `MaintainServerList` as follows:-

```
MaintainServerList      Reg_Sz     Auto
```

to be

```
MaintainServerList      Reg_Sz     No
```

2.c. Close REGEDIT (using “REGISTRY” menu, “Exit”)

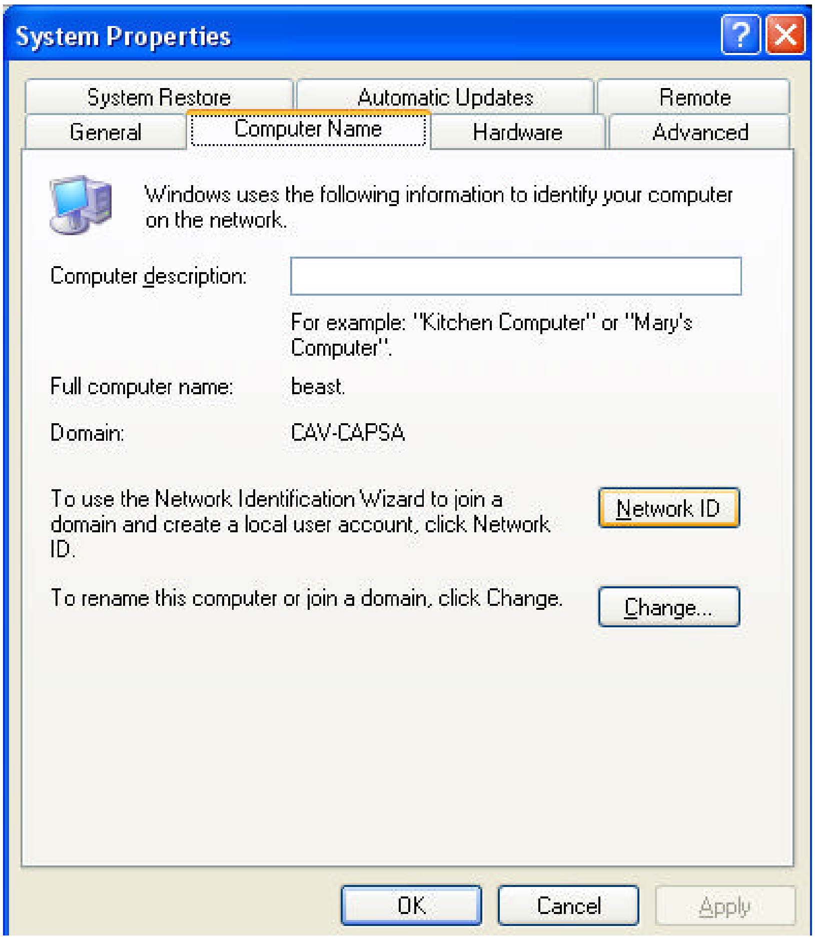
Note: REGEDIT *does not* ask to save changes … they are made instantly so edit with care !!!

[2] Double-click on the item name in the right hand window; delete the current “Value data” and replace it with the required one. Regard the value as case-sensitive!!!

3. Basic administrative maintenance – Hints & Tips and FAQs

3.a. "How do I change my computer name?"

Network identification details can be found by RIGHT-clicking on "My Computer", then clicking "Properties". Under the "Computer Name" you will now see the necessary buttons to change your name and domain[3].



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: beast.

Domain: CAV-CAPSA

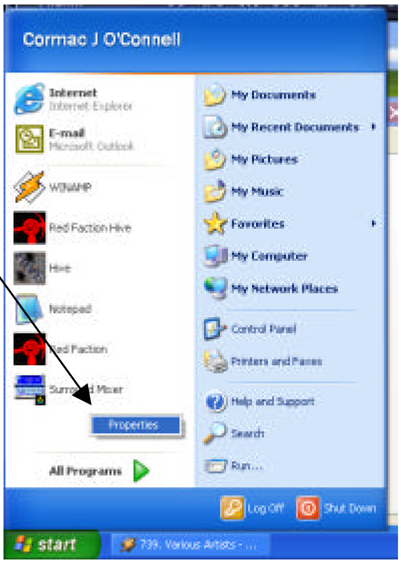
To use the Network Identification Wizard to join a domain and create a local user account, click Network ID.

To rename this computer or join a domain, click Change.

[3] Please note – if the machine is part of a domain rather than a workgroup, the domain systems administrator will have to re-add the machine to the domain and the UCS IP-register must be informed of ***any*** change (e-mail cav-ipregister@phy.cam.ac.uk).

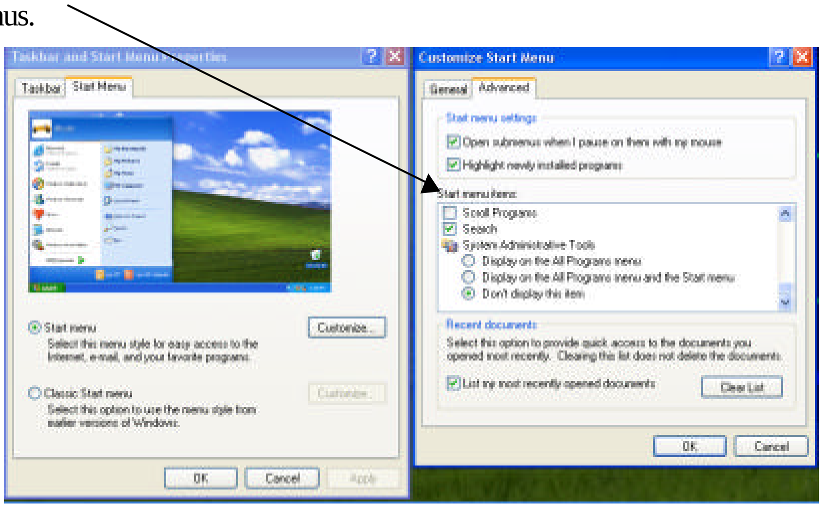
3.b. “Where are my administrative tools?”

Click “Start”, then right click in a blank area of the start menu. You should now be able to left click on “properties”.



This will bring up a window entitled “Taskbar and Start Menu Properties”. Click on the “Start menu” tab and there you will see a check box for “c ustomize”.

This will bring up a second window. Under the advanced tab, there is the option to add/remove various group menus.



● Start menu
Select this menu style for easy access to the Internet, e-mail, and your favorite programs.

○ Classic Start menu
Select this option to use the menu style from earlier versions of Windows.

Start menu settings

☑ Open submenus when I pause on them with my mouse

☑ Highlight newly installed programs

Start menu items:

☐ Scroll Programs

☑ Search

System Administrative Tools

○ Display on the All Programs menu

○ Display on the All Programs menu and the Start menu

● Don't display this item

Recent documents

Select this option to provide quick access to the documents you opened most recently. Clearing this list does not delete the documents.

☑ List my most recently opened documents

To ensure that during normal operation, administrative tools are not invoked by mistake, by default these tools are hidden from the start menu - even as an administrator.
Although the majority of the tools required on a daily basis are contained within the management console.

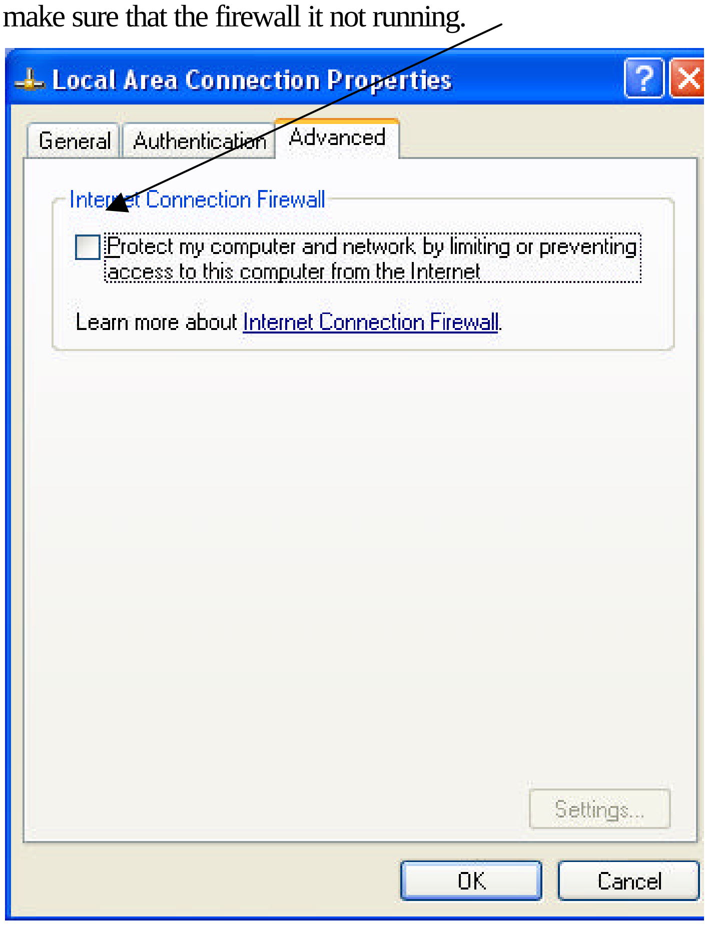
3.c. “Encryption on network transmissions, and network security”

IPSec or IP Security (To the best of our knowledge) can only run properly on a Windows 2000 network. The computer must also be fitted with an Ipsec capable network adaptor. This is a card that has a processor on board to decrypt the transmissions, and apparently they are expensive.

They appear to have dropped IPSec from Win XP in favour of a personal firewall.

It is the opinion of the author, that if you know enough about firewalls to use them, then you know enough to run a system that is secure enough not to require a firewall. If you do not know enough about firewalls, then you have no place running one.

Either way, you should make sure that the firewall it not running.



Internet Connection Firewall

□ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

3.d. “My computer is taking a long time to logon to the network!”

If you are having problems with the amount of time it takes to log on to the network, then chances are that the machines on the network are having “Arguments” with each other as to who is going to be what is known as the “Master Browser”. This is one machine that holds the list of all the machines on its segment of the network. In the NT environment it is/was normally the Server that was given this task, unless it was told otherwise. With XP by default, any machine is set to be the Master Browser.

To prevent this from happening there are 2 ways to fix this. Refer to the section 1 and 2 for details.

Alternatively, if you have a mixed NT/2000 network, and you are running roaming profiles, you may be waiting for your profile to be converted from NT 4 to 2000.

You can fix this by either having 2 login names (One for NT and one for 2000) or if you only use one 2000 machine you can turn off the roaming profiles on that machine. This means that you will not get the same appearance but you will find that your login delay should be fixed.