NavLabs NTP Service Installation and Configuration

Version: 1.01
May 4, 2010

Table of Contents

Introduction

The NavLabs GPS simulator can be equipped to provide a Network Time Protocol (NTP) Server service that accurately reports the simulation time. This document describes the steps to install and configure the service. The NTP server runs as a service in daemon mode and must be installed accordingly. The NTP service is built from the Open source NTP project that is maintained by a group of volunteers and adheres to the Network Time Protocol that is maintained by the IETF NTP Working Group. This organization maintains a number of clock sources and as such the build product requires configuration for any particular implementation.

Once the service is installed and configured, the NavLabs simulation will control the service, starting and stopping it as required to properly function with the NavLabs simulation environment.

Installation

Three files are required to run the service. Other than the ntp.conf file, there is no particular location requirement for the installation of these files. It is recommended that an 'ntp' folder be created as a subdirectory of the 'Voyager' folder.

Distribution files

ntpd.exe	- The NTP daemon
instsrv.exe	- An executable file that installs ntpd as a service
ntp.conf	- The NTP configuration file

Installation Procedure

The recommended procedure is to create the directory: "Voyager\ntp" and put the three distribution files into the "ntp" folder.

To install the NTP service, run the 'instsrv.exe' application from a command shell.
Instsrv.exe Installs or removes the NTP service.
To install the NTP service, type:

```
INSTSRV <path>
```

Where:

path is the absolute path to the NTP service, name.exe. You must use a fully qualified path and the drive letter must be for a fixed, local drive.

For example, `INSTSRV c:\Voyager\ntp\ntpd.exe`

To remove the NTP service, type `INSTSRV remove`

Configuration

The NTP service will look for the ntp.conf file in a few places, however it is recommended that the ntp.conf file be placed in the 'etc' folder of your Windows boot drive, most likely here:

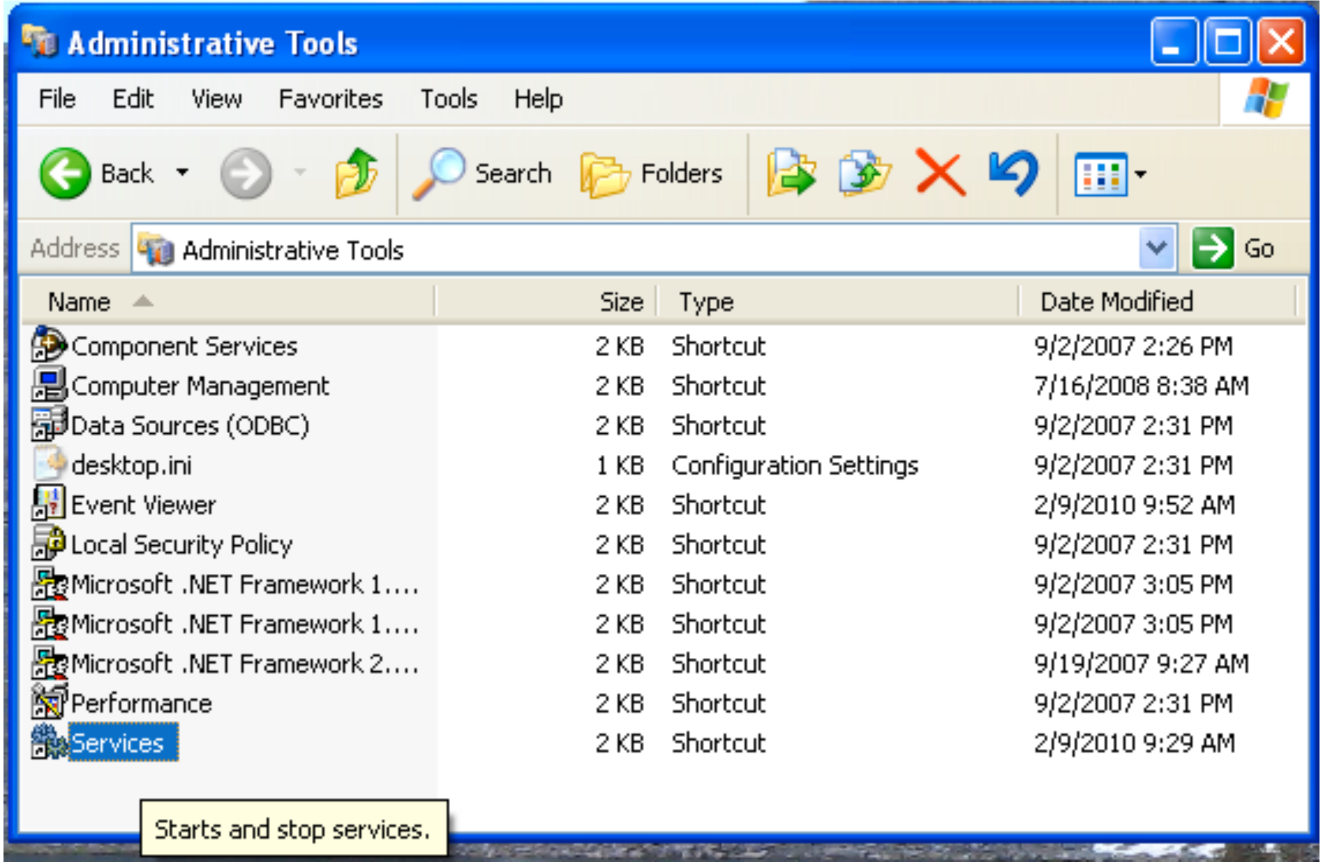
```
<bootDrive>:\Windows\System32\drivers\etc
```

'ntp.conf' must contain the following lines:

```
server 127.127.45.1   #NavLabs Simulator Clock value = 45, device = 1
#
broadcast  224.0.1.1 autokey     #multicast
broadcast  128.4.1.255 autokey   #local subnet broadcast
```

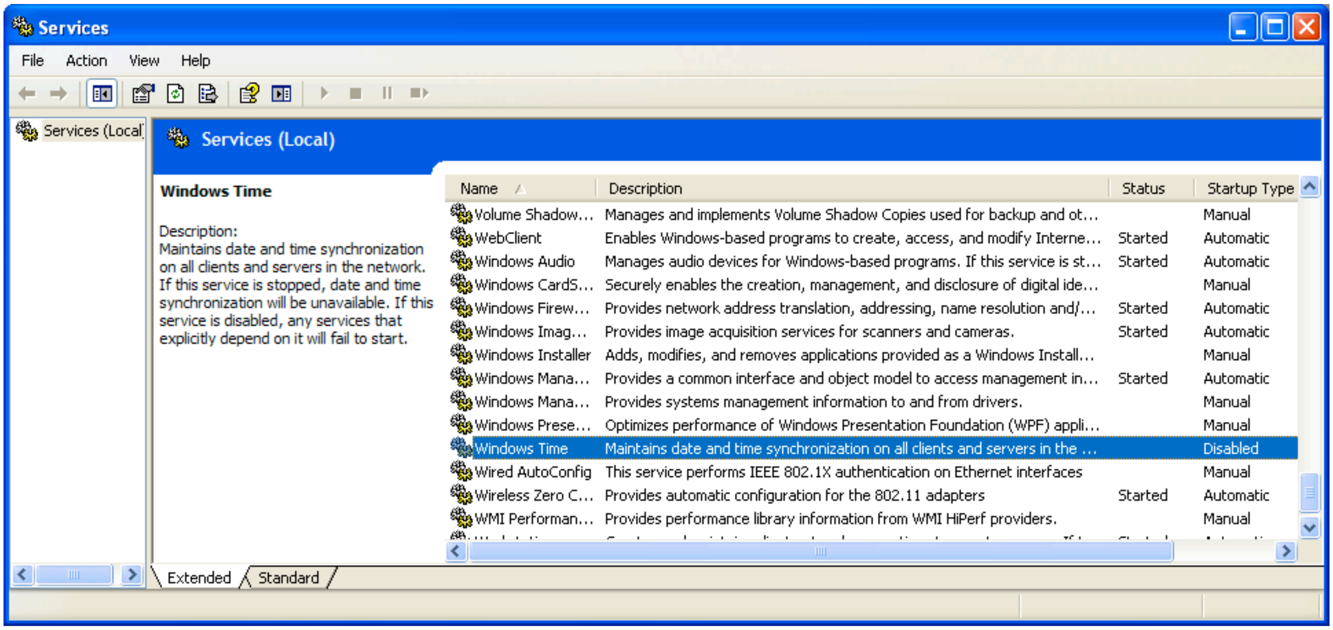
Turn off the Windows NTP Service:

From the control panel open the 'Administrative Tools', then open the 'Services' application. Scroll down to find the Windows Time Service. Double click this to open a dialog box that will allow you to manipulate this service. Click the 'Stop' button to stop the service. Ensure that subsequent system restarts does not start this service; set the 'Startup Type' to 'Disabled'. This sequence is illustrated below.



Name	Size	Type	Date Modified
Component Services	2 KB	Shortcut	9/2/2007 2:26 PM
Computer Management	2 KB	Shortcut	7/16/2008 8:38 AM
Data Sources (ODBC)	2 KB	Shortcut	9/2/2007 2:31 PM
desktop.ini	1 KB	Configuration Settings	9/2/2007 2:31 PM
Event Viewer	2 KB	Shortcut	2/9/2010 9:52 AM
Local Security Policy	2 KB	Shortcut	9/2/2007 2:31 PM
Microsoft .NET Framework 1....	2 KB	Shortcut	9/2/2007 3:05 PM
Microsoft .NET Framework 1....	2 KB	Shortcut	9/2/2007 3:05 PM
Microsoft .NET Framework 2....	2 KB	Shortcut	9/19/2007 9:27 AM
Performance	2 KB	Shortcut	9/2/2007 2:31 PM
Services	2 KB	Shortcut	2/9/2010 9:29 AM

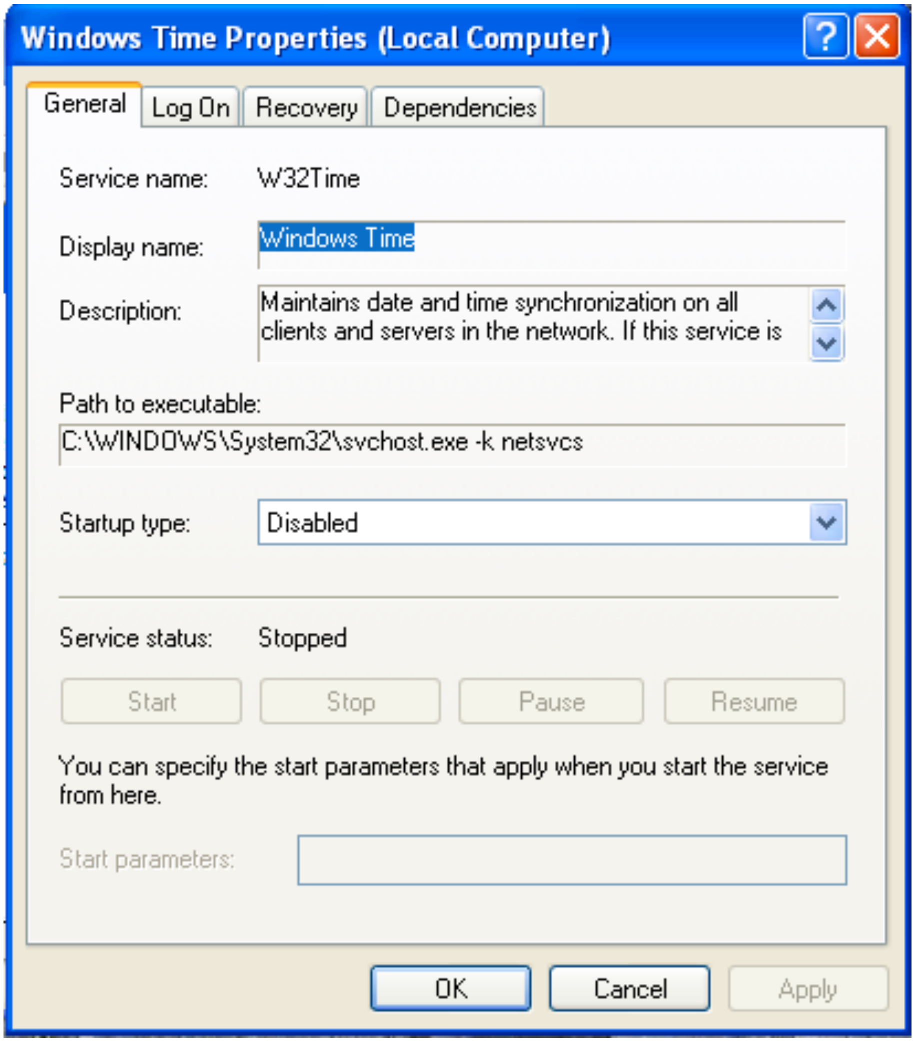
Starts and stop services.



Windows Time

Description:
Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type
Volume Shadow...	Manages and implements Volume Shadow Copies used for backup and ot...		Manual
WebClient	Enables Windows-based programs to create, access, and modify Interne...	Started	Automatic
Windows Audio	Manages audio devices for Windows-based programs. If this service is st...	Started	Automatic
Windows CardS...	Securely enables the creation, management, and disclosure of digital ide...		Manual
Windows Firew...	Provides network address translation, addressing, name resolution and/...	Started	Automatic
Windows Imag...	Provides image acquisition services for scanners and cameras.	Started	Automatic
Windows Installer	Adds, modifies, and removes applications provided as a Windows Install...		Manual
Windows Mana...	Provides a common interface and object model to access management in...	Started	Automatic
Windows Mana...	Provides systems management information to and from drivers.		Manual
Windows Prese...	Optimizes performance of Windows Presentation Foundation (WPF) appli...		Manual
Windows Time	Maintains date and time synchronization on all clients and servers in the ...		Disabled
Wired AutoConfig	This service performs IEEE 802.1X authentication on Ethernet interfaces		Manual
Wireless Zero C...	Provides automatic configuration for the 802.11 adapters	Started	Automatic
WMI Performan...	Provides performance library information from WMI HiPerf providers.		Manual



Service name: W32Time

Display name: Windows Time

Description: Maintains date and time synchronization on all clients and servers in the network. If this service is

Path to executable:
C:\WINDOWS\System32\svchost.exe -k netsvcs

Startup type: Disabled

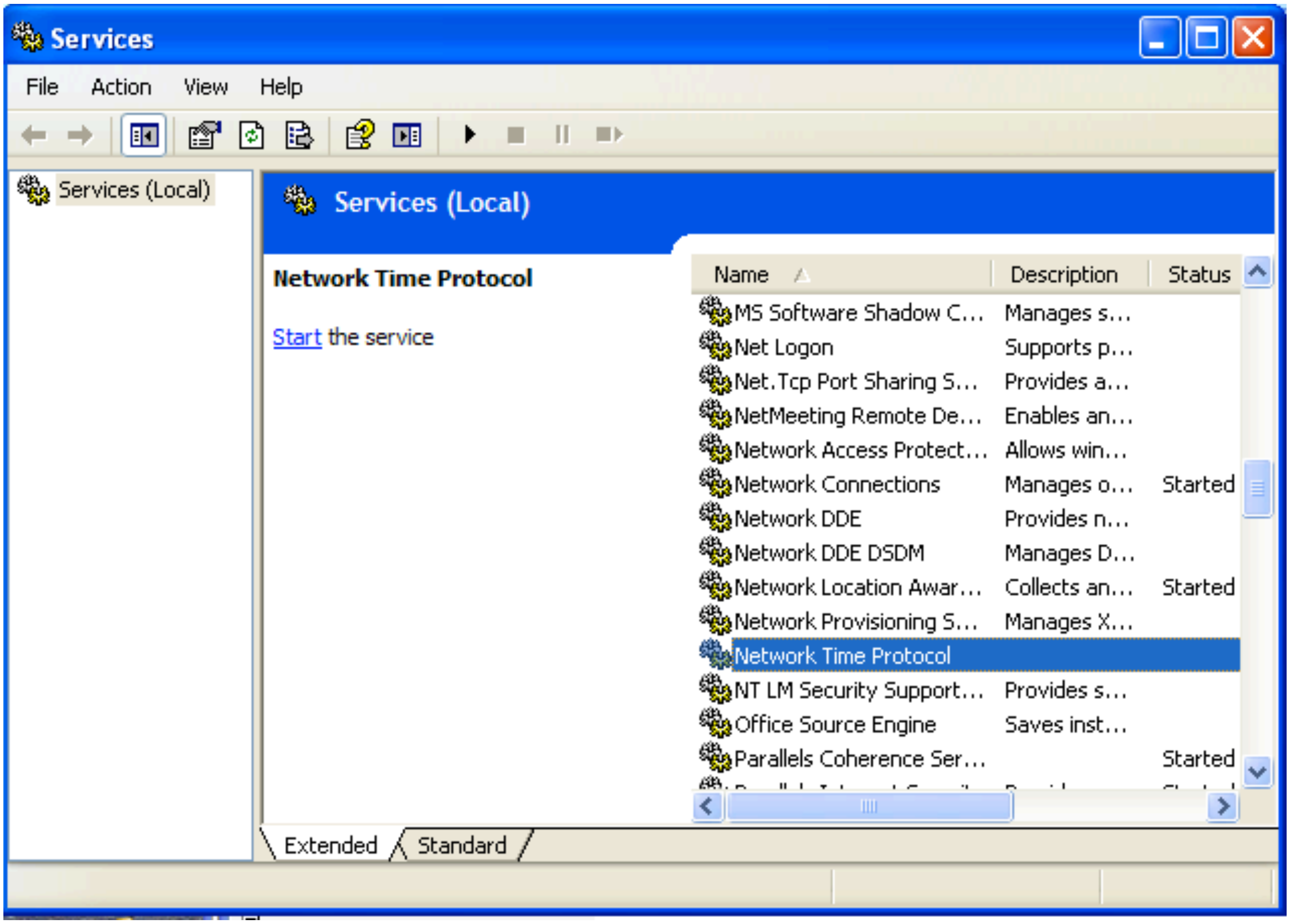
Service status: Stopped

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

Start parameters:

Configure the NTP service startup

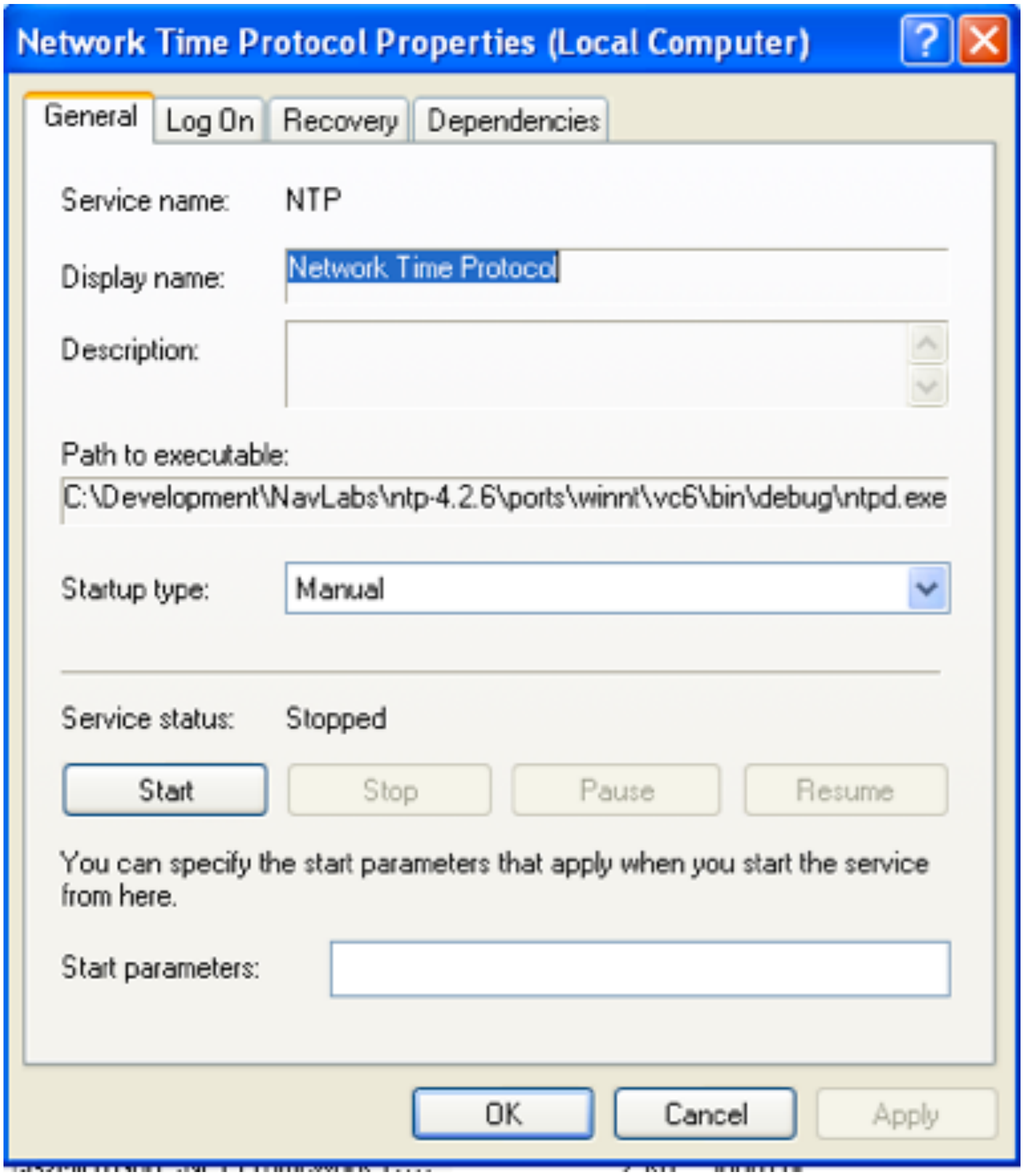
The NTP service startup also needs to be configured to allow the NavLabs simulation process to control the running of this service. To do this, open the services application in the 'Administrative Tools' group and scroll down to the "Network Time Protocol" line. If this line is not present please read the Installation section and how to use the Instsrv.exe program to install this service. Open this service and select 'Manual' as the startup type. The following snapshots illustrate this.



Network Time Protocol

Start the service

Name	Description	Status
MS Software Shadow C...	Manages s...	
Net Logon	Supports p...	
Net.Tcp Port Sharing S...	Provides a...	
NetMeeting Remote De...	Enables an...	
Network Access Protect...	Allows win...	
Network Connections	Manages o...	Started
Network DDE	Provides n...	
Network DDE DSDM	Manages D...	
Network Location Awar...	Collects an...	Started
Network Provisioning S...	Manages X...	
Network Time Protocol		
NT LM Security Support...	Provides s...	
Office Source Engine	Saves inst...	
Parallels Coherence Ser...		Started



Network Time Protocol Properties (Local Computer)

Service name: NTP

Display name: Network Time Protocol

Description:

Path to executable:
C:\Development\NavLabs\ntp-4.2.6\ports\winnt\vc6\bin\debug\ntpd.exe

Startup type: Manual

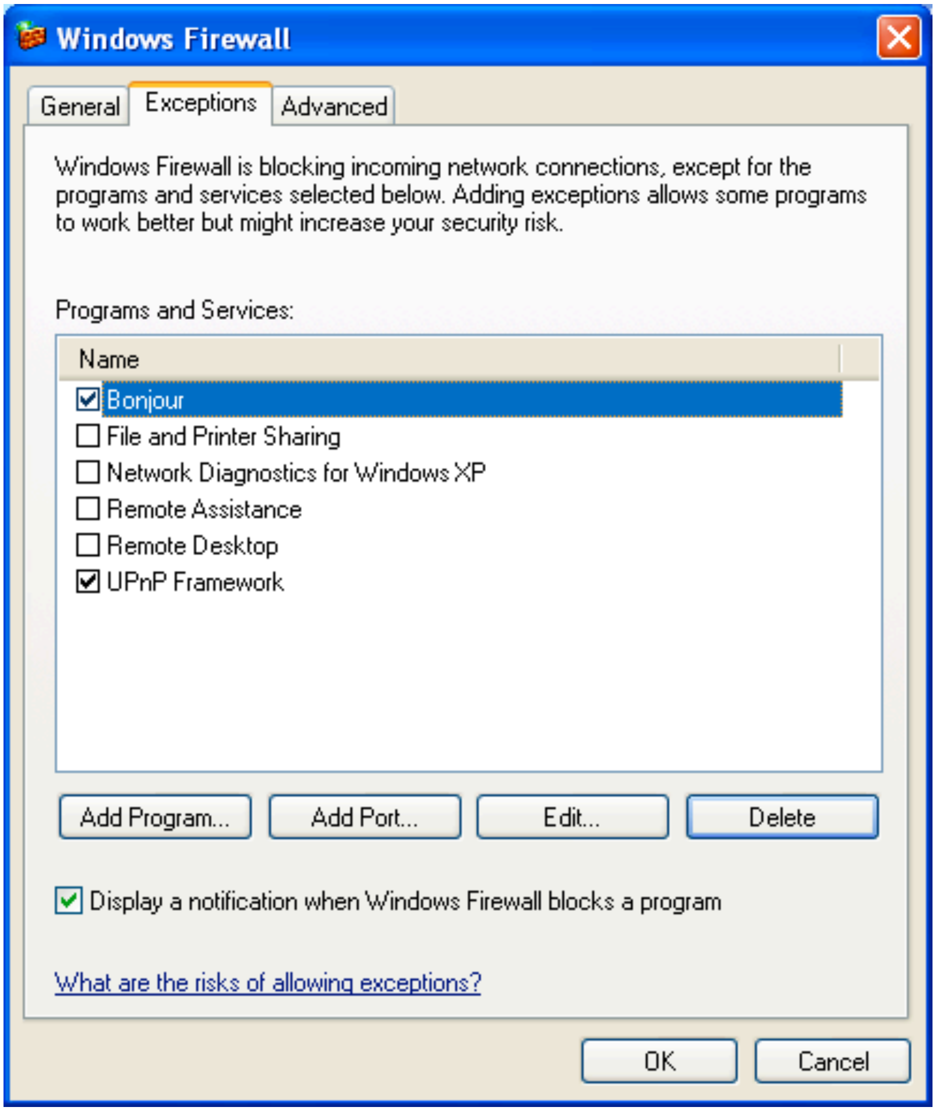
Service status: Stopped

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

Start parameters:

Open the NTP port in the Windows Firewall

If the Windows firewall is active the NTP port needs to be opened. To do this, run the "Windows Firewall" application found within the Control Panel. The Firewall application has three tabs: "General", "Exceptions", and "Advanced". Select the Exceptions tab and click the "Add Port" button. NTP uses port 132 for UDP messaging. The port can be named anything, but it is recommended to provide the name "NTP". Enter 123 for the Port number, and select the UDP radio button. This configuration step is shown below. Note that the list of exceptions on your firewall display may be very different that what is shown here. Depending on the applications and services that have been or are running on your system the list may look quite different. The important point is to locate the "Add Port" button. The "Add a Port" dialog box shown depicts the fields properly configured. Press "OK" to accept the modifications. The NTP port should be shown among the list of exceptions and it should be checked. Click 'OK' again to accept the modifications to the firewall configuration. The system should now allow NTP messaging in and out of the system over port 123.



Windows Firewall

Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

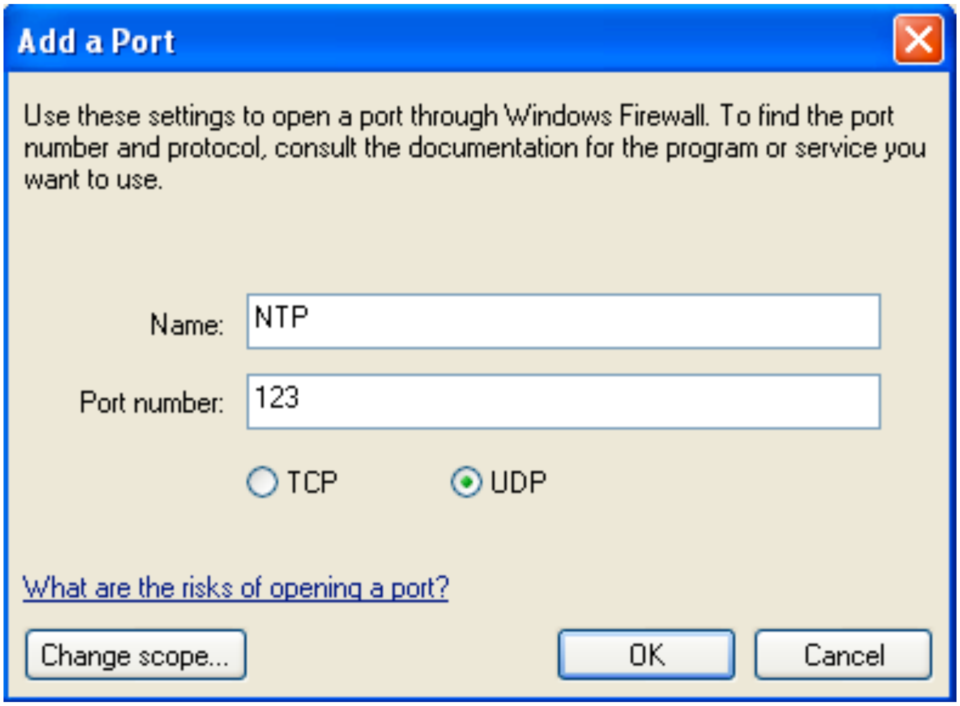
Programs and Services:

Name

- ☑ Bonjour
- □ File and Printer Sharing
- □ Network Diagnostics for Windows XP
- □ Remote Assistance
- □ Remote Desktop
- ☑ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?



Add a Port

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: NTP

Port number: 123

○ TCP ● UDP

What are the risks of opening a port?