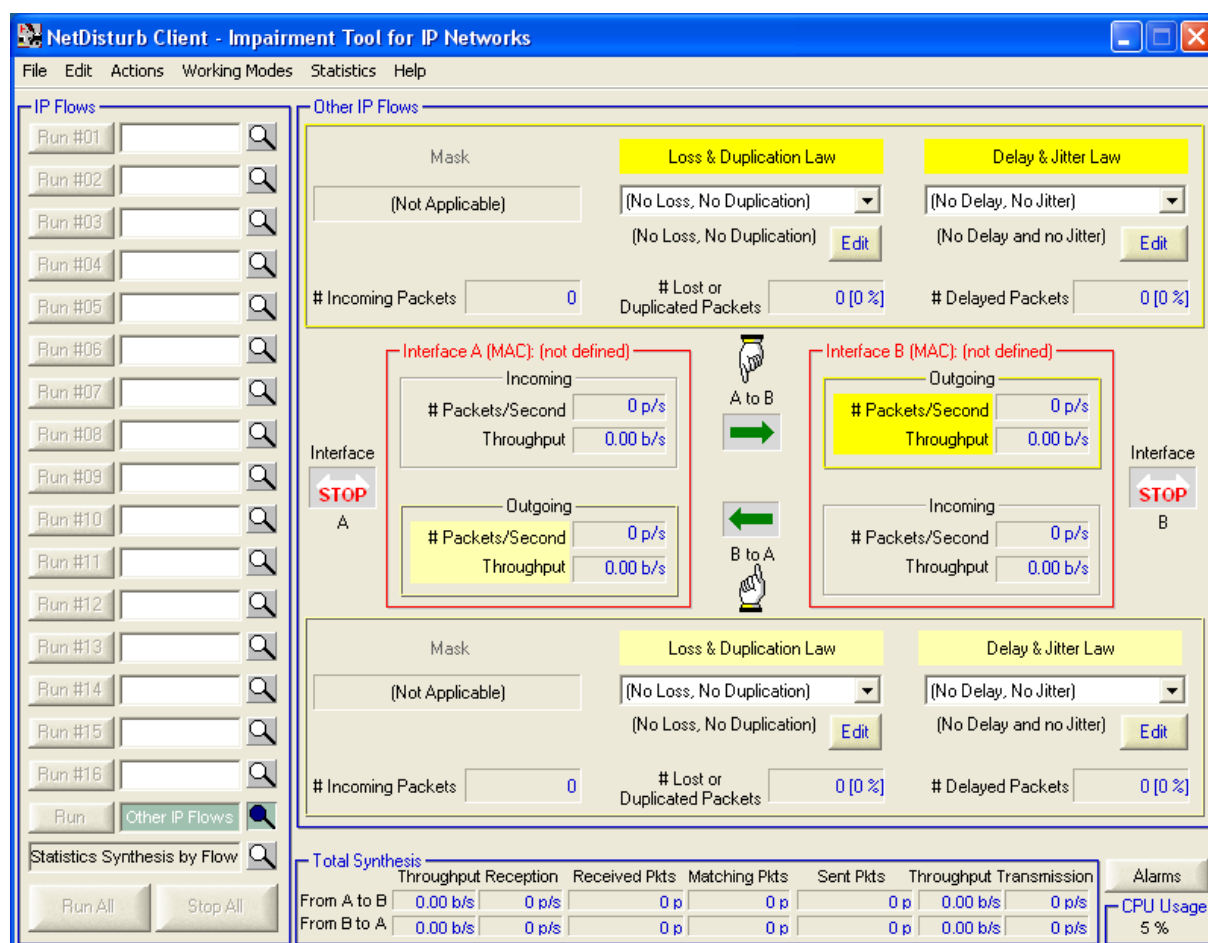




NetDisturb

Version 4.2

Impairment tool for IP networks



User Guide

WARNING

The content of this user guide is provided for informational use only. It is subject to change without notice, and must not be used as a commitment by ZTI.

ZTI could not be liable for any direct or indirect damages caused by the software or user guide imperfection.

By any chance, if mistakes have slipped into this guide, do not hesitate to contact our client support and make remarks.

Except when allowed by license agreement between ZTI and the user, no part of this guide or the software may be reproduced, transmitted in any form or by any means.

This guide allows the user to discover NetDisturb and is not an exhaustive user manual.

To contact us:

ZTI

1 Boulevard d'Armor
BP 20254
22302 Lannion Cedex
France

Phone: +33 2 96 48 43 43

Fax: +33 2 96 48 14 85

Web: <http://www.zti-telecom.com> or <http://www.zti.fr>

E-mail: contact@zti-telecom.com (marketing & sales)
support@zti-telecom.com (technical support)

Copyright, ZTI 1998-2005
France Telecom licensed product.
Reproduction rights reserved.

The software described in this manual is furnished under a License Agreement and may only be used in accordance with the terms of this agreement.

All products and company names mentioned in this document are trademarks or registered trademarks of their respective owners.

Ref# NETDISTURB USER GUIDE V4.2

Table of contents

Part 0	Document Presentation	5
Part 1	NetDisturb Overview	6
Part 2	Install NetDisturb	8
2.1	INSTALL THE DOWNLOADED TRIAL VERSION OF NETDISTURB	8
2.1.1	NetDisturb Driver Installation for Windows 2000 or Windows XP	9
2.1.2	NetDisturb Driver Installation for Windows NT4	10
2.1.3	Start Menu Shortcuts Created:	11
2.2	INSTALL NETDISTURB FROM THE CD-ROM	11
Part 3	License Configuration	12
3.1	TO CONFIGURE A LICENSE	12
3.2	LICENSE TRANSFERS	15
3.2.1	Direct Transfer: move a license from one local directory to another	15
3.2.2	Transfer by Media (floppy disk or USB key) : from a source PC to a target PC	16
3.3	KILL A LICENSE	22
Part 4	Uninstall NetDisturb.....	24
Part 5	Run NetDisturb.....	25
5.1	FIRST RUN	25
5.2	DETAILED DESCRIPTION OF SERVER AND CLIENT STARTUP.....	30
5.2.1	NetDisturb Server Startup Modes.....	30
5.2.2	NetDisturb Client Startup Options.....	30
5.2.3	Windows XP Service Pack 2	32
Part 6	Using NetDisturb Client.....	33
6.1	NETDISTURB CLIENT MAIN WINDOW.....	33
6.2	MENU DESCRIPTION.....	35
6.2.1	File Menu	35
6.2.1.1	New.....	35
6.2.1.2	Open	35
6.2.1.3	Save	35
6.2.1.4	Save as	35
6.2.1.5	Recent Files	36
6.2.1.6	Exit	36
6.2.2	Edit Menu.....	36
6.2.2.1	Copy.....	36
6.2.2.2	Paste.....	36
6.2.2.3	Move xxx Up	36
6.2.2.4	Move xxx Down.....	36
6.2.2.5	Insert before xxx.....	37
6.2.2.6	Delete xxx	37
6.2.2.7	Reset xxx	37
6.2.3	Actions Menu	38
6.2.3.1	Configuration	38
6.2.3.2	Reset Counter	39
6.2.3.3	Reset Server	39
6.2.4	Working Mode Menu.....	40
6.2.4.1	Enable/Disable Desequencing Packets	40
6.2.4.2	IP Flow versus TCP/UDP Connection IP Flow Mode	40
6.2.5	Statistics.....	41
6.2.5.1	Start	41
6.2.5.2	Stop.....	41
6.2.5.3	Configuration.....	42
6.3	IP FLOWS.....	43
6.3.1	General Description	43
6.3.2	Status of IP Flows	44
6.3.3	The Other IP Flows Entry	44
6.3.4	The Statistics Synthesis View.....	45

6.3.4.1	Detailed Description	45
6.4	IMPAIRMENT PARAMETERS AND ASSOCIATED COMMANDS	47
6.4.1	Selection of a Filter Mask, or Lost and Delay/Jitter Law	48
6.4.2	Mask Configuration	49
6.4.2.1	Mask Identifier	51
6.4.2.2	Mask Definition	51
6.4.2.3	Action Buttons	52
6.4.2.4	To Create a New Mask	52
6.4.2.5	List of Values	53
6.4.2.5.1	Individual Value	53
6.4.2.5.2	List of Individual Values	53
6.4.2.5.3	Range of Values	53
6.4.2.5.4	Complex List	53
6.4.3	Loss/Duplicate laws Configuration	54
6.4.3.1	Loss Laws and Working Mode	55
6.4.3.2	How to create or to edit Loss Laws	55
6.4.3.3	Constant Loss Law	58
6.4.3.4	Uniform Loss Law	59
6.4.3.5	Burst Uniform Loss Law	60
6.4.3.6	User-defined Loss File	61
6.4.3.7	Percentage Loss	63
6.4.3.8	One packet every N Packets Loss	64
6.4.3.9	General Rules concerning the Duplication of Packets	65
6.4.3.9.1	What does Duplication mean in the Context of NetDisturb	65
6.4.3.9.2	How many Times is a Packet Duplicated	65
6.4.3.10	Percentage Duplication	66
6.4.3.11	Duplication every M Packets	67
6.4.3.12	Uniform Duplication	68
6.4.3.13	Loss (1/N) then Duplication (1/M)	69
6.4.4	Delay/Jitter laws Configuration	70
6.4.4.1	Delay & Jitter Laws and Working mode	70
6.4.4.2	Delay & Jitter Accuracy	70
6.4.4.3	Delay & Jitter Laws Selection	71
6.4.4.4	Constant Delay Law	74
6.4.4.5	Constant Delay with Exponential Jitter Law	75
6.4.4.6	Constant Delay with Uniform Jitter Law	76
6.4.4.7	Constant Delay & User File with Jitter Values	77
6.4.4.8	User File with Constant Delay & Jitter Values	78
6.4.4.9	Router Simulation & Constant Delay	79
6.4.4.10	Router Simulation & User File	80
6.4.5	Loss and Delay Dynamic	81
6.4.6	Loss with Duplication and Delay/Jitter Dynamic	82
6.5	NETDISTURB CLIENT STATISTICS	83
6.6	ERRORS DETECTED BY NETDISTURB DRIVER	83
6.6.1	Details for Incoming Errors	85
6.6.2	Details for Outgoing Errors	86
6.6.3	Alarm Management	86
Part 7	Using NetDisturb Server	88
Part 8	Annexes	91
8.1	DEFAULT CONTEXT VALUES	91
8.2	NETDISTURB REGISTRY VALUES	91
8.2.1	Registry related to NetDisturb Client	92
8.2.1.1	Configuration Parameters	92
8.2.1.2	Most Recent File list	93
8.2.2	Registry related to NetDisturb Server	93
8.2.3	Registry related to NetDisturb Driver	94
8.2.3.1	NetDisturb Driver Traces	94
8.2.4	Windows Registry (Windows XP)	94
8.3	MATHEMATICAL LAWS	95
8.3.1	Uniform Law	95
8.3.2	Uniform Correlated Law	95
8.3.3	Exponential Law	96

Part 0 Document Presentation

This User's guide is aimed to help you to discover and use NetDisturb. It is composed of eight parts.

Part 1 is a general presentation of the NetDisturb software.

Installation of NetDisturb is explained in Part 2, and license configuration is detailed in Part 3. Uninstall of NetDisturb is described in Part 4.

To run NetDisturb Server and NetDisturb Client, you must refer to Part 5.

Part 6 explains how to use NetDisturb Client and Part 7 describes the use of NetDisturb Server.

In Part 8, annexes add information such as the default context values, the registry values and a short description of mathematical laws used.

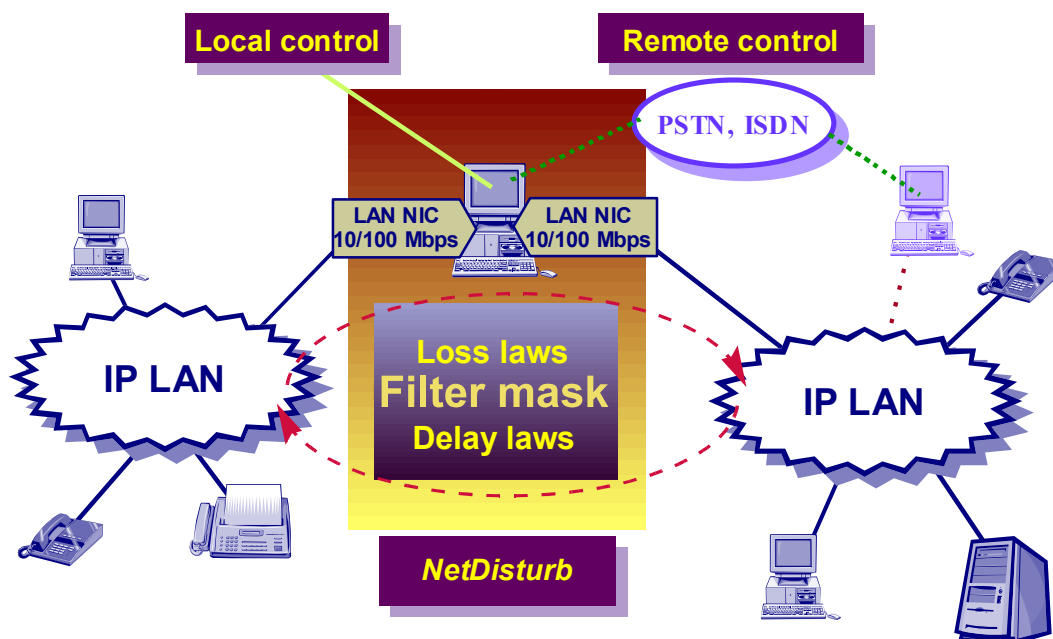
Part 1 NetDisturb Overview

NetDisturb is an impairment tool for IP networks. It allows to disturb a network and so to study the behavior of applications, devices or services in a disturbed network environment.

The software must be installed on a PC with Microsoft Windows NT4 (SP6 recommended), Windows 2000 or Windows XP equipped with at least two LAN cards 10/100/1000 Mbps and inserted between two physical networks. It can be remotely controlled via PSTN, ISDN or LAN. Minimal required screen resolution is 1024 x 768 pixels.

NetDisturb generates packet loss, packet duplication, packets delay including jitter in the transmission between the two parts of the network. Loss, duplication and/or delay are following mathematical laws programmed by User. A filter called mask allows selecting the stream of packets to impair. Up to 16 masks can be defined plus the rest of the IP traffic.

A mask is composed of different elements: VLAN number, source MAC address, destination MAC address, protocol, TOS (Type Of Service), source IP address, destination IP address, source port list and destination port list where each element is optional.



NetDisturb is composed of two parts (or applications): a Client part (NetDisturb Client) and a Server part (NetDisturb Server). These two parts can be installed on the same computer or on two different computers.

❖ **The NetDisturb Server part:**

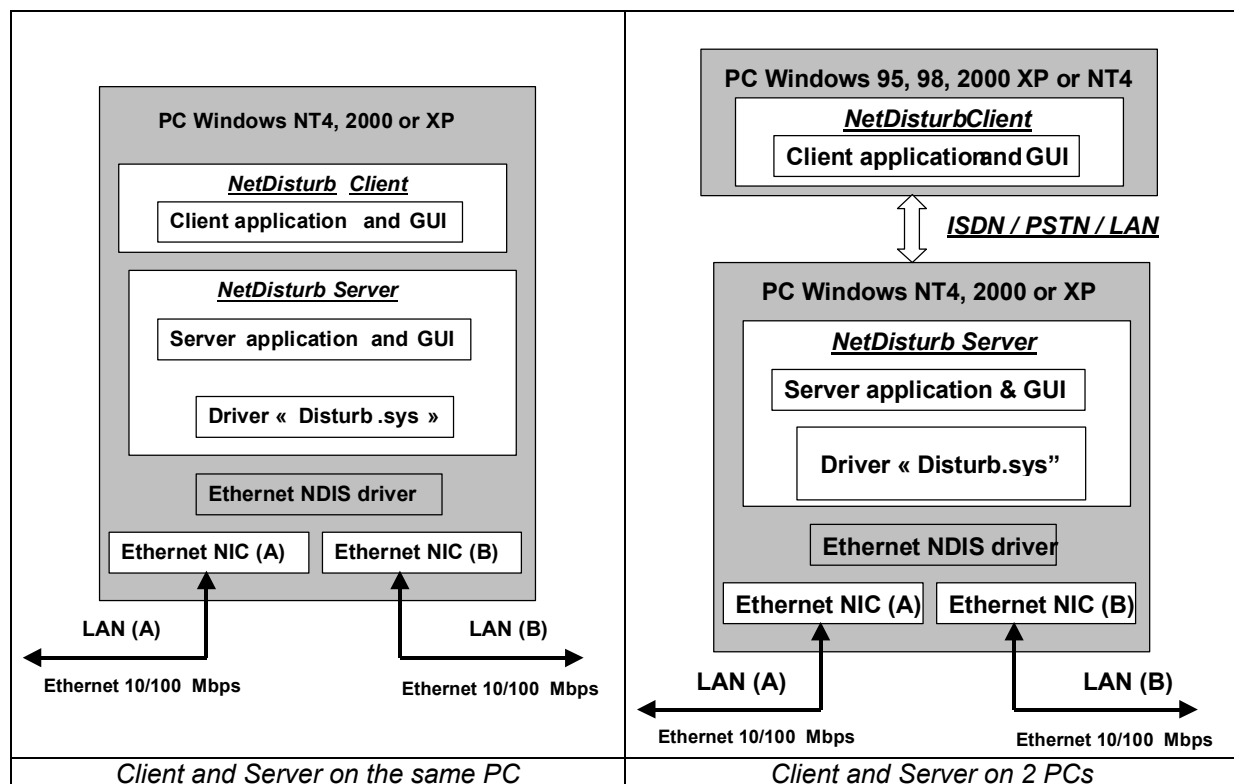
- ⇒ It is installed on the machine that is physically set between the two physical networks. This machine must have at least two Ethernet cards, and optional remote controls access (an ISDN or PSTN equipment, or a third LAN card). For the Server part, required operating system is Window NT 4 (SP 4 at least with SP 6 recommended), Windows 2000 or Windows XP.
- ⇒ It applies the perturbations to the selected packets in the two directions:
 - Selected packets incoming on interface A (LAN NIC) and outgoing processed on interface B (LAN NIC).
 - Selected packets incoming on interface B and outgoing processed on interface A.
 - Non-selected packets are transferred without perturbations from one interface to the other.
- ⇒ It offers a thorough view of traffic statistics, selected parameters and traces.

❖ **The NetDisturb Client part;**

- ⇒ It can be installed either directly on the server machine or on a remote PC with a Windows 32 bits System (95, 98, NT4, 2000 or XP). In this case, the remote PC will control NetDisturb Server via ISDN or PSTN using RAS or directly via a LAN card.
- ⇒ It allows configuring masks and laws, to manage NetDisturb functions, and displays statistics.

Two configurations may be used:

- ⇒ NetDisturb Client and NetDisturb Server on the same PC,
- ⇒ NetDisturb Client and NetDisturb Server on two different PCs.



NetDisturb Client and NetDisturb Server use RPC on TCP/IP to dialog (see also paragraph 5.2.3).

Part 2 Install NetDisturb

To install this software testing tool, you need a PC Windows NT 4 / SP4 (Service Pack 4 or more), Windows 2000 or Windows XP, and 1024 x 768 display resolution. If you have the NetDisturb CD-ROM version, please refer directly to paragraph 2.2.

NetDisturb is configured by default with a 15-days limited license. When the time limit expires, NetDisturb will cease to run. See the License configuration part for more information about the license program.

2.1 Install the Downloaded Trial Version of NetDisturb

The installation procedure is a standard installation program.

Please note that the installation procedure of NetDisturb will be different in the last part, depending on the target Operating System: Windows NT4 or Windows 2000 and Windows XP.

*Warning: The installation procedure requires to be logged on with **administrator privileges**.*

- If you have downloaded NetDisturb trial version from our website, you have downloaded the file NetDisturb.zip containing the [Setup_NetDisturb.exe](#) file.
- Before to proceed with the NetDisturb Setup, please be sure your system does meet the following minimum requirements:
 - ⇒ OS supported: Windows NT4 (SP4 at least), Windows 2000 or XP.
 - ⇒ Minimum screen resolution: 1024 x 768
 - ⇒ Your PC needs at least 2 NIC already installed, configured and fully operational.

NetDisturb is composed of two parts: NetDisturb Client and NetDisturb Server.
This setup will install both Client and Server parts on the same system.

- Run "[Setup_NetDisturb.exe](#)" and follow the "NetDisturb" setup instructions to proceed with the installation.

By default, NetDisturb will be installed in the following directory:
C:\Program Files\NetDisturb with the following subdirectories:

- C:\Program Files\NetDisturb
- C:\Program Files\ NetDisturb \Client
- C:\Program Files\ NetDisturb \Driver
- C:\Program Files\ NetDisturb \Server
- C:\Program Files\ NetDisturb \Server\Script

At the end of setup, a manual driver installation is required if Windows NT4 is used. In that case, please refer to paragraph 2.1.2.

Otherwise, the only necessary operation is to uncheck protocols from NICs used with NetDisturb.

2.1.1 NetDisturb Driver Installation for Windows 2000 or Windows XP

NetDisturb Driver sets in the kernel of Windows 2000. NetDisturb Driver is installed on top of the driver of each Network Interface Card (NIC) installed in your PC. For Windows 2000 or XP, the NetDisturb Driver is considered as a protocol. The NetDisturb Driver handles the exchanges between two NICs.

The setup procedure realizes the installation of the NetDisturb Driver transparently. The NetDisturb Driver is mapped on top of each Ethernet or wireless NIC if the driver of the NIC is NDIS compatible.

The NetDisturb Driver linked to the selected NICs remains available transparently: it doesn't appear in the protocol list.

There is still an important manual operation you have to make before to use NetDisturb:

1. In order to avoid unexpected traffic generated by the protocol stack (TCP/IP, Client or Microsoft Networks, etc.) on the NICs that NetDisturb will be use, you have to unselect all protocols.
2. To unselect protocols from a NIC used by NetDisturb, use the "Control Panel/Network and Dial-up Connections" or the "Control Panel/Network Connections" program and uncheck all protocols.

2.1.2 NetDisturb Driver Installation for Windows NT4

At the end of the setup, after the files have been copied to the system:

- A text file is automatically opened to explain the next step: installation of the NetDisturb Driver on the system
- The control panel is automatically opened in order to proceed with the driver installation.

NetDisturb Driver sets in the kernel of Windows NT. This driver must be installed over the driver of network cards. For Windows NT, it is considered as a protocol. The NetDisturb Driver goal is to handle exchanges between two networks interface cards (NIC).

NetDisturb Driver is a protocol named '[Disturbing Ethernet Driver over NDIS](#)'.

The NetDisturb Driver installation is carried out as any usual network driver installation. It must be installed after the network cards drivers. Different protocols can be bound to your NIC. NetDisturb Client and NetDisturb Server need a TCP protocol stack for data exchange. So before installation, check that your Windows NT4 computer gets 2 NIC installed and a TCP stack installed.

To install the NetDisturb Driver, you have to use the Windows control panel, and select the following items:

1. Choose "Network" icon,
2. Choose "Protocols" tab,
3. Click on "Add"
4. Choose "Have Disk..."
5. Type the folder where following files are located: OEMSETUP.INF and DISTURB.SYS (by default: C:\Program Files\NetDisturb\Driver) and press 'OK'
6. Then select the " Disturbing Ethernet Driver over NDIS " and click on "OK"
7. The item 'Disturbing Ethernet Driver over NDIS' appears in the protocol list of 'Protocols' tab
8. Disable the other protocols bound to the network adapters as follows:
 - * Choose "**Bindings**" tab,
 - * In the list box select "**show bindings for all adapters**",
 - * Disable all protocols bound to each Network adapter used by NetDisturb except Disturb protocol: "**Disturbing Ethernet Driver over NDIS**" (you need to do it for the 2 used network adapters)
 - * Disable "**Disturbing Ethernet Driver over NDIS**" for all other adapters
9. As a TCP stack is required for NetDisturb Client and NetDisturb Server exchanges, you must bind the TCP protocol to another one adapter - for example to a modem or another adapter.

This is an example to add a TCP/IP stack onto a modem, which is not necessarily physically connected to your PC. The procedure is as follows:

- a) Add a modem via Control Panel / Modem, select **"add"**, then **"don't detect my modem, I will select it from a list"** and click on **"Next"**
- b) Select any standard modem from the Standard Modem Types manufacturer list (for example Standard 14400 bps modem). Click on **"Next"**
- c) Select a port and click on **"Next "**
- d) Windows NT should present you a dialog box indicating the end of modem installation

When you have finished to use the control panel, press **Close** to save all changes.

Your system is now configured: **you need to reboot your PC** to take changes into account.

2.1.3 Start Menu Shortcuts Created:

At the end of the installation, some shortcuts have been created in the Start Menu.

Start > All Programs > **NetDisturb**
⇒ **1) NetDisturb Server**
⇒ **2) NetDisturb Client**
⇒ **License help**
⇒ **Read Me First**
⇒ **Uninstall NetDisturb**
⇒ **User Guide**

2.2 Install NetDisturb from the CD-ROM

The installation procedure is a standard installation program. On the CD-ROM, you will find the "Setup_NetDisturb.exe" file. **This setup will install NetDisturb Client and NetDisturb Server on the same system.**

Execute this setup and follows the installation steps as described in the previous paragraph.

On the CD-ROM, a second setup allows to install NetDisturb Client on a system. This is useful if you want to install NetDisturb Server and NetDisturb Client on two different systems.

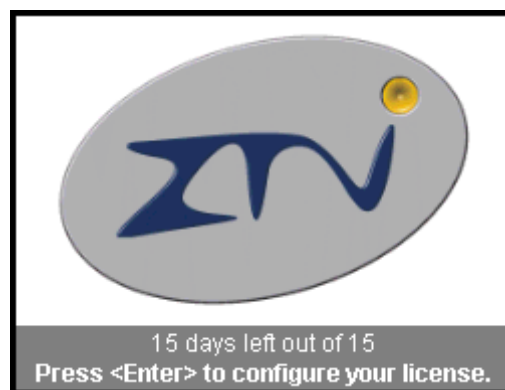
To install NetDisturb Client on a system (Windows 95, 98, NT4, 2000 or XP), run "**Setup_NetDisturbClient.exe**", and follow the setup instructions to proceed with the installation.

Part 3 License Configuration

Note: The NetDisturb software is licensed on a per workstation basis. You will need to have a separate license for each machine that you install it on. Each licensed copy of the software installed on a system has a unique Site Code which requires the corresponding unique Site Key to be entered before the tool is operational (except for a trial version: a duration of 15 days is automatically enabled at the first installation of the software. If you try to install again the software, the license program disables the trial period).

3.1 To Configure a License

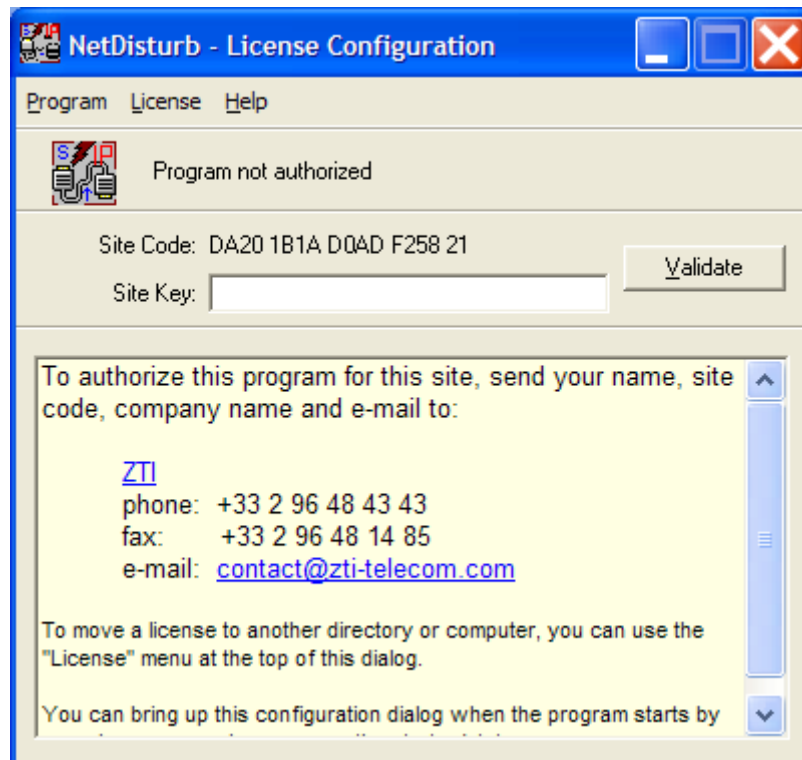
If you wish to configure your license before trial period end, please press **Enter** when the following message is displayed:



Therefore, you will obtain the license configuration dialog as follows:



Note: at the end of the trial period when you launch NetDisturb Server, the same license configuration dialog appears, with a specific mention instead of the remaining days of use: "Program not authorized".

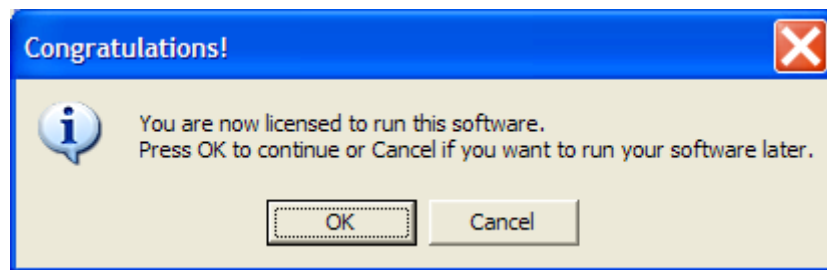


To get the 'Site Key' and obtain an unlimited version, please send your name, 'Site Code' (specific to your installation), company name, e-mail and preferred method of payment (if you haven't bought the NetDisturb software yet) to: contact@zti-telecom.com.

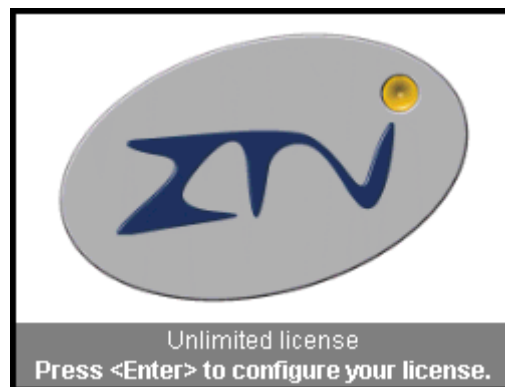
We will send you your 'Site Key' once we receive payment.

If you have already bought, please email your Site Code and we will email you back the Site Key.

After you have entered your 'Site Key', you get the following message:



Note: you will see the following dialog when you will launch NetDisturb Server if you have an unlimited license:



3.2 License Transfers

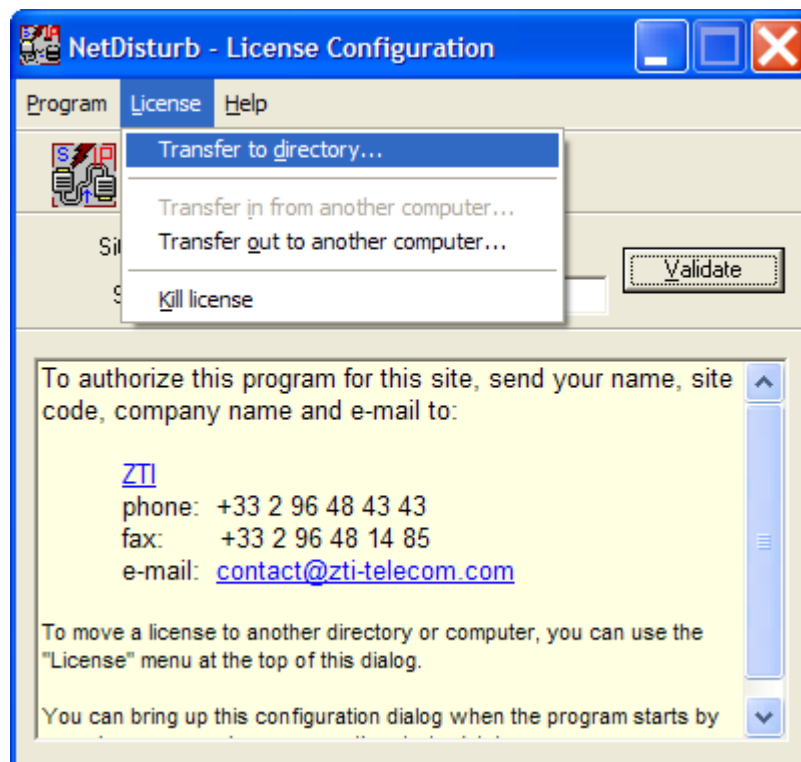
Warning: a license transfer is not a duplication of any type – please contact us for site license information and for several licenses purchase.

Licenses can be transferred using either of the following methods:

- Direct Transfer: to move a license from one local directory to another.
- Removable media: to move a license from one networked PC to another or from two PCs that are not networked, via floppy disk or USB Key

3.2.1 Direct Transfer: move a license from one local directory to another

- First, copy the program (copy the folder “NetDisturb”) to the target directory.
For example from “C:\Program Files\ NetDisturb” to “C:\Temp\NetDisturb”
- Then run the program in the original directory (from “C:\Program Files\NetDisturb”). When the license configuration window appears, press **Enter** and select in the menu “License > Transfer to directory”, as shown below.



- Provide the path name of the target program (for example C:\Program Files\NetDisturb\NetDisturbServer.exe). The program copy now has the license awarded the original.

3.2.2 Transfer by Media (floppy disk or USB key) : from a source PC to a target PC



A floppy disk or an USB key is needed for this kind of transfer.

To transfer the license from the source PC (PC #1) to the target PC (PC #2), proceed as described in the following points.

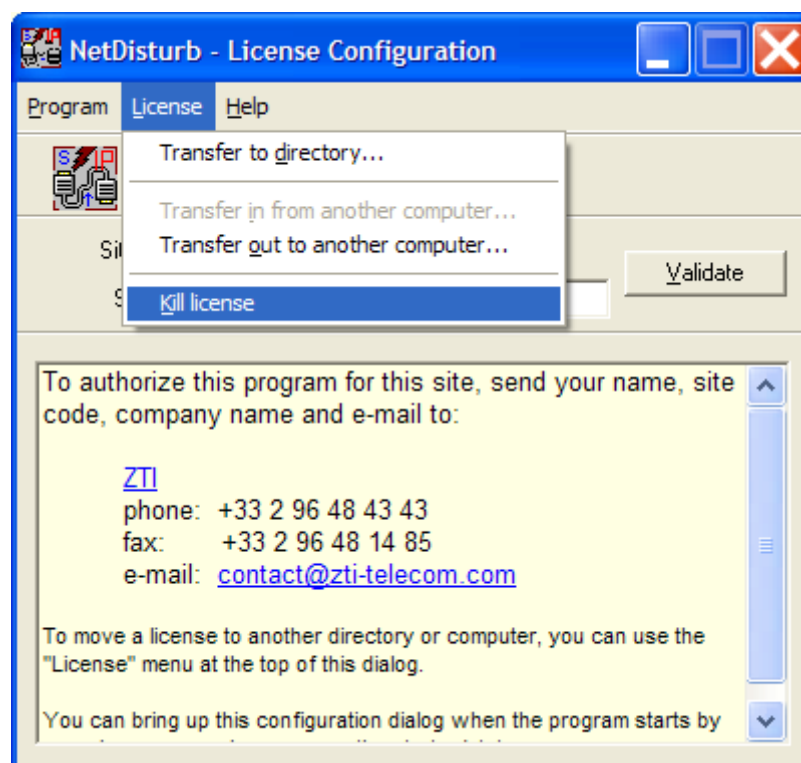
Point 1: First, install the program on the target PC (PC #2).

Point 2: Run the software on PC # 2 and kill the trial license in order to have an unauthorized license on this PC.

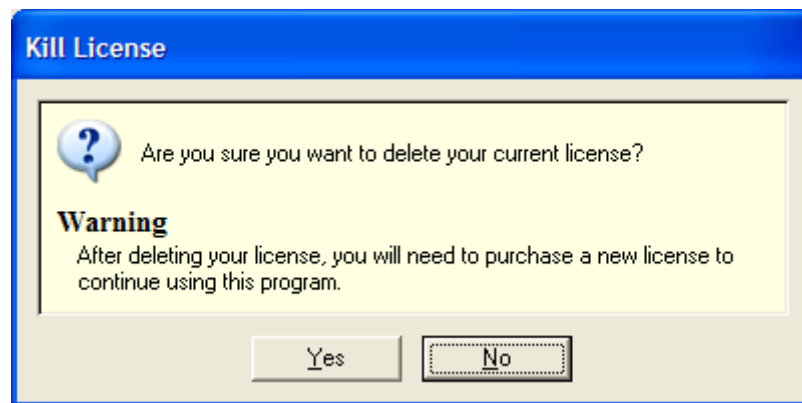
You need to kill the license if the "Transfer in from another computer ..." item of the license menu is disabled.

To kill the license, please proceed as follows.

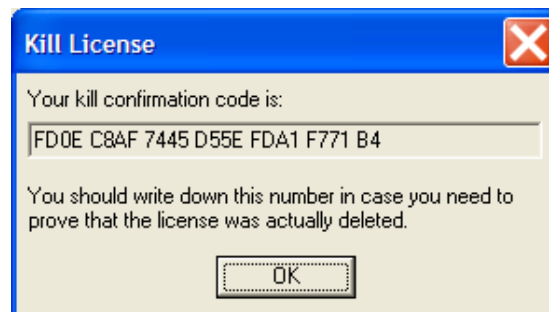
When the license configuration window appears, press **Enter** and select in the menu "License > Kill license".



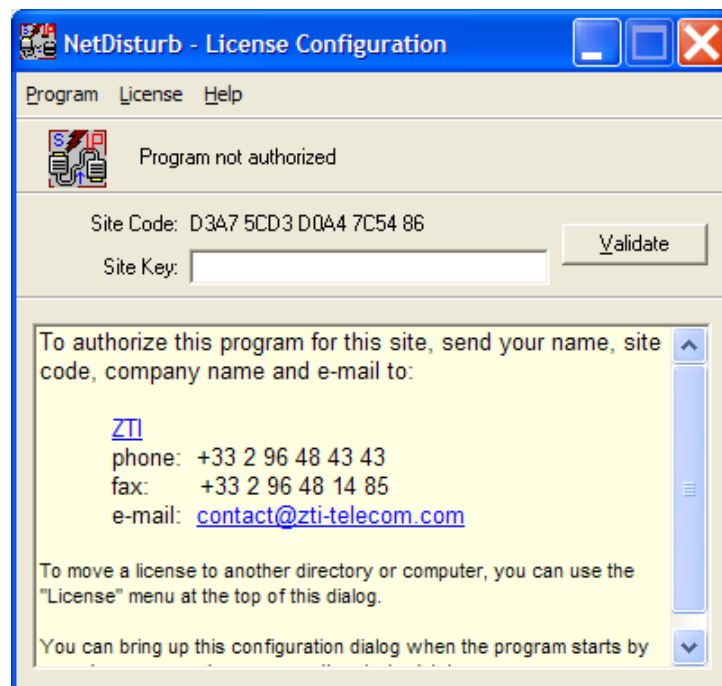
A message box appears, press 'Yes' to kill the license.



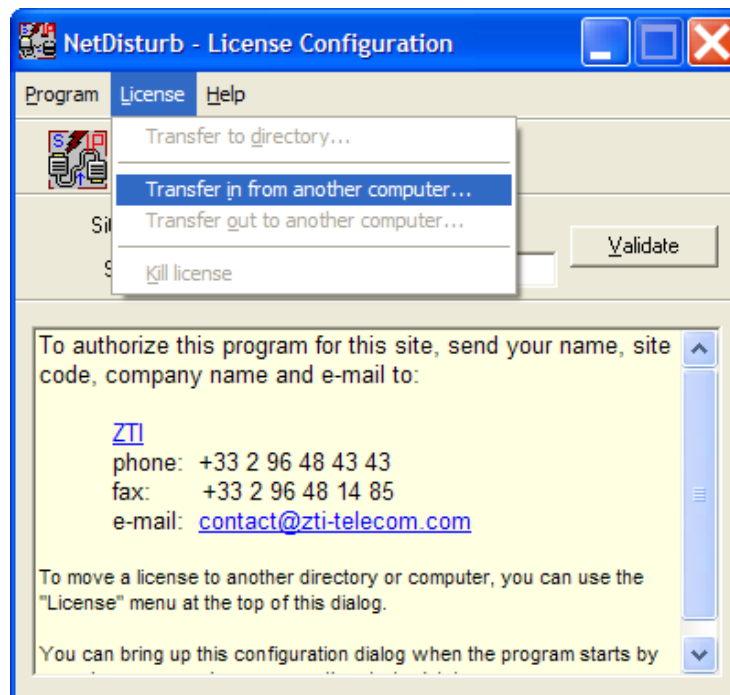
And a kill confirmation code is displayed.



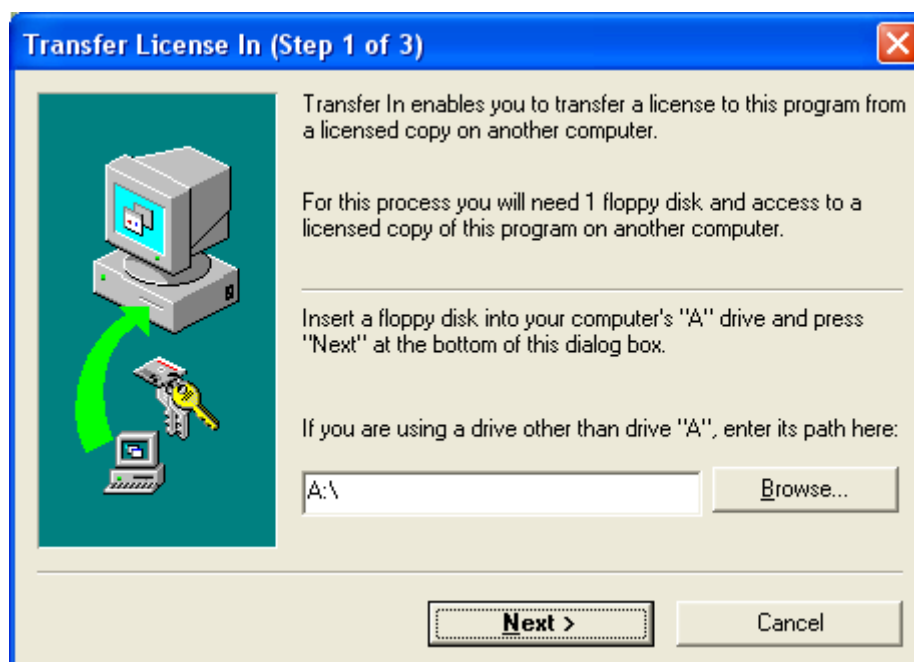
The license window displays now "Program not authorized" as following:



Point 3: select in the license menu, the item: "License > Transfer in from another computer ..."

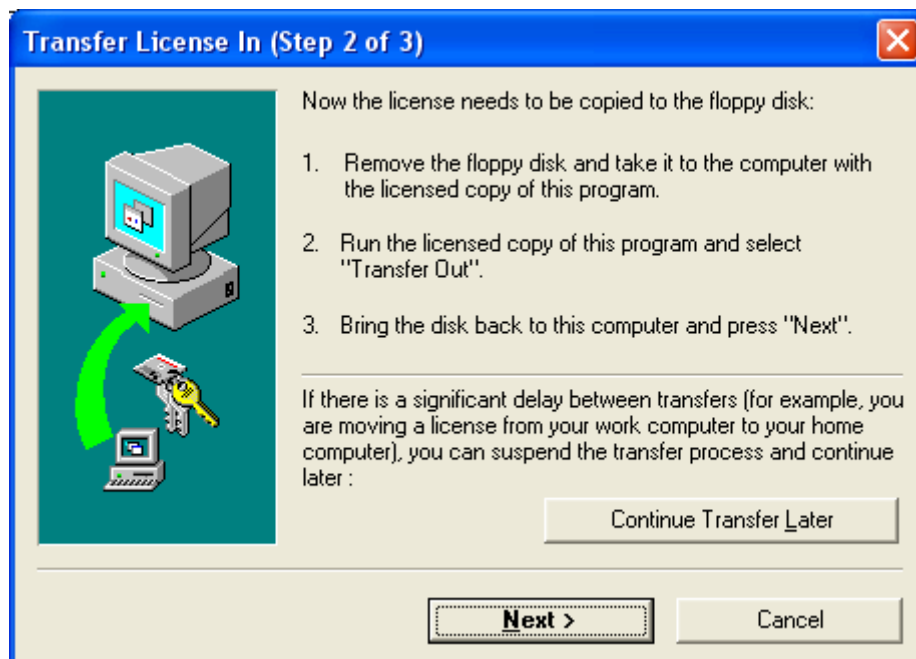


and the "Transfer License In (Step 1 of 3)" window is displayed:

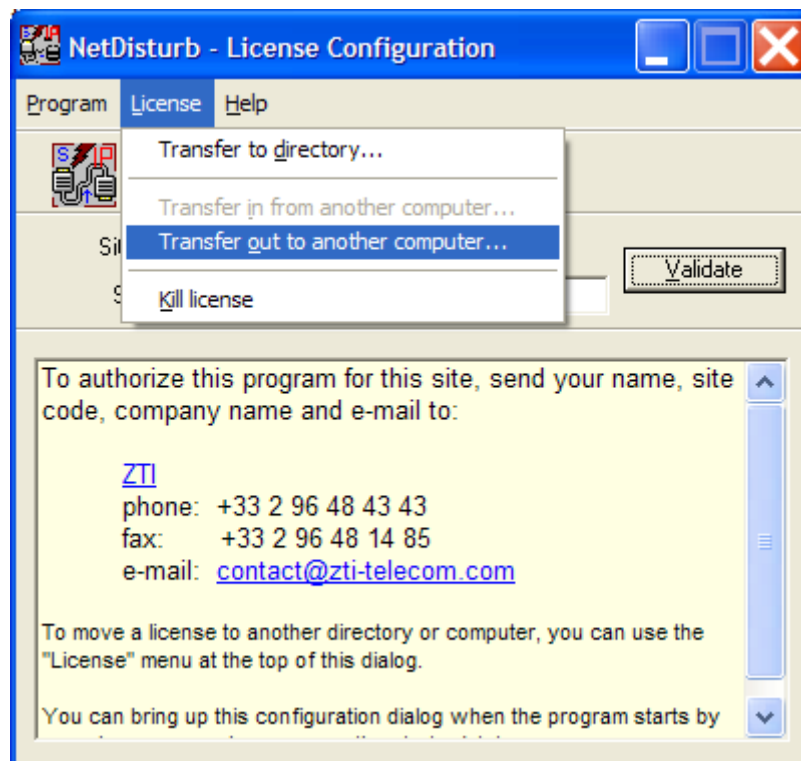


Point 4: Insert a floppy disk or use a USB key as requested in step 1 of 3 and specify the path.

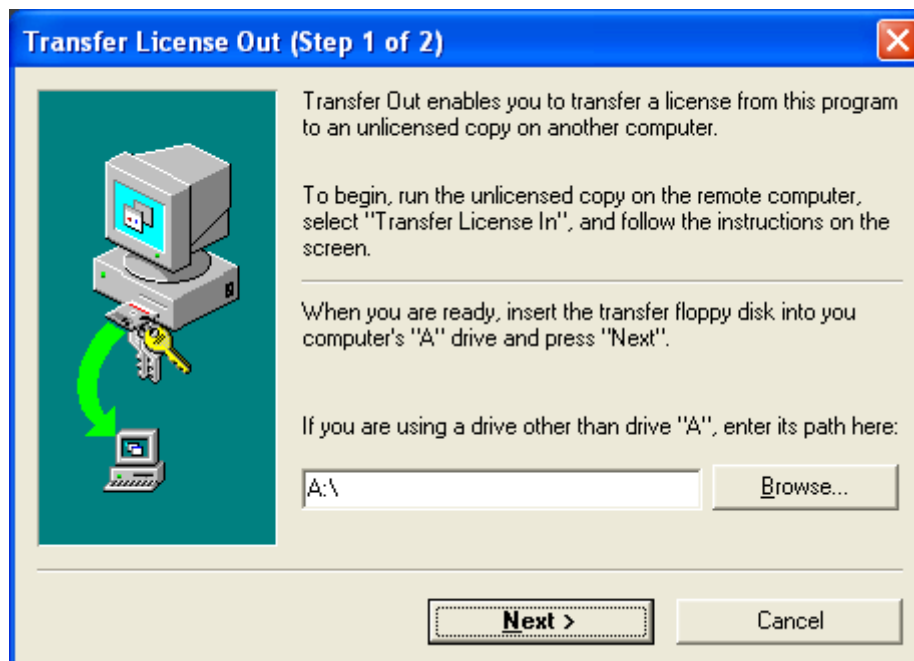
Then press “Next >” and the “Transfer License In (Step 2 of 3)” window is displayed:



Point 5: go to the source PC (PC #1) and insert the media (floppy disk or USB key). Then start the program on PC #1. When the license configuration window appears, press **Enter** and select in the menu “License > Transfer out to another computer ...” as shown below:

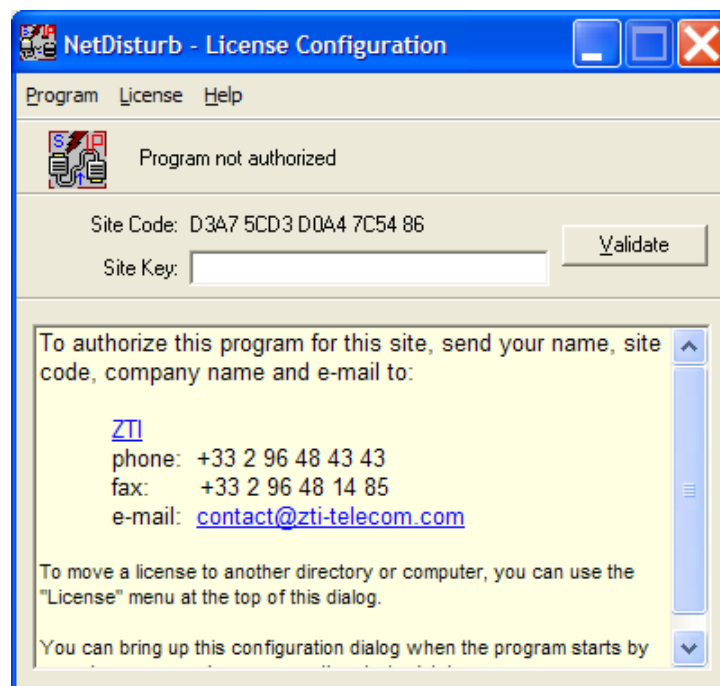


Then the following window is displayed:



Input the media path (floppy disk or USB key) and then press "Next >".

When the license is put on the media, you get the "Program not authorized" message:



You can check that the license is no more available on the source PC since the NetDisturb software license is on a per workstation basis. Contact us to get information on site license (contact@zti-telecom.com).

Point 6: Remove the media from PC #1 and return to PC #2.

Click the 'Next' button on the step 2 of 3 of the “Transfer license in” window (on PC #2) to complete the transfer.

The unlimited license key is now transferred from the source PC to the target PC, and you get the following message:

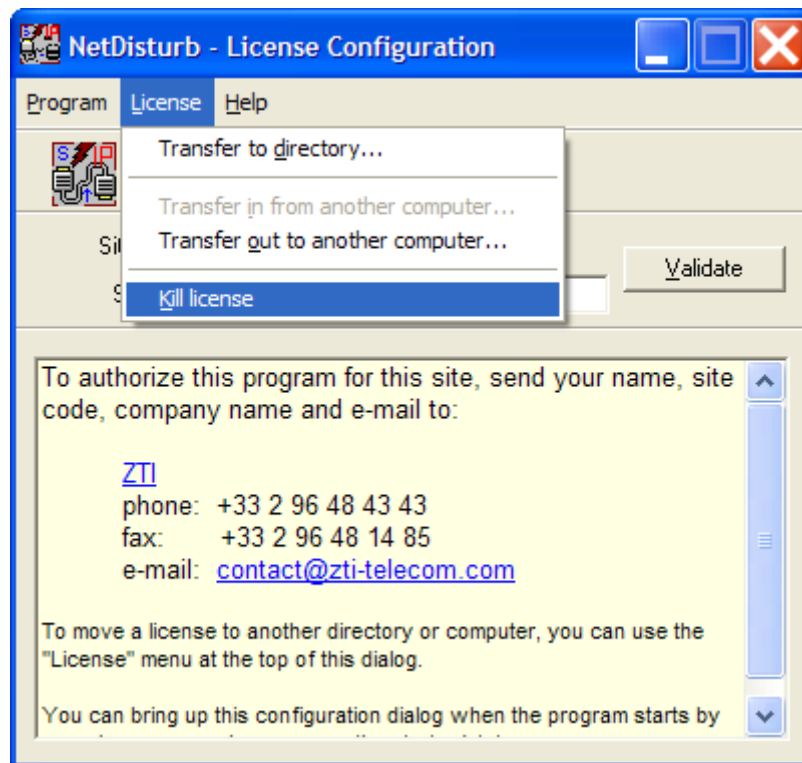


Click Finish to continue.

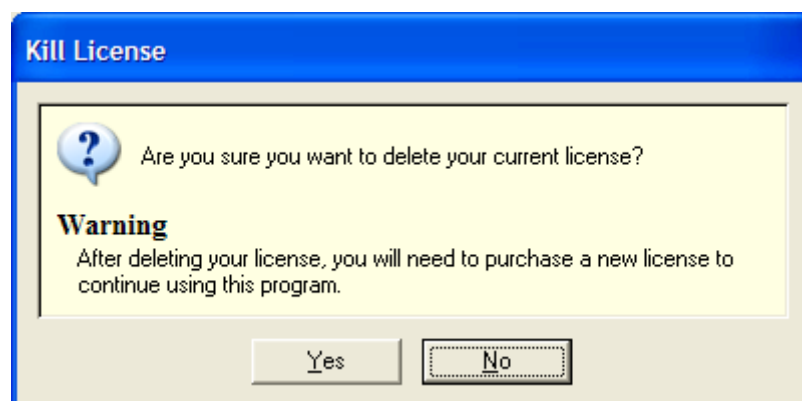
3.3 Kill a License

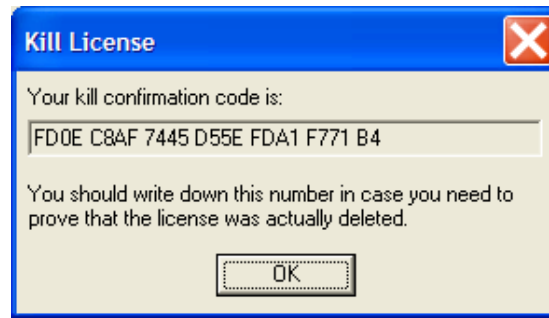
If you would like to transfer an unlimited license key onto a PC where a trial period is still active, you should first kill the active trial period. If you don't kill the active trial period, you will not be able to transfer an unlimited license. To kill the trial license, you should proceed as follows:

- In the license configuration window, select in the menu “License > Kill License” as shown below.



- A message box appears, press ‘Yes’ to kill the license.





- Your license is now killed. Please, write down the kill confirmation code. This code may be requested by ZTI.

Part 4 Uninstall NetDisturb

The uninstall procedure is a standard uninstall program.

In the “Start > Programs > NetDisturb” Menu, select “Uninstall NetDisturb”.

The uninstall procedure is executed.

How to uninstall the NetDisturb Driver

⇒ Windows 2000 or XP

All software components installed by the installation procedure are removed during the uninstall procedure, including NetDisturb Driver.

⇒ Windows NT4

In Windows NT4, Disturb Driver is not removed by the un-installation procedure because it has not been added by the installation procedure.

At the end of the uninstall Procedure, a text file is automatically opened in order to explain how to uninstall NetDisturb Driver when you are using Windows NT4.

You use the Control Panel, run "Network" and choose the "Protocols" tab. Then select the driver "Disturbing Ethernet Driver over NDIS" and you click on "Remove".

Then you must restart your PC.

Part 5 Run NetDisturb



As NetDisturb is composed of 2 parts (NetDisturb Server and NetDisturb Client), you need to run these two programs with the following order:

1. **NetDisturb Server**
2. **NetDisturb Client**

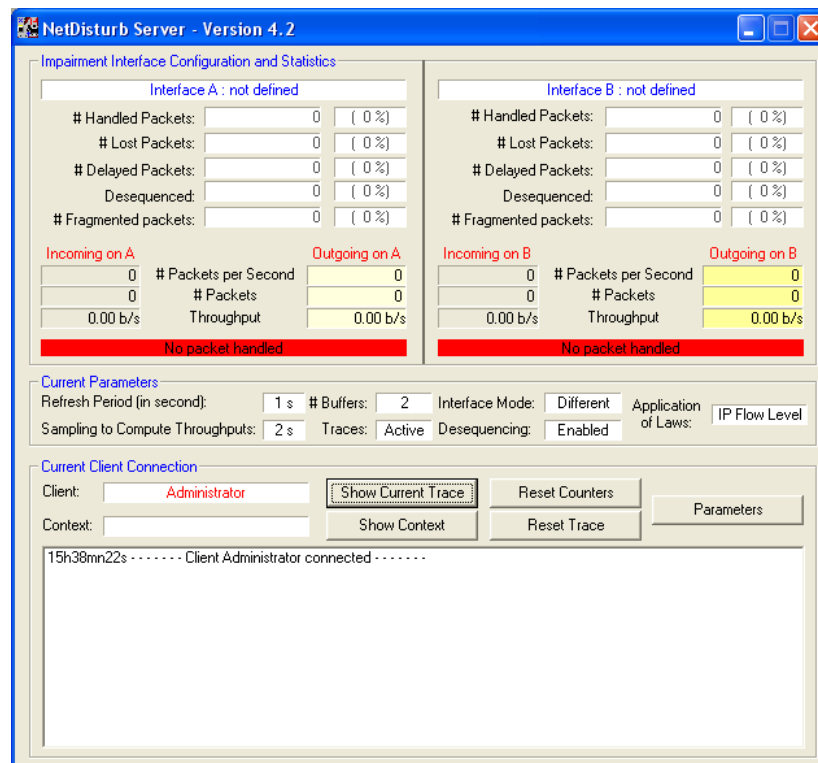
5.1 First Run

1. To start the **NetDisturb Server**, click in the Start Menu on
'Start > Programs > NetDisturb > 1) NetDisturb Server'

Depending of your license, you will get the following license window:

Limited license	Unlimited license
 <p>NetDisturbServer 15 days left out of 15 Press <Enter> to configure your license.</p>	 <p>NetDisturbServer Unlimited license Press <Enter> to configure your license.</p>

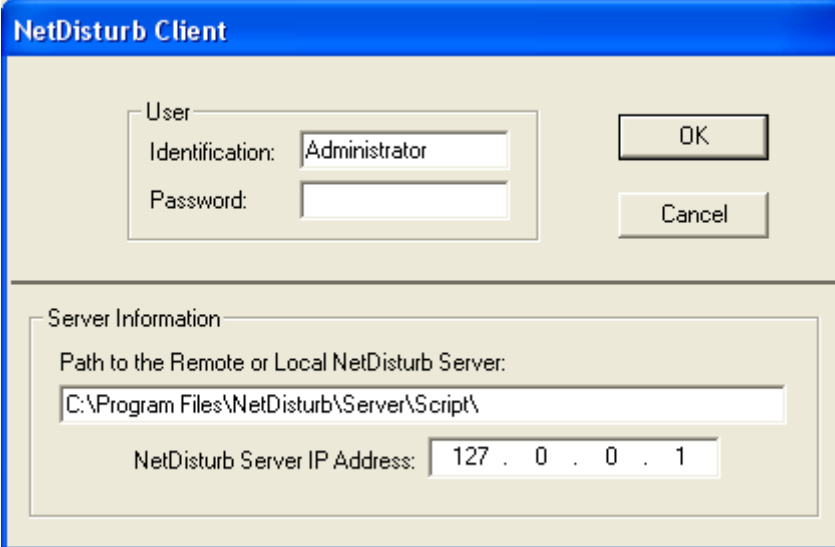
When you run NetDisturb Server for the first time, the default window is displayed:



No board (or NIC) has been selected: NetDisturb Client is used to select the network interfaces (or NICs).

2. To start the **NetDisturb Client**, click in the Start Menu on
'Start > Programs > NetDisturb > 2) NetDisturb Client'

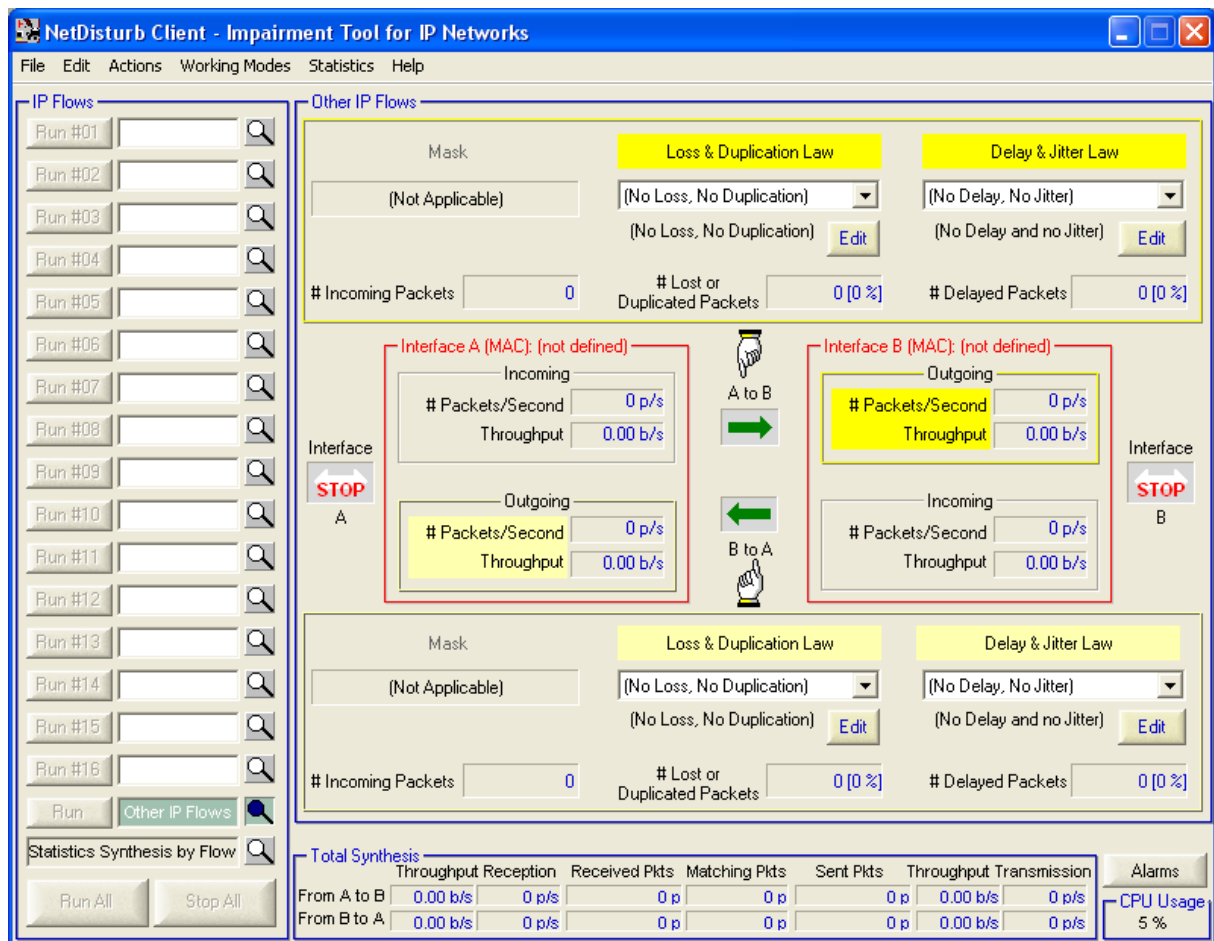
NetDisturb Client will ask you to input parameters, as shown in the following window:



The screenshot shows the 'NetDisturb Client' window. It has a blue title bar. Inside, there are two main sections. The top section is for user identification, with labels 'User Identification:' and 'Password:'. The 'User Identification' field contains the text 'Administrator'. To the right of these fields are 'OK' and 'Cancel' buttons. The bottom section is titled 'Server Information' and contains two fields. The first is 'Path to the Remote or Local NetDisturb Server:' with the text 'C:\Program Files\NetDisturb\Server\Script\'. The second is 'NetDisturb Server IP Address:' with the text '127 . 0 . 0 . 1'.

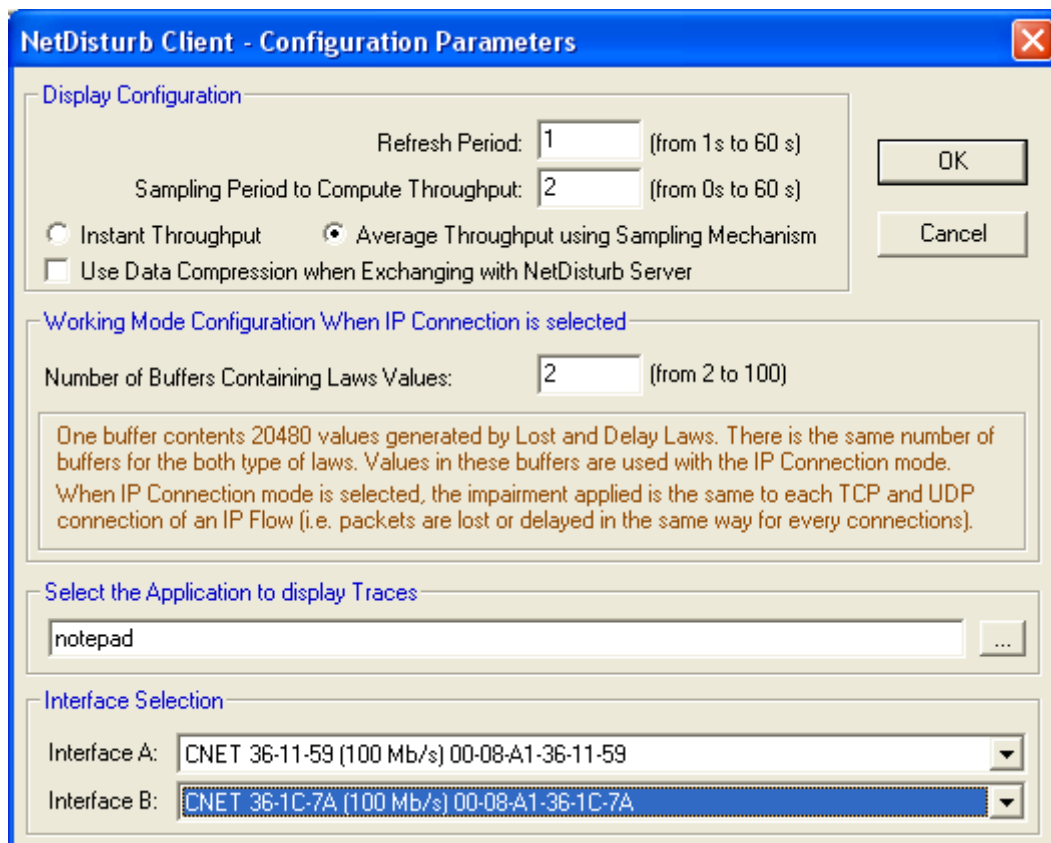
- **User Identification** = Administrator
- **User Password** = (no password needed)
- **Path to the remote NetDisturb Server** (Script folder) = C:\Program Files\NetDisturb\Server\Script (if NetDisturb Server is located at C:\Program Files\NetDisturb\Server)
- **NetDisturb Server IP address** = 127.0.0.1 (default local IP address, if NetDisturb Server is installed on the same system).

Click on “OK” and then the NetDisturb Client window is pop up:



Then, you should select the NICs that NetDisturb Server is going to use.

Open the “Action/Configuration” menu in the menu bar. The configuration parameters window is displayed:



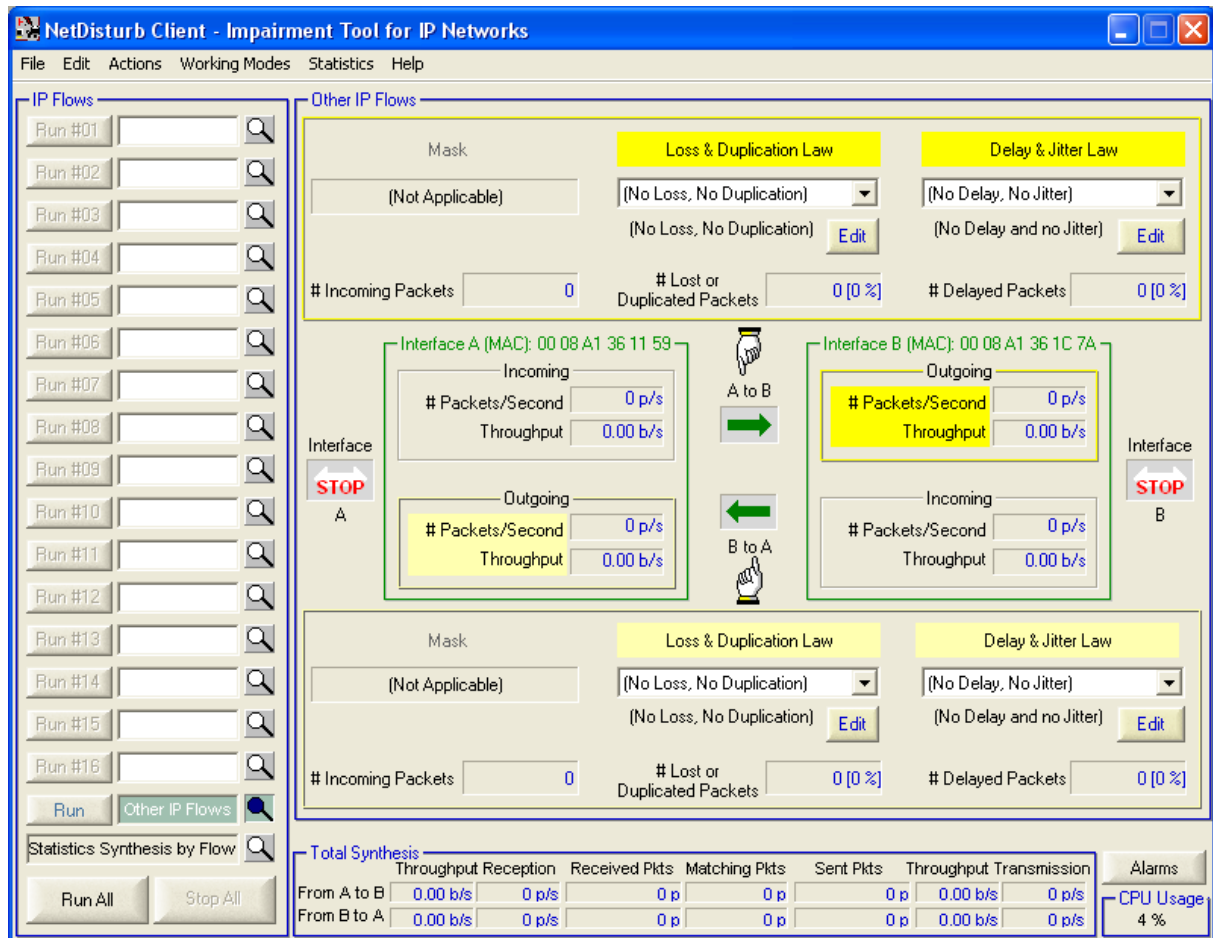
Select one NIC for Interface A and another NIC for Interface B, and then validate with “OK”.

Note: you must see in the combo-box (Interface A or Interface B) all NICs available and operational. If you don't see any NICs, please do the following steps:

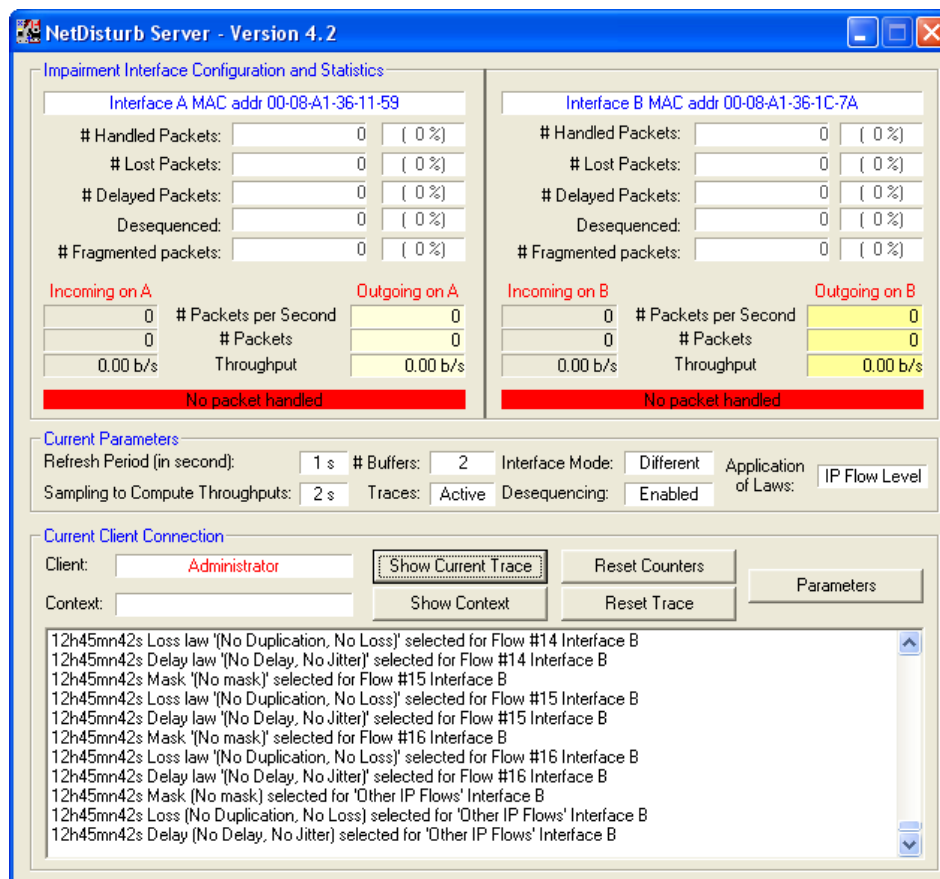
- Verify that your NICs are installed and enabled.
- Enable needed NICs.
- Stop NetDisturb Client.
- Stop NetDisturb Server.
- Reboot your system if necessary.
- Start NetDisturb Server.
- Start NetDisturb Client.

Then, you should see your installed NICs in the Interface A and B combo-boxes.

As soon as configuration is done, NetDisturb Server recognizes “Interface A” and “Interface B”. The MAC Address of the selected interfaces is displayed in the NetDisturb Client and NetDisturb Server windows:



Graphical user interface for NetDisturb Client with two Ethernet cards configured.



Graphical user interface for Server part with two Ethernet cards configured

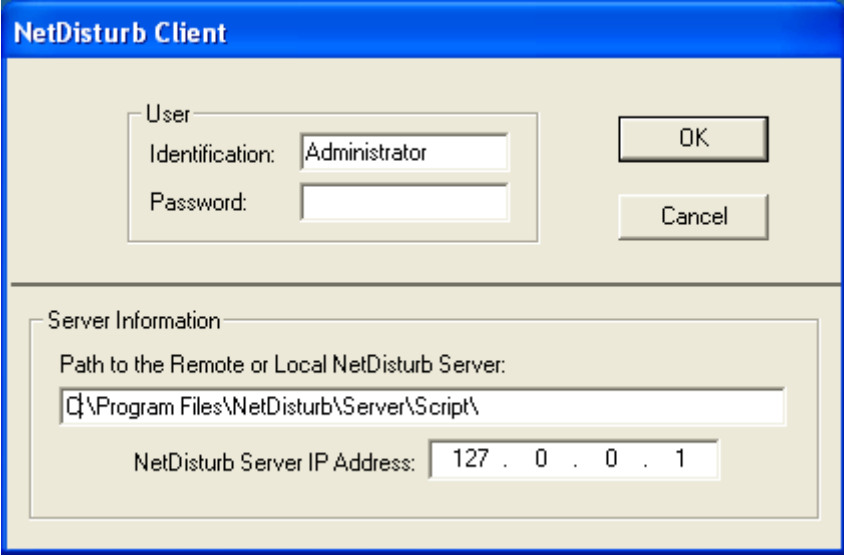
5.2 Detailed Description of Server and Client Startup

5.2.1 NetDisturb Server Startup Modes

Offered functionality level depends on the availability or not of NetDisturb Driver. If NetDisturb Driver is lacking, a message warns the user. In this case it is possible to continue, however only some functions will not be available - this is called “restricted mode”.

5.2.2 NetDisturb Client Startup Options

When starting the **NetDisturb Client**, the User identification and Server parameters window is displayed.



The user identification window is composed of two sections:

❖ User section

This section allows user identification. The identification could be either any user name, or the 'Administrator' name depending of the chosen mode (Administrator or User mode). Password is necessary only in association with Administrator name.

ADMINISTRATOR mode:

To be connected as Administrator, NetDisturb Client must provide the corresponding password. With this mode the NetDisturb Client functionalities are fully available: NetDisturb Client can modify laws, stop or activate the relaying process, change context, write or execute scenarios.

USER mode:

To be connected as User, NetDisturb Client provides a different identification than Administrator. Password is not necessary. NetDisturb Client functionality is reduced to the use of contexts located on the PC Server. Masks and laws can't be defined.

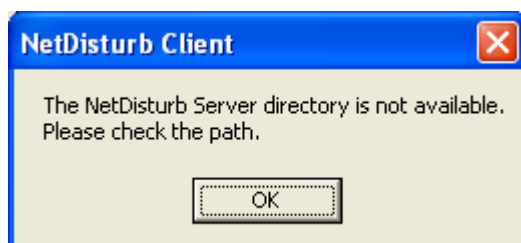
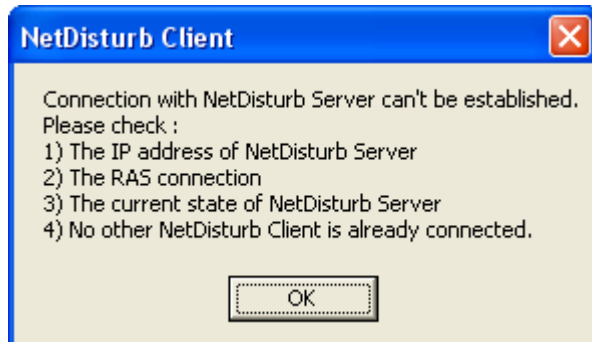
❖ Server Information section

In order to connect with NetDisturb Server, NetDisturb Client needs following information:

1. Path to the remote NetDisturb Server folder
This path is composed of two parts:
 - The drive, the virtual drive or the name of the NetDisturb Server machine.
 - The directory location of the NetDisturb Server where the script subdirectory (containing NetDisturb.tst) can be found.
2. NetDisturb Server IP address

In case of connection failure (if one of the parameters is invalid), an error window pops up to specify the connection error. Then the identification window is displayed again.

Errors windows may be:



Check:

- 1) The IP address is correct.
- 2) The RAS link is correctly established and that data are exchanged between client and server.
- 3) NetDisturb Server is running.
- 4) Another user is not already connected to NetDisturb Server or NetDisturb Client is already running on the Server machine.

Check that the remote machine name is correct. If necessary, try a connection with the remote machine using the Window Explorer: browse the Neighborhood Network until to reach the Script folder (this handling could reveal a necessary password to reach the Server)

5.2.3 Windows XP Service Pack 2

NetDisturb Client and NetDisturb Server use RPC to dialog. Windows XP Service Pack 2 may deactivate the RPC service. To activate it and to allow dialog between NetDisturb Client and NetDisturb Server, you need to change the registry.

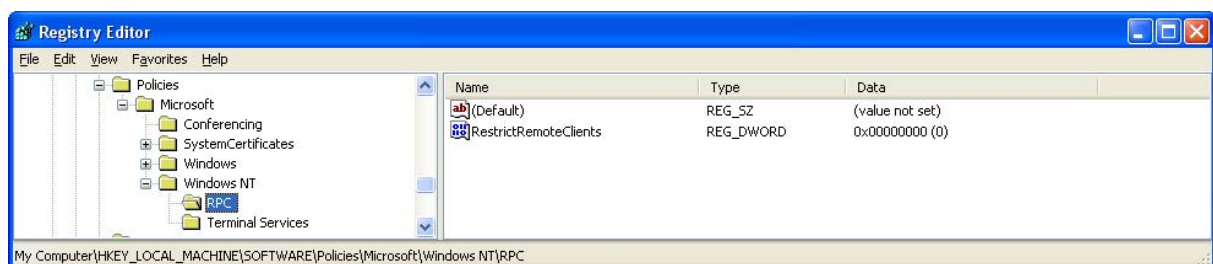
The registry key is:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\RPC

The value is:

RestrictRemoteClients REG_DWORD 0x00000000

If the value doesn't exist, you should create it. The result looks like the following figure:



The installation procedure creates the registry entry if needed and it set the value as explained above.

Part 6 Using NetDisturb Client

NetDisturb Client is the main NetDisturb Man to Machine Interface. With NetDisturb Client you can:

- ⇒ Select packet stream to process and configure impairments to apply,
- ⇒ Run / Stop traffic following the configured impairments,
- ⇒ Open, save... contexts,
- ⇒ Configure NetDisturb Server and NetDisturb Driver.

All parameters entered in NetDisturb Client are automatically transmitted to the NetDisturb Server.

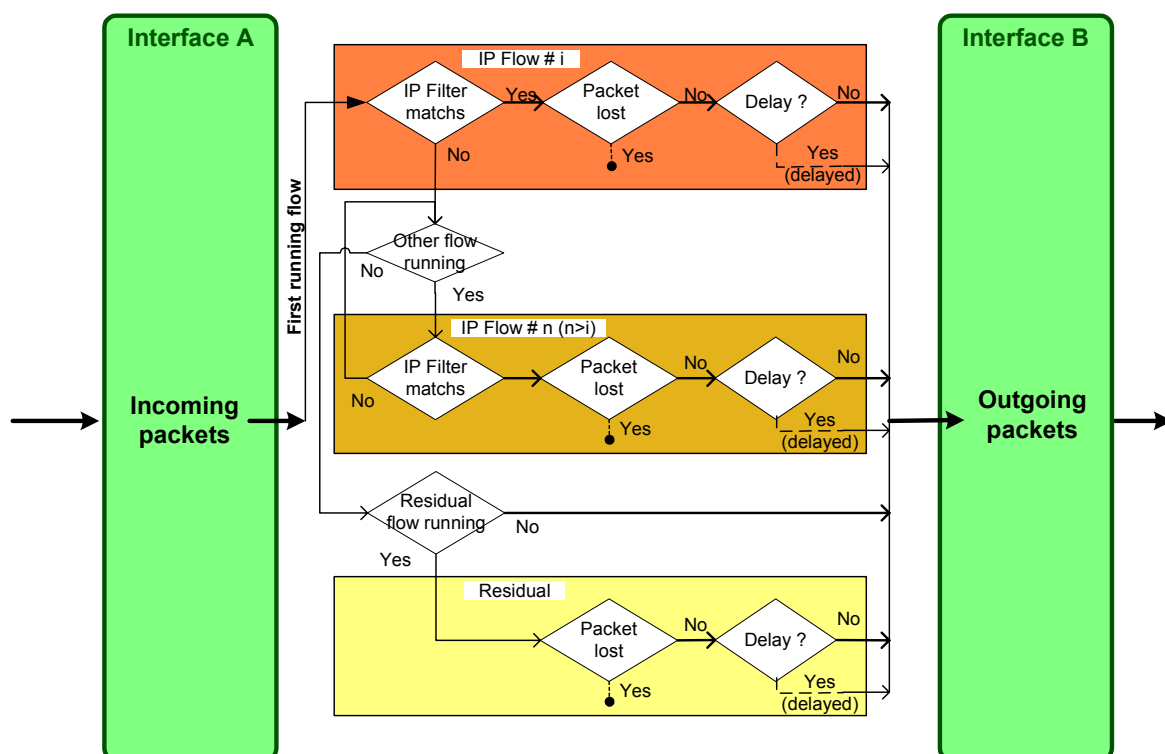
Remind

To use NetDisturb:

- ⇒ **First run NetDisturb Server**
- ⇒ **Then run NetDisturb Client**

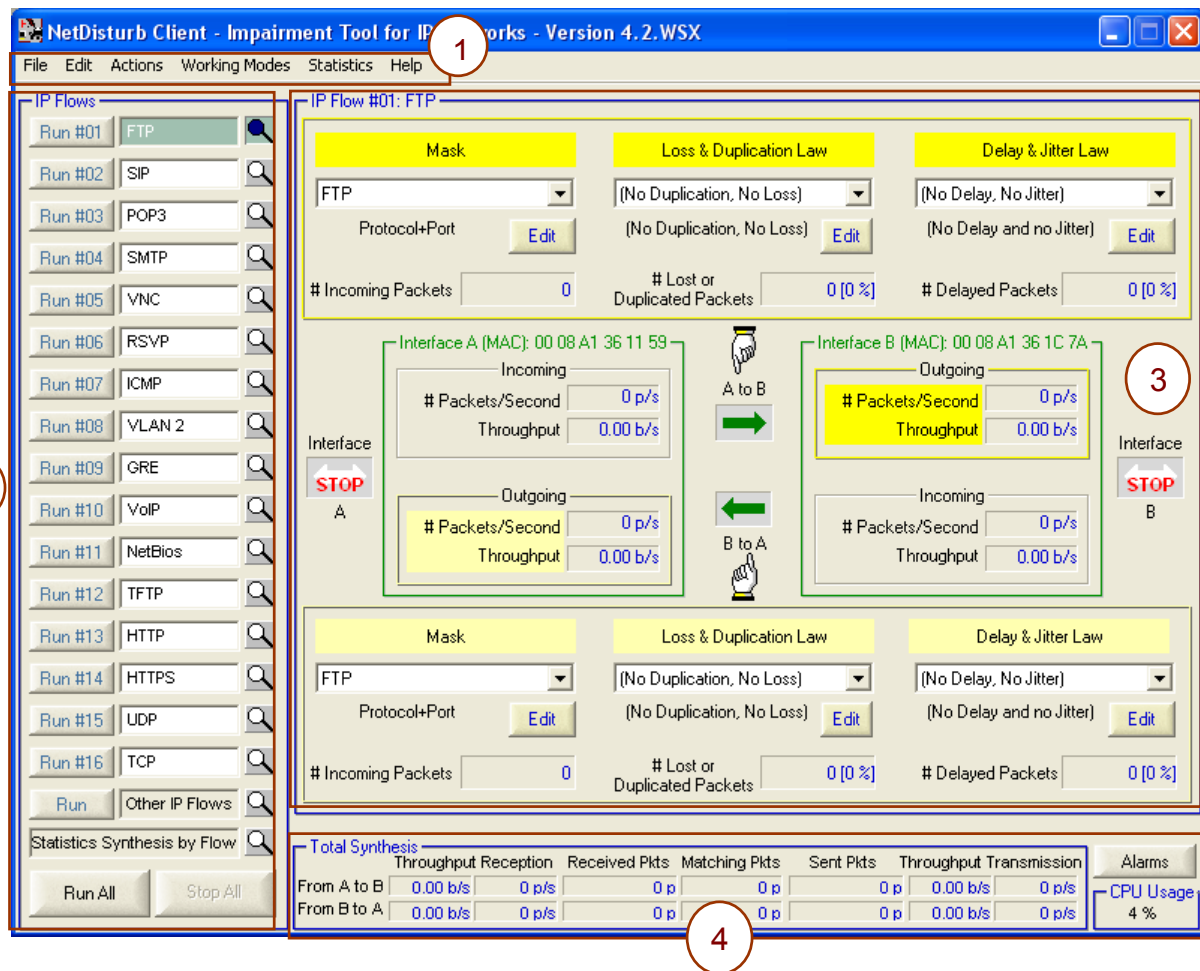
6.1 NetDisturb Client Main Window

The NetDisturb Client main window is displayed after client identification. Traffic and impairment representation on Client main window is based on the following scheme:



Treatments synoptic for selected packets in a flow from A to B
(B to A direction may be configured from the same manner, but isn't shown on this scheme)

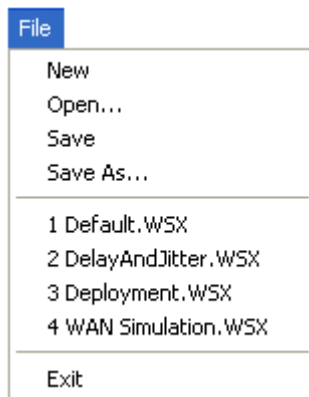
The NetDisturb Client main window is composed of four areas:



- 1 The menu is a standard application menu. Item of the menu are detailed in reply to paragraph 6.2.
- 2 The 'IP Flows' area lists mnemonic-names of flows. This area is used to start and to stop IP Flow unitary or all flows at the time. The loop button is used to selected flow individually. The last two flows have predefined behavior: The 'Other IP Flows' allows applying specific loss and delay laws to non-previously filtered IP packets. The 'Statistics Synthesis by Flow' loop summarizes flows #1 to #16 and the 'Other IP Flows' as shown in paragraph 6.3.
- 3 This central-part presents traffic statistics on each IP Flow #1 to #16 or the 'Other IP Flows'. It is used to create, delete and modify loss/duplication and delay/jitter laws, or IP masks.
- 4 The total synthesis area is a reference area where global statistics information is presented. It includes 'Alarms' returned by the NIC drivers or by NetDisturb Driver when memory errors occur. The CPU information is provided for information about load of the PC.

6.2 Menu Description

6.2.1 File Menu



In order to keep parameters configuration for further tests sessions, NetDisturb Client and NetDisturb Server use context files. Context files are saved as **.wsx** extension. They are usually saved in the Script folder of the NetDisturb Server directory.

A context file contains:

- Impairment parameters (selected mask & laws),
- Configuration values.

Default context is opened at each run of NetDisturb Client. The most recent files list is kept from sessions to sessions.

6.2.1.1 New

This command opens a new default context. The default context doesn't include laws.

6.2.1.2 Open

This command allows opening an existing context file (.WSX files). The version 4.1 contexts are imported silently.

6.2.1.3 Save

This command allows saving parameters and laws defined by User in a context file (.WSX files). The version 4.2 contexts can't be used by an older version of NetDisturb.

6.2.1.4 Save as

This command allows save parameters and laws defined by User in a context file, which name is requested in a standard dialog box. The version 4.2 contexts can't be used by an older version of NetDisturb.

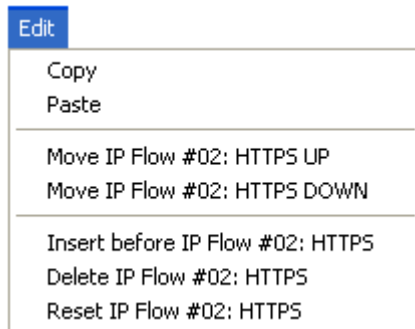
6.2.1.5 Recent Files

The 4 most recent files used are located in the file menu.

6.2.1.6 Exit

This command stops NetDisturb Client. If changes were made, the user gets the opportunity to save them into a context file.

6.2.2 Edit Menu



The edit menu helps to handle IP Flows.

6.2.2.1 Copy

The Copy item makes a copy of the current IP Flow into memory for further use. Copy includes current selected Mask, Lost Law and Delay Law of both directions. It includes the IP Flow mnemonic name too.

6.2.2.2 Paste

The Paste item changes current IP Flow parameters by the previously memorized IP Flow parameters, via Copy. It applies to the Mask, Lost Law and Delay Law of both directions, and to the IP Flow mnemonic name.

6.2.2.3 Move xxx Up

The Move Up item changes the selected IP flow to one position up. The Move Up item includes the item's mnemonic on which the operation applies. For example 'Move IP Flow #03 Up' switches IP Flow #03 with IP Flow #02, where the content of IP Flow #03 is moved into the second item, while the content of IP Flow #02 is moved into the third position. IP Flow mnemonic moves too if defined.

6.2.2.4 Move xxx Down

The Move Down item moves the IP flow location to one position down. The Move Down item includes the item's mnemonic on which the operation applies. For example 'Move IP Flow #04 Down' switches IP Flow #04 with IP Flow #05, where the

content of IP Flow #04 is moved into the fifth position, while the content of IP Flow #05 is moved into the fourth position. IP Flow mnemonic moves too if defined.

6.2.2.5 Insert before xxx

The 'Insert before ...' item makes a room available at current item location, whose mnemonic is added. Items located after the current item move one position down; this includes the current item. The current item becomes empty. The 16th item is lost. If the current item is the 16th, no change appends to the 15th previous but the current – the 16th - is reset.

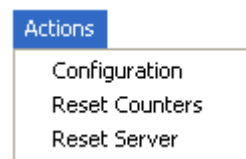
6.2.2.6 Delete xxx

The 'Delete before ...' item deletes the current item and moves lower items to one position up. The 16th item becomes empty.

6.2.2.7 Reset xxx

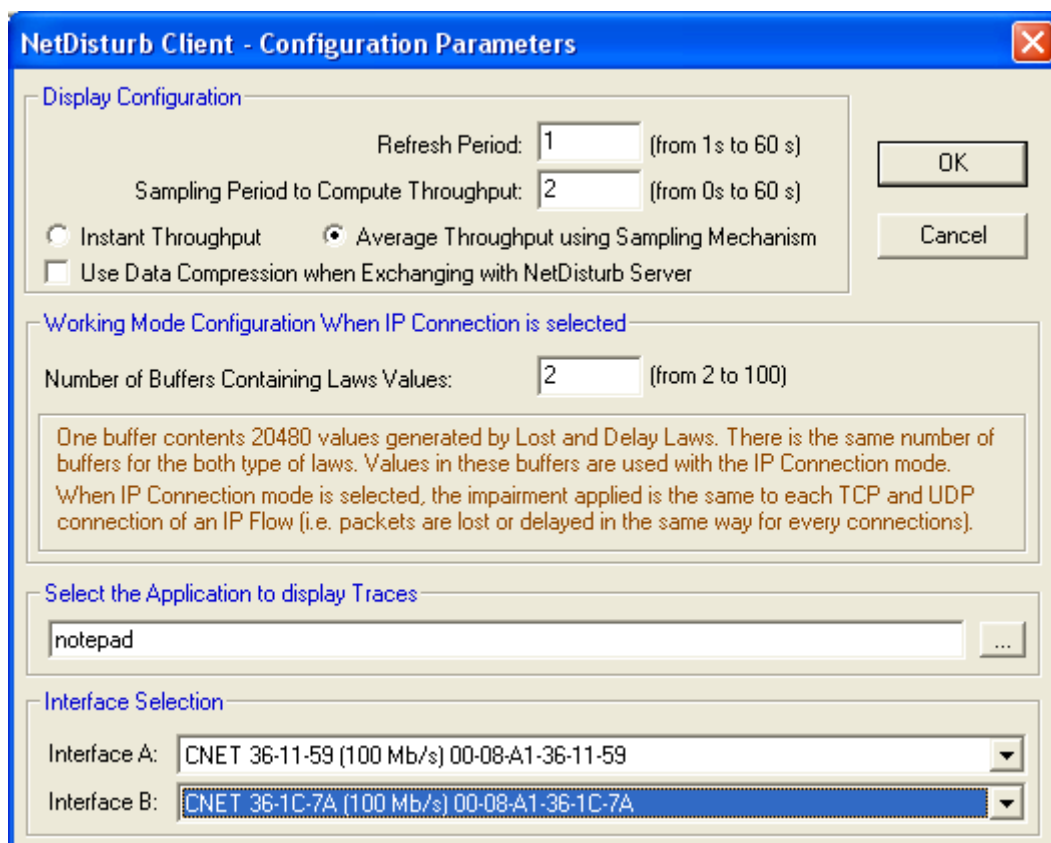
The 'Reset before ...' item set the content of the current item with default values. The IP Flow mnemonic is empty.

6.2.3 Actions Menu



6.2.3.1 Configuration

The Configuration Parameters window is displayed when the Configuration menu item is selected.



The window is divided in four parts: Display configuration, Multi-flow mode configuration, viewer to consult traces, and Ethernet board selection:

❖ Display configuration

From this area, User can:

- Define the refresh period for display of GUI's counters.
- Define the sampling period to compute throughput.
- Define the way throughput will be computed (instant or average by using sampling mechanism). Average computing means computing statistics with values of the latest x seconds (x is the sampling period). Instant computing means computing with value of the latest second.

Remark: Define an average throughput computing with a sampling period of 0 allows to obtained an average throughput on the whole period of NetDisturb use (since the last Reset).

- Activate or not the data compression of exchanges between Server and Client.

Remark: Data compression is useful when NetDisturb Client and NetDisturb Server exchange scenario or trace and are connected via ISDN or modem. When NetDisturb Client and NetDisturb Server are exchanging on the same PC, data compression is not relevant.

❖ Working Mode Configuration When IP Connection is selected

When NetDisturb is running in the IP Connection mode, user can define the number of buffers to allocate for the laws. The number of allocated buffers will be taken on Server machine RAM memory, said that one buffer consumes 80 Kb. (See “6.2.4.2” section).

❖ Select the Program to display Traces

From this section, User can define the full path name of the program used to read traces (word processor program). Notepad is entered by default.

❖ Interface selection

This section allows selecting the Ethernet cards to use.

6.2.3.2 Reset Counter

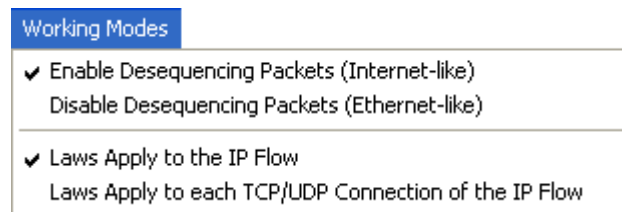
The Reset counter item impacts both local Client and Server counters. It set to zero all counters and percentage. It doesn't reset Laws counters in use by lost and delay laws i.e. counters used in Associated Uniform Lost law or Fixed Throughput / Fixed Throughput Extended delay laws.

6.2.3.3 Reset Server

The Reset server item stops the Server Part. When the Server stops, the NetDisturb Driver is stopped too. Then the Client is closed and the user should restart the Server and Client parts manually.

To stop and to free pending packets, you should reset the server. When you stop the IP Flow, pending packet remains in the output queue.

6.2.4 Working Mode Menu



Impairment may introduce changes in the packet sequence. It is an option to keep the packet sequence or not.

NetDisturb Driver analyzes IP packets to split them into the TCP or UDP connection they belong to. This mode makes possible to apply the same impairment values to each packet of each connection, e.g. to loose the third packet of each connection.

6.2.4.1 Enable/Disable Desequencing Packets

One of the Ethernet characteristics is to keep packets received in order. Internet hasn't this constraint regarding the packet ordering: some packets can use one way while others another one, with the consequence the receiver may get packets unordered. NetDisturb Driver can simulate an Internet network or can react as Ethernet does.

How NetDisturb creates an unordered case:

It may append a delay to apply to one packet makes this packet to be sent before previous ones, because the delay to apply to the latest packet is smaller than the inter-packet delay and the delay applied to older packets are reduced to be sent before the new packet.

6.2.4.2 IP Flow versus TCP/UDP Connection IP Flow Mode

❖ IP Flow

When the 'Law Apply to the IP Flow' option is selected, every packet meeting running filter masks requirements are considered to belong to the same flow. Processing is carried out in "continue". When User defines to loose 1 packet on 3, the third received packet is lost, whatever the TCP/UDP connection it belongs to.

❖ Connection IP Flow

When the 'Law Apply to each connection of the IP Flows' is selected, NetDisturb Driver analyses each IP packet trying to put the IP packet into a TCP or UDP connection, using protocol, IP addresses and port numbers. If the connection doesn't exist, a new one is created.

Let's take an example. When the [Connection IP Flow](#) is selected, if the lost law is to loose 1 packet on 3, the third packet of each TCP or UDP connection will be lost. Up to 10000 connections can be handled simultaneously.

A flow disappears automatically when the TCP connection is closed and after a configurable time for UDP connections. This time is configurable in the Registry parameters of the NetDisturb Driver.

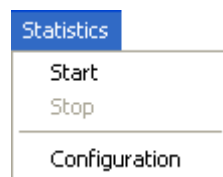
❖ Buffers (for Connection IP Flow only)

The number of buffers defines the number of values (delay or loss) kept by NetDisturb Driver and used for each [Connection IP Flow](#).

One buffer contains 20480 values and the minimum number of buffers is 2.

In [Connection IP Flow](#) mode, NetDisturb Server generates delay and lost values as much as NetDisturb Driver can keep. When NetDisturb Driver detects a new flow, it gets its own pointer to lost and delay values exclusive of other flows. This pointer starts at the beginning of the set of values. In case of connection with a large number of packets, the pointer increases fast; when connections have few packets their pointer increases slowly. When the pointer reached the latest value, it restarts at the beginning in a circular way.

6.2.5 Statistics



NetDisturb Client statistics can be saved into a text file. Values saved are shown in the 'Statistics Synthesis' view (see 6.3 for more details). They are saved at the same rate they are visually refreshed.

Columns and IP Flows to put in the statistics file can be selected via the configuration dialog box.

6.2.5.1 Start

Start to save statistics into the file. An abstract of each selected connection (Mask name, Lost and Delay law) is saved at the beginning of the file, followed by the list of statistics, one column per statistics.

Each following record gets the format:

Column separated by a tab	Comment
MM/DD/YYYY hh:mm:ss.mmm	Month/Day/Year Hour:Minute:Second.millisecond
#xx	Connection number
<i>Statistic value</i>	One value per selected statistic

When the statistics are writing, the file can be opened for reading but it can't be changed.

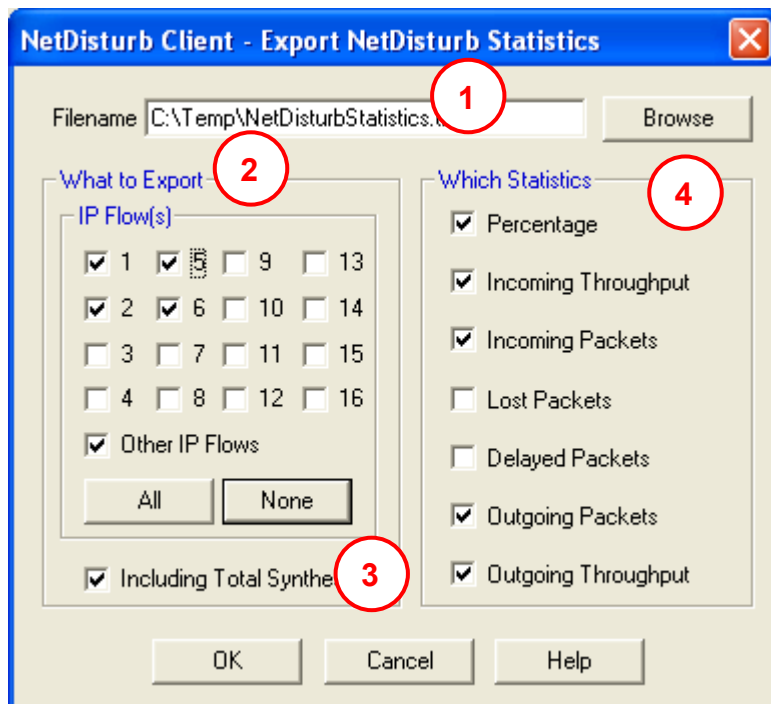
Throughput values are expressed in Kbps.

6.2.5.2 Stop

Stop to save statistics into the file. The file can be renamed or copied.

6.2.5.3 Configuration

This option allows defining various configuration parameters.



Statistics can start if at least the filename, one flow and one Statistics item are selected.

❖ Filename ①

The filename edit box contains the target file name where statistics will be written. If the file still exists, new statistics are appended at the end of the file.

❖ What to Export ②

This section is used to select IP Flow to include in the statistics file. IP Flow #01 to IP Flow #16, plus the **Other IP Flows** can be selected. The Total Synthesis ③ refers to the bottom part of the Client Windows (part 4 in the detailed description 6.1).

❖ Which statistics ④

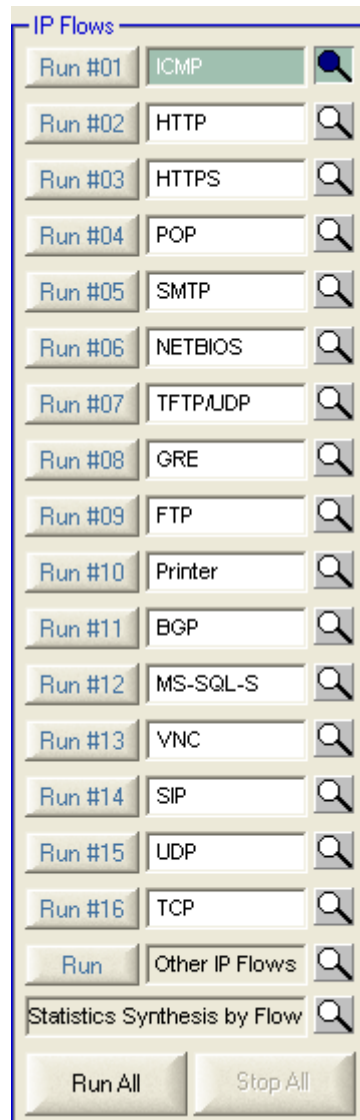
This section is used to select the statistic items to save.

- Rx and Tx Throughput
These statistics include the volume throughput (b/s, Kb/s, etc) and the packet throughput (packet per second)
- Packets Filtered, Lost or Delayed
These statistics include the number of packets and the percentage
- Packet Sent
This statistic includes the number of packets

6.3 IP Flows

This section describes the IP Flow Client part area.

6.3.1 General Description



Left buttons (Run #xx/Stop #xx)



- Each IP Flow can be started or stopped unitary.
- The button 'Run/Stop #xx' indicates the status of the IP Flow will get if the button is pressed. This button is grayed when Interface A and B aren't defined.

Edit area



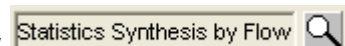
- IP Flow #01 to IP Flow #16 can be named with a mnemonic that helps to remember impairment parameters or filter mask used.
- The Other IP Flows can't be renamed: it has specific characteristics described in paragraph 6.3.3.

Loop buttons



- This button is used to access the details configuration and statistics of a specific IP Flow.
- The color changes to show the current status of the flow.

Statistics Synthesis flow



- When selecting this view by pressing the loop button, the user can get an abstract of the activity of all flows. Details can be found in paragraph 6.3.4



Bottom buttons

- The 'Run All' button starts all non-yet-started IP Flows, event IP Flows that don't have a filter defined.
- The 'Stop All' button stops all running IP Flows.

6.3.2 Status of IP Flows

Idle status

The idle status is the default status of the IP Flow. It is indicated by the button 'Run #XX' and by the loop with a white color as shown:



If IP Flow details are shown, the edit part and loop button is **pale green**, whatever the status is:



Active Status

The active status is indicated by the button 'Stop #XX' pressed and the loop button **orange** as shown:



When the current IP Flow is in active state, the active status is indicated by the button 'Stop #XX' remains pressed but the label and the loop are **orange**, as shown:



6.3.3 The Other IP Flows Entry

The **Other IP Flows** is in charge to handle IP packets that haven't been filtered by IP Flows #01 to #16. This is why the filter mask isn't available for this IP Flow.

This flow can be used to filter other IP packets not defined by previous IP Flows.

The same operations apply to this '17th' flow as other flows (Run/Stop, Run All / Stop All, etc.)

The colored rules described in paragraph 6.3.2 are relevant to the **Other IP Flows**.

6.3.4 The Statistics Synthesis View

The next picture shows the statistics Synthesis view, when with IP Flow running.

The screenshot shows the NetDisturb Client interface. On the left, there is a list of IP flows (Run #01 to Run #16) with protocols like FTP, SIP, POP3, SMTP, VNC, RSVP, ICMP, VLAN 2, GRE, VoIP, NetBios, TFTP, HTTP, HTTPS, UDP, and TCP. The main table displays statistics for these flows, including Incoming Throughput, Incoming Pkts, Lost Pkts, Delayed Pkts, Outgoing Pkts, and Outgoing Throughput. At the bottom, the 'Statistics Synthesis by Flow' section is active, showing a 'Total Synthesis' table with columns for Throughput Reception, Received Pkts, Matching Pkts, Sent Pkts, and Throughput Transmission. A red arrow points to the 'Statistics Synthesis by Flow' button in the bottom left corner.

To get this view, the user has pressed the loop button of the 'Statistics Synthesis by Flow' item.

6.3.4.1 Detailed Description

IP Flows	%	Incoming Throughput	Incoming Pkts	Lost Pkts	Delayed Pkts	Outgoing Pkts	Outgoing Throughput
#01 { A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#01 { B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s

There is one line per direction of the exchange. The upper line refers to the Interface A to Interface B direction. The second line is the opposite direction.

IP Flows

This column presents the flow number and the direction reference

%

This column presents the flow number and the direction reference

Incoming Throughput

This column presents the instant throughput, computed between two refresh periods. Both volume and packet throughputs are shown.

The Incoming Throughput shown in the upper line refers to data received by the 'Interface A' applying the IP Filter mask (or 'Interface B' for the second line respectively).

Incoming Pkts

This column presents the number of packet received. It is a cumulated value.

Lost Pkts

This column presents the number of packet lost, and the percentage of those packets regarding the global number of packets filtered, for the relevant direction.

Delayed Pkts

This column presents the number of packet delay, and the percentage of those packets regarding the global number of packets filtered (column **Incoming Pkts**), for the relevant direction.

Outgoing Pkts

This column presents the number of packet sent from one interface to the other. It is the number of packets filtered (column **Incoming Pkts**) minus the number of packets lost (column **Lost Pkts**), for the relevant direction.

Outgoing Throughput

This column presents the instant throughput, computed between two refresh periods of packet sent to the outgoing Interface. Both volume and packet throughputs are shown.

The Outgoing Throughput column shown in the upper line refers to data sent to the Interface B (or Interface A for the second line respectively).

When some IP Flows are active, corresponding lines are colored as shown:

NetDisturb Client - Impairment Tool for IP Networks - Version 4.2.WSX

File Edit Actions Working Modes Statistics Help

IP Flows

Stop #01 FTP [Icon]
Run #02 SIP [Icon]
Stop #03 POP3 [Icon]
Stop #04 SMTP [Icon]
Run #05 VNC [Icon]
Run #06 RSVP [Icon]
Stop #07 ICMP [Icon]
Run #08 VLAN2 [Icon]
Run #09 GRE [Icon]
Run #10 VoIP [Icon]
Stop #11 NetBios [Icon]
Run #12 TFTP [Icon]
Stop #13 HTTP [Icon]
Run #14 HTTPS [Icon]
Stop #15 UDP [Icon]
Stop #16 TCP [Icon]
Stop [Icon] Other IP Flows [Icon]

Statistics Synthesis by Flow [Icon]

Run All Stop All

IP Flows	%	Incoming Throughput	Incoming Pkts	Lost Pkts	Delayed Pkts	Outgoing Pkts	Outgoing Throughput
#01 A to B	4	263 Kb/s	36 p/s	1051	0 [0 %]	1051 [100 %]	246 Kb/s
B to A	1	282 Kb/s	44 p/s	1194	0 [0 %]	1194	282 Kb/s
#02 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#03 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#04 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#05 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#06 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#07 A to B	0	592 b/s	1 p/s	52	0 [0 %]	52	592 b/s
B to A	0	592 b/s	1 p/s	126	0 [0 %]	126	592 b/s
#08 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#09 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#10 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#11 A to B	0	0.00 b/s	0 p/s	1	0 [0 %]	1	0.00 b/s
B to A	0	0.00 b/s	0 p/s	1	0 [0 %]	1	0.00 b/s
#12 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#13 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#14 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
#15 A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	14	0 [0 %]	14	0.00 b/s
#16 A to B	96	925 Kb/s	455 p/s	27571	0 [0 %]	27312	903 Kb/s
B to A	98	3.88 Mb/s	699 p/s	80169	0 [0 %]	80169	3.88 Mb/s
..... A to B	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s
B to A	0	0.00 b/s	0 p/s	0	0 [0 %]	0	0.00 b/s

Total Synthesis

	Throughput Reception	Received Pkts	Matching Pkts	Sent Pkts	Throughput Transmission
From A to B	1.16 Mb/s	491 p/s	28675 p	28381 p	1.12 Mb/s
From B to A	4.16 Mb/s	745 p/s	81630 p	81630 p	4.16 Mb/s

Alarms [Red Button]
CPU Usage 18 %

6.4 Impairment Parameters and associated Commands

Impairment parameters are Mask, Loss laws and Delay laws. These parameters can be modified from the top (for A to B direction) and bottom part (for B to A direction) of the NetDisturb Client main window.

Mask	Loss & Duplication Law	Delay & Jitter Law
TCP	Duplicated if not Lost	Exponential Jitter
Protocol	Loss then Duplicate 1/10 & 1/20	Delay & Exponential Jitter From 20ms to 72ms
# Incoming Packets	# Lost or Duplicated Packets	# Delayed Packets
17191	1719 [10 %]	15472 [90 %]

Top part of Client main window

This frame is composed of three parts: IP Filter mask, Loss law and Delay law.

In each part, you will find one “combo-box”, which allows selecting process to apply. Below this “combo-box”, there is a “comment” area which sums up the selected processing features.

“Edit” button allows reaching configuration window of the impairment parameter.

❖ Mask

On the left part, the IP Filter mask is presented. This parameter allows selecting packets to process. The number of packets that meet the mask is displayed (# Incoming Packets) below the list box. The percentage, displayed in parenthesis just besides, is the number of filtered packets for that IP Flow on the total packets filtered.

❖ Loss & Duplication Law

This part presents the loss and/or duplication law applied on the selected packets. It displays the number of lost packets and the ratio of packets lost on the number of filtered packets for the current IP Flow.

There isn't any counter about the duplication but the number of outgoing packet includes the number of duplicated packets.

❖ Delay & Jitter law

The right part of the frame presents the delay law applied to the filtered packets that were not lost. The number of delayed packets and the percentage of delayed packets on number of filtered & no lost packets are displayed.

Once created a new mask or a new law, it will be available in the list box for the two directions.

6.4.1 Selection of a Filter Mask, or Lost and Delay/Jitter Law

To change the selection of the mask (or law), select the requested mask (or law) from the list. The mask (or the law) is automatically selected.

6.4.2 Mask Configuration

A mask is a set of parameters to select the packets to lose and to delay. It is composed of a combination of nine items where each one of them is optional:

1. MAC Destination Address
2. MAC Source Address
3. VLAN-ID **list** (802.1Q)
4. Type Of Service (TOS)
5. Protocol
6. IP Destination Address
7. IP Source Address
8. Destination Ports **list**
9. Source Ports **list**

The **list** format is detailed in the paragraph 6.4.2.5.

By default, the following masks are included in the file Default.wsx:

Combo-box	Comment area	Description
(No mask)	<i>No parameter</i>	This mask disables the IP Flow because no packet can match a Mask without selection criteria.
TCP	Protocol	This filter considers only IP packets with a protocol set to TCP.
UDP	Protocol	This filter considers only IP packets with the UDP protocol.
HTTP	Protocol+Ports	This filter considers IP packets with the TCP protocol and the destination ports 80 or 8080.
FTP	Protocol+Ports	This filter considers IP packets with the TCP protocol and the destination ports 20 or 21.
SMTP	Protocol+Ports	This filter considers IP packets with the TCP protocol and the destination port 25.
POP3	Protocol+Ports	This filter considers IP packets with the TCP protocol and the destination port 110.
VNC	Protocol+Ports	This filter considers IP packets with the TCP protocol and the destination port 5900.
HTTPS	Protocol+Ports	This filter considers IP packets with the TCP protocol and the destination port 435.
TFTP	Protocol+Ports	This filter considers IP packets with the UDP protocol and the destination port 69.
NTP	Protocol+Ports	This filter considers IP packets with the TCP protocol and the destination port 123.
TELNET	Protocol+Ports	This filter considers IP packets with the TCP protocol and the destination port 23.
GRE	Protocol	This filter considers IP packets with the GRE (x2F) protocol.
RSVP	Protocol	This filter considers IP packets with the RSVP (x2E) protocol.
ICMP	Protocol	This filter considers only IP packets with ICMP (01) protocol.
NETBIOS	Protocol+Ports	This filter considers IP packets with the TCP protocol and destination ports 137, 138 or 139.
Printer/Port	Protocol+Ports	This filter considers IP packets with the TCP protocol and destination port 9100.
VLAN	VLAN-ID	This filter considers IP packets when the VLAN ID is included between 1 and 5.

Other protocols may be defined, depending the sub-release of the product.

To edit a new mask click on “Edit” button from the main window in the Mask area.

The screenshot shows the main window of the NetDisturb Client. It has three main sections: 'Mask', 'Loss & Duplication Law', and 'Delay & Jitter Law'. In the 'Mask' section, the 'Protocol' dropdown is set to 'TCP' and the '# Incoming Packets' is 17191. The 'Edit' button next to the 'Protocol' dropdown is circled in red. In the 'Loss & Duplication Law' section, the 'Loss then Duplicate' is set to '1/10 & 1/20' and the '# Lost or Duplicated Packets' is 1719 [10 %]. In the 'Delay & Jitter Law' section, the 'Delay & Exponential Jitter' is set to 'From 20ms to 72ms' and the '# Delayed Packets' is 15472 [90 %].

The following window is pop up:

The screenshot shows the 'NetDisturb Client - Edition of Masks' dialog box. It has a title bar with a close button. The dialog is divided into several sections:

- Mask Identifier:** Contains a 'Current List' dropdown set to 'HTTP', a 'New Identifier' text field, and buttons for 'Rename', 'Delete', and 'Add'.
- Important:** A text box containing two notes:
 - * A Mask combines different optional parameters: Ethernet header, list of VLAN-ID, IP header and list of ports.
 - * The same mask can be used for the directions A to B and B to A. According to the direction from which you edit the mask, the following parameters will be inverted: destination and source addresses (MAC & IP), destination and source of ports lists.
- Mask Definition:** Contains four sub-sections:
 - Mask related to the Ethernet Header:** Fields for 'MAC Destination Address' and 'MAC Source Address' (hexadecimal).
 - Mask related to VLAN (802.1Q):** Field for 'VLAN-ID List' (see note 1).
 - Mask related to the IP Header:** Fields for 'Type of Service (byte)' (none), 'Protocol' (06 TCP), 'Destination IP Address', and 'Source IP Address' (decimal) (see note 2).
 - Mask related to the Protocol (available with UDP and TCP protocols):** Fields for 'Destination Port List' (80;8080) and 'Source Port List' (see note 1).
- Buttons:** 'Add Changes into the Mask' and 'Reset the Mask Definition'.
- Notes:**
 - Note 1:** As VLAN-ID list and lists of ports, you can enter:
 - a range of values (i.e from 120 to 250 should be written 120-250)
 - or individual values separated by semicolon (i.e. 500;600)
 - or both (i.e. 500;550-560;599)
 - Note 2:** The Type of Service and Protocol fields accept User-defined values. The syntax is the following:
 - 2 hexadecimal digits,
 - at least one space followed by an optional mnemonic text.
- Bottom Buttons:** 'OK' and 'Cancel'.

This window is composed of 2 main areas: mask identifier and mask definition, with various buttons.

The reference for the Source and Destination addresses and ports depend on the original Interface 'Edit selection. In case the 'Edit' button from the Interface A was pressed, the direction from Interface A to Interface B is the reference direction. If the mask is re-edited from the Interface B, then fields Source and Destination are inverted automatically by NetDisturb Client to match the new direction.

6.4.2.1 Mask Identifier

The mask identifier is used to select an existing mask in the “Mask Identifier” combo-box. An existing mask can be deleted by pushing the “Delete” button.

From this part, User can also add a new mask, by entering a name in the “New Identifier” area and clicking on “Add” button”.

6.4.2.2 Mask Definition

The central part of the window is dedicated to the parameters that the mask defines. When a parameter is defined, the IP packet should contain all parameters of the mask to belong to the IP Flow.

A mask is defined by the combination of four types of parameters:

Ethernet header

- **MAC destination address** (enter a hexadecimal value)
- **MAC source address** (enter a hexadecimal value)

VLAN-ID list

- **VLAN-ID number** (enter a decimal value or a list – see 6.4.2.5 for more details).

The VLAN-ID can be used only with Ethernet type 8100 frames. In that case, the IEEE 802.1Q format is assumed.

Dest.	Src.	TPID	TCI	Standard Ethernet Frame
-------	------	------	-----	-------------------------

TPID means **T**ag **P**rotocol **I**dentifier. It is equal to 8100.

TCI means **T**ag **C**ontrol **I**nformation. It includes the VLAN-ID as shown:

TCI	→	Prioritv	CFI	VLAN ID
16 bits		3 bits	1 bit	12 bits

IP Header

- **Type of Service (TOS)** – Select an existing value or enter a new hexadecimal value (2 digits plus an optional comment)
- **Protocol** (ICMP, TCP, UDP, ...) – Select an existing value or enter a new hexadecimal value select a protocol by using the combo-box (2 digits plus an optional comment)
- **IP destination address** (enter a decimal value: ex. 192.168.000.017)
- **IP source address** (enter a decimal value: ex. 194.001.001.076)

Ports (for TCP or UDP packets)

- **Destination port number** (enter a decimal value or a list – see 6.4.2.5 for more details)
- **Source port number** (enter a decimal value or a list – see 6.4.2.5 for more details)

Each parameter of a mask is optional. When sets, the parameter(s) should be present in the IP Frame to match the mask.

Each mask is defined in reference to a direction in order to identify to which interface the source and destination addresses belongs to. Eventually, if processing is applied on the other direction, NetDisturb Driver reverses automatically the source and destination addresses and ports.

6.4.2.3 Action Buttons

To manage the Mask list, various buttons are available:

Rename: This button should be used to change the Mask identifier.

Delete: This button should be used to remove a Mask from the current list.

Add: This button should be used to insert a new Mask Identifier into the current Mask Identifier list.

Add Changes into the Mask: This button saves the values for the current mask. It inserts the new Mask Identifier if the Identifier was not already in.

Reset the mask definition: This button blanks all fields.

OK: This button saves in the current context all modifications made i.e. new Mask identifiers as well as changes on the existing masks.

Cancel: This button ignores all modifications made i.e. new Mask identifiers as well as changes on existing mask.

6.4.2.4 To Create a New Mask

1. Enter a name in the "New Identifier" edit field,
2. Click on "**Add**" to memorize the Identifier,
3. Define mask parameters in the "Mask definition" area,
4. Click on "**Add Changes into the Mask**" to save this new mask,
5. Press "OK" to quit the "Edit a mask" window or restart the operation at 1.

Up to 100 masks can be created.

6.4.2.5 List of Values

Some parameters in the Filter mask can be a list of values. To match the filter, the IP packet should include one value from the list. The syntax of lists allows a set of individual values or ranges of values. Both individual values and ranges can be mixed. **Values are decimal.**

The separator character between individual values or ranges is semi-coma (;). The syntax used is very near the syntax of the printer for a set of pages.

6.4.2.5.1 Individual Value

An individual value is one and only one value.

Ex: 135

6.4.2.5.2 List of Individual Values

A list of values is multiple individual values, each separated by a semi-coma.

Ex: 25; 80; 110; 435

6.4.2.5.3 Range of Values

A range of values is a set of values indicated by the first and the last of the range of the range, both included. The first value is separated from the last value by a dash

Ex: 2009-2020; 3000-3100

6.4.2.5.4 Complex List

Here is an example including individual and ranges.

List: **12; 13; 25-30; 50-100; 120**

Values matching: 12, 13, 25 to 30 included, 50 to 100 included, and 120

Values not matching: 11, 24, 31, 101, 119, and 121

6.4.3 Loss/Duplicate laws Configuration

NetDisturb is able to loss and/or duplicate packets. Three modes are available:

- NetDisturb losses the selected IP packets following mathematical laws configured by User, following a percentage, a 1 on N law or following values extracted from a user file.
- NetDisturb is able to duplicate IP packets following the Uniform mathematical law configured by User, following a percentage or a 1 on N law.
- NetDisturb is able to loss packets the duplicate non-lost packets following a 1 on N law.

Up to 100 Loss/Duplication laws can be created.

By default the following laws are defined in the Default.wsx context file:

Combo-box (law identifier)	Comment area	Description
(No Duplication, No Loss)	(No duplication, No Loss)	With this option, no duplication and no loss applies to the IP Flow.

<i>Loss laws</i>		
Constant Loss	Button "Lose 12 packets"	12 packets are lost each time the user activates this button.
Uniform Loss	Uniform Loss From 1 to 100	Domain values [1 to 100] Threshold = 30
Burst Uniform Loss	Burst Uniform Loss Domain: [10. – 1000.]	Domain values [10 to 1000] Threshold (n) = 350 Threshold (n+x) = 380 Depth = 2
OnePerTen	User-defined Loss File	Sample file: OnePerTen.txt Loss of 1 packet per 10 packets
Percentage Loss	Percentage Loss 15%	Percentage: 15
One each 10 Loss	Range Loss 1/10 (10%)	Range (N): 10

<i>Duplication laws</i>		
Percentage Duplication	Duplicate 10%	Percentage = 10 % Minimal Duplication = 1 Maximal Duplication = 3
Duplication 1 Packet every 20	Range Duplication 1/20 (5%)	Range (N): 20 Minimal Duplication = 1 Maximal Duplication = 3
Uniform duplication	Uniform Duplicate From 1 to 50	Alpha: 1 – Beta: 50 Threshold: 10 Minimal Duplication = 1 Maximal Duplication = 1
Duplicate if Not Loss	Loss else Duplicate 1/100 & 1/50	Loss Range (N): 100 Duplication Range (M): 50 Minimal Duplication = 1 Maximal Duplication = 3

6.4.3.1 Loss Laws and Working Mode

Working Mode: Laws applying to IP Flows

When a loss law is selected on a given IP Flow, the law applies to all packets matching the mask. For each new packet, a new loss value is extracted from the law or from the file, depending on the type of law selected. These values are stored in a global table by NetDisturb. When the table is empty, NetDisturb Server provides a new table to NetDisturb Driver with new values depending on the law.

This value is compared to the Threshold: if the value is greater or equal than the Threshold, the packet is lost. Otherwise, the packet continue to be handled and may be delayed.

Working Mode: Laws applying to each TCP/UDP connection of the IP Flows

When a loss law is selected on a given IP Flow, the law applies to all packets matching the mask.

These values are stored in a table maintained by NetDisturb. NetDisturb Server provides once a table to the NetDisturb Driver with values depending on the law. NetDisturb loops on values from this table: when the end of the table is reached, NetDisturb Driver restarts at the beginning.

If the packet is TCP or UDP, the 5-tuple IP addresses, protocol and ports is used to classify the packet. Else, only the IP addresses and protocol are used. For each packet, a loss value is extracted from the loss value buffer, at the current index of the packet of the given connection. When the end of the table is reached, values extracted restart at the beginning.

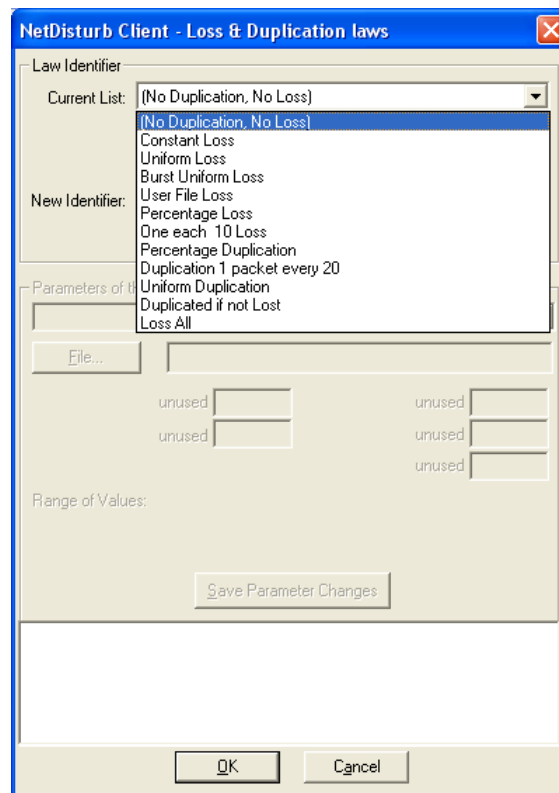
This value is compared to the Threshold: if the value is greater or equal than the Threshold, the packet is lost. Otherwise, the packet continue to be handled and may be delayed.

6.4.3.2 How to create or to edit Loss Laws

To configure loss laws click on “Edit” button from Client main window “Loss law” top or bottom part.

Mask	Loss & Duplication Law	Delay & Jitter Law
TCP	Duplicated if not Lost	Exponential Jitter
Protocol	Loss then Duplicate 1/10 & 1/20	Delay & Exponential Jitter From 20ms to 72ms
# Incoming Packets	# Lost or Duplicated Packets	# Delayed Packets
17191	1719 [10 %]	15472 [90 %]

The following window is pop up:



Loss Laws window is divided in three parts:

❖ **Law identifier:**

It is used to choose an existing law from the “Law Identifier” combo-box. An existing law can be deleted by pushing the “Delete the Law” button.

From this part, the user can also add a new law, by entering a name in the “Add a New Identifier” area and by clicking on “Add the Identifier” button”.

❖ **Action buttons:**

The ‘NetDisturb Client - Loss laws’ window handles a temporary list of laws until the user press the **OK** or **Cancel** button.

Button	Action
Rename the Law Identifier:	Change the law identifier.
Delete the Law Identifier:	Remove the law from the temporary list.
Add the Identifier	Add the Identifier in the temporary list.
Save Parameters Changes:	Temporary saves changes in parameters of the current law.
OK:	Permanently saves changes (addition, deletion and parameters changes) and closes the window.
Cancel:	Allows ignoring all modifications made since the window has been opened.

❖ Parameters of the Law:

This area is composed of a list box to select the loss law to apply, and different edit areas may be enabled in order to input parameters.

The “[Value range](#)” allows seeing the range of values generated by the law for the user-defined parameters. It applies to Uniform Loss law and Burst Uniform Loss law.

A list box allows selecting one type of law; four kinds of loss law are available:

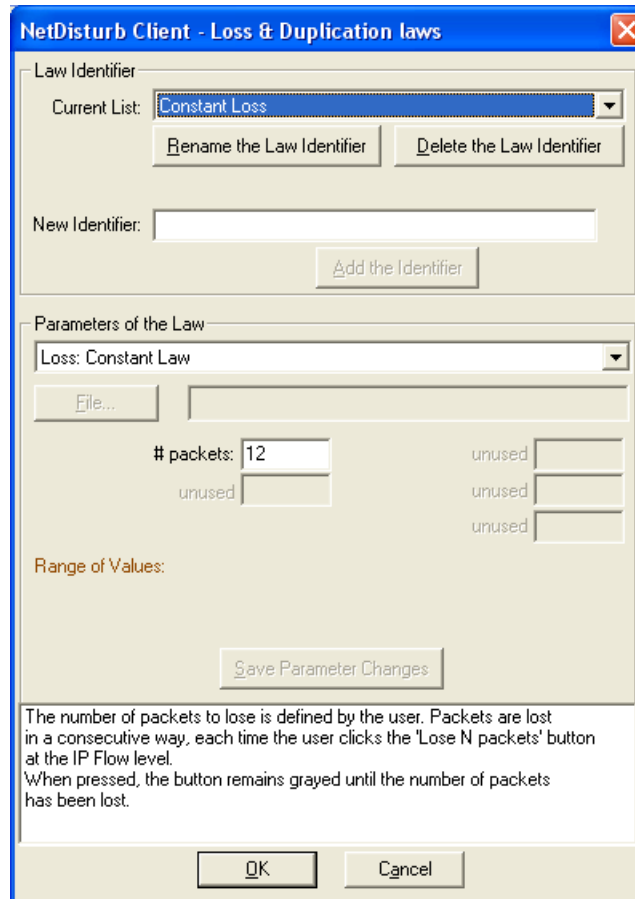
- Constant law: #packets to lose
- Uniform loss law: $dx/[\text{beta} - \text{alpha}]$; threshold
- Associated uniform law: $dx/[\text{beta} - \text{alpha}]$; threshold; increment
- Law imported from a file: file name; threshold

To create a new Loss & Duplication law:

1. Enter a name in the “Add a new Law Identifier” edit field,
2. Then click on the “Add the Identifier” button.
3. Select one kind of law in the ‘Parameters of the Law’,
4. Enter law parameter(s),
5. Press the “Save Parameters Changes” button.
6. Press “OK” to quit the “Duplication & Loss laws” window and to save new Identifiers and changes.

6.4.3.3 Constant Loss Law

When a fix loss law is selected, NetDisturb Driver will lose the number of packets defined by User. A button «**Lose xx packets**» replaces the summary area in the main window. Each time this button is pressed, xx packets are lost.



For this law, only one parameter must be defined: **# packets**

6.4.3.4 Uniform Loss Law

When a uniform loss law is selected, a uniform distribution of numbers contained between the Alpha and Beta supplied by the user is computed and stored in a table. This table and the threshold (also supplied by the user) are then transmitted to NetDisturb Driver.

NetDisturb Driver picks a number in the table (see also 6.4.3.1) for each selected packet. If this number is greater or equal than the threshold, then the packet is lost.

Mathematical function (see Uniform law in Part 8 for more information):

Uniform law on (α, β) range

$$f(x) = 1/(\beta - \alpha) \quad \text{if } \alpha < x < \beta$$

$$f(x) = 0 \quad \text{else}$$

For this law, three parameters must be defined:

- Alpha:** min value of the range
- Beta:** max value of the range
- Threshold:** if the calculated number by the law is greater or equal than the Threshold value, the packet is lost.

6.4.3.5 Burst Uniform Loss Law

As in the Uniform Law, the Burst Uniform Law calculates a table of numbers uniformly distributed between Alpha and Beta. This table is transmitted to NetDisturb Driver with two thresholds T1 (Threshold (n)) and T2 (Threshold (n+x)) and one depth value (D).

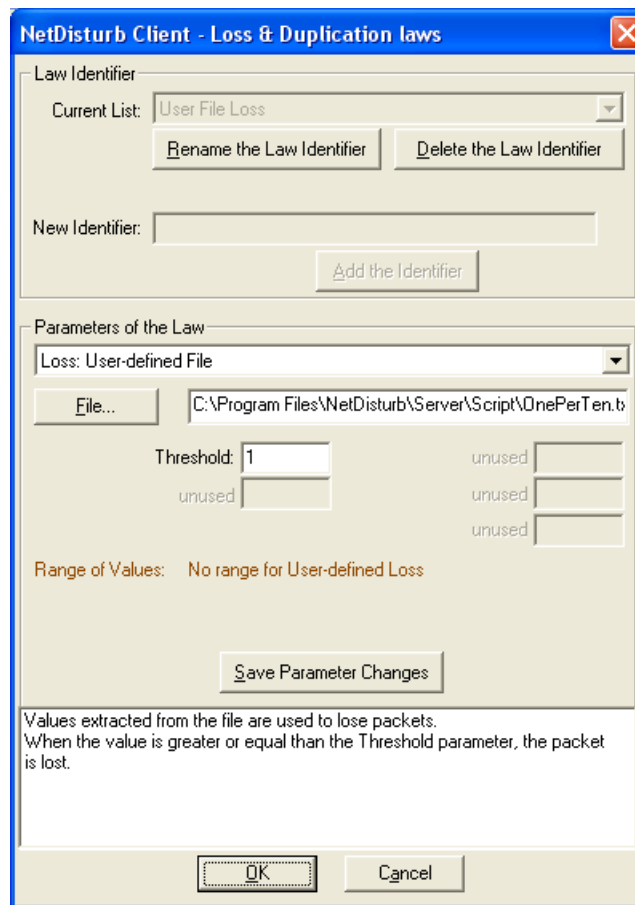
The T1 threshold is the first loss factor.

The T2 threshold is the second loss factor, used in correlation with T1 and for a maximum number of packets defined by the D parameter. T2 may be greater or lower than T1.

This law allows generating burst losses. Processing is applied as follows:

- ⇒ NetDisturb Driver picks a number from the table for each packet (see also 6.4.3.1)
- ⇒ For the packet n, NetDisturb Driver picks one number from the table (current number), and lost it if this number is greater or equal than T1.
- ⇒ If the packet n is lost, the following packets (up to n+D) will be lost if the picked up number is superior to T2. This threshold (T2) is applied to process the following D (depth) packets with the following rules:
 - If the packet n+i (with $i < D$) is not lost, the threshold comes back to T1 (the burst loss is stopped).
 - If the packets (from n+1 up to n+D) are all lost, the threshold comes back to T1 (the burst loss is stopped).

6.4.3.6 User-defined Loss File



When this law is selected, loss values are extracted from a file supplied by the user. File must be a text file. Losses are expressed in integer positive number. Separators used for decoding are End of Line (CR or CR-LF), semicolon, coma, and tab or space characters.

To assure performance, file is read in one shot, and stored in memory at law selection time. Values are used to load the table transmitted to NetDisturb Driver. In order to not overload the memory resources, maximum read number of loss is limited to 40 960.

If the file size exceeds table size, only the part that can be memorized will be read. The rest of the file will be used for the next loading.

If the file size is too small to fulfill the table, fulfillment is done by reading back the file from its beginning.

NetDisturb Driver picks a number in the table (see also 6.4.3.1) for each selected packet. If this number is greater or equal than the threshold, then the packet is lost. When the end of the file is reached, NetDisturb Driver restarts with the first values of the file.

The file sample (OnePerTen.txt) illustrates a loss of 1 packet for 10 packets sent when the Threshold value τ is $0 < \tau < 100$.

(The content of the file OnePerTen.txt is: 0 0 0 0 0 0 0 0 0 0 100)

- For any Threshold value greater than 1 and smaller or equal than 100, only the 10th packet is lost.
- If the Threshold value is greater than 100, no packet is lost.
- If the Threshold value is 0, all packets are lost.

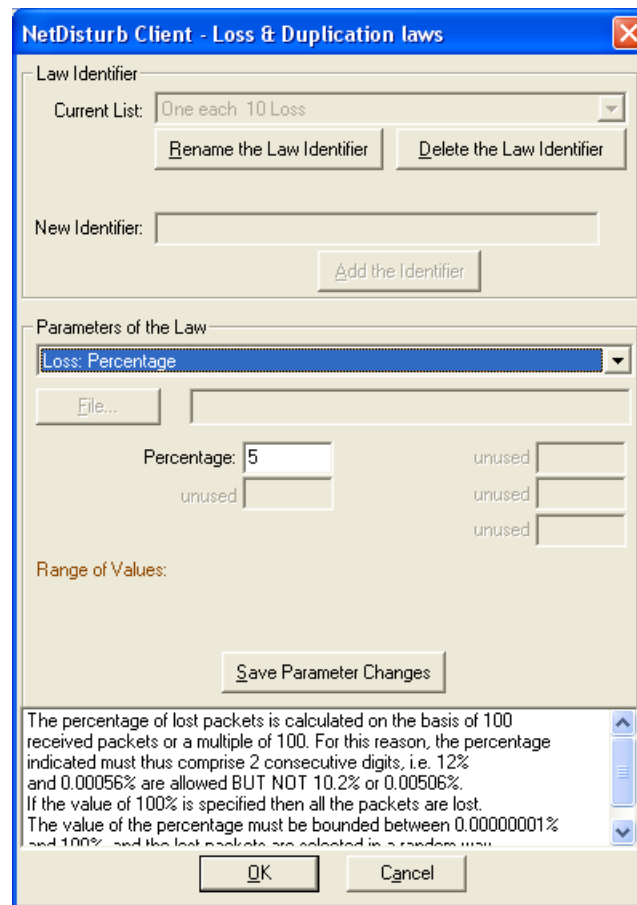
Here is another example of the impact of the threshold value. The file content of the file is: 10 20 30 40 50 60 70 80 90 100

Packet #	Value extracted	Lost result with Threshold = 95	Value extracted	Lost result with Threshold = 50	Value extracted	Lost result with Threshold = 15
1	10	Continue	10	Continue	10	Continue
2	20	Continue	20	Continue	20	LOST
3	30	Continue	30	Continue	30	LOST
4	40	Continue	40	Continue	40	LOST
5	50	Continue	50	LOST	50	LOST
6	60	Continue	60	LOST	60	LOST
7	70	Continue	70	LOST	70	LOST
8	80	Continue	80	LOST	80	LOST
9	90	Continue	90	LOST	90	LOST
10	100	LOST	100	LOST	100	LOST
11	10	Continue	10	Continue	10	Continue
12	20	Continue	20	Continue	20	LOST
13	30	Continue	30	Continue	30	LOST
14	40	Continue	40	Continue	40	LOST
15	50	Continue	50	LOST	50	LOST
16	60	Continue	60	LOST	60	LOST
17	70	Continue	70	LOST	70	LOST
18	80	Continue	80	LOST	80	LOST
19	90	Continue	90	LOST	90	LOST
20	100	LOST	100	LOST	100	LOST
21	10	Continue	10	Continue	10	Continue

Note: *Continue* means the packet is not lost and may be handled by the Delay & Jitter law, if defined.

A more detailed description with delays and jitters is also available in paragraph 6.4.5 and 6.4.6.

6.4.3.7 Percentage Loss



The dialog box is titled "NetDisturb Client - Loss & Duplication laws". It contains two main sections: "Law Identifier" and "Parameters of the Law".

Law Identifier:

- Current List:** A dropdown menu showing "One each 10 Loss".
- Buttons:** "Rename the Law Identifier" and "Delete the Law Identifier".
- New Identifier:** A text input field.
- Button:** "Add the Identifier".

Parameters of the Law:

- Loss:** A dropdown menu showing "Percentage".
- File...** A button.
- Percentage:** A text input field with the value "5".
- unused:** Three text input fields, each labeled "unused".
- Range of Values:** A label.
- Button:** "Save Parameter Changes".

Help Text:

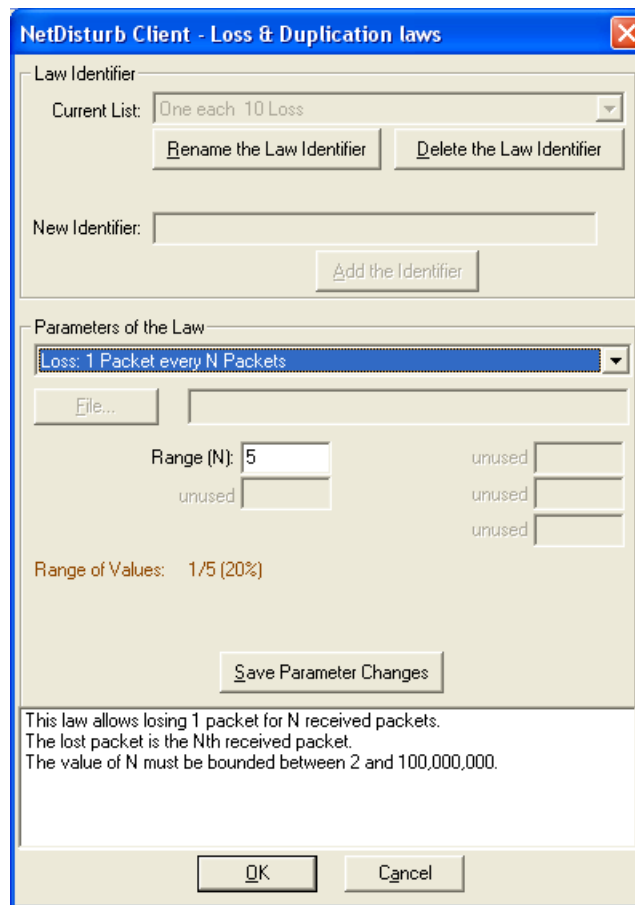
The percentage of lost packets is calculated on the basis of 100 received packets or a multiple of 100. For this reason, the percentage indicated must thus comprise 2 consecutive digits, i.e. 12% and 0.00056% are allowed BUT NOT 10.2% or 0.00506%. If the value of 100% is specified then all the packets are lost. The value of the percentage must be bounded between 0.00000001% and 100% and the lost packets are selected in a random way.

Buttons: "OK" and "Cancel".

This loss law allows losing a percentage of packets. Packets to lose are randomly selected.

The percentage is in the range of 100% (all packets) to 0.0000001% with the constraint to specify up to 2 digits for the significant value, i.e. 12%, or 0.015%. This constraint is due to the internal data format.

6.4.3.8 One packet every N Packets Loss



This loss law affects a same packet based on its order.

The range N indicates which packet is going to be lost i.e. considering N is 12 the 12th packet then the 24th packet then the 36th packet, and so on are lost.

The range N should be a value between 2 and 100,000,000.

6.4.3.9 General Rules concerning the Duplication of Packets

This paragraph details some general terms used to describe the Duplication of packets.

6.4.3.9.1 What does Duplication mean in the Context of NetDisturb

The duplication refers to the action to send more than once the same packet. If the packet N should be duplicated, the packet N is send at least twice consecutively.

6.4.3.9.2 How many Times is a Packet Duplicated

The Minimal Duplication and Maximal Duplication parameters help to select the number of times the packet should be duplicated. When those parameters have the same value, the number of duplications is constant. Otherwise, the number of duplications is randomly selected, where the smallest value is "Minimal Duplication" and the highest value is "Maximal Duplication".

6.4.3.10 Percentage Duplication

NetDisturb Client - Loss & Duplication laws

Law Identifier

Current List: One each 10 Loss

Rename the Law Identifier Delete the Law Identifier

New Identifier:

Add the Identifier

Parameters of the Law

Duplication: Percentage

File...

Percentage: 5 unused

Minimal Duplication: 1 Maximal Duplication: 3 unused

Range of Values:

Save Parameter Changes

The duplication of packets enables to transmit the same received packet several times. The duplicated packets are just inserted after the original packet to transmit.
 The percentage of duplicated packets is calculated on the basis of 100 received packets or a multiple of 100.
 For this reason, the percentage indicated must thus comprise 2 consecutive digits, i.e. 12% and 0.00056% are allowed but BUT NOT 10.2%

OK Cancel

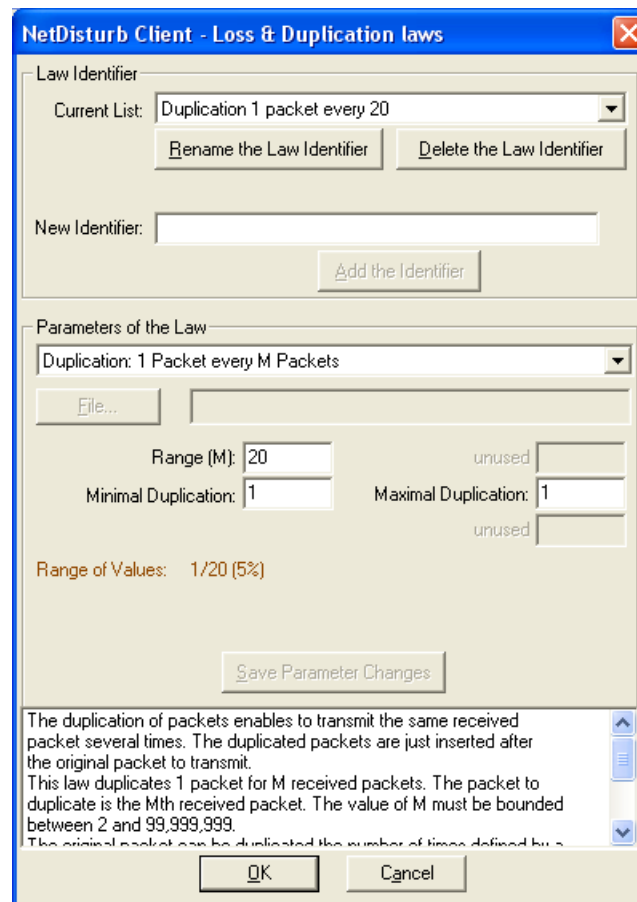
The Percentage duplication law is defined to duplicate an amount of a packets based on the number of received packets.

Packets to duplicate are selected randomly. It is guaranty the percentage is not exceeded, based on a multiple number of 100 packets received. Let's take few examples:

- If the Percentage is 10, there are 10 packets duplicated each 100 received packets.
- If the Percentage is 5, there are 5 packets duplicated each 100 received packets.
- If the Percentage is 2.5, there are 25 packets duplicated each 1,000 received packets.
- If the Percentage is 0.012, there are 12 packets duplicated each 100,000 received packets.

See also paragraph 6.4.3.9 for general rules and terms relevant to the Duplication of packets.

6.4.3.11 Duplication every M Packets



This duplication law reproduces a packet based on its order.

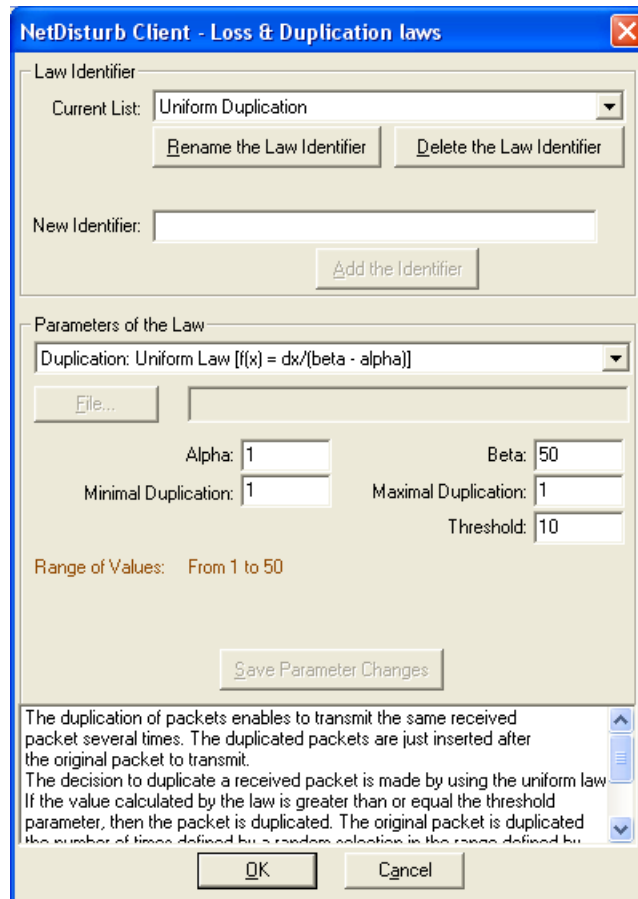
The range M indicates which packet is going to be duplicated i.e. considering M is 9 the 9th packet then the 18th packet then the 27th packet, and so on are duplicated.

The number of times a packet is duplicated is based on the value of “Minimal Duplication” and “Maximal Duplication” parameters.

See also paragraph 6.4.3.9 for general rules and terms relevant to the Duplication of packets.

6.4.3.12 Uniform Duplication

When a uniform duplication law is selected, a uniform distribution of numbers contained between the Alpha and Beta supplied by the user is computed and stored in a table. This table and the threshold (also supplied by the user) are then transmitted to NetDisturb Driver.



NetDisturb Driver picks a number in the table for each selected packet. If this number is greater or equal than the threshold, then the packet is duplicated.

Mathematical function (see Uniform law in Part 8 for more information):

Uniform law on (α, β) range

$$f(x) = 1/(\beta - \alpha) \quad \text{if } \alpha < x < \beta$$

$$f(x) = 0 \quad \text{else}$$

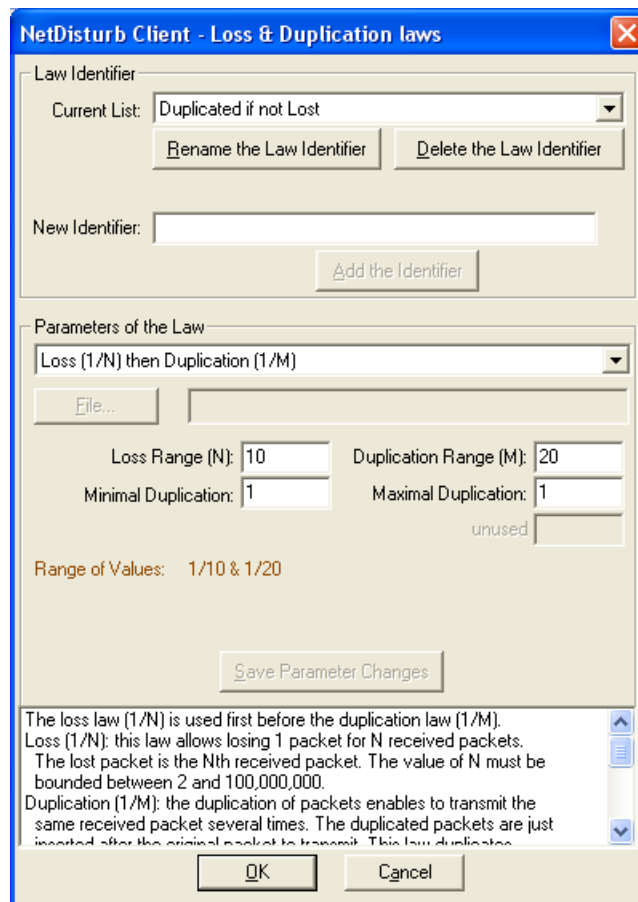
For this law, three parameters must be defined:

- Alpha:** min value of the range
- Beta:** max value of the range
- Threshold:** if the calculated number by the law is greater or equal than the Threshold value, the packet is duplicated.

The number of times a packet is duplicated is based on the value of “Minimal Duplication” and “Maximal Duplication” parameters. *See also paragraph 6.4.3.9 for general rules and terms relevant to the Duplication of packets.*

6.4.3.13 Loss (1/N) then Duplication (1/M)

The law combines the two laws 'Loss: 1 packet every N' with 'Duplication: 1 packet every M'.



The first law applying to the selected packets is the 'Loss (1/N)'. The packet to lose is each N received packet.

For every not lost packet, the second law to apply is 'Duplication (1/M)': here the packet to duplicate is each M **not lost packet**.

Let's take the example of 100 packets received with $N = 10$ and $M = 20$: Packets lost are the 10th, the 20th, the 30th, the 40th ... the 100th. Packet duplicated are the 22nd (because packet #10 and #20 have been lost), the 44th (because packet #30 and #40 have been lost and because the first packet of the next set of 20 none lost packets is the 23rd), the 66th (because packet #50 and #60 have been lost, and the first packet of this 20 packet set is the 45th) and the 88th (because packet #70 and #80 have been lost with a 20 packets set starting at 67th).

The number of times a packet is duplicated is based on the value of "Minimal Duplication" and "Maximal Duplication" parameters. [See also paragraph 6.4.3.9 for general rules and terms relevant to the Duplication of packets.](#)

6.4.4 Delay/Jitter laws Configuration

NetDisturb can delay IP packets following mathematical laws configured by the user or using values extracted from an input file. These values apply to IP packets matching to the selected mask and when a loss law doesn't lose the packet.

If the value is constant, it is a Delay. When values vary, that is the case with mathematical laws, it is a Delay & Jitter value.

Up to 100 Delay & Jitter laws can be created.

6.4.4.1 Delay & Jitter Laws and Working mode

Working Mode: Laws applying to IP Flows

When a Delay & Jitter law is selected on a given IP Flow, the law applies to all packets matching the mask that haven't been lost. For each packet, a new Delay & Jitter value is extracted from the law or from the file, depending on the type of law selected. These values are stored in a global table by NetDisturb Driver. When the table is empty, NetDisturb Server provides a new table to NetDisturb Driver with new values depending on the law.

The value is the number of milliseconds the packet is delayed.

Working Mode: Laws applying to each TCP/UDP connection of the IP Flows

When a Delay & Jitter law is selected on a given IP Flow, the law applies to all packets matching the mask that haven't been lost.

These values are stored in a table maintained by NetDisturb Driver. NetDisturb Server provides the table once to NetDisturb Driver with values depending on the law. NetDisturb Driver loops on values from this table: when the end of the table is reached, NetDisturb Driver restarts at the beginning.

If the packet is TCP or UDP, the 5-tuple IP addresses, protocol and ports is used to classify the packet. Else, only the IP addresses and protocol are used. For each packet, a Delay & Jitter value is extracted from the buffer, at the current index of the packet for the connection i.e. the n^{th} packet received for the given connection is delayed by the n^{th} value of the table. When n reaches the end of the table, values extracted restart at the beginning of the table.

6.4.4.2 Delay & Jitter Accuracy

NetDisturb Driver accuracy is ± 2 milliseconds. It means that a delay variation of one millisecond between two packets can't be taken into account. With such Delay & Jitter, the result is either no Delay & Jitter or a Delay & Jitter of 2ms at least.

Note: NetDisturb Driver uses the OS timer accuracy to delay packet. Because Windows is not a real-time OS, it may append Windows is not able to wake up NetDisturb Driver in the timely manner. In such case, the delay and/or jitter value is increased unexpectedly.

6.4.4.3 Delay & Jitter Laws Selection

To edit or change Delay & Jitter laws click on “Edit” button from the main window in the ‘Delay & Jitter Law’ area.

Mask	Loss & Duplication Law	Delay & Jitter Law
TCP	Duplicated if not Lost	Exponential Jitter
Protocol	Loss then Duplicate 1/10 & 1/20	Delay & Exponential Jitter From 20ms to 72ms
# Incoming Packets	# Lost or Duplicated Packets	# Delayed Packets
17191	1719 [10 %]	15472 [90 %]

Then, the following window is pop up:

NetDisturb Client - Delay & Jitter laws

Law Identifier

Current List: (No Delay, No Jitter)

New Identifier:

- (No Delay, No Jitter)
- Constant Delay
- Exponential Jitter
- Constant Delay & User File Jitter
- User File Delay & Jitter
- Router Simulation with Delay
- Router Simulation & User File

Parameters of the Law

File...

unused

unused

Range of Values:

Save Parameter Changes

OK Cancel

Delay laws configuration window

By default, the following laws are present in the Default.wsx context file:

Combo-box	Comment area	Description
(No Delay, No Jitter)	(No Delay, No Jitter)	With this option, no delay or jitter is applied to the IP flow.
Constant delay	Constant Delay 20 ms	A 20 ms delay is applied to IP packets
Exponential jitter	Delay & Exponential Jitter From 20ms to 124ms	Delay & Jitter to apply: from 20 to 124 ms. The delay is 20 ms and the jitter varies from 0 to 104 ms.
Uniform jitter	Delay & Uniform Jitter From 3ms to 102ms	Delay & Jitter to apply: from 3 to 102 ms. The delay is 2 ms and the jitter varies from 1 to 100 ms.
Constant Delay & User File Jitter	Constant Delay & User File	The file Random_delay.txt contains jitter values to add to the constant 10 ms delay.
User File Delay & Jitter	User File with Constant Delay & Jitter	The file RandomValues.txt contains values used as Delay & Jitter.
Router Simulation with delay	Router Simulation & Constant Delay	Constant delay = 20 ms IP Throughput = 1000 Kb/s Max memory = 500 Ko
Router Simulation & User File	Router Simulation & User File with Delay and Jitter	IP Throughput = 1000 Kb/s Max memory = 250 Ko Delay & Jitter values are extracted from a user file (RandomValues.txt).

The “Delay laws” window is divided in three parts:

❖ Law identification:

The “law identifier” combo-box is used to select an existing law. An existing law can be deleted by pushing the “Delete” button.

From this part, User can also create a new law, by entering a name in the “New Identifier” area and by clicking on “Add” button”.

❖ Action buttons:

Delay & Jitter Laws window handles a copy of laws until the user presses the OK or Cancel button.

Button	Action
Rename the Law Identifier:	Change the Identifier of the law
Delete the Law Identifier:	Remove the law from the temporary list.
Add New Identifier	Add the Identifier in the temporary list.
Save Parameters Changes:	Temporary saves changes in parameters of the current law.
OK:	Permanently saves changes (addition, deletion and parameters changes) and closes the window.
Cancel:	Allows ignoring all modifications made since the window has been opened.

❖ Law Parameters:

A list box allows selecting a law; seven kinds of delay law are available:

- Constant Delay law,
- Constant Delay with Exponential Jitter law,
- Constant Delay with Uniform Jitter law,
- Constant Delay and User File containing Jitter values,
- User File containing Constant Delay and Jitter values,
- Router simulation with IP Throughput, Maximum memory and Constant Delay,
- Router simulation with IP Throughput, Maximum memory and User File containing Constant Delay and Jitter values.

This area is composed of a list box to select the delay law to apply, and different edit areas may be enabled in order to input parameters.

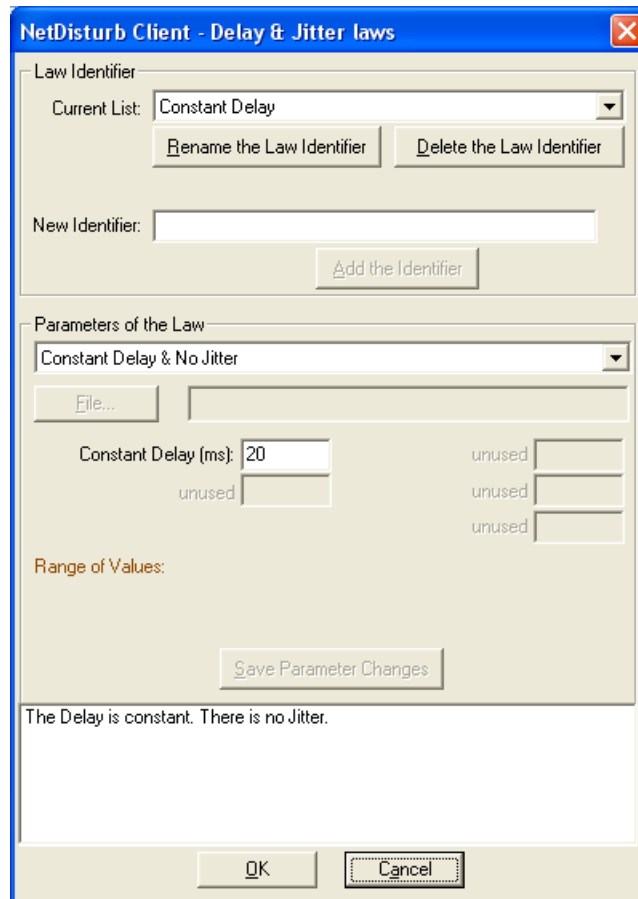
The “[Range of Values](#)” area allows seeing the range of values generated by the law based on the user-defined parameters.

To create a new delay law:

1. Enter a name in the “New Identifier” edit field,
2. Click on “Add the Identifier”,
3. Select a law in the ‘Parameters of the Law’ combo-box,
4. Enter law parameters if needed,
5. Press the “Save Parameter Changes” button.
6. Press “OK” to quit the “Delay & Jitter laws” window.

6.4.4.4 Constant Delay Law

The user supplies a constant delay that is applied to packets relevant to the IP Flow, to all not loss packets.



The dialog box is titled "NetDisturb Client - Delay & Jitter laws". It contains two main sections: "Law Identifier" and "Parameters of the Law".

Law Identifier:

- Current List:** A dropdown menu showing "Constant Delay".
- Buttons:** "Rename the Law Identifier" and "Delete the Law Identifier".
- New Identifier:** A text input field.
- Button:** "Add the Identifier".

Parameters of the Law:

- Dropdown:** "Constant Delay & No Jitter".
- File...** button.
- Constant Delay (ms):** A text input field containing "20".
- unused** labels next to empty input fields.
- Range of Values:** A section with a "Save Parameter Changes" button.
- Status:** A text area containing "The Delay is constant. There is no Jitter."

Buttons: "OK" and "Cancel" at the bottom.

Only the "Constant Delay (ms)" parameter must be defined. All packets will be delayed in a constant manner.

6.4.4.5 Constant Delay with Exponential Jitter Law

When this law is selected, an exponential distribution of jitter is computed from the **Lambda** parameter supplied by User. This distribution is stored in a table. This table is then transmitted to the NetDisturb Driver, finally coupled with a **Constant Delay (ms)** (also supplied by the user) that will be added to the calculated jitter.

Mathematical function (see Exponential law in annex 8 for more information):

Exponential law ($\lambda > 0$)

$$f(x) = (1/\lambda)e^{-x/\lambda} \quad \text{if } x \geq 0$$

$$f(x) = 0 \quad \text{if } x < 0$$

For this law, two parameters must be defined:

Constant Delay (ms): fixed value added

Lambda: parameter of the law

The **Range of Values** area presents see the values domain after parameters computation.

6.4.4.6 Constant Delay with Uniform Jitter Law

When this law is selected, a uniform distribution of jitter is computed from the **Alpha** and **Beta** parameters supplied by the user. This distribution is stored in a table. This table is then transmitted to NetDisturb Driver, finally coupled with a **Constant Delay (ms)** (also supplied by the user) that will be added to the calculated jitter.

NetDisturb Client - Delay & Jitter laws

Law Identifier

Current List: Uniform Jitter

Rename the Law Identifier Delete the Law Identifier

New Identifier:

Add the Identifier

Parameters of the Law

Constant Delay and Uniform Jitter [f(x) = dx/(beta - alpha)]

File...

Constant Delay (ms): 2 Alpha: 1

Beta: 100 unused unused

Range of Values: From 3ms to 102ms

Save Parameter Changes

The Delay is constant. The law f(x) computes the Jitter. The Jitter is uniformly distributed. Beta should be greater than Alpha. Alpha can be zero

OK Cancel

The Mathematical function is the following (see Uniform law in annex 8 for more information):

Uniform law on (α, β) range

$$f(x) = 1/(\beta - \alpha) \quad \text{if } \alpha < x < \beta$$

$$f(x) = 0 \quad \text{else}$$

For this law, three parameters must be defined:

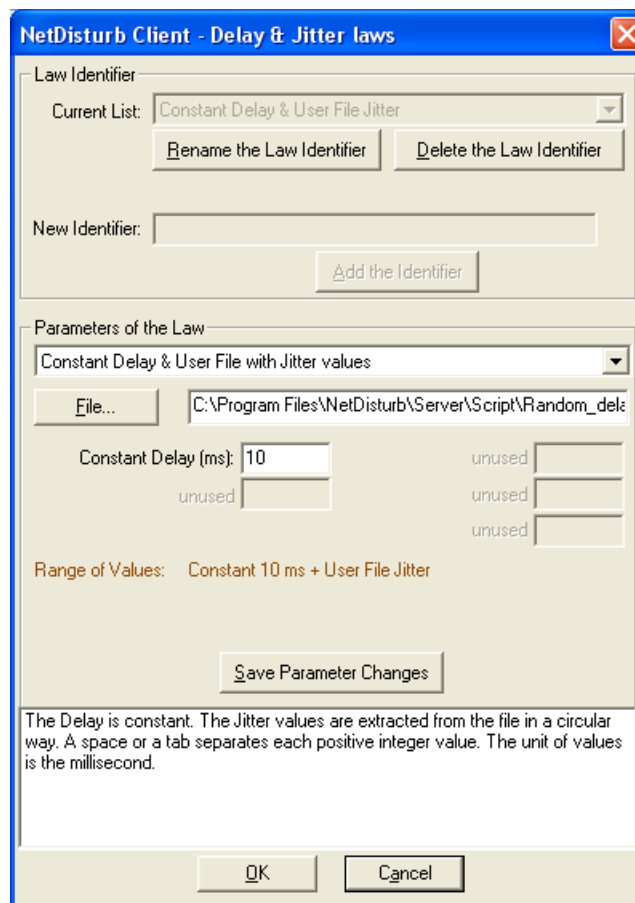
- Alpha:** min value of the range
- Beta:** max value of the range
- Constant Delay (ms):** fixed value added

The **Range of Values** area presents see the values domain.

6.4.4.7 Constant Delay & User File with Jitter Values

When this law is selected, the delay rate is obtained from a file supplied by User. Total delay applied to the packet = fixed delay (defined by user with the “**Constant Delay (ms)**” parameter) + delay read from the file for this packet.

The **Jitter values file** (provided by the user) must be a text file. Delays are expressed in integer positive number. The unit is the millisecond. Separators used for decoding are End of Line (CR or CR-LF), semicolon, coma, and tab or space characters. One Jitter value is picked for each packet handled (see also “Working Mode Menu” 6.2.4.2). When the end of the file is reached, NetDisturb Driver restarts with the first values of the file.



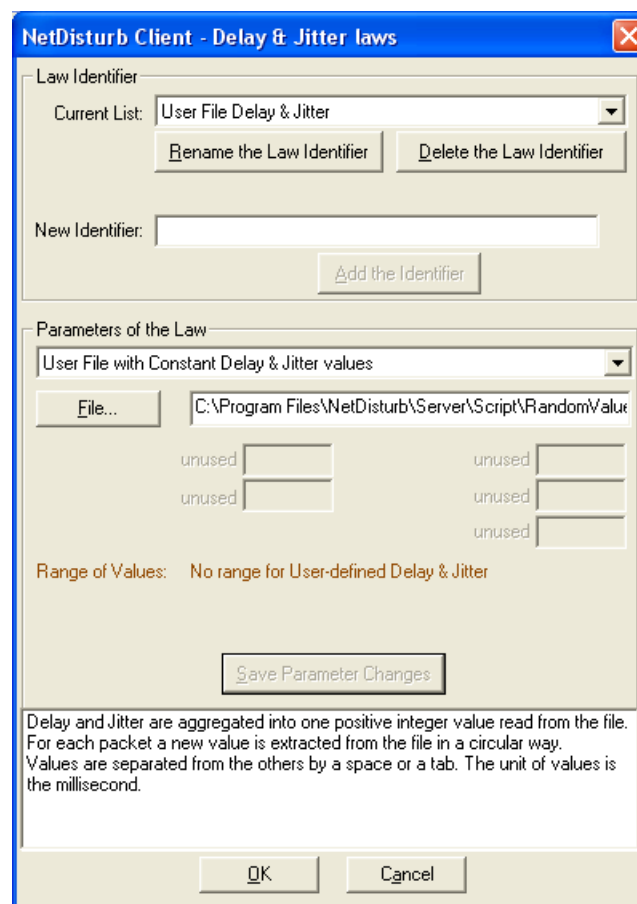
For performance reason, the file is read in one shot, and stored in memory when the law IP Flow is set in the Run state. Values are used to load the table transmitted to NetDisturb Driver. In order to not overload the memory resources, maximum read number of delays is limited to 40 960.

If the file size exceeds table size, only the part that can be memorized will be read. The rest of the file will be used for the next loading. If the file size is too small to fulfill the table, fulfillment is done by read back the file from its beginning.

6.4.4.8 User File with Constant Delay & Jitter Values

When this law is selected, the total delay to apply to the packet is read from the provided by the user.

The [Delay & Jitter values file](#) (provided by the user) must be a text file. Delays are expressed in integer positive number. The unit is the millisecond. Separators used for decoding are End of Line (CR or CR-LF), semicolon, coma, and tab or space characters. One Delay/Jitter value is picked for each packet handled (see also "Working Mode Menu" 6.2.4.2). When the end of the file is reached, NetDisturb Driver restarts with the first values of the file.



The first packet initializes the T_0 time. Then the value T is calculated: $T = T_0 + D_1$ (with D_1 = first delay read in the user file). T is the time when the second packet must be transmitted on the output interface. The second IP packet is received at the T_1 time.

If $T_1 < T$ then this second packet is queued with a delay defined as: $T_0 + D_1 - T_1$

If $T_1 \geq T$ then this second packet is sent immediately on the outgoing interface.

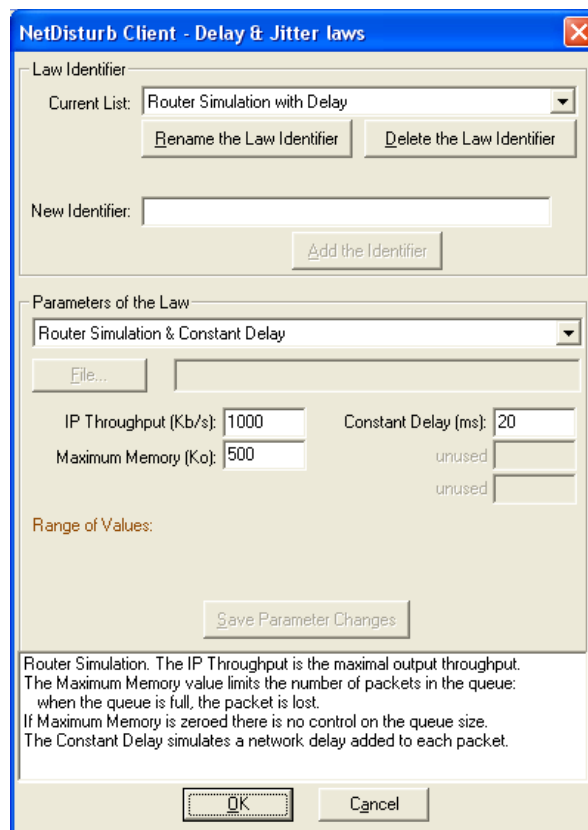
Then the new value T is calculated for the third packet: $T = T_0 + D_1 + D_2$ (with D_2 = second delay read in the user file). T is now the time when the third packet must be transmitted. And the process continues ... when the end of file is reached, the process continues by the beginning of the file and it loops ... So, values defined in the user file correspond to inter packet delays.

6.4.4.9 Router Simulation & Constant Delay

This law is used to simulate a real network by offering:

- A limited **IP Throughput** on the output interface in Kbps.
- A **Constant Delay** (to simulate a network transit delay)
- A loss of packets as soon as the virtual output queue is full (the parameter **Maximum memory** defined by the user is the virtual output queue size). When the output queue is virtually full, all new incoming packets are not transmitted on the output interface.

The example displayed below illustrates the 3 parameters used by the “Router Simulation & Constant Delay” law: **IP Throughput**, **Constant Delay** and **Maximum memory**.



The output queue is a virtual queue because there isn't any real queue associated to the IP Flow.

When the IP Flow is started i.e. when the 'Run' button is pressed, the internal remaining size is the Maximum Memory parameter value.

Each time a packet is received, the internal remaining size parameter is decreased by the packet size. When the remaining size parameter is 0, the queue is marked as full. Any new packet is lost until the remaining size becomes positive. When the packet is sent, the relevant queue size parameter is increased.

In the meantime, each packet to send is first moved in the **global output queue** and, if needed, the number of packets delayed is increased.

This is why there may be packets not yet send when the IP Flow is stopped. Those packets continue to be sent until the **global output queue** is free.

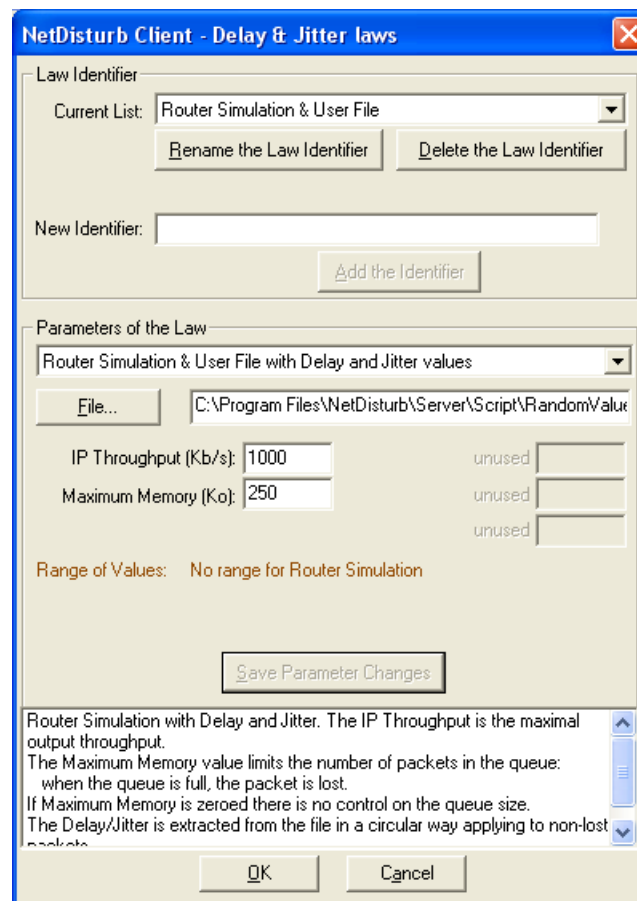
You shouldn't be surprised if packets continue to be sent even if no packet has been received: it is in most cases the **global output queue** that is not yet empty.

6.4.4.10 Router Simulation & User File

This law is used to simulate a real network by offering:

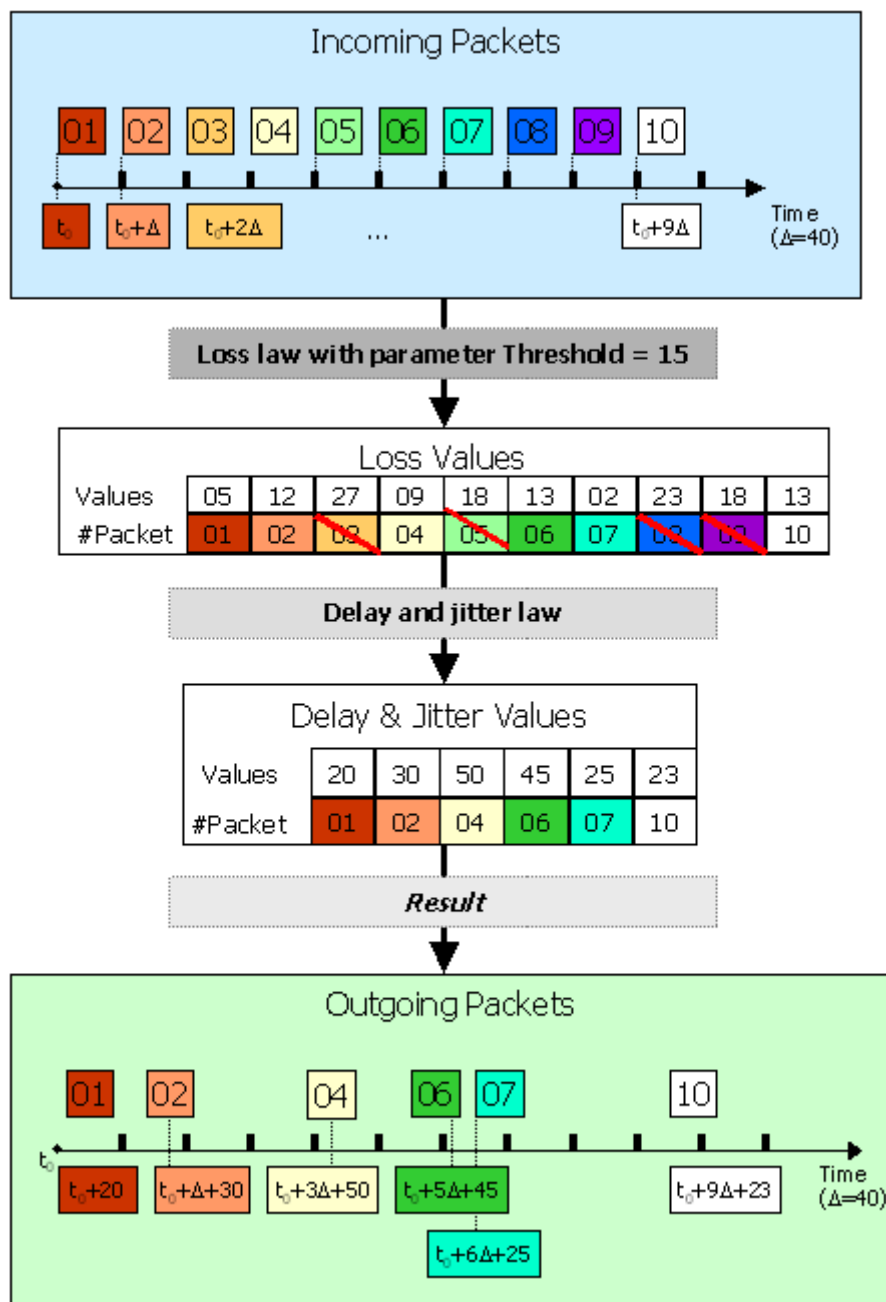
- A limited **IP Throughput** on the output interface in Kbps.
- A loss of packets as soon as the output queue is full (the parameter **Maximum memory** defined by the user is the output queue size). When the output queue is full, all new incoming packets will not be transmitted on the output interface.
- A Constant Delay & Jitter (to simulate a real network transit delay) from the (real) values provided by the user into a text file. Values are expressed in integer positive number. The unit is the millisecond. Separators used for decoding are End of Line (CR or CR-LF), semicolon, coma, and tab or space characters. One Delay & Jitter value is picked for each packet handled (see also “Working Mode Menu” 6.2.4.2). When the end of the file is reached, NetDisturb Driver restarts with the first values of the file.

The example displayed below illustrates the 3 parameters used by the “Router Simulation & Constant Delay” law: **IP Throughput**, **Maximum memory** and **the user file name containing Constant Delay & Jitter values**.



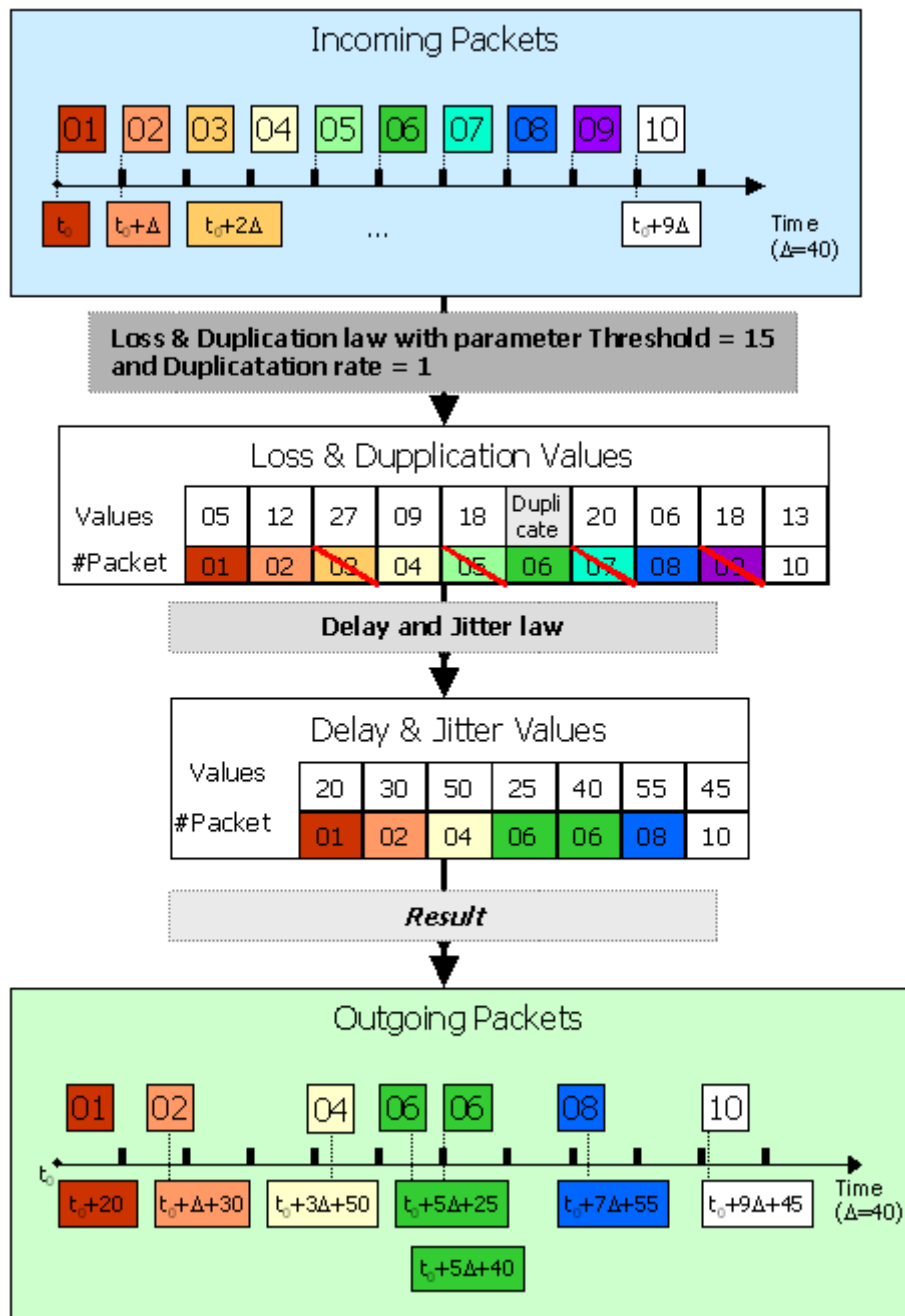
6.4.5 Loss and Delay Dynamic

The next figure shows the impact of a Loss law and a Delay & Jitter law on a set of packets.



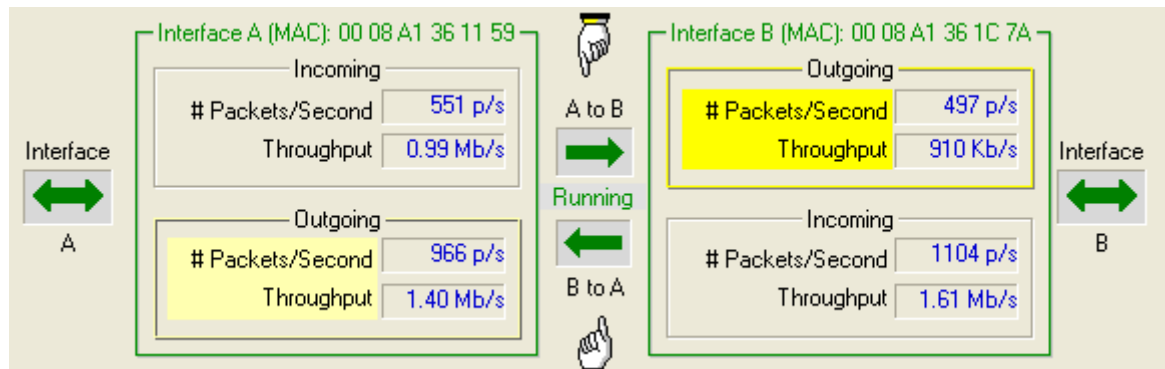
6.4.6 Loss with Duplication and Delay/Jitter Dynamic

The next figure shows the impact of a Loss & Duplication law with a Delay & Jitter law on a set of packets.



6.5 NetDisturb Client Statistics

Traffic on the two interfaces is displayed in the central part of the window when an IP Flow is selected. One frame is reserved for each interface; each frame includes one receiving area (incoming) and one sending area (outgoing). The GUI displays the following statistics:




- ◆ # Packets/Second: This field presents the instant throughput in packets by second on the IP Flow.
- ◆ Throughput: This field displays the instant throughput in bits/Kbits/Mbits per second, according to the sampling period defined in the NetDisturb Client configuration.

6.6 Errors Detected by NetDisturb Driver

If new errors occur at the NetDisturb Driver level, the 'Alarm' button located in the right bottom of the client area is red colored.



Click on the  button to get details about new errors, in the Alarm List dialog.

NetDisturb Client - Alarms Summary

Alarms Linked to the Direction from Interface A to Interface B

Incoming on A		Outgoing to B	
# Packets Lost:	0	# Packets Lost:	0
# Bytes Lost:	0	# Bytes Lost:	0
# Driver Errors:	0	# Driver Errors:	0
# Buffer Missing Errors:	0		
# Flows Exceeded:	0		

A to B
→

Details

Alarms Linked to the Direction from Interface B to Interface A

Outgoing to A		Incoming on B	
# Packets Lost:	2	# Packets Lost:	0
# Bytes Lost:	596	# Bytes Lost:	0
# Driver Errors:	2	# Driver Errors:	100
		# Buffer Missing Errors:	0
		# Flows Exceeded:	0

B to A
←

Details

OK Clear Alarms Update Alarms Summary

Alarms are classified per direction: **A to B** and **B to A**.

Information is different depending on the direction (incoming or outgoing).

Incoming on B

# Packets Lost:	0
# Bytes Lost:	0
# Driver Errors:	100
# Buffer Missing Errors:	0
# Flows Exceeded:	0

On incoming direction:

- Number of packets lost
- Number of bytes lost
- Number of errors returned by the Driver of the Interface
- Number of buffers that were missing to keep packets
- Number of ignored flows (when the multi-flows option is in use).

Outgoing to A

# Packets Lost:	2
# Bytes Lost:	596
# Driver Errors:	2

On outgoing direction:

- Number of lost packets
- Number of lost bytes
- Number of errors returned by the Driver of the Interface

6.6.1 Details for Incoming Errors

Incoming on B	
# Packets Lost:	0
# Bytes Lost:	0
# Driver Errors:	100
# Buffer Missing Errors:	0
# Flows Exceeded:	0

► **#Packet Lost**

Number of packets lost due to memory allocation errors or interface access errors.

► **#Bytes Lost**

Number of bytes lost (total packet size including MAC header) due to memory allocation errors or interface access errors.

► **#Driver Errors**

This error counter is the number of alarms returned by the NIC Driver indicating that some errors have occurred from the started time of the NIC. Errors can be due to one of the following reasons:

- CRC error
- NIC or Driver Buffer overrun error

► **#Buffer Missing Errors**

When a packet is received and memory allocation done by NetDisturb Driver failed, this counter is increased. You can increase the number of buffers allocated by NetDisturb Driver by changing registry parameters (see paragraph 8.2 to increase the number of buffers)

► **#Flows Exceeded**

This counter is handled only when Laws applying to each IP Flow is active (see Working Modes menu paragraph 6.2.4.2). In that case, when a packet is received on a new flow but that new flow cannot be added because the maximum number of flow configured has been reached or due to memory allocation error, this counter is increased for each packet received (see paragraph 8.2 to increase the number of flow)

6.6.2 Details for Outgoing Errors

Outgoing to A

# Packets Lost:	2
# Bytes Lost:	596
# Driver Errors:	2

► #Packet Lost

Number of packets lost due to memory allocation errors or interface access errors.

► #Bytes Lost

Number of bytes lost (total packet size including MAC header) due to memory allocation errors or interface access errors.

► #Driver Errors

This error counter is the number of alarms returned by the NIC Driver indicating that some errors have occurred from the started time of the NIC. Errors can be due to one of the following reasons:

- CRC error
- NIC or Driver Buffer overrun error

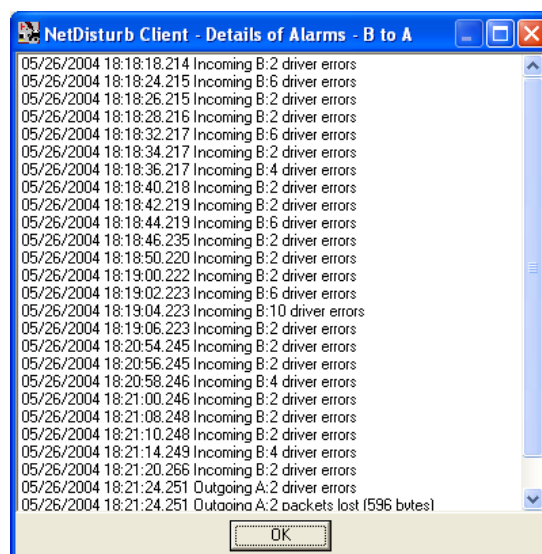
6.6.3 Alarm Management

Four buttons are used to manage these alarms.

► Details

This button gives details in a list window about alarms:

- Timestamp
- Number of errors
- Error type



► **Clear Alarms**

The 'Clear Alarms' button resets the alarms list and number for all direction and interfaces.

► **Update Alarms Summary**

The 'Update Alarms' button interrogates NetDisturb Driver to refresh the error list.

► **OK**

The OK button closes the Alarm List windows and reset the status of the Alarm Button in the Client Window.

The Alarm Button moves from red  to gray  until new errors occur.

Part 7 Using NetDisturb Server

NetDisturb Server links NetDisturb Driver and NetDisturb Client. In addition, it performs following tasks:

- ⇒ To get a thorough view of the traffic on the two interfaces and on the perturbations made.
- ⇒ To follow the command entered by the connected client, to see the driver configuration, and the applied mask and laws.
- ⇒ To configure password for Administrator connections.

The NetDisturb Server window is composed of three sections:

NetDisturb Server - Version 4.0

Impairment Interface Configuration and Statistics

Interface A MAC addr 00-08-A1-36-1C-7A			Interface B MAC addr 00-08-A1-36-11-59		
# Handled Packets:	193196	(100 %)	# Handled Packets:	7186	(95 %)
# Lost Packets:	0	(0 %)	# Lost Packets:	0	(0 %)
# Delayed Packets:	521	(0 %)	# Delayed Packets:	0	(0 %)
Desequenced:	0	(0 %)	Desequenced:	0	(0 %)
# Fragmented packets:	0	(0 %)	# Fragmented packets:	0	(0 %)

Incoming on A		Outgoing on A		Incoming on B		Outgoing on B	
6	# Packets per Second	8		8	# Packets per Second	6	
193197	# Packets	7541		7543	# Packets	193197	
42.8 Kb/s	Throughput	3.64 Kb/s		3.64 Kb/s	Throughput	42.8 Kb/s	

Active relaying process

Current Parameters

Refresh Period (in second): 1 s # Buffers: 2 Interface Mode: Different Application of Laws: IP Flow Level

Sampling to Compute Throughputs: 2 s Traces: Active Desequencing: Enabled

Current Client Connection

Client: Administrator

Context:

Buttons: Show Current Trace, Reset Counters, Parameters, Show Context, Reset Trace

Log:

- 18h17mn48s Mask (No mask) selected for Flow 6 Interface B
- 18h17mn48s Mask POP3 selected for Flow 8 Interface A
- 18h17mn48s Mask (No mask) selected for Flow 8 Interface B
- 18h17mn50s Mask TFTP selected for Flow 10 Interface A
- 18h17mn50s Mask (No mask) selected for Flow 10 Interface B
- 18h17mn51s Mask PRINTER/PORT selected for Flow 12 Interface A
- 18h17mn51s Mask (No mask) selected for Flow 12 Interface B
- 18h17mn52s Mask UDP selected for Flow 14 Interface A
- 18h17mn52s Mask (No mask) selected for Flow 14 Interface B
- 18h17mn53s Mask (No mask) selected for Flow 16 Interface A
- 18h17mn53s Mask (No mask) selected for Flow 16 Interface B

❖ Impairment Interface Configuration & Statistics

This section displays the used cards. Statistics (percentages or absolute values) are associated to each impairment parameter: number of handled, lost, delayed, desequencing packets.

The # Fragmented Packets statistics shows the number of packets rejected by NetDisturb Driver because NetDisturb Driver can't handle IP packet with the fragment flag set.

The section also displays the numbers of incoming, outgoing packets, the number of packets per second and the throughput.

Indication on relaying process is presented as follows:

No packets handled (red color)	NetDisturb Driver doesn't handle any packet (physical cut off of the Ethernet link).
Active relaying process (green color)	NetDisturb Driver is running, relayed packets are processed following the selected masks, and they are lost and delayed following the selected laws.

❖ Current Parameters

Current Parameters				
Refresh Period (in second): ① 1 s	# Buffers: ③ 2	Interface Mode: ⑤ Different	Application of Laws: ⑦ IP Flow Level	
Sampling to Compute Throughputs: ② 2 s	Traces: ④ Active	Desequencing: ⑥ Enabled		

This section reminds the current configuration; it includes:

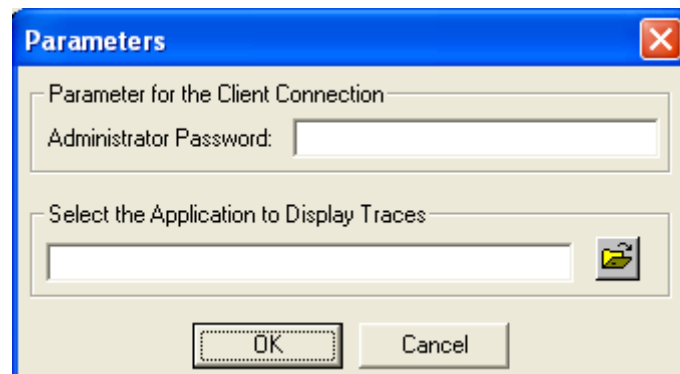
1. The refresh period to redisplay statistics of NetDisturb Server.
2. The sampling period used to calculate the throughput displayed by NetDisturb Server.
3. The number of buffers for laws' values related to TCP/UDP connections.
4. The Trace mode: active or inactive
5. The Interface Mode: always different in that version.
6. The desequencing mode: it can be Enabled or Disabled mode
7. The way to make use of laws: 'IP Flow level' or 'TCP/UDP connections'.

❖ Current Client Connection

This section shows the currently connected client. From this section, the following action can be carried out:

- **“Show Current Traces”** allows opening the trace file in order to examine the commands entered by the Client. The program path used to display the traces must be configured in the parameters of NetDisturb Server.

- **“Reset Counters”** allows resetting the NetDisturb Server User Interfaces counters. This action has no incident on NetDisturb Client. This button is available only when driver is running.
- **“Show Context”** displays the content of the current context.
- **“Reset Traces”** This command clears the traces displayed in the window bottom part. It does not affect the trace file.
- **“Parameters”** allows opening Parameters window of NetDisturb Server. The available parameters are the administrator password and the viewer for the traces.



- This section also displays the name of the last opened context and the scenario in use.

Part 8 Annexes

8.1 Default Context Values

• Refreshing time for statistics display	1s
• Sampling period for throughput computing	2s
• Relaying process	Relaying packets without operations on both interfaces
• Mode	Internet
• Interface mode	Identical for both interfaces
• Traces	Active
• Driver relaying status	Running
• Buffer number	2
• Flow mode	Mono-flow
• For the 16 definable masks	
Mask	All packets
Loss & Duplication law	<i>Not defined</i>
Delay & Jitter law	<i>Not defined</i>
• Other IP Flows	
Loss & Duplication law	<i>Not defined</i>
Delay & Jitter law	<i>Not defined</i>

8.2 NetDisturb Registry Values

Warning

This chapter contents description of parameters for NetDisturb Cleint, NetDisturb Server and NetDisturb Driver. You should be careful when changing in one of these values because inappropriate value may render NetDisturb unusable. We recommend to backup the registry or, at least, to save the key's values before any change.

You need administrator rights access to change the registry database. The system 'regedit.exe' program can be used to check and modify the registry. Each parameter is identified by a name, a type and a value; parameters are located into a hierarchical key tree. This paragraph gives the key location, the parameter name with its type and possible set of value, and default value when applicable.

8.2.1 Registry related to NetDisturb Client

This part is related to NetDisturb Client parameters located in the registry. Some parameters refer to dialog with NetDisturb Server and you should be changed accordingly.

8.2.1.1 Configuration Parameters

Key: HKEY_LOCAL_MACHINE\SOFTWARE\ZTI\NetDisturbClient

Name	Type	Value
AcroReadInfo	REG_SZ	Date of the help file (the user should not change it)
AcroReadTimer	REG_DWORD	Internal timeout related to the Adobe Reader®
ExchangeTimeout	REG_DWORD	Internal timeout related to the NetDisturb Client to NetDisturb Server dialog (default is 5000 ms)
Help_Menu	REG_DWORD	Index in the help file (the user should not change it)
IPAddress	REG_SZ	NetDisturb Server IP Address (default: 127.0.0.1)
ServerPath	REG_SZ	Full server path to the script sub directory (There is no default value but a typical value is: C:\Program Files\NetDisturb\Server\Script\)
TCPPort	REG_SZ	RPC port number used to dialog with the NetDisturb Server part (default: 2020)
TraceLevel	REG_DWORD	Trace level generated by the Client (see note) (default: 0)
TraceFileName	REG_SZ	File name where traces are saved in when the TraceLevel flag is saved. (default: empty)
UserName	REG_SZ	Latest user name

Note:

- ☐ The level of trace is a set of flags. When the flag is set (1) the level is active. When the flag is reset (0) the level is inactive. Ex: TraceLevel=5, the flag 4 and 1 are active, other are inactive.
- ☐ Traces are displayed to the standard debug port.
- ☐ Flag values are shown in **hexadecimal**:
 - 0001 Errors level
 - 0002 Information level
 - 0008 Verbose level
 - 0010 Time: add timestamp information
 - 0100 File: trace are saved into a file too (the TraceFileName entry is used)
 - 1000 RPC: add the RPC trace information
 - Example:
If TraceLevel = 113 means Error and Information level of traces are saved also into a file and including the timestamp for each trace.

8.2.1.2 Most Recent File list

This list is for information only. **It is handled by the system and the user should not change it.**

Key: HKEY_CURRENT_USER\Software\ZTI\NetDisturbClient\Recent File List

Name	Type	Value
File1	REG_SZ	The most recent path context file used
File2	REG_SZ	A more recent path context file used
File3	REG_SZ	A more recent path context file used
File4	REG_SZ	The oldest path context file used

8.2.2 Registry related to NetDisturb Server

Key: HKEY_LOCAL_MACHINE\SOFTWARE\ZTI\NetDisturbServer

Name	Type	Value
ApplicationName	REG_SZ	Trace viewer
IHMRefresh	REG_DWORD	Period of refresh, in second. (default is 1)
Interface A	REG_SZ	MAC address of the latest selected Interface A
Interface B	REG_SZ	MAC address of the latest selected Interface B
Password	REG_SZ	Password required for the 'Administrator' user (default: empty)
Sampling	REG_DWORD	Sampling period to compute throughput (default: 2)
TCPPort	REG_SZ	RPC port number used to dialog with the Client part (default: 2020)
TraceLevel	REG_DWORD	Trace level generated by NetDisturb Server (see note) (default: 0)

Note:

- ❑ The level of trace is a set of flags. When the flag is set (1) the level is active. When the flag is reset (0) the level is inactive. Ex: TraceLevel=5, the flag 4 and 1 are active, other are inactive.
- ❑ Traces are displayed via the standard debug mechanism (for trace display program such as dbmon or DebugMon).
- ❑ Flag values are shown in **hexadecimal**:
 - 0001 Error level
 - 0002 Important level
 - 0008 Information level
 - 0100 Verbose level (1)
 - 0200 Verbose level (2)
 - 1000 Put trace generated into the NetDisturb Server trace window
 - Example:
If TraceLevel = 1001 means Error level of traces shown into the window trace.

8.2.3 Registry related to NetDisturb Driver

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetDisturb

Key (Windows NT only):

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disturb

Name	Type	Value
DisplayName	REG_SZ	Name of the service (Default is "NetDisturb Impairment")
ErrorControl	REG_DWORD	1
ImagePath	REG_SZ	system32\drivers\disturb.sys
Start	REG_DWORD	3
Type	REG_DWORD	1

8.2.3.1 NetDisturb Driver Traces

There is another key related to the level of traces generated by NetDisturb Driver. These traces can be captured via a tool such as DebugMon for OSR, Inc (www.osronline.com selection Download)

Cautions: Changing the level of traces may block your PC until you reboot. The level of traces provided by the NetDisturb Driver should be modified only with the help of the technical ZTI support (support@zti-telecom.com).

The key is:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetDisturb\Parameters

TraceLevel	REG_DWORD	Trace level generated by NetDisturb Driver (see note) (default: 0)
Note: The level of trace is a set of flags. Values aren't provided here to avoid mishandling of NetDisturb Driver. Please contact the technical support of ZTI if you need more details.		

8.2.4 Windows Registry (Windows XP)

The goal of this modification of the Windows system parameters is to enable the RPC service that is required by NetDisturb Server and NetDisturb Client to dialog.

Key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\RPC

Name	Type	Value
RestrictRemoteClients	REG_DWORD	0x00000000

8.3 Mathematical Laws

8.3.1 Uniform Law

❖ *Presentation:*

Uniform law has two parameters: α and β . It generates a random number included uniformly between α and β . If α is equal to β , the generated number is always $\alpha = \beta$.

❖ *Mathematical function:*

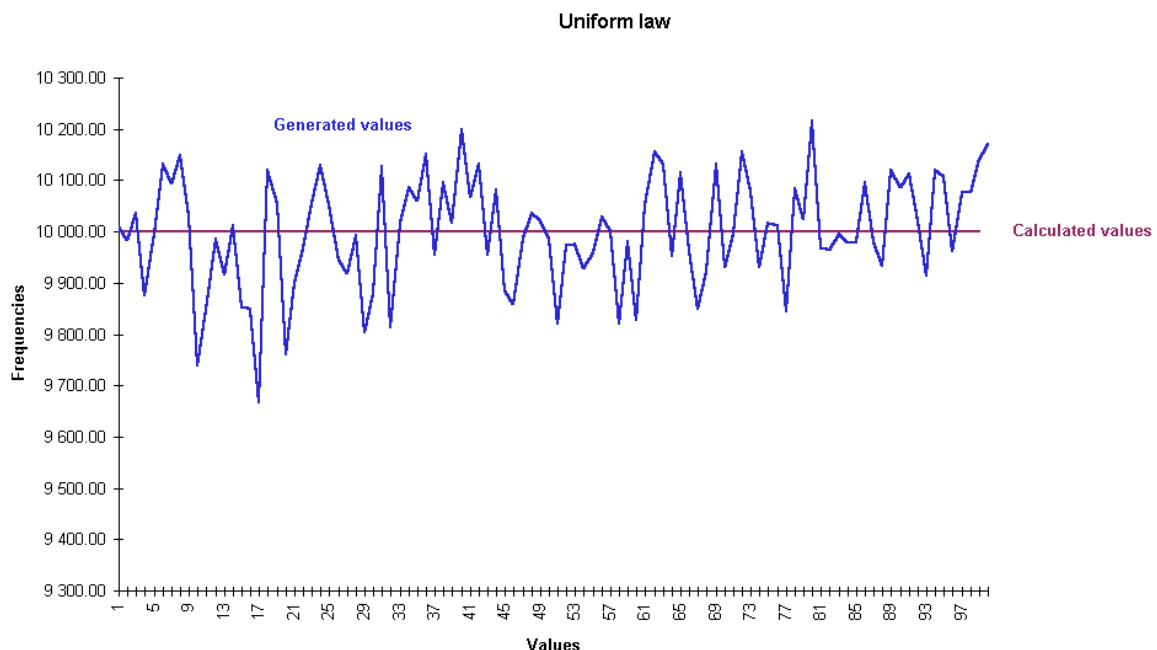
Uniform law on (α, β) range

$$f(x) = 1/(\beta - \alpha) \quad \text{if } \alpha < x < \beta$$

$$f(x) = 0 \quad \text{else}$$

❖ *Uniform law - example of generated values for 1000000 draws for this law with:*
 $\alpha = 0$ and $\beta = 100$.

The factor 1000000 is because the figure intends to show the actual behavior of the random generator. To do that, we draw 1000000 times a random value and count the actual frequencies. The theoretical (= calculated values) curve and actual (= generated values) curve are displayed below.



8.3.2 Uniform Correlated Law

The Uniform Correlated law is the same law as Uniform law. Only the process differs: the difference is related to the two thresholds used by NetDisturb Driver (see the “Loss laws configuration” paragraph for more details).

8.3.3 Exponential Law

❖ Presentation

Exponential Law has only one parameter: λ . The more λ is small, the more the power of 10 of the generated number is high.

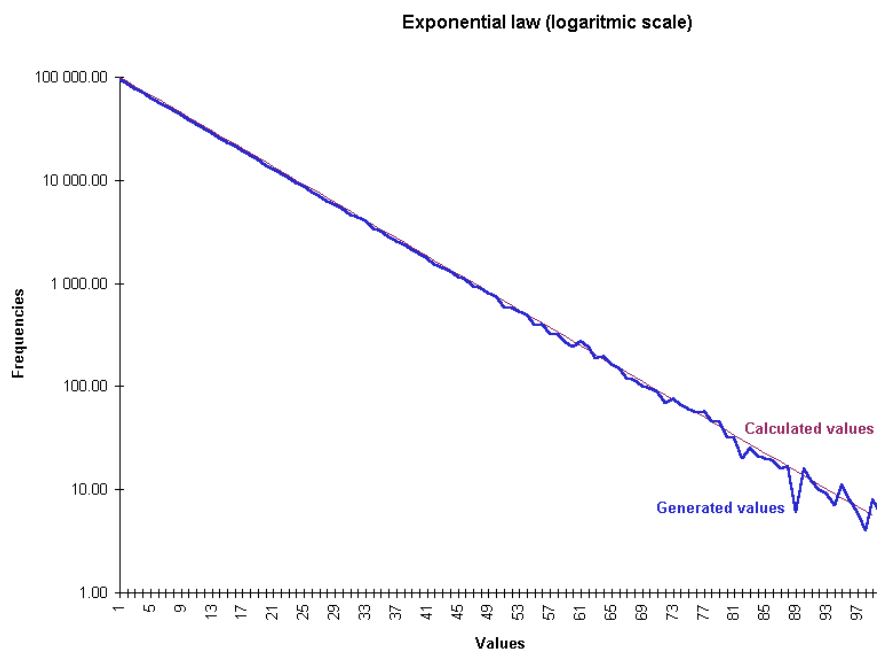
❖ Mathematical function:

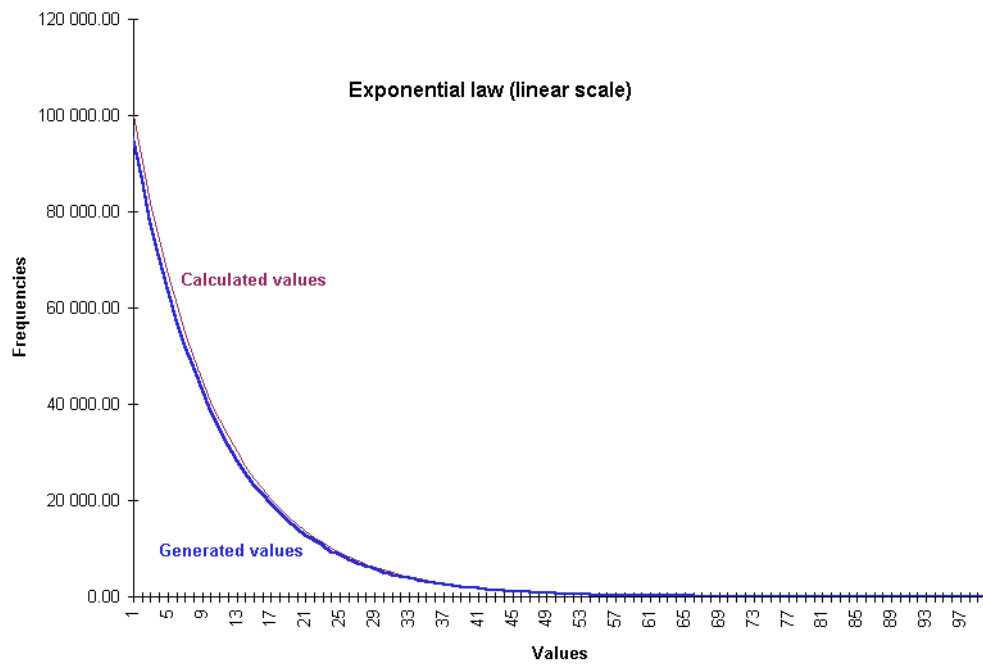
Exponential law ($\lambda > 0$)

$$\begin{aligned} f(x) &= \lambda e^{-\lambda x} & \text{if } x \geq 0 \\ f(x) &= 0 & \text{if } x < 0 \end{aligned}$$

❖ Exponential law - example of generated values for 1000000 draws with: $\lambda = 0,1$.

The factor 1000000 is because the figure intends to show the actual behavior of the random generator (not to show the theory of the exponential law). To do that, we draw 1000000 times a random value and count the actual frequencies. The theoretical (=calculated values) and actual (=generated values) curves match perfectly for bigger values.





❖ *Exponential law- Table of generated values:*

<u>Values</u>	<u>Delay law results</u>
$\lambda = 1$	10 ms
$\lambda = 0,1$	100 ms
$\lambda = 0,01$	1s
$\lambda = 0,001$	10s
$\lambda = 0,0001$	1mn43
$\lambda = 0,00001$	17mn19
$\lambda = 0,000001$	2h53
-- Precision limit of λ --	