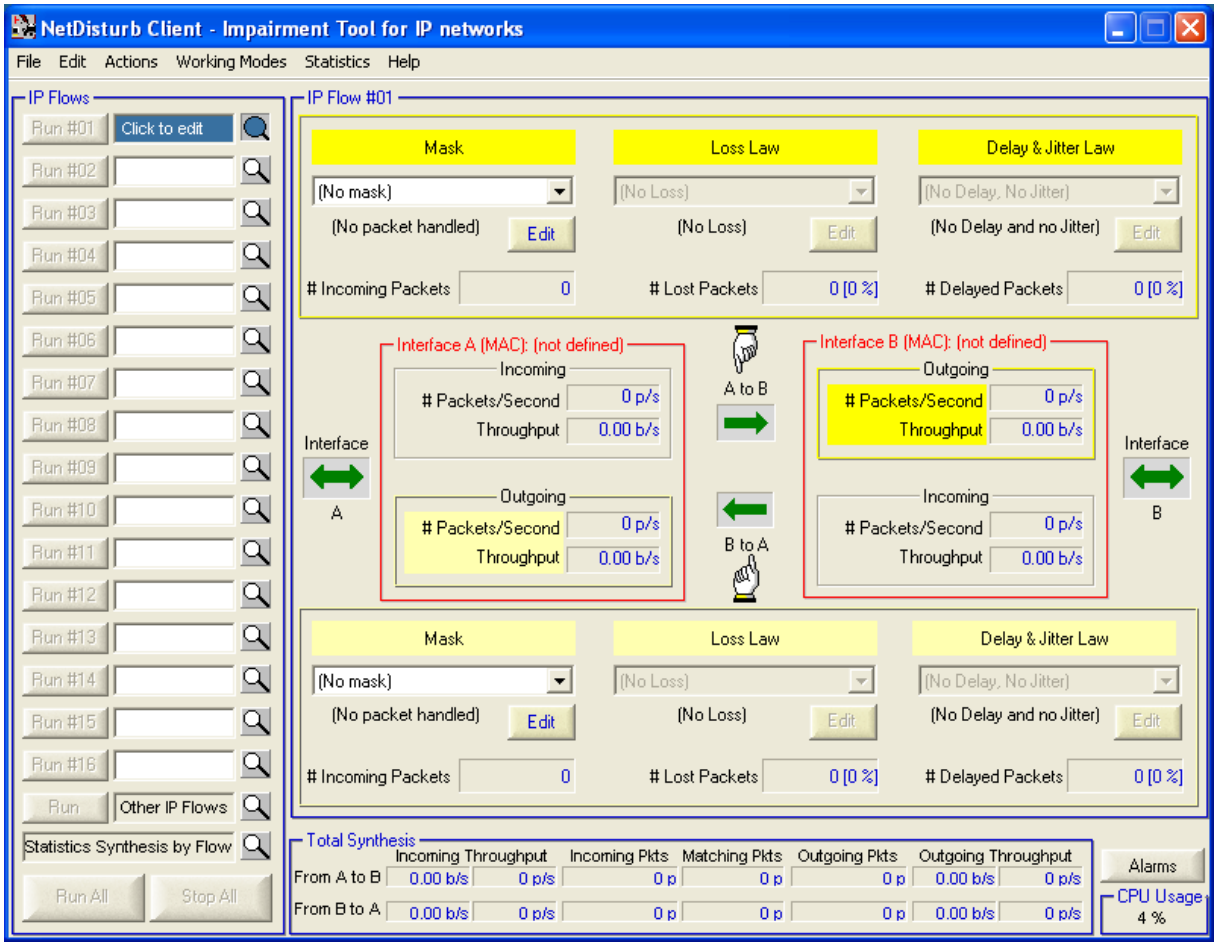
# NetDisturb

**Version 4**

## *Impairment emulator software for IP networks*




## *User Guide*


**ZTI** - 1, Boulevard d'Armor - B.P. 154 - 22302 Lannion Cedex - France
Phone: +33 2 96 48 43 43 Fax: +33 2 96 48 14 85 Email: contact@zti-telecom.com Web: www.zti-telecom.com

**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
B.P. 154
22302 Lannion Cedex
France

Phone: +33 2 96 48 43 43
Fax: +33 2 96 48 14 85

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



**Ref#** NETDISTURB USER GUIDE V4-Ed 1

# Table of contents

# Part 0 Document presentation

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

Part 1 is a general presentation of the NetDisturb software.

NetDisturb installation is explained in Part 2, and license configuration and license transfer are detailed in Part 3. The uninstall procedure of the NetDisturb software is described in Part 4.

To run NetDisturb, you must refer to Part 5.

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

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

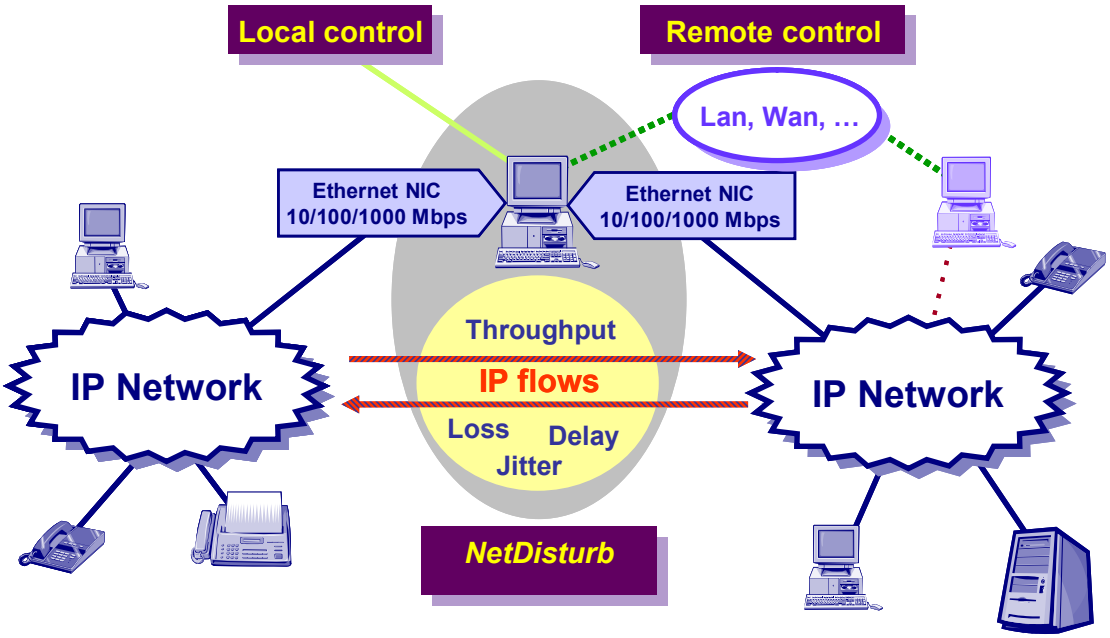
 

# Part 1 NetDisturb software presentation

NetDisturb is an IP network emulator software that can generate impairments (latency, delay, jitter, limited bandwidth, lost packets) over IP networks. NetDisturb allows the user to disturb flows on an IP 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 Ethernet, Fast Ethernet and Gigabit network interface cards and inserted between two physical networks. It can be remotely controlled via PSTN, ISDN or LAN. Minimal required screen resolution is 800 x 600 pixels.

NetDisturb generates packet loss and/or packets delay in the transmission between the two parts of the network. Loss and/or delay are following mathematical laws programmed by the 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 various 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 and a Server part. These two applications can be installed on the same computer or on two different computers.

### ❖ The Server part

⇨ 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 6 is recommended), Windows 2000 or Windows XP.

⇨ 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.

⇨ Offers a thorough view of traffic statistics, selected parameters and traces.

### ❖ The Client part

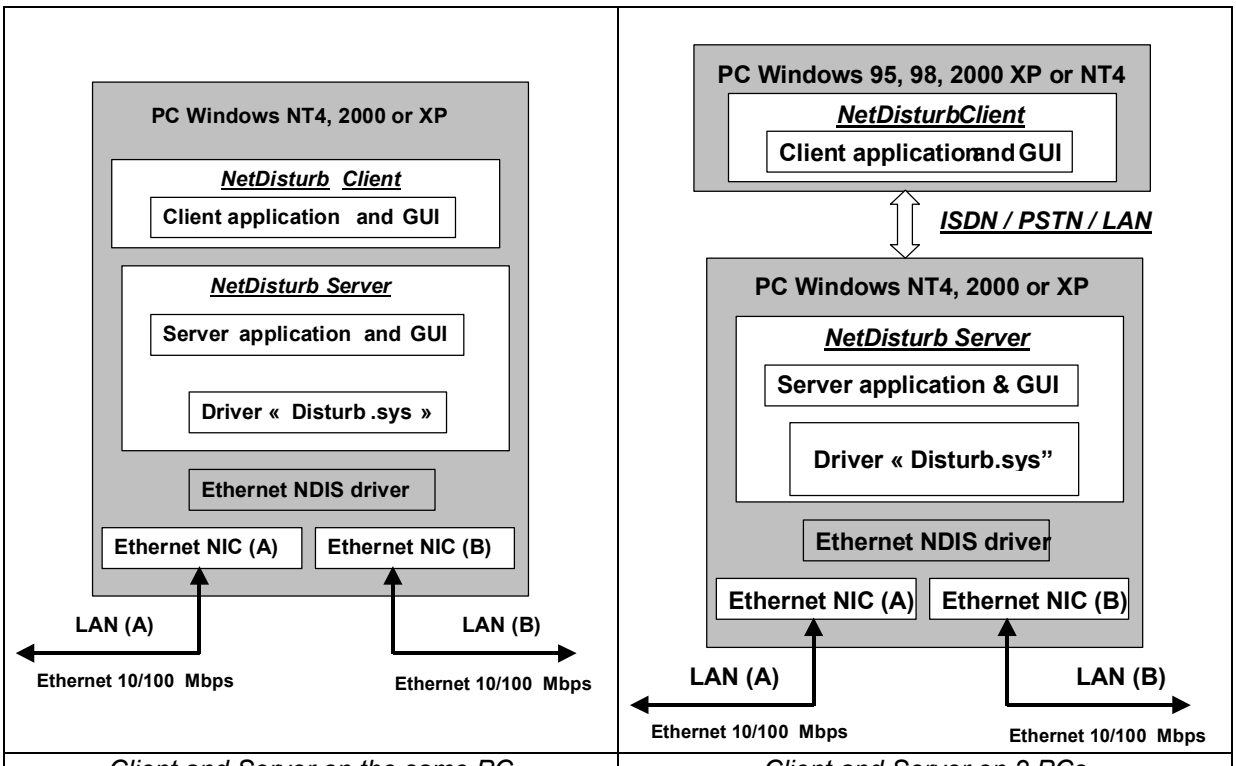
⇨ Can be installed either directly on the server machine or on a remote PC with a Windows 32 bits System (95, 98, NT4, 2000 or XP). In this case, the remote PC will control Server application via ISDN or PSTN using RAS or directly via a LAN card.

⇨ Allows configuring masks and laws, to manage NetDisturb functions, and displays statistics.

Two configurations may be used:

⇨ Client and Server on the same PC,

⇨ Client and Server on two PCs.




*Client and Server on the same PC* | *Client and Server on 2 PCs*

Client and Server applications use RPC on TCP/IP to dialog.

# Part 2 Install the NetDisturb software

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 a 800 x 600 display resolution. If you have the NetDisturb CD-ROM software version, please refer directly to paragraph 2.2.

The NetDisturb software 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 NetDisturb from a downloaded trial version

The installation procedure is a standard installation program.

*Please note that the installation procedure of the NetDisturb software 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 the NetDisturb software 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: 800 x 600
  - ⇨ Your PC needs at least 2 NIC already installed, configured and fully operational.

  NetDisturb is composed of two parts: Client and Server. **This setup will install 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, the NetDisturb software 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 the setup, after copying files 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.

The NetDisturb driver installation depends of the target O.S. (NT4 or 2000/XP).

## NetDisturb - driver installation for Windows 2000 or Windows XP

The NetDisturb driver sets in the kernel of Windows 2000. This driver is installed on top of the driver of network cards. For Windows 2000 or XP, it is considered as a protocol. The NetDisturb Driver goal is to handle the exchanges between two Network Interface Cards (NICs).

The installation of the driver is realized transparently. The Driver is mapped on top of each Ethernet or wireless NIC when the interface returns by that NIC is NDIIS compatible.

In order to avoid unexpected traffic generated by the protocol stack (TCP/IP, Client or Microsoft Networks, etc.) on the NIC that will use NetDisturb, you should unselect all protocols to have only the NetDisturb component linked to the selected NICs. Then close this window. The NetDisturb driver is now linked to all LAN connections defined in your system.

**To unselect protocols from the NIC used by NetDisturb, use the "Control Panel/Network and Dial-up Connections" application (Windows 2000) or "Control Panel/Network Connections" application (Windows XP) to *uncheck* protocols.**

## NetDisturb - driver installation for Windows NT4

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).

The NetDisturb Driver is a protocol named 'Disturbing Ethernet Driver over NDIS'.
The 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 applications need a TCP protocol stack for Client/Server 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/Server applications exchange, 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 using the control panel, press close to save all changes.

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

**Start Menu shortcuts created:**

Start > Programs > **NetDisturb**
- ⇨ **1) NetDisturb Server**
- ⇨ **2) NetDisturb Client**
- ⇨ **License help**
- ⇨ **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 Client and Server parts 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 the NetDisturb Client on a system. This is useful if you want to install the Server and the Client on two different systems.
To install the 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.

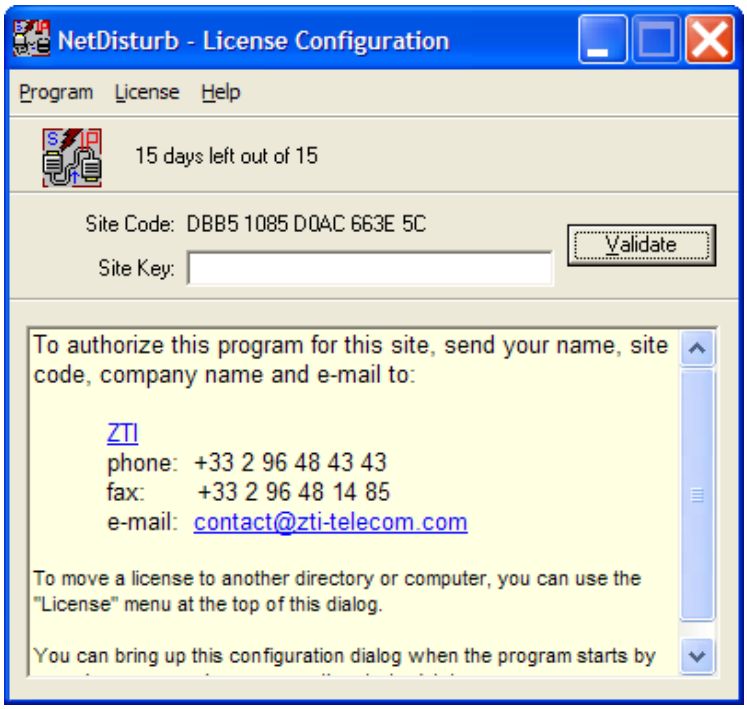
# Part 3 License configuration

*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).*

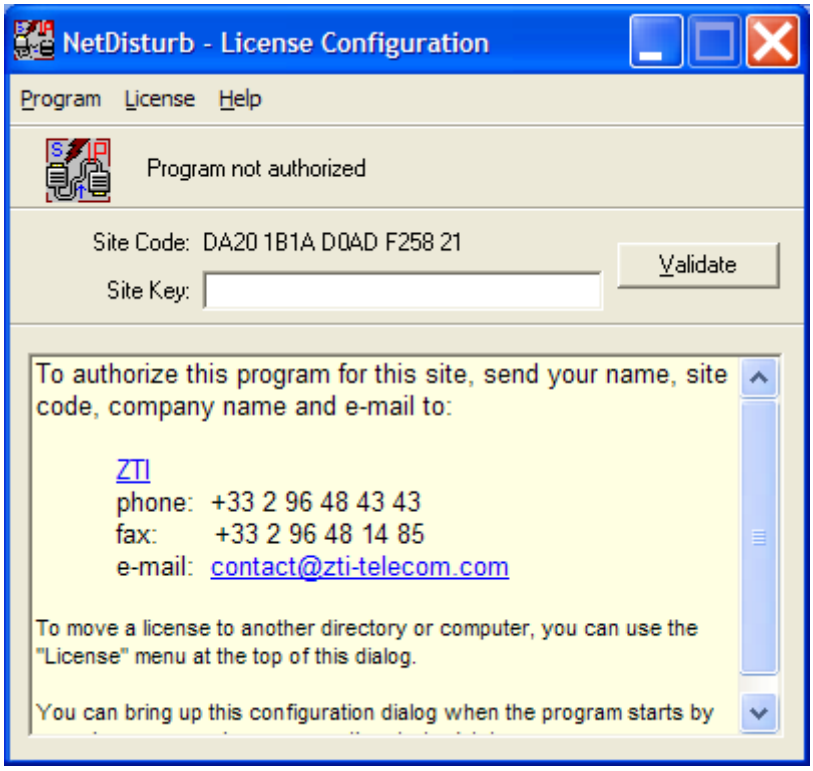
## 3.1 To configure a license

If you have a NetDisturb trial version, when you launch NetDisturb Server a message is displayed showing remaining days of use (for example, 15 days left out of 15 in the following example).


If you wish to configure your license before trial period end, please press <Enter> when this message is displayed. So you will obtain the *License Configuration* window.

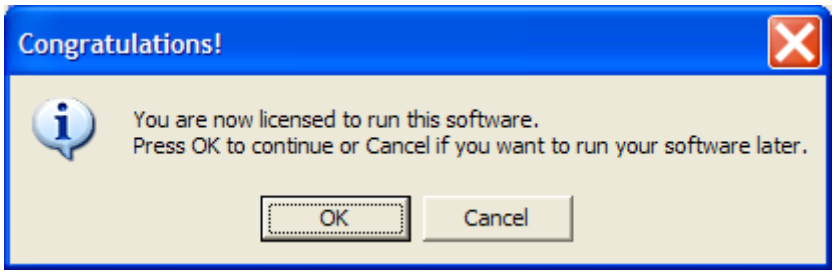


*Note: at the end of the trial period when you run "NetDisturb Server" the same license configuration dialog appears, with a specific mention instead of the remaining days of use: "Program not authorized" as shown below.*



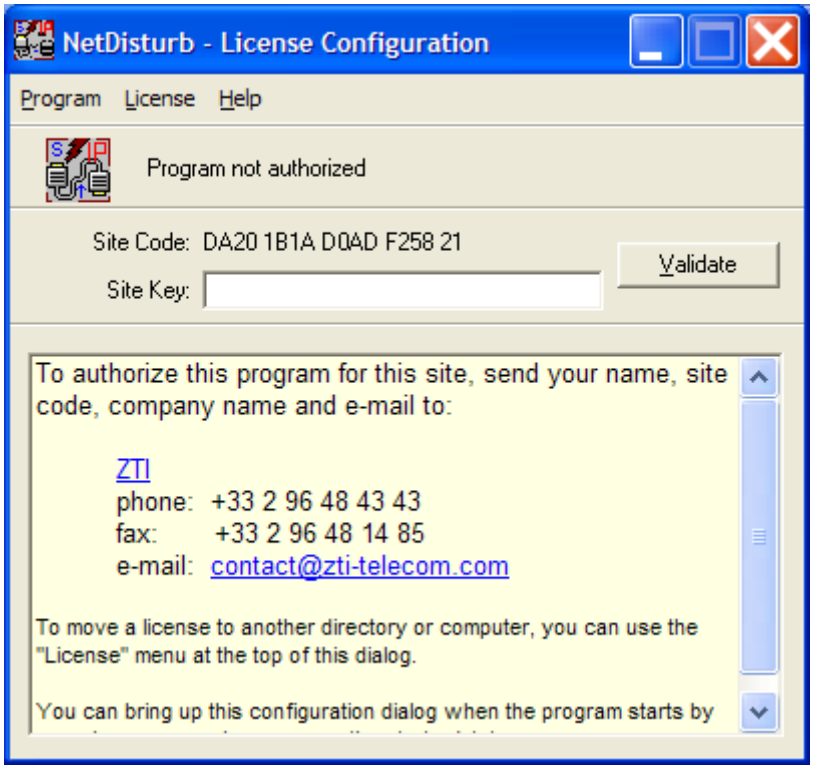

To get the 'Site Key' and obtain an unlimited version, please send your name, 'Site Code' (specific to your system), company name, email and preferred method of payment (if you haven't bought the NetDisturb software yet) to: contact@zti.fr or contact@zti-telecom.com.
We will send you your Site Key once we receive payment.
If you have already bought, please email your Site Code and we will email you back the Site Key for an unlimited license.

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



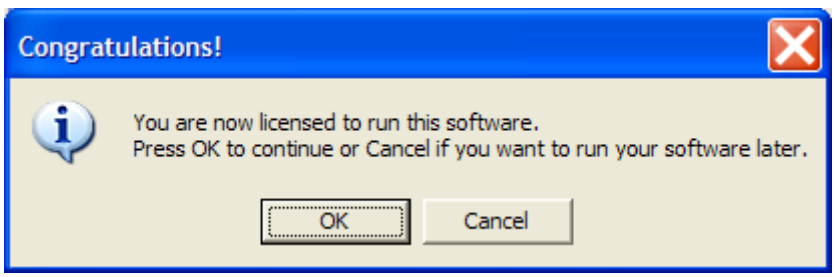

*Note: the following window is displayed when you run NetDisturb if you have an unlimited license.*


At the end of the trial period, when you run NetDisturb Server (the server part), the following *License Configuration* window will be displayed:




To get the site key, please send your 'Site Code' (specific to your installation), company name, e-mail and preferred method of payment to: contact@zti.fr or contact@zti-telecom.com

We will send you your site key when we receive your payment.
After you have entered your Site key, you will get the following message:



## 3.2 License transfers

*Warning: a license transfer is not a duplication of any type.*
*Please contact ZTI or your authorized distributor for site license information and for several licenses purchase.*

Licenses can be transferred using one of the following methods:

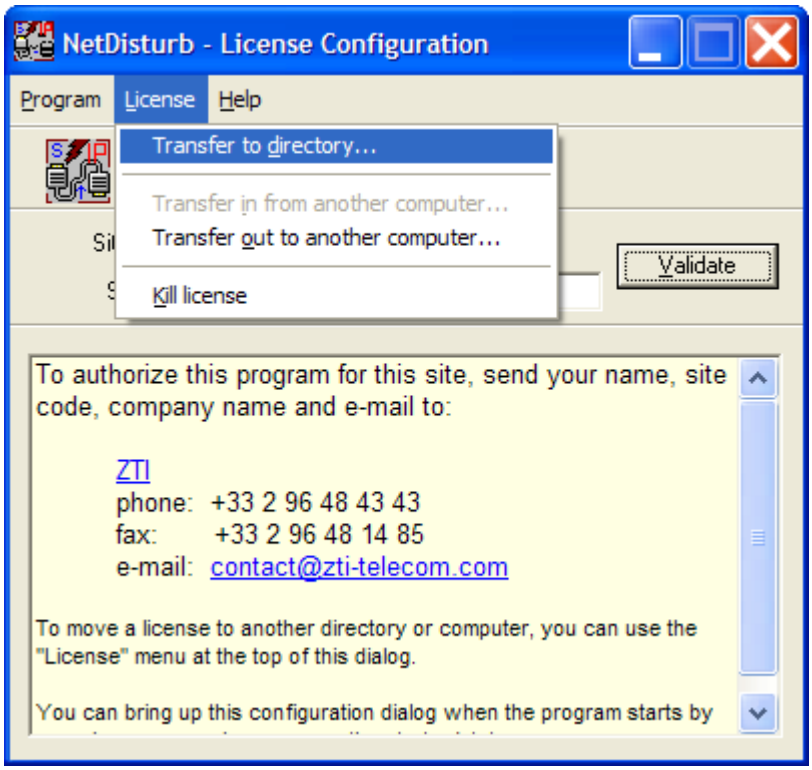
- ⇨ Direct transfer: move the license to another directory on the same PC or between two networked PCs.
- ⇨ Transfer by media: move the license from a source PC to a target PC by using a floppy disk or USB key.

### 3.2.1 Direct transfer: move the license from one local directory to another

This transfer mechanism must be used to move a license in two cases:
- from a source to a target directory of the same PC
- from a source to a target directory of networked PCs

- 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\Server”*). 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\Server\NetDisturbServer.exe*).
  The program copy now has the license awarded the original.

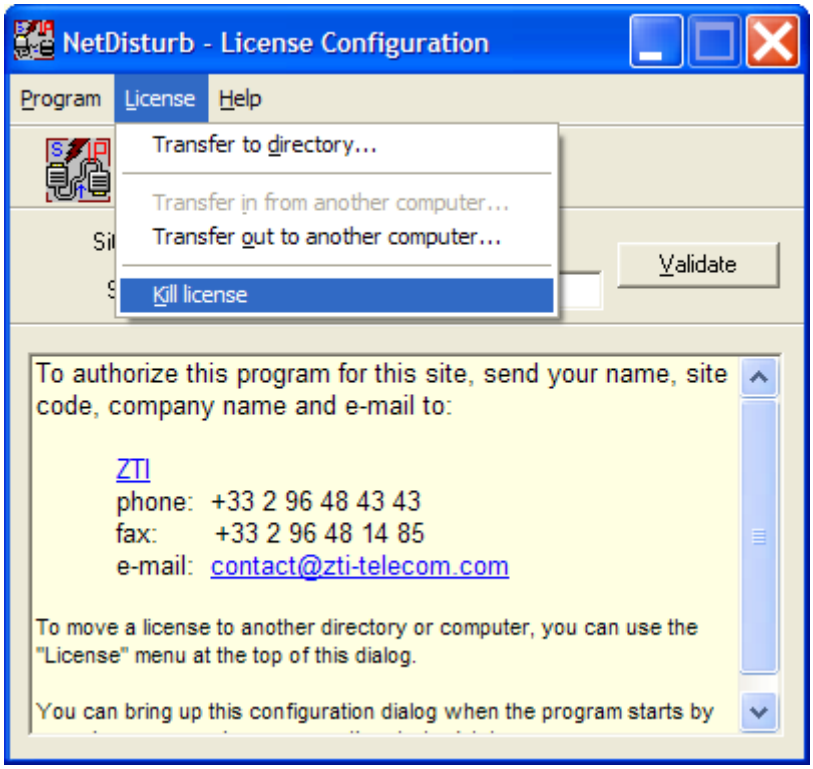
### 3.2.2 Transfer by media (floppy disk or USB key) from a PC to another PC

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

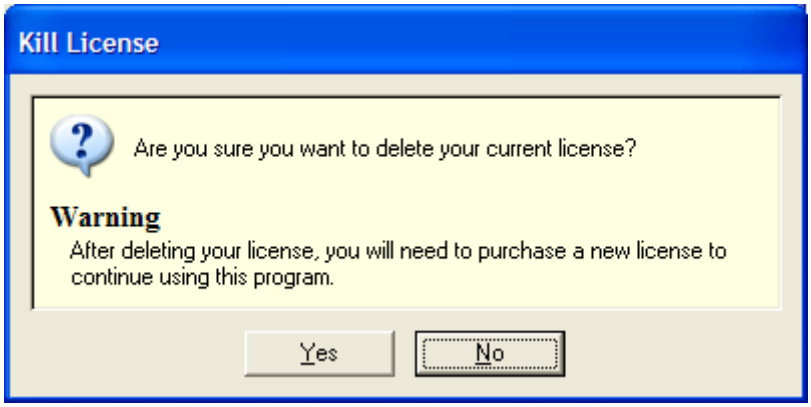
**Point 1:** First install the program on the target PC (PC# 2).

**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.

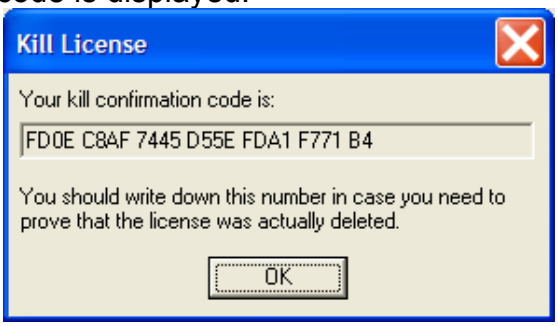
To kill the license, please proceed as follows.
When the license configuration window appears, press enter and select in the menu “License > Kill license”.



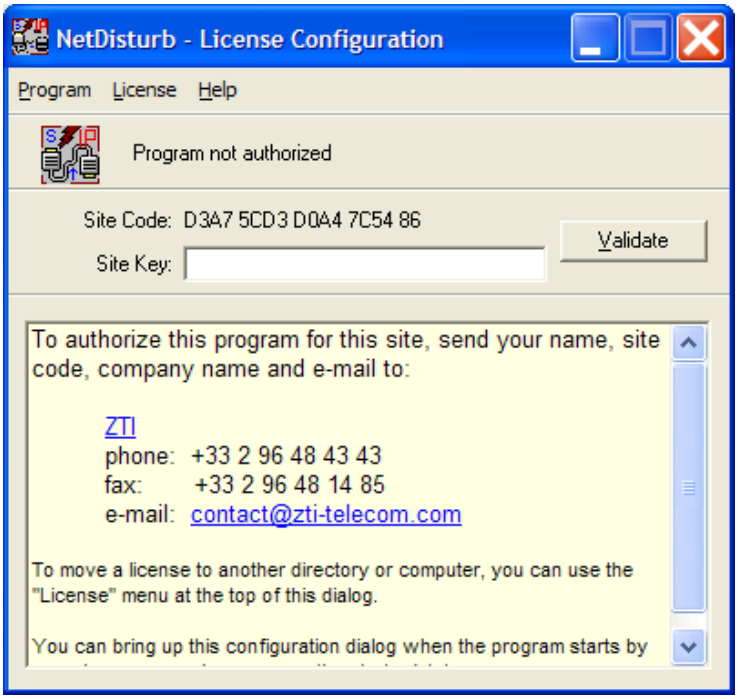

A message box appears, press ‘Yes’ to kill the license.



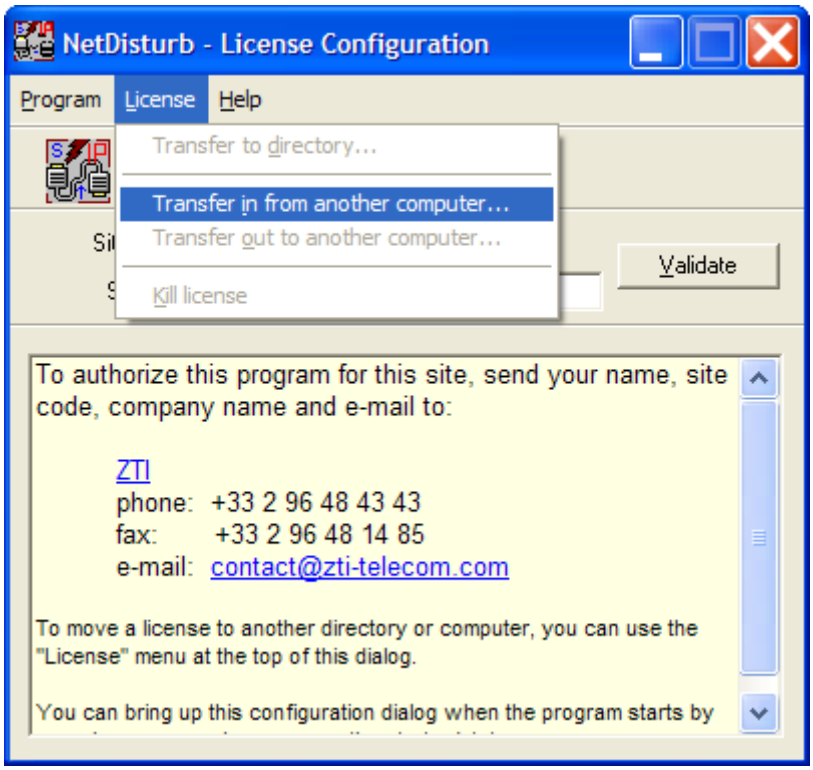

And a kill confirmation code is displayed.



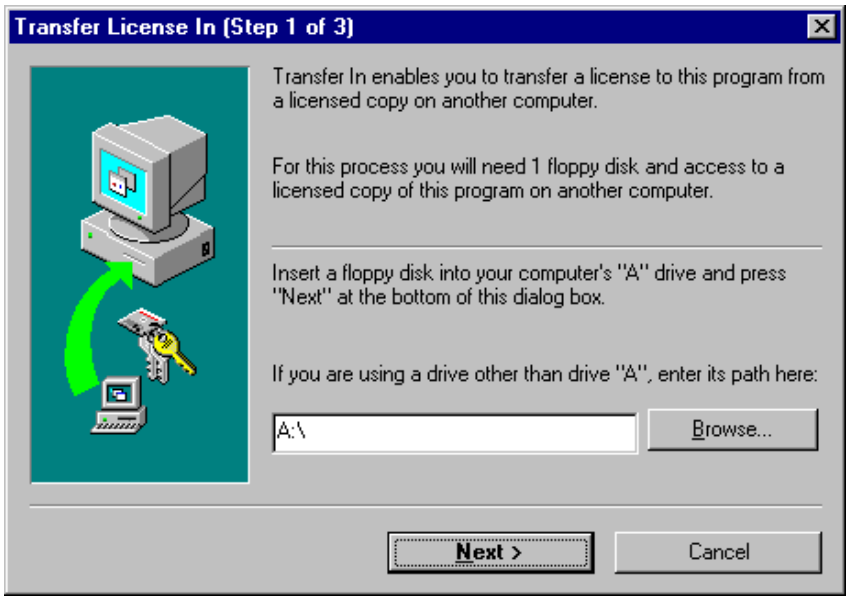

The license window displays now "Program not authorized" as shown below:



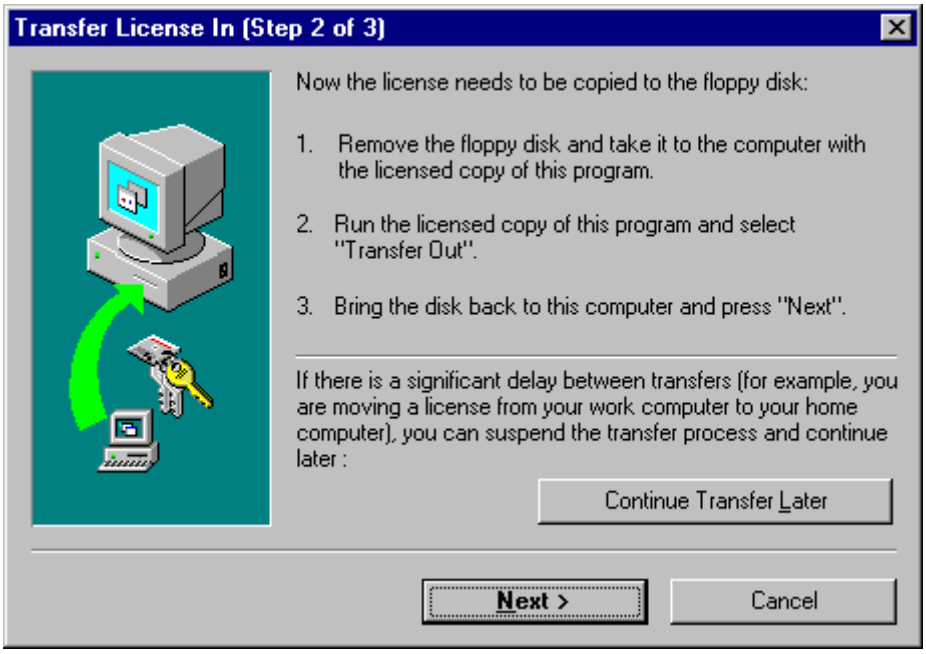
**Point 3:** select in the license menu, the item: “License > Transfer in from another computer …”.



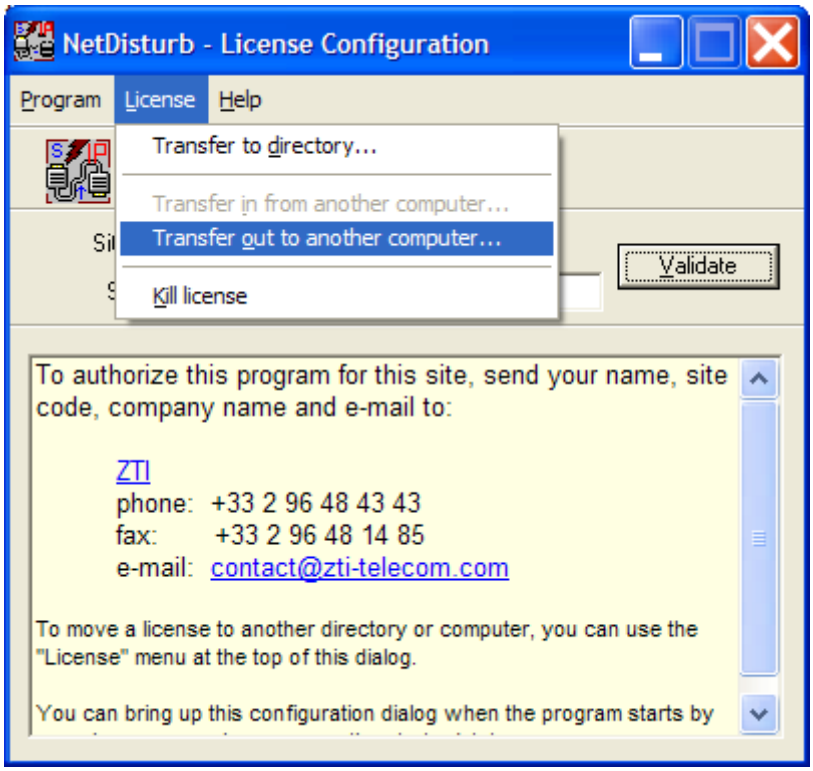

and the "Transfer License In (Step 1 of 3)" window is displayed:



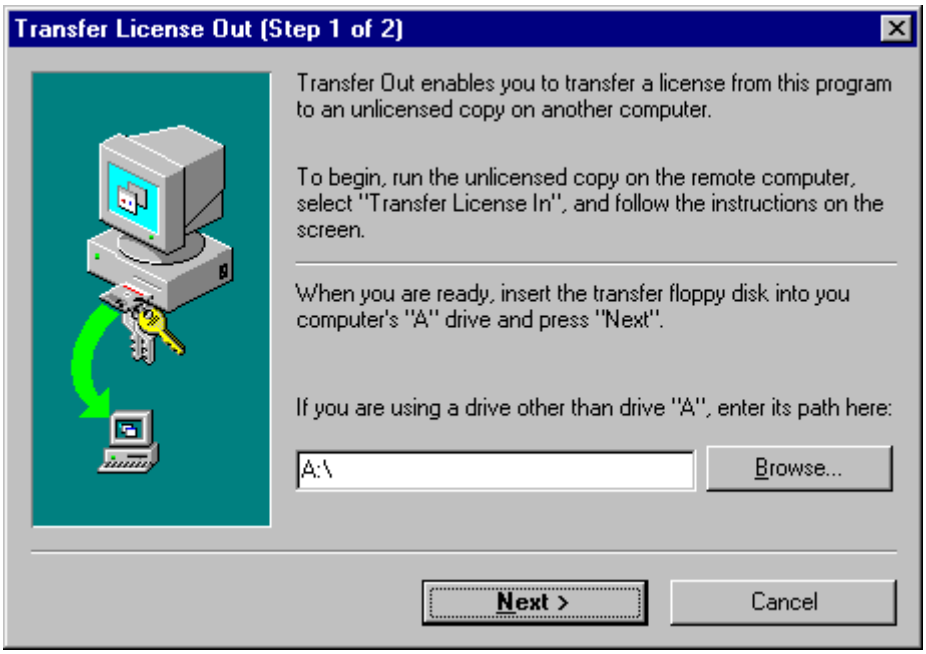

**Point 4:** Insert a floppy disk or use a USB key as requested in step 1 of 3 and specify the path.
Then press “Next >” and the "Transfer License In (Step 2 of 3)" window is displayed:




**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:

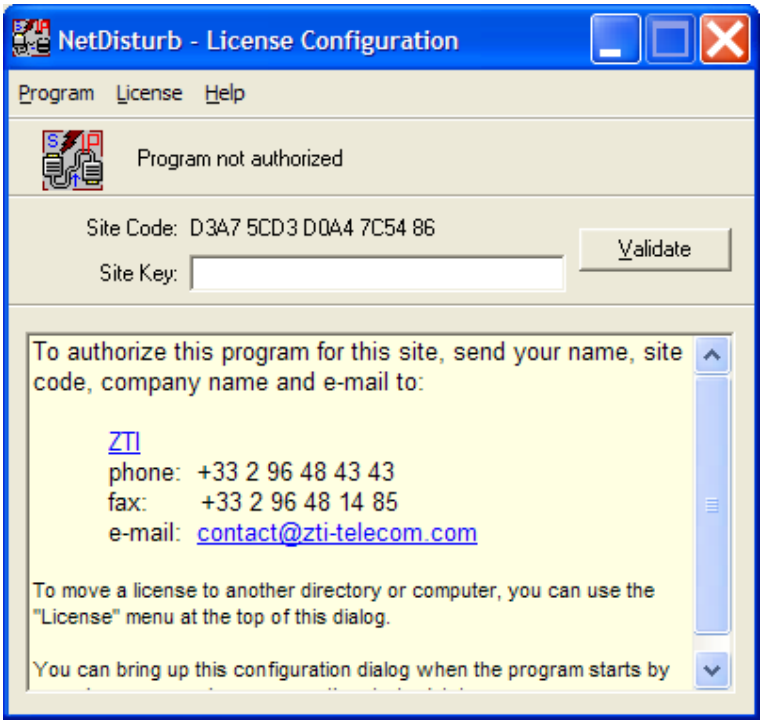


Then the following window is displayed:



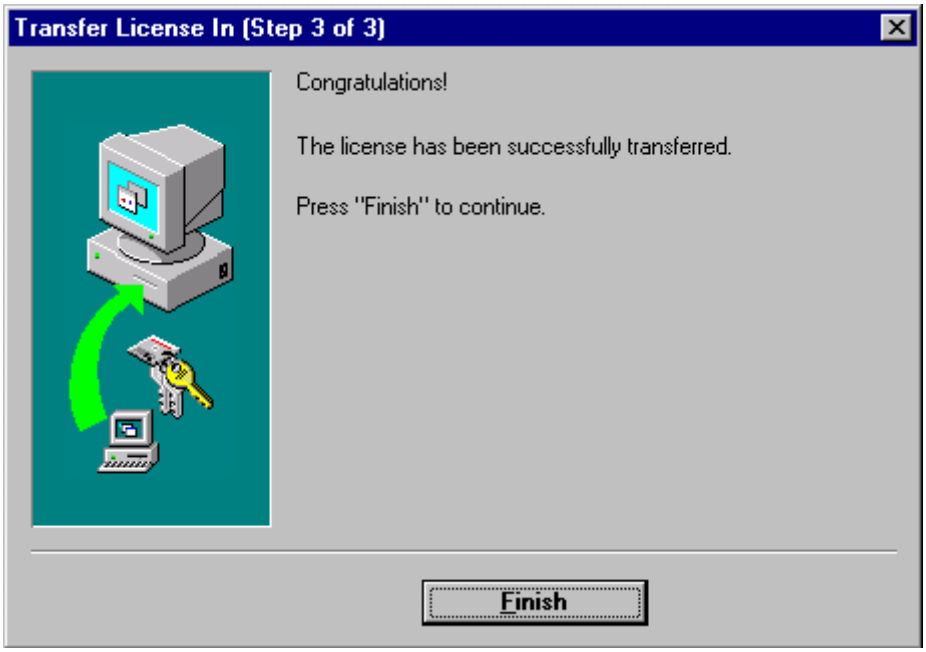

Input the media path (floppy disk or USB key) and then press "Next >".

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.fr or 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:

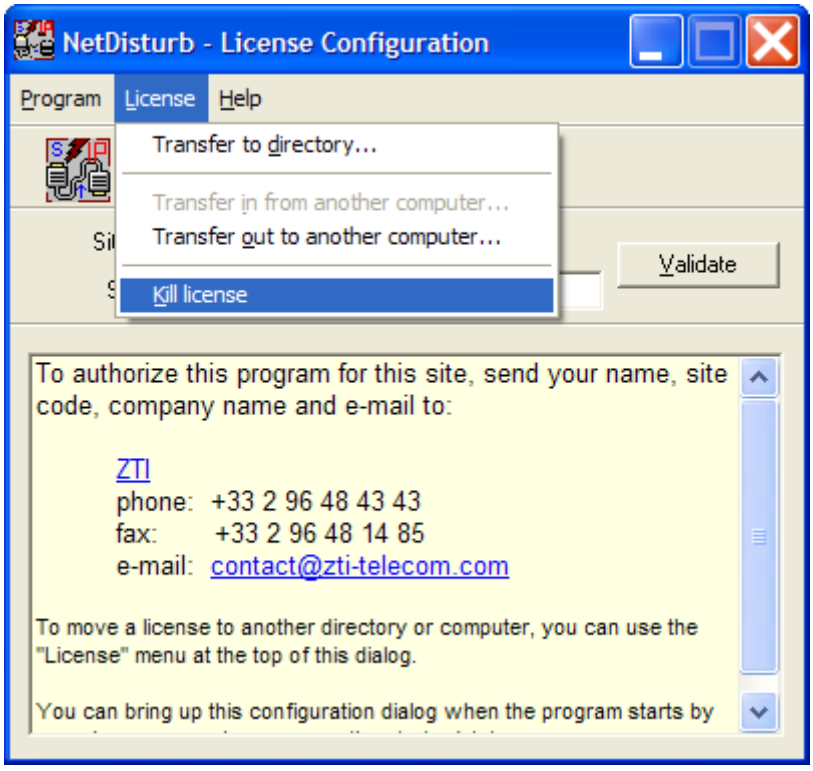



Click Finish to continue.

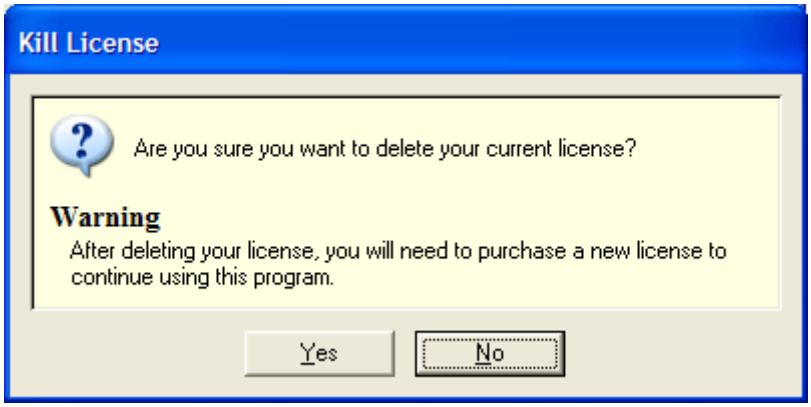
## 3.3 To kill a License

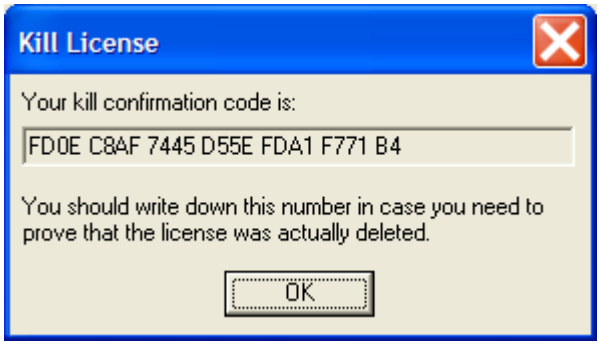
If you would like to transfer an unlimited license key onto a PC where a trial period is still active, you should first kill the active trial period. If you don’t kill the active trial period, you will not be able to transfer an unlimited license. To kill the trial license, you should proceed as follows:

- 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”.

### ⇨ Windows 2000 or XP

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

### ⇨ Windows NT4

The uninstall procedure is executed and a text file is automatically opened in order to explain how to uninstall the NetDisturb driver.

In Windows NT, the Disturb Driver is not removed by the uninstall procedure because it has not been added by the installation procedure. You should use the Control Panel, run "Network" and choose the "Protocols" tab. Then select the driver "Disturbing Ethernet Driver over NDIS" and click on "Remove".
Then you must restart your PC.

# Part 5 Run NetDisturb

As the NetDisturb tool is composed of 2 parts (Server and 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'

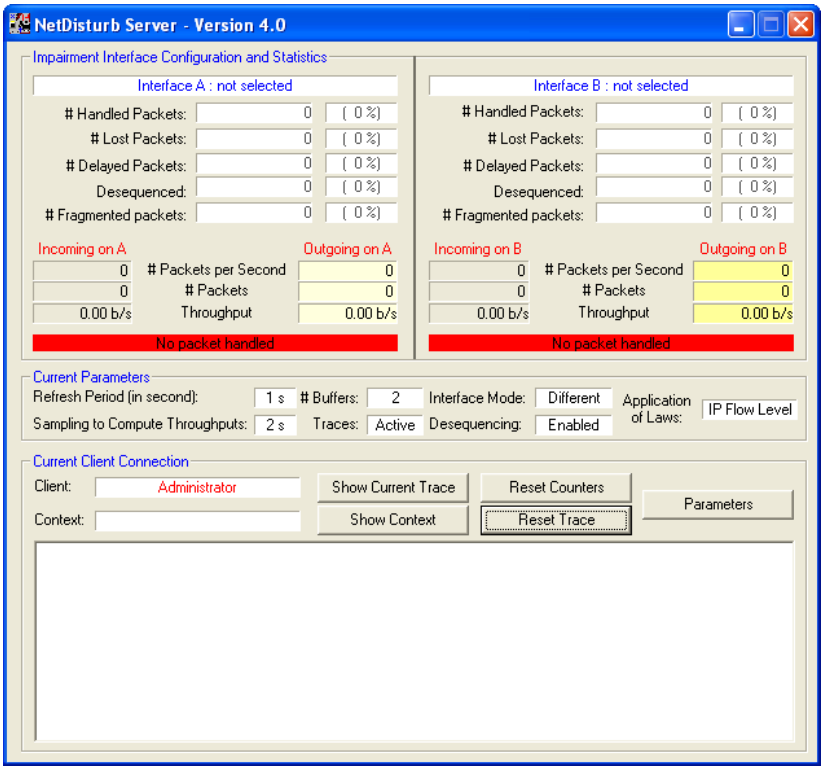
*Depending of your license, you will get the following license window:*

| *Limited license* | *Unlimited license* |
|---|---|
|  |  |





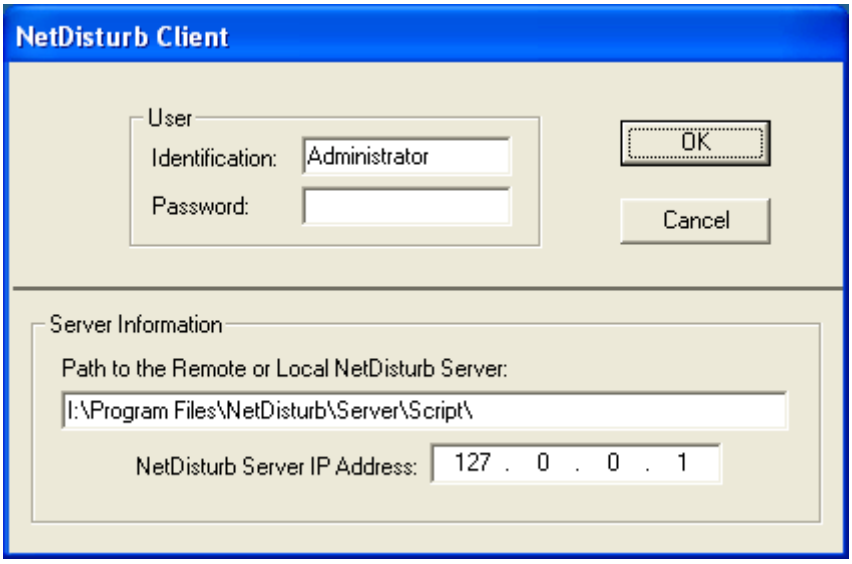
When you run NetDisturb server for the first time, the default window is displayed:




No board (or NIC) has been selected: NetDisturb Server selection interfaces (or NICs) will be done later by the NetDisturb Client application.

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:

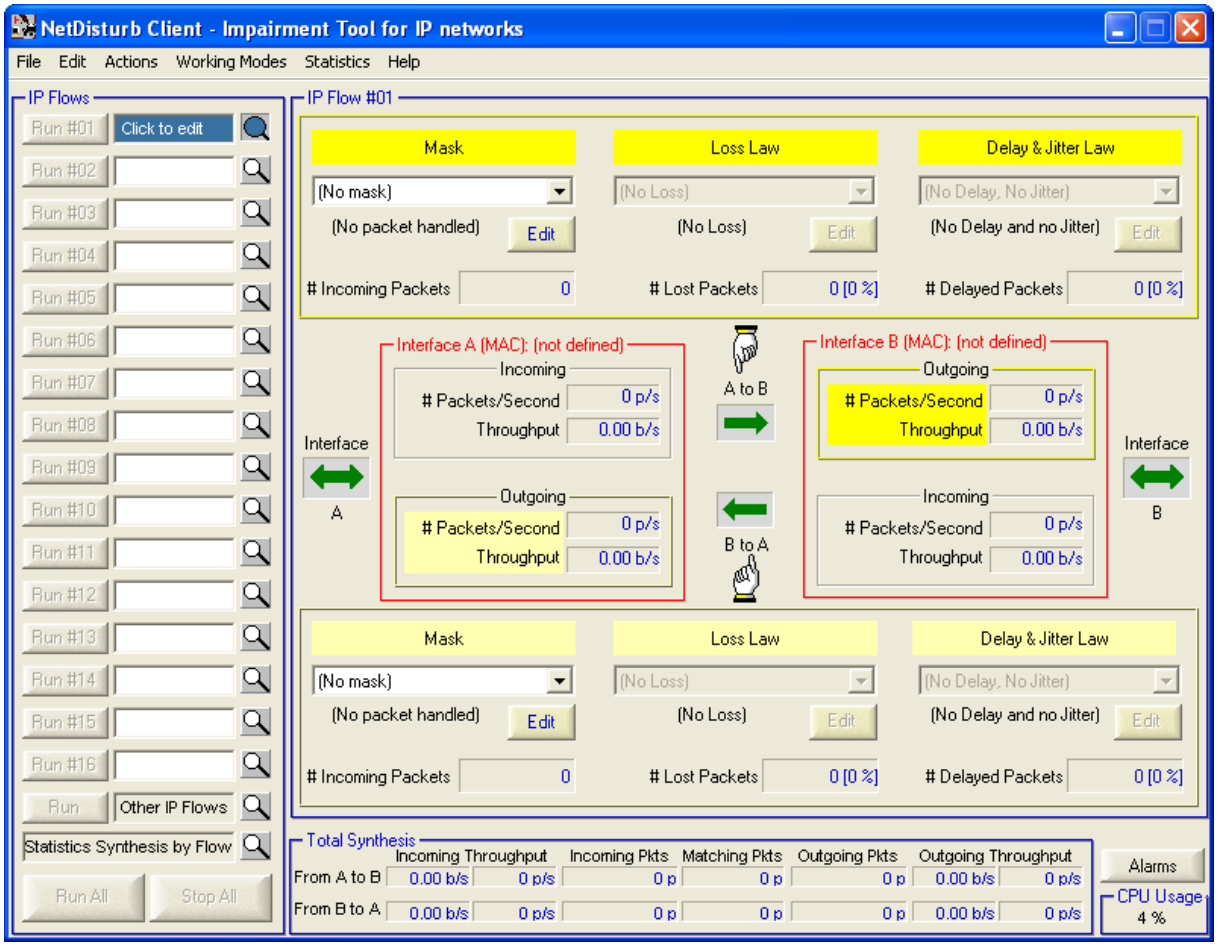



- **User Identification** = Administrator
- **User Password** = (no password needed)

- **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)

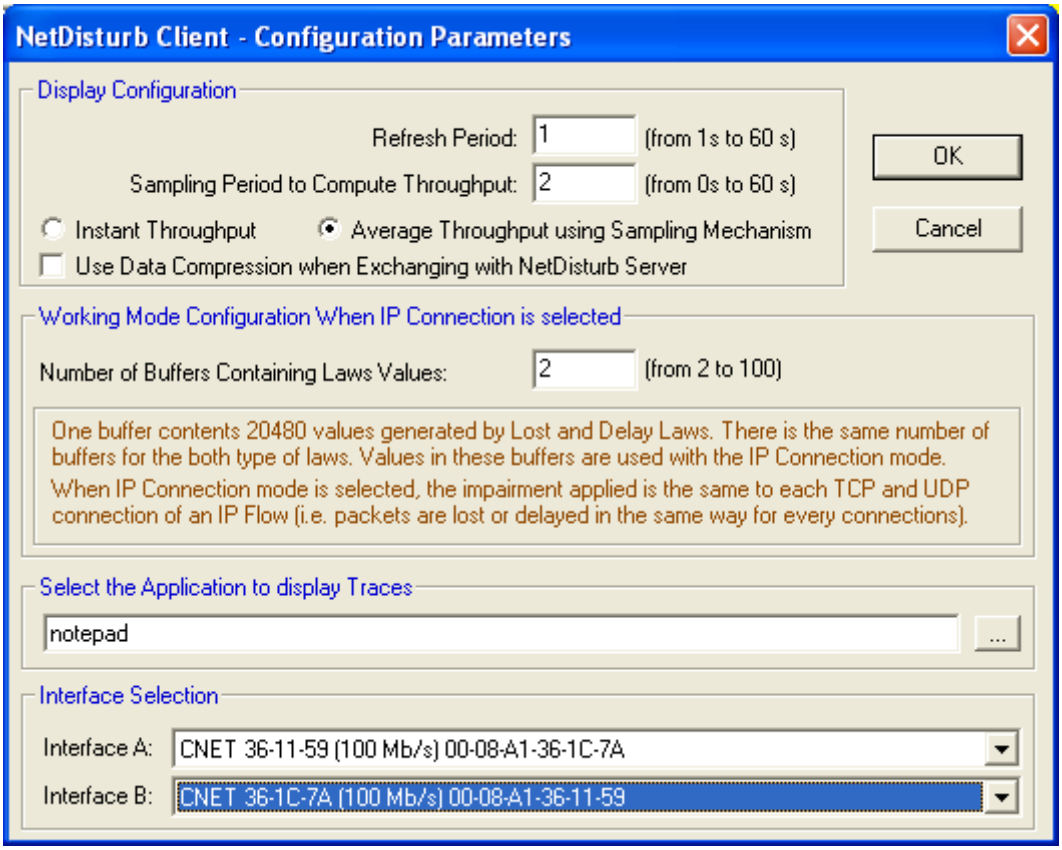
- **NetDisturb Server IP address** = 127.0.0.1 (default local IP address, if NetDisturb Server is installed on the same system).

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




You must configure the NetDisturb Server and select the NICs that NetDisturb 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”.

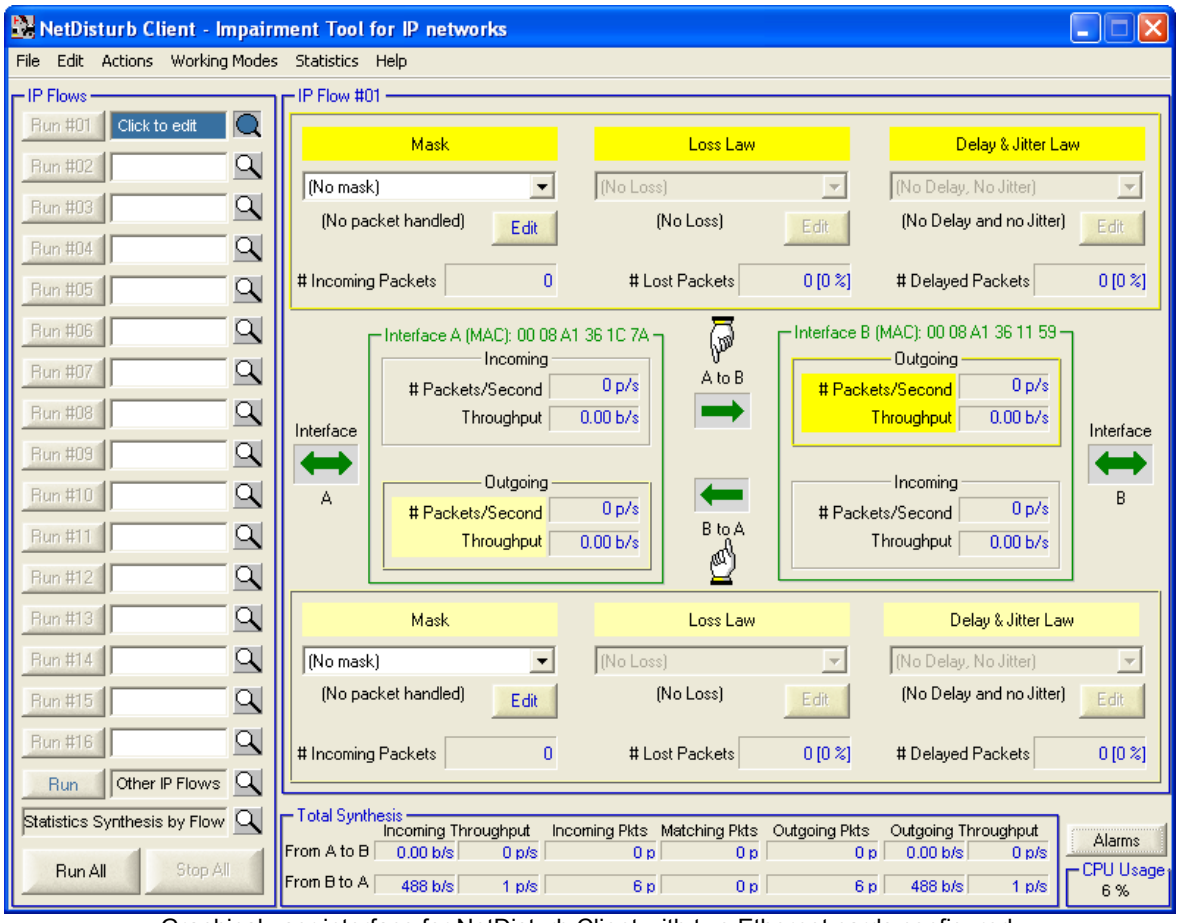
***Note***: you must see in the combo-box (Interface A or Interface B) all NICs available and operational. If you don’t see any NICs, please do the following steps:

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

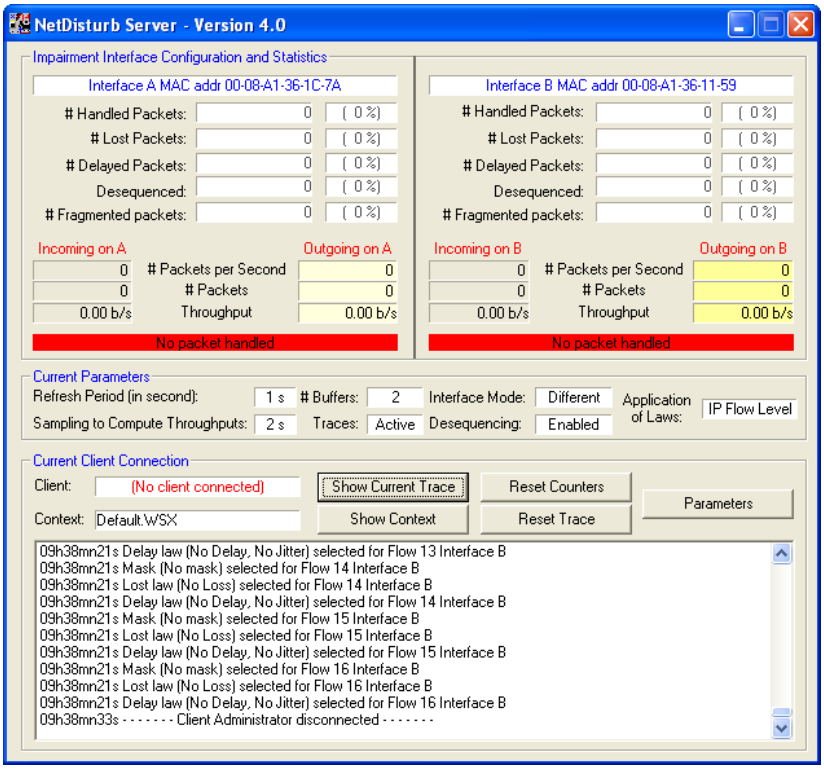
Normally, you should see your installed NICs in the Interface A combo-box.

As soon as the configuration is done, “Interface A” and “Interface B’ are recognized by NetDisturb. The MAC Address of the interfaces is displayed in the Client and in the Server window as shown:




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




Graphical user interface for Server part with two Ethernet cards configured

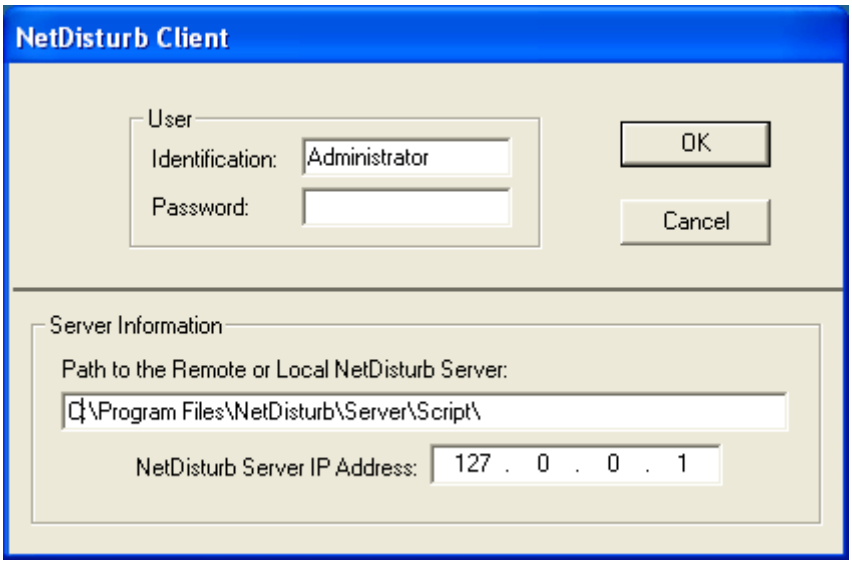
## 5.2 Detailed description of Server and Client startup

### 5.2.1 Server startup modes

The level of functionality depends on the availability of the NetDisturb Driver. If the Driver is lacking, a message warns the user. In this case it is possible to continue, however only some functions will be available - this is called “Restricted Mode”.

### 5.2.2 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, Client must provide the corresponding password. With this mode the NetDisturb functionalities are fully available: Client can modify laws, stop or activate the relaying process or change contexts.

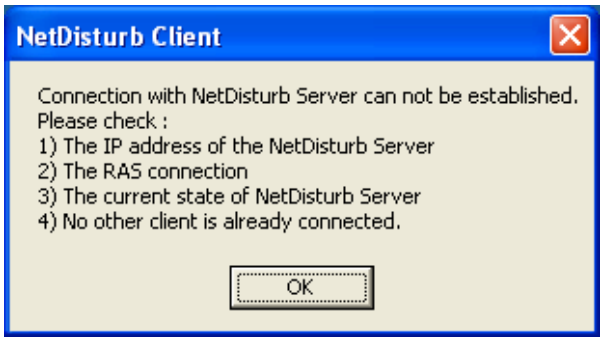
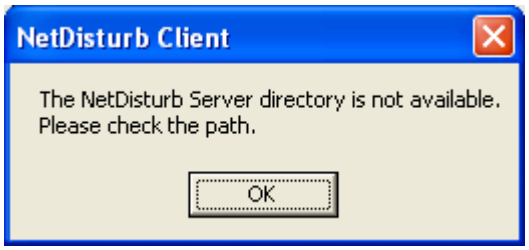
USER mode:
To be connected as User, Client provides a different identification than Administrator. Password is not necessary. NetDisturb functionality is reduced to the use of contexts located on the PC Server. Masks and laws can’t be defined.

### ❖ Server Information section

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

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

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

| Errors windows may be: | Check: |
|---|---|
|  | 1) The IP address is correct.<br>2) The RAS link is correctly established and that data are exchanged between client and server.<br>3) Server application is running.<br>4) Another user is not already connected to the Server or the 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) |

# Part 6 Using NetDisturb Client application

Client application is the main NetDisturb Man 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.

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

Remind

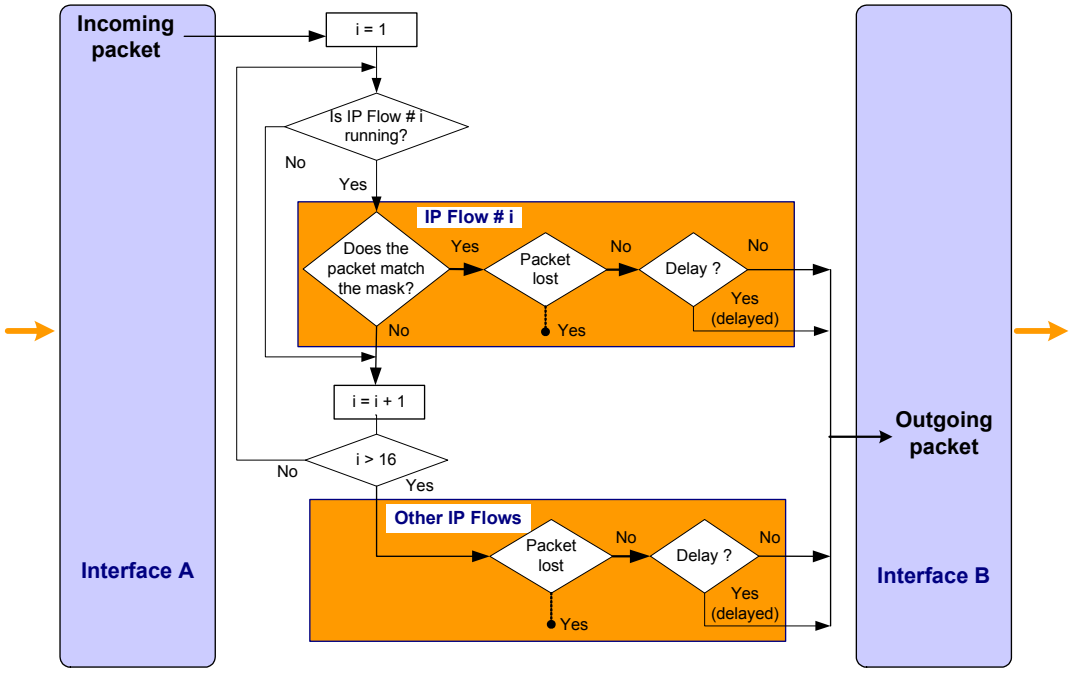
To use NetDisturb:

⇨ **First run NetDisturb Server**

⇨ **Then run NetDisturb Client**

## 6.1 NetDisturb Client Main Window

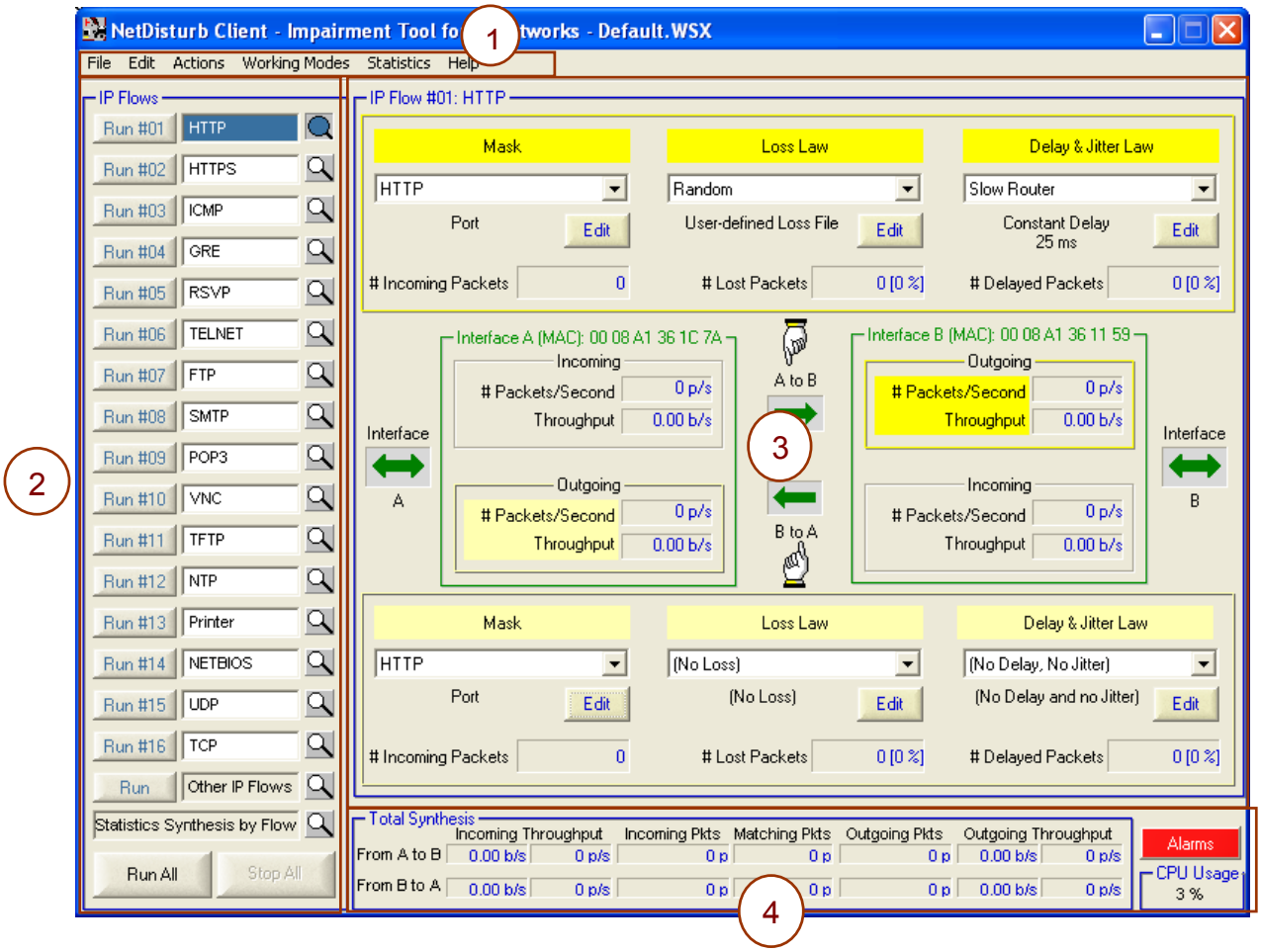
The NetDisturb Client main window is displayed after client identification. Traffic and impairment representation on Client main window is based on the following scheme:




***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 paragraph 6.2.

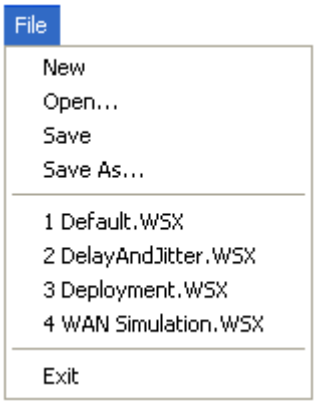
2 The ‘IP Flows’ area lists mnemonic-names of flows. This area is used to start and to stop IP Flow unitary or all flows at the time. The button in shape of a magnifying glass is used to select the flow individually. The last two objects have predefined behavior: The ‘Other IP Flows’ allows applying specific loss and delay laws to non-previously filtered IP packets. The ‘Statistics Synthesis by Flow’ object 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 lost and delay laws, or IP masks.

4 The total synthesis area is a reference area where total statistics information is presented. It includes ‘Alarms’ returned by the NIC drivers or by the NetDisturb driver when memory errors occur. The CPU information is provided for information about the current activity of the PC.

## 6.2 Menu description

### 6.2.1 File menu




In order to keep parameters configuration for further tests sessions NetDisturb is based on context files management. Context files are saved with a **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.

The latest context is opened each time the NetDisturb Client starts.

#### 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).

#### 6.2.1.3 Save

This command allows saving parameters and laws defined by the user in a context file (.WSX files).

#### 6.2.1.4 Save as

This command allows saving parameters and laws defined by the user in a context file, which name is requested in a standard dialog box.

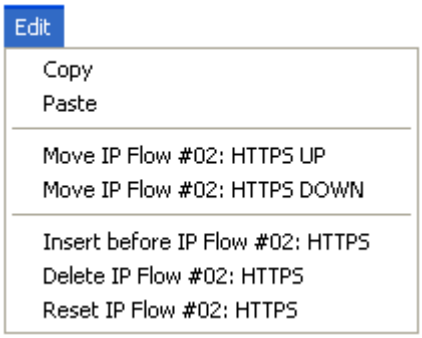
#### 6.2.1.5 Recent Files

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

#### 6.2.1.6 Exit

This command stops the NetDisturb Client part. If changes where 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 in a temporary buffer 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 and 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 mnemonics move too if they have been 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 and 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 mnemonics move too if they have been 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 16$^{th}$ item is lost. If the current item is the 16$^{th}$, no change appends to the 15$^{th}$ previous but the current – the 16$^{th}$ - is reset.

#### 6.2.2.6 Delete xxx

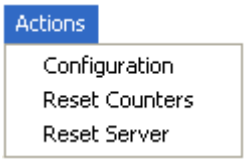
The 'Delete before …' item deletes the current item and moves lower items to one position up. The 16$^{th}$ item becomes empty.

#### 6.2.2.7 Reset xxx

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

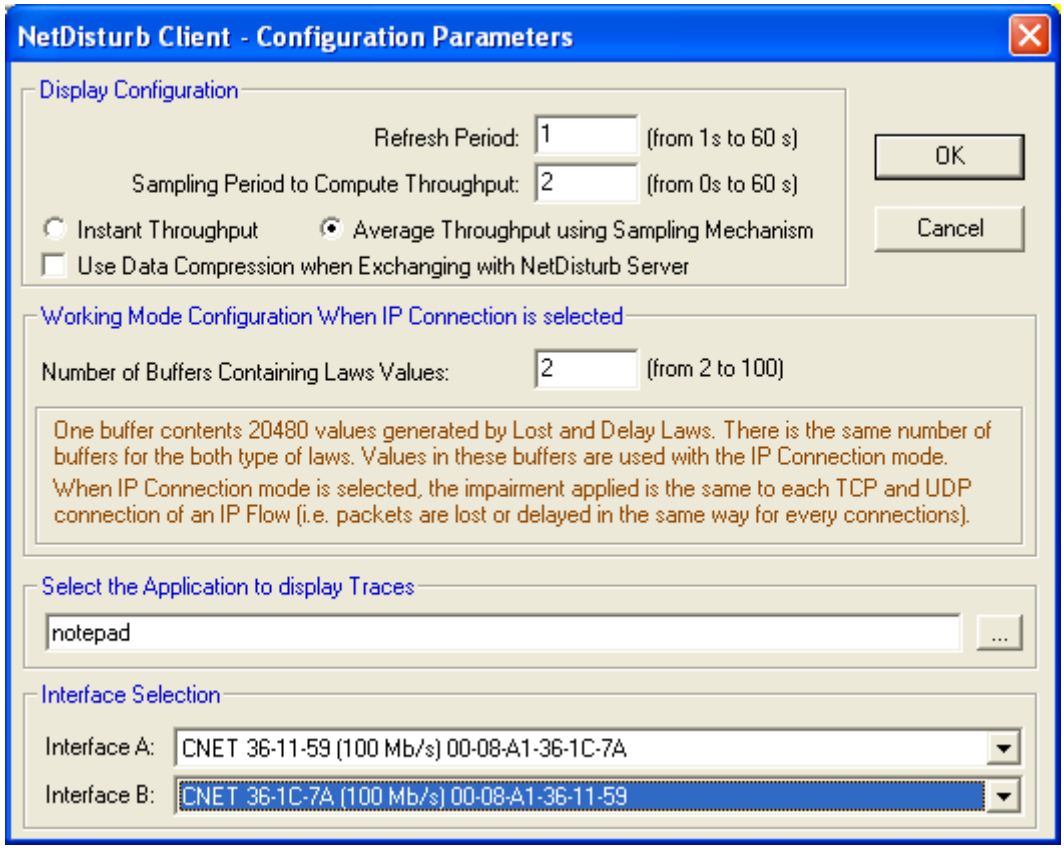
 

### 6.2.3 Actions Menu




#### 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, the user can:

- Define the refresh period for display of GUI's counters.
- Define the sampling period to compute throughput.
- Define the way the throughput will be computed (instant throughput or average throughput 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 Server applications exchange trace and are connected via ISDN or modem. When NetDisturb Client and Server applications are exchanging on the same PC, data compression is not relevant.

#### ❖ Working Mode configuration

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 paragraph 6.2.4.2).

#### ❖ Select traces viewer

From this section, the user can define the application used to read traces (word processor application). Notepad is entered by default.

#### ❖ Ethernet board selection

This section allows selecting the Ethernet cards to use.
When quitting NetDisturb, configuration may be saved in context file. This configuration is automatically reloaded when the NetDisturb Client restarts.

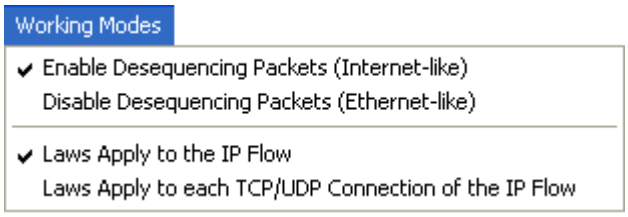
### 6.2.3.2 Reset Counter

The Reset counter item impacts both local Client and Server counters. It set to zero all counters and percentage. It doesn't reset internal law counters in use by lost and delay laws i.e. counters used in Burst Uniform Lost law or Router Simulation laws Delay & Jitter 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.

## 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 can analyze 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 can simulate an Internet network or can react as Ethernet does.
How NetDisturb is face or creates to 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 modes

❖ 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 the user defines to lose 1 packet on 3, the third received packet is lost, whatever the TCP/UDP connection it belongs to.

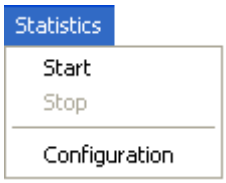
❖ Connection IP Flow

When the 'Law Apply to each connection of the IP Flows' is selected, NetDisturb 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 TPC 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 application 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 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. Both A to B and B to A direction are saved.

#### 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 save at the beginning of the file, followed by the list of statistics, one column per statistics.

Each following record gets the format:

| Columns separated by a tab | Comment |
|---|---|
| MM/DD/YYYY | Month/Day/Year |
| hh:mm:ss.mmm | Hour:Minute:Second.millisecond |
| #xx or Total | Connection number or Total Synthesis when it refers to A to B direction. When B to A direction, this column is empty. |
| *Statistic value* | One value per selected statistic as described in the paragraph 6.2.5.3. |

When the statistics are writing, the file can be opened but not changed. If the file exists it is rewritten.

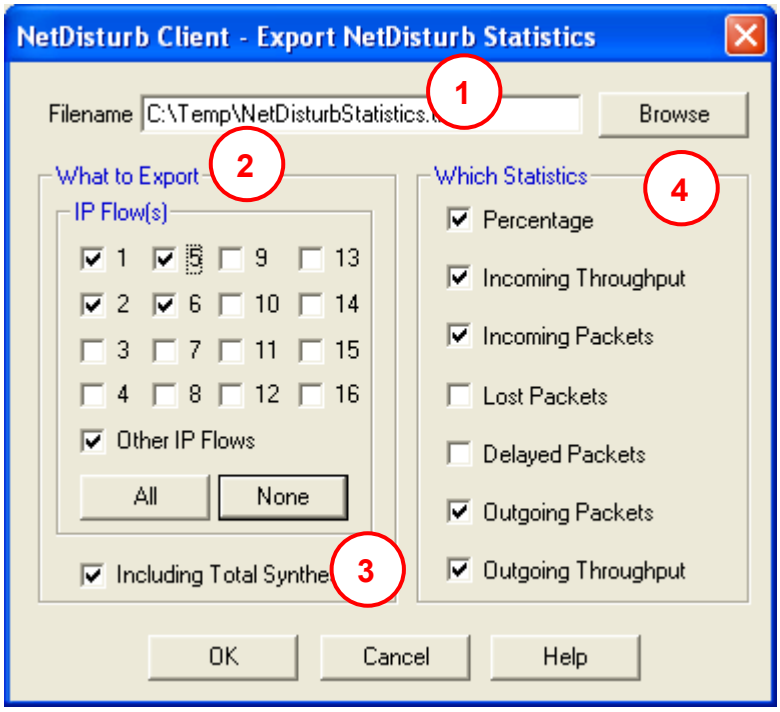
Throughput values are expressed in Kbps. Throughput packets are expressed in packets per second (pkts/s).

#### 6.2.5.2 Stop

Stop to save statistics into the file. The file is closed: it can be renamed or copied.

#### 6.2.5.3 Configuration

This option allows defining various export parameters.




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

### ❖ Filename ❶

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 ❷

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

### ❖ Which statistics ❹

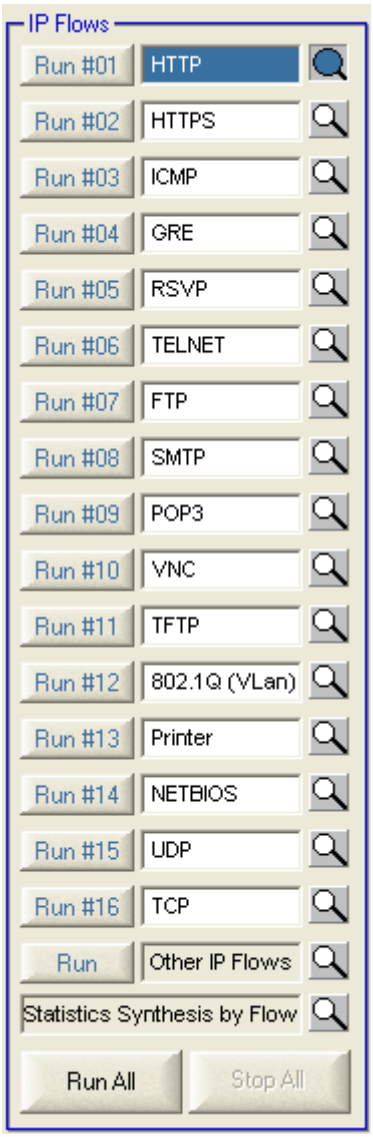
This section is used to select the statistic items to save.

- Percentage
  This statistics presents the relative part of the IP Flow, direction dependant, against the number of filtered packet. It is not relevant for the Total Synthesis.
- Incoming and Outgoing Throughputs
  These statistics include the volume throughput (in Kb/s) and the packet throughput (packet per second), one statistics per column. They are relevant for the Total Synthesis.
- Lost or Delayed Packets
  These statistics include the number of packets. They are not relevant for the Total Synthesis.
- Incoming and Outgoing Packets
  These statistics include the number of packets. They are relevant for the Total Synthesis.

## 6.3 IP Flows

This section describes the IP Flow Client part area.

### 6.3.1 General description




**Left buttons (Run #xx/Stop #xx)** 

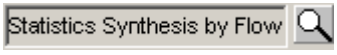

- Each IP Flow can be started or stopped unitary.
- The button 'Run/Stop #xx' indicates the status of the IP Flow will get if the button is pressed. This button is grayed when Interface A and B aren't defined.

**Edit area** 


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

**Buttons in shape of a magnifying glass** 

- 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 button  , the user can get an abstract of the activity of all flows. Details can be found in paragraph 6.3.4

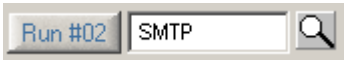
**Bottom buttons** 


- The 'Run All' button starts all non-yet-started IP Flows, event IP Flows that don't have a mask 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.
The 'Run #XX' button is colored in blue and the button in shape of a magnifying glass is white colored:




If IP Flow details are shown, the edit part and button in shape of a magnifying glass are blue, whatever the status is:


#### Active Status

The active status is indicated by the 'Stop #XX' button and button in shape of a magnifying glass colored in green:


When the current IP Flow is in active state, the active status is indicated by the button 'Stop #XX' remains green but the label and the button in shape of a magnifying glass are blue:


### 6.3.3 The 'Other IP Flows'

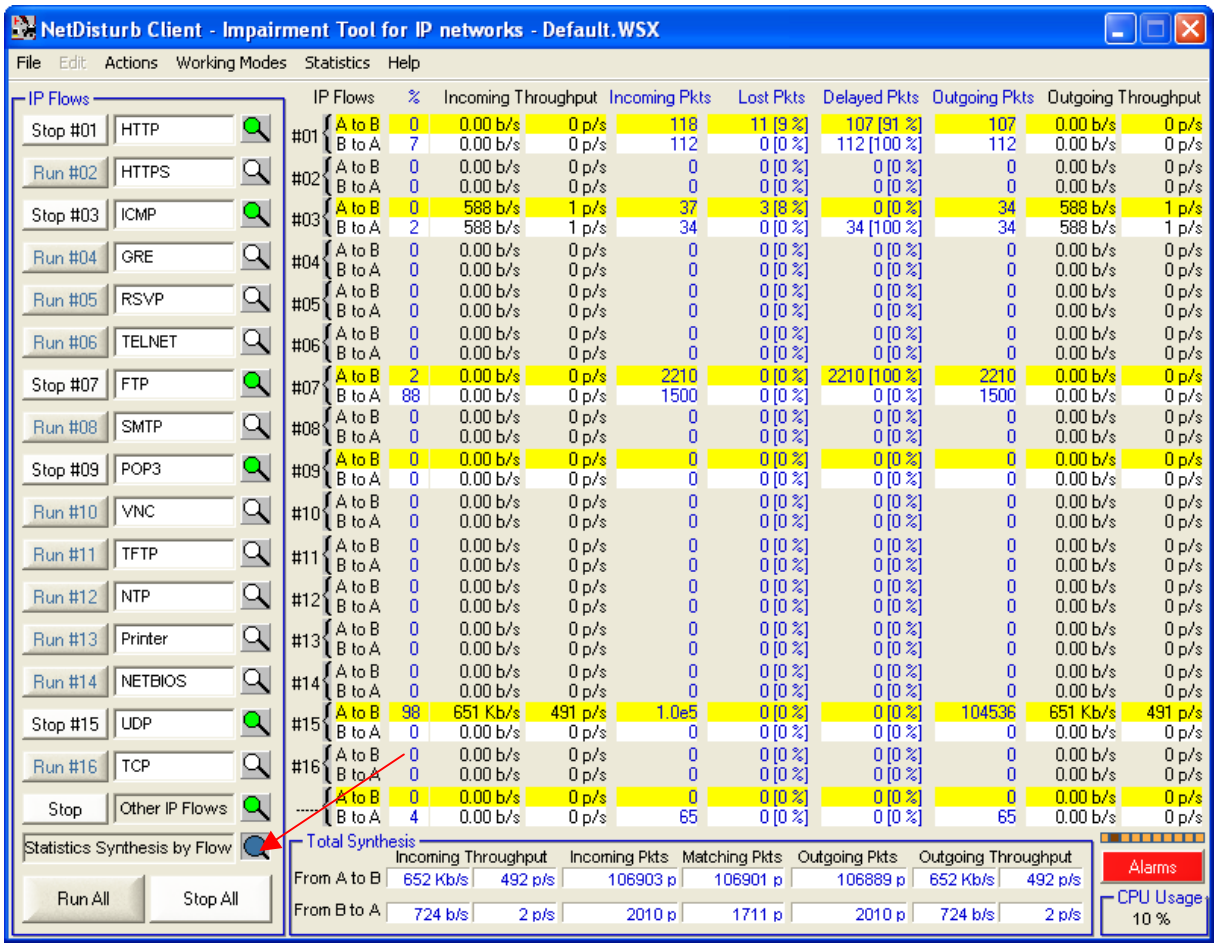
The 'Other IP Flows' is in charge to handle IP packets that haven't been filtered by IP Flows #01 to #16. This is why the mask isn't available for this predefined IP Flow.

The 'Other IP Flows' can be used to lose the IP packets not filtered by previous IP Flows. The same operations apply to the 'Other IP Flows' as to 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 IP Flow is running.




To get this view, press the button in shape of a magnifying glass 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 %] | 0 | 0.00 b/s | 0 p/s |
| | B to A | 0 | 0.00 b/s | 0 p/s | 0 | 0 [0 %] | 0 [0 %] | 0 | 0.00 b/s | 0 p/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 Flow

This column presents the flow number and the direction reference

%

This column presents the percentage for a given direction of a given IP flow of the number of Incoming packets relative to the overall number of matching packets.

Incoming Throughput

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

Incoming Pkts

This column presents the number of packets that applies to the IP Flow for a given direction.

Lost Pkts

This column presents the number of packet lost, and the percentage of those packets regarding the number of Incoming packets of the IP Flow, for the relevant direction.

Delayed Pkts

This column presents the number of packet delay, and the percentage of those packets regarding the number of Incoming packets of the IP Flow, for the relevant direction.

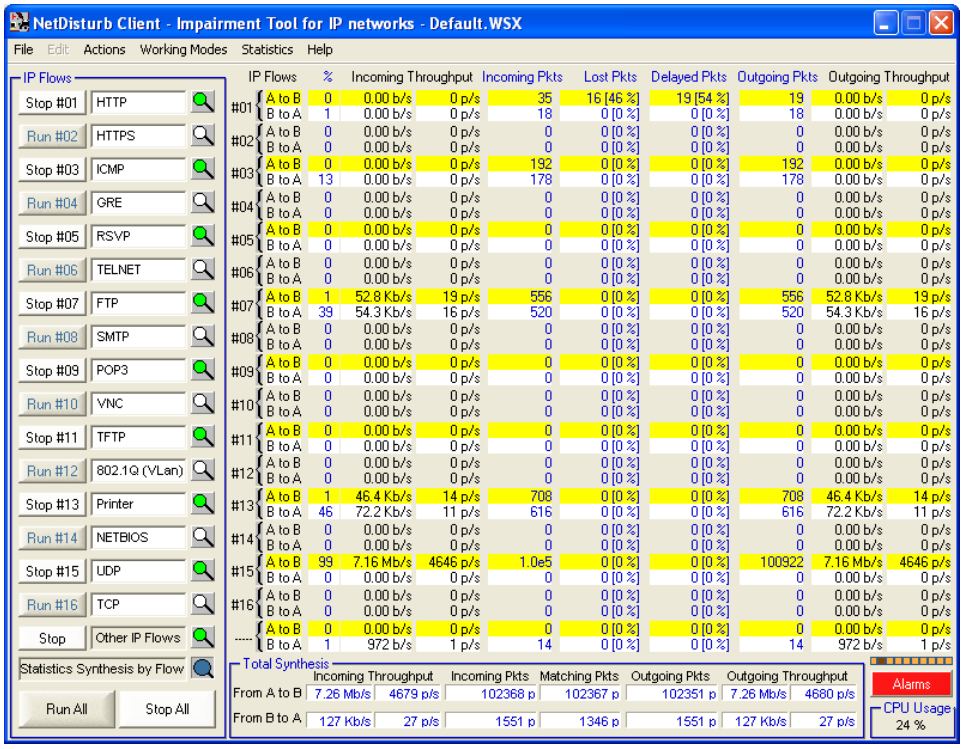
Outgoing Pkts

This column presents the number of packet sent to the opposite interface for the given IP flow and direction. It should be the number of packets filtered minus the number of packets lost, for this IP Flow and direction.

Outgoing Throughput

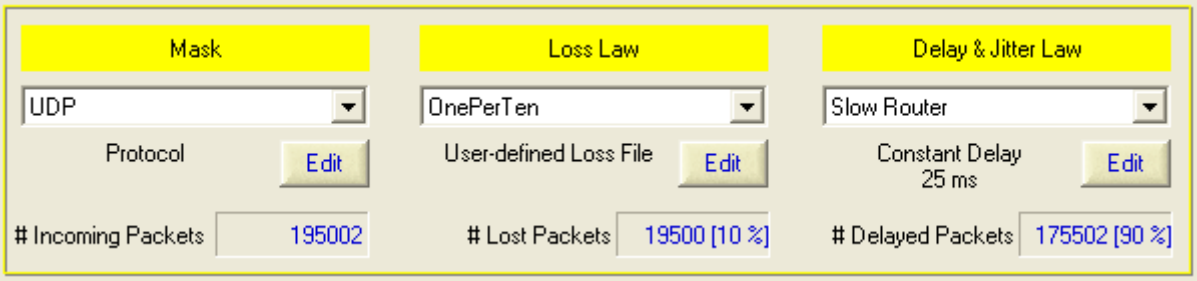
This column presents the instant throughput, computed between two refresh periods of packet sent to the outgoing Interface. Both volume and packet throughputs are shown.

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



## 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.




*Top part of Client main window*

This frame is composed of three parts: 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 Mask is presented. This set of parameters allows selecting packets to process. The number of packets that match the mask is displayed (# Incoming Packets) below the list of defined masks.

### ❖ Loss Law

This part presents the loss law applied on the selected packets. This is the first process applying to the matching 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.

### ❖ Delay & Jitter law

The rights part of the frame presents the delay & jitter 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 & not lost packets are displayed.

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

### 6.4.1 Selection of a 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:

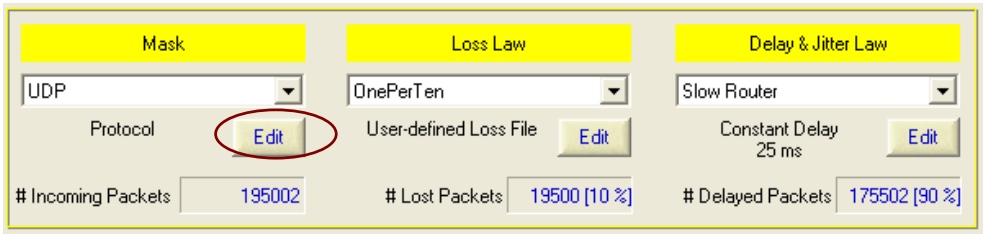
1. MAC Destination Address
2. MAC Source Address
3. VLAN-ID **list** (802.1Q)
4. Type Of Service (TOS)
5. Protocol
6. IP Destination Address
7. IP Source Address
8. Destination Ports **list**
9. Source Ports **list**

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

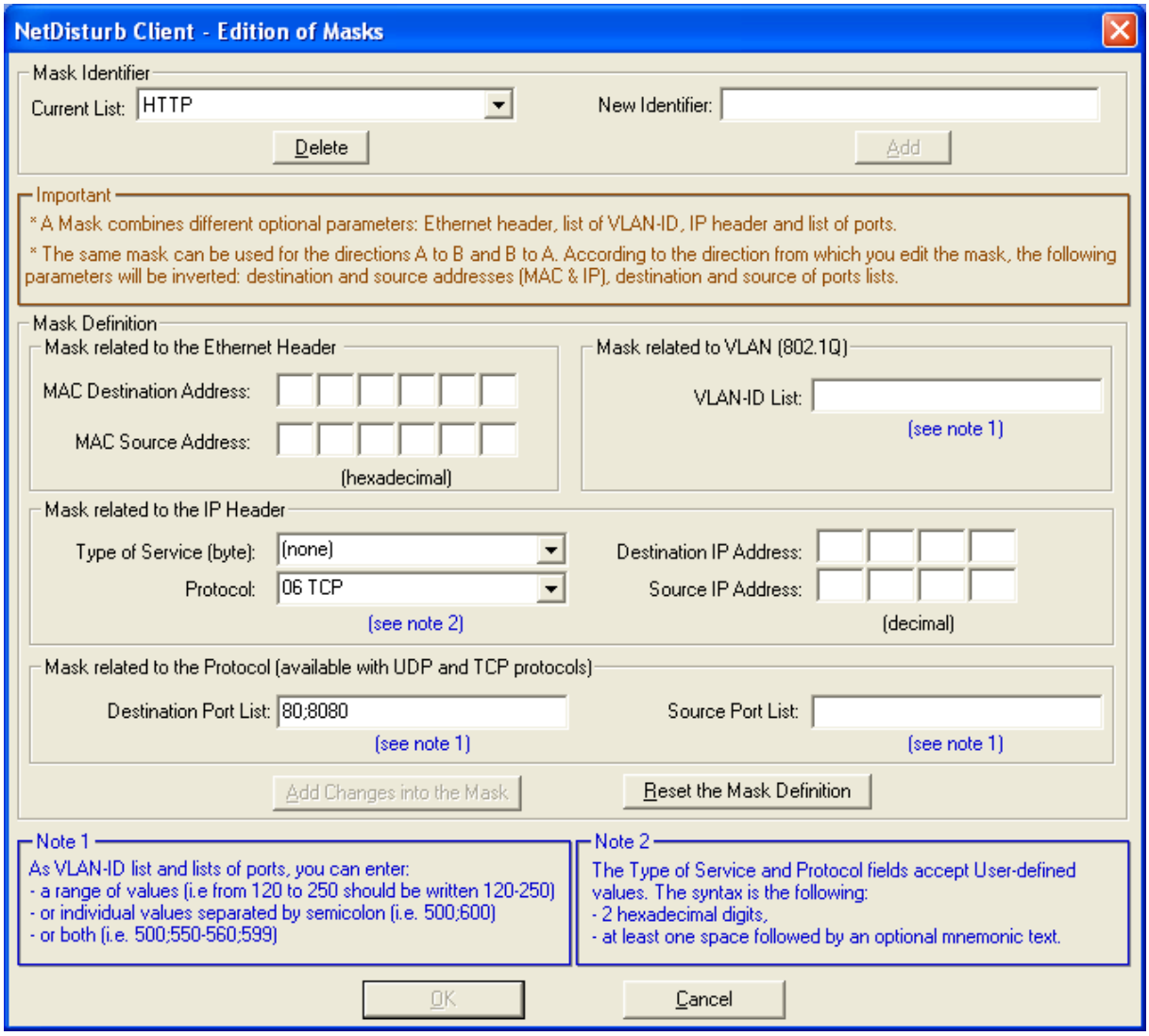
By default, the following masks are included in the file Default.Wsx:

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

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




The following window is pop up:




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 the 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, the user can also add a new mask, by entering a name in the “New Identifier“ area and clicking on the “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.

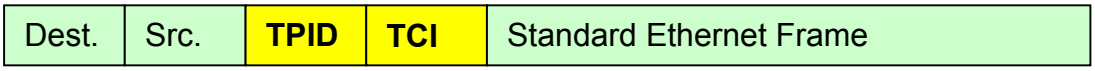
A mask is defined by the combination of four types of parameters:

**Ethernet header**

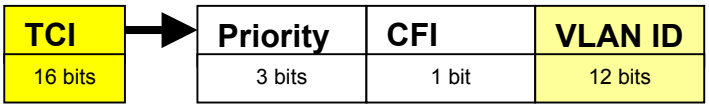
- MAC destination address (enter a hexadecimal value).
- MAC source address (enter a hexadecimal value).

**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.




**TPID** means **T**ag **P**rotocol **Id**entifier. It is equal to 8100.
**TCI** means **T**ag **C**ontrol **I**nformation. It includes the VLAN-ID as shown:




**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. When processing applies on the other direction, NetDisturb reverses automatically the source and destination addresses and ports.

#### 6.4.2.3 Action buttons

To manage the Mask list, various buttons are available:

**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 mask can be a list of values. To match the mask, 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, 120 |
| Values not matching: | 11, 24, 31, 101, 119, 121 |

### 6.4.3 Loss laws configuration

NetDisturb losses the selected IP packets following mathematical laws configured by the user. Up to 100 loss 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 Loss) | (No Loss) | With this option, no loss is applied to the IP Flow. |
| Constant loss | Button "Lose 12 packets" | 12 packets are lost each time the user activates this button. |
| Uniform loss | Uniform Loss<br>From 1 to 100 | Domain values [1 to 100] Threshold = 30 |
| Burst Uniform loss | Burst Uniform Loss<br>Domain: [10. – 1000.] | Domain values [10 to 1000]<br>Threshold (n) = 350 Threshold (n+x) = 380<br>Depth = 2 |
| User File loss | Values from file | Sample file: OnePerTen.txt<br>Loss of 1 packet per 10 packets |

#### 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 table by NetDisturb. When the table is empty, NetDisturb Server provides a new table to the 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.

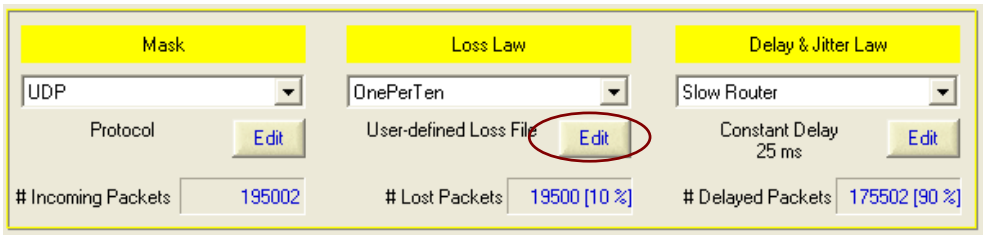
**Working Mode: Laws applying to each TCP/UDP connection of the IP Flows**

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 continues to be handled and may be delayed.

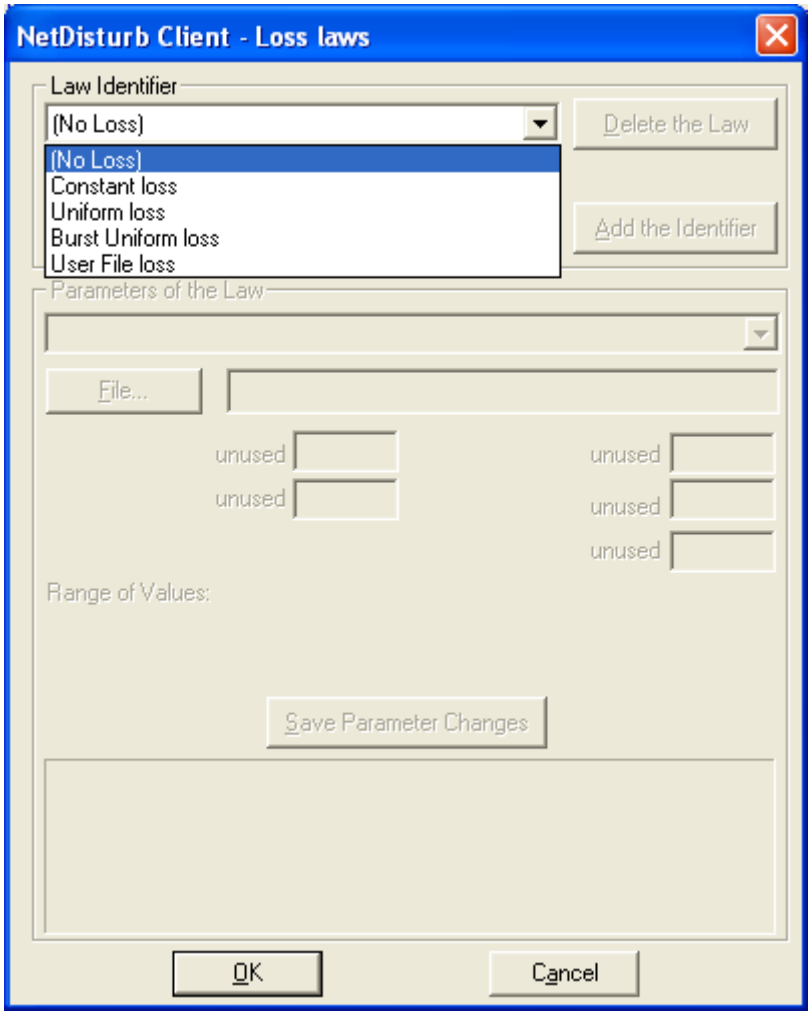
 

### 6.4.3.2 How to create or to edit Loss laws

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




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 |
|---|---|
| **Delete the Law:** | 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/[beta – alpha]; threshold
- Associated uniform law: dx/[beta – alpha] ; threshold ; increment
- Law imported from a file: file name; threshold

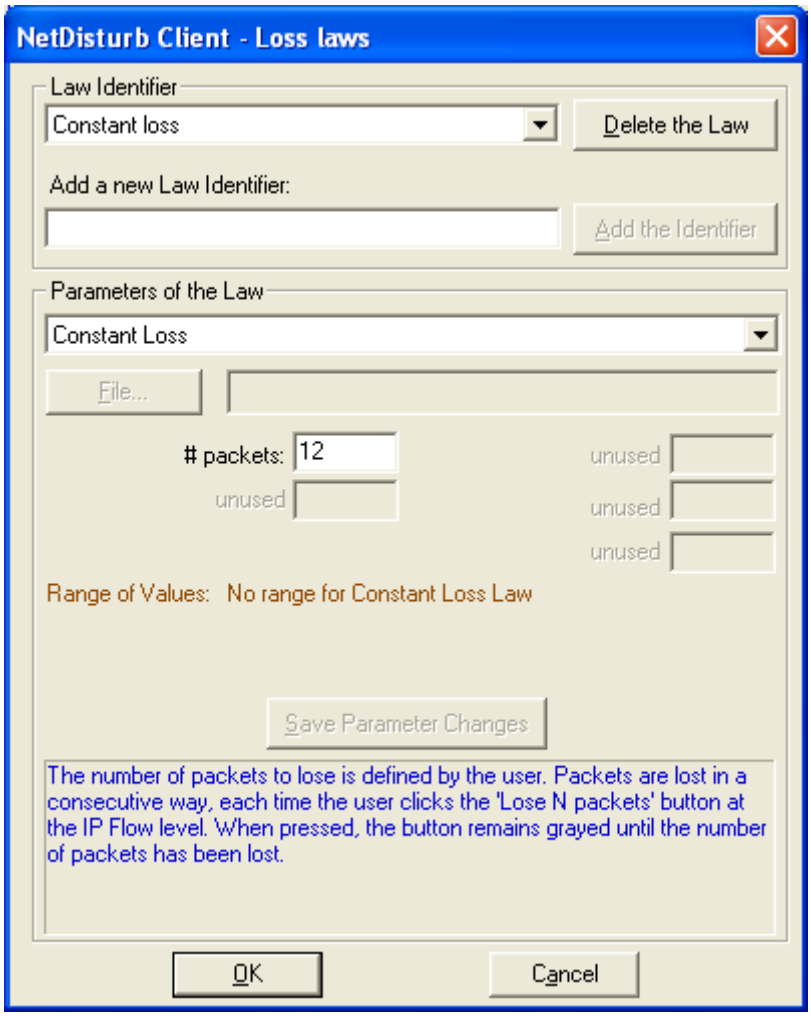
**To create a new loss law:**

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

### 6.4.3.3 Constant Loss law

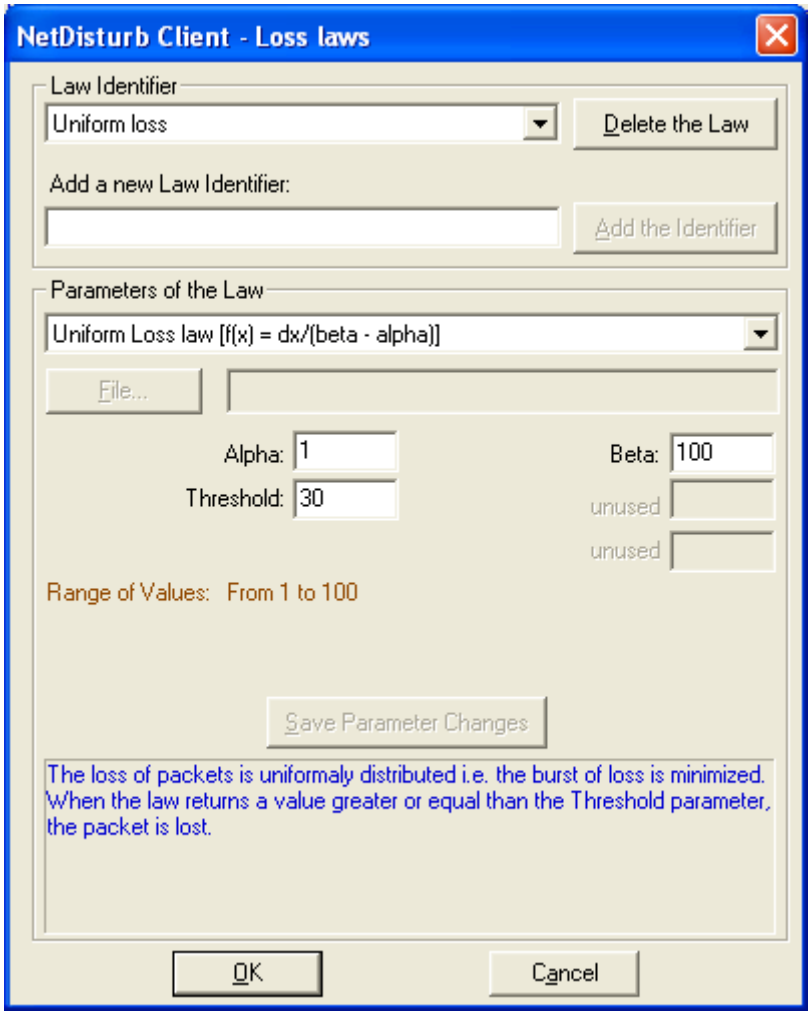
When a fix loss law is selected, NetDisturb will lose the number of packets defined by the user. A button «Lose xx packets» replaces the summary area in the main window. Each time this button is pressed, xx packets are lost.




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 the NetDisturb Driver.




The 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 annex 8 for more information):

Uniform law on $(\alpha, \beta)$ range

$f(x) = 1/(\beta - \alpha)$ if $\alpha < x < \beta$

$f(x) = 0$ else

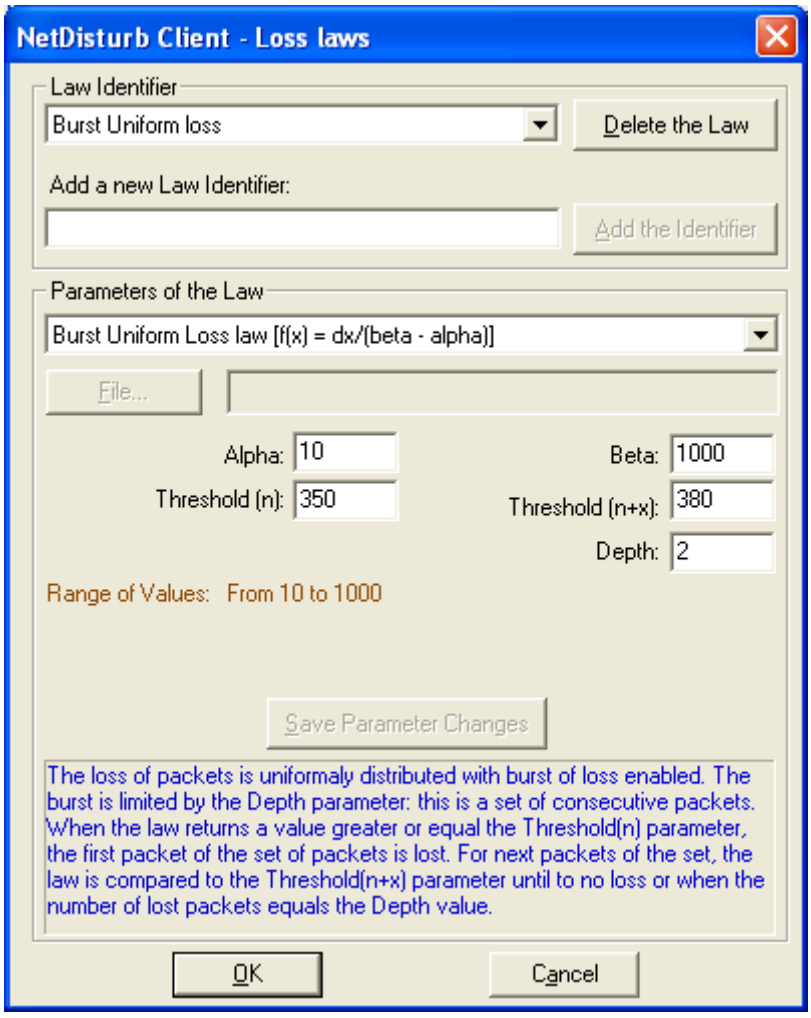
For this law, three parameters must be defined:

**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 the 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.

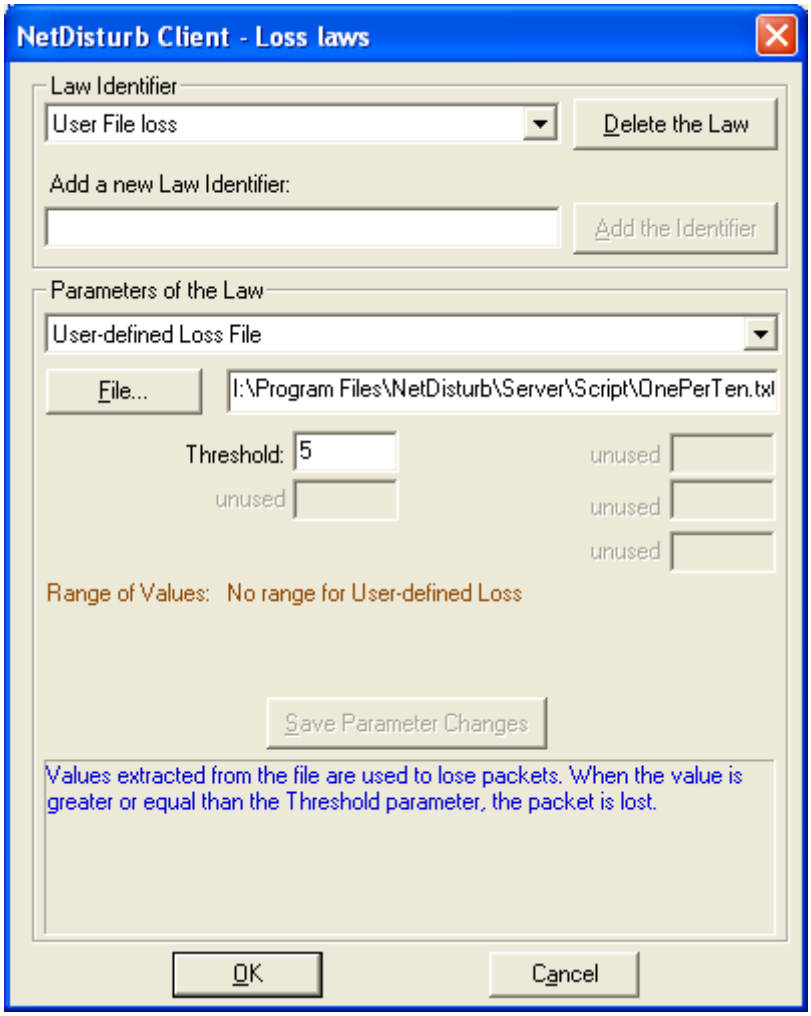
Processing is applied as follows:

⇨ NetDisturb Driver picks a number from the table for each packet (see also 6.4.3.1)
⇨ For the packet n, the 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 the 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.

The 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.

The file sample (OnePerTen.txt) illustrates a loss of 1 packet for 10 packets sent when the Threshold value $T$ is $0 < T < 100$.
(The content of the file OnePerTen.txt is: `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.

### 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 table by NetDisturb. When the table is empty, NetDisturb Server provides a new table to the 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. NetDisturb Server provides the table once 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 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

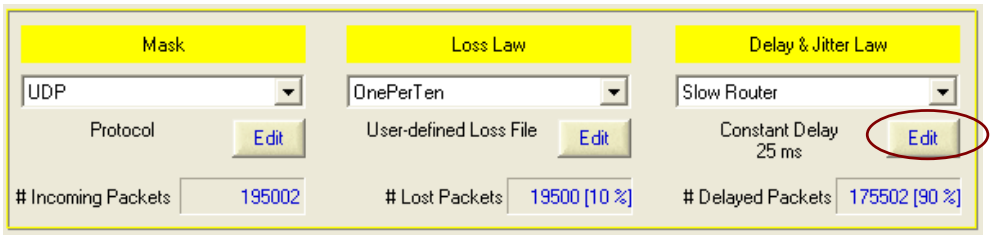
The NetDisturb Driver accuracy is ±5 milliseconds, which mean that a delay variation of one millisecond between two packets can't be taken into account. With such Delay & Jitter the result is either no Delay &Jitter or a Delay & Jitter of 5ms at least.

Note: NetDisturb uses the OS timer accuracy to delay packet. On most systems, the timer accuracy is 10 milliseconds. When the system timer wakes up NetDisturb, the software looks for packets to send in the range of ±5 ms of the current time. So, packets can be sent before of after the expected time, in the range of 5 ms.

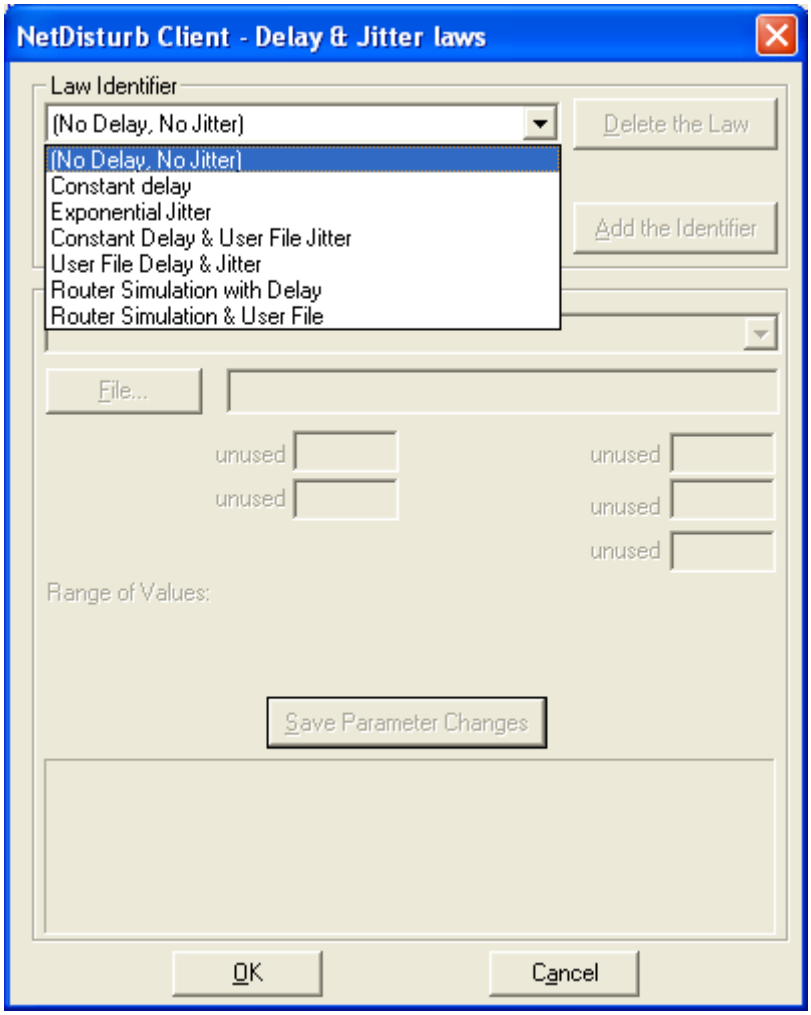
 

### 6.4.4.3 Delay & Jitter laws selection

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




Then, the following window is pop up:




*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<br>20 ms | A 20 ms delay is applied to IP packets |
| Exponential jitter | Delay & Exponential Jitter<br>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. |
| 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<br>IP Throughput = 1000 Kb/s<br>Max memory = 500 Ko |
| Router Simulation & User File | Router Simulation & User File with Delay and Jitter | IP Throughput = 1000 Kb/s<br>Max memory = 250 Ko<br>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 and existing law. An existing law can be deleted by pushing the “Delete” button.
From this part, the user can also create a new law, by entering a name in the “New Identifier“ area and clicking on “Add” button”.

### ❖ Action buttons:

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

| Button | Action |
|---|---|
| **Delete the Law:** | 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 one mathematical law - three loss laws are available:
- Fix delay law,
- Exponential,
- User own value law.

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 "Value range" button allows seeing the range of values generated by the law for the user-defined parameters.

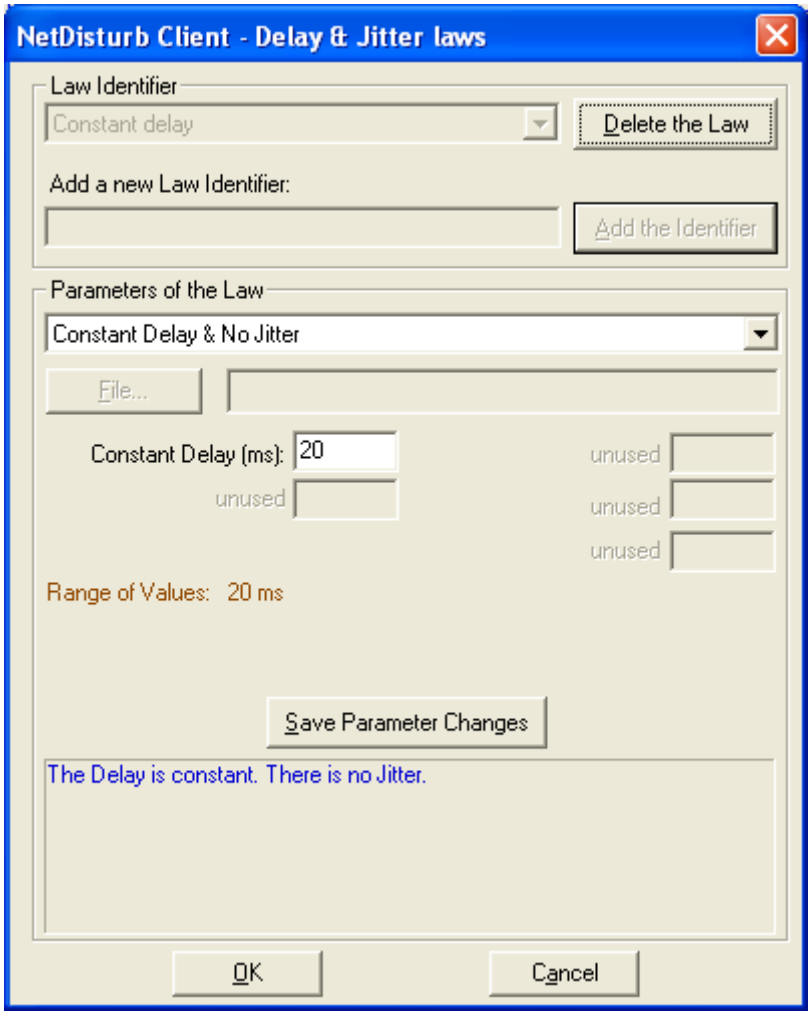
A list box allows selecting one mathematical law - five delay laws are available:
- Constant delay law,
- Exponential delay law: lambda * exp(- lambda * x) * dx; constant delay,
- Law imported from a file: file name; constant delay,
- Throughput,
- File containing the delay applied in a contextual manner.

**To create a new delay law:**

1. Enter a name in the "New law identifier" edit field,
2. Click on "Add",
3. Select a law in the combo-box,
4. Enter law parameters if needed,
5. Press the "Value range" button to see the range of values generated by this new law,
6. Press the "Save "button.
7. Press "Close" to quit the "Delay laws" window.

### 6.4.4.4 Constant delay law

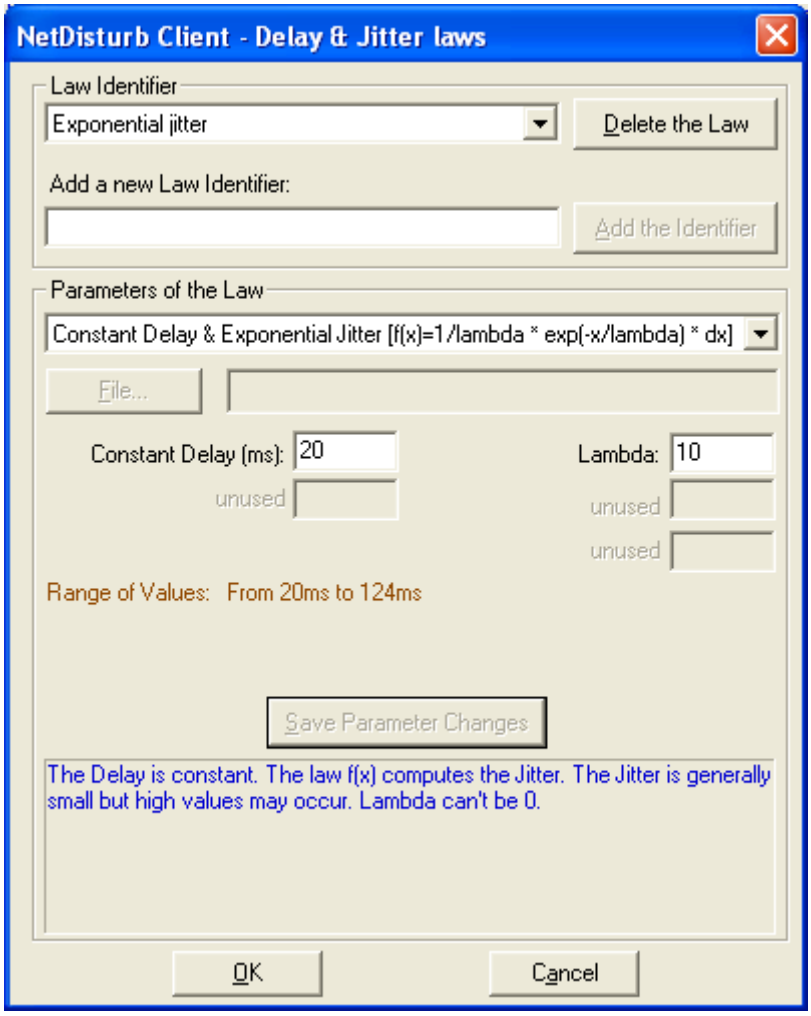
A constant delay is supplied by the user and applied to all selected and no lost packets.




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

### 6.4.4.5 Constant Delay with Exponential jitter law

When this law is selected, an exponential distribution of delay is computed from the Lambda parameter supplied by the 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 delay.




9

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

Exponential law $(\lambda > 0)$

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

$f(x) = 0$ if $x < 0$

For this law, two parameters must be defined:

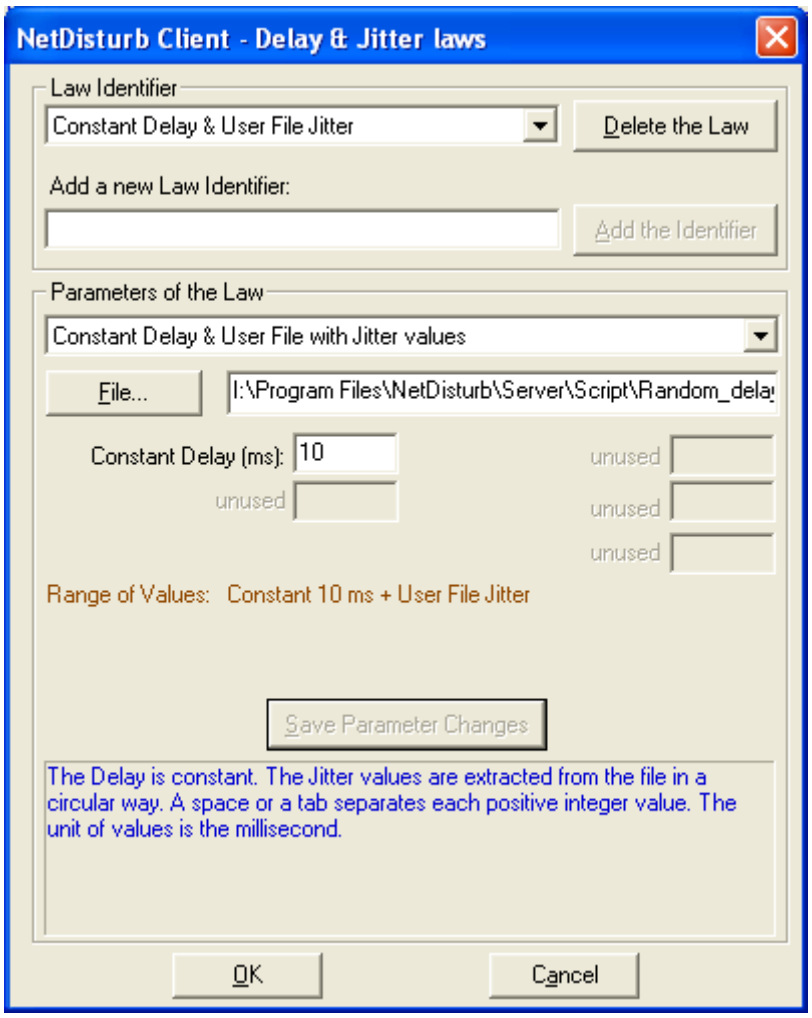
**Constant Delay (ms):** fixed value added
**Lambda:** parameter of the law

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

### 6.4.4.6 Constant Delay & User File with Jitter values

When this law is selected, the delay rate is obtained from a file supplied by the 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.

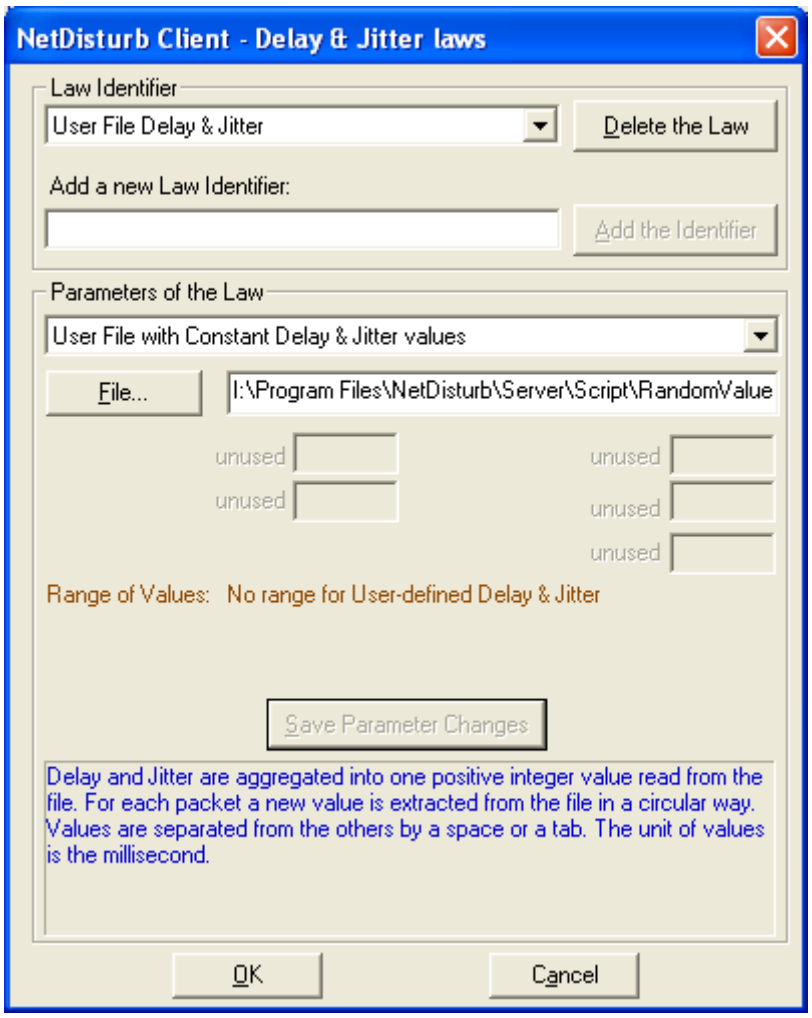



For performance reason, the file is read in one shot, and stored in memory when the law IP Flow is set in the Run state. Values are used to load the table transmitted to the NetDisturb Driver. In order to not overload the memory resources, maximum read number of delays is limited to 40 960.
If the file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

### 6.4.4.7 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.




The first packet initializes the T0 time. Then the value T is calculated: T = T0 + D1 (with D1 = 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 T1 time.

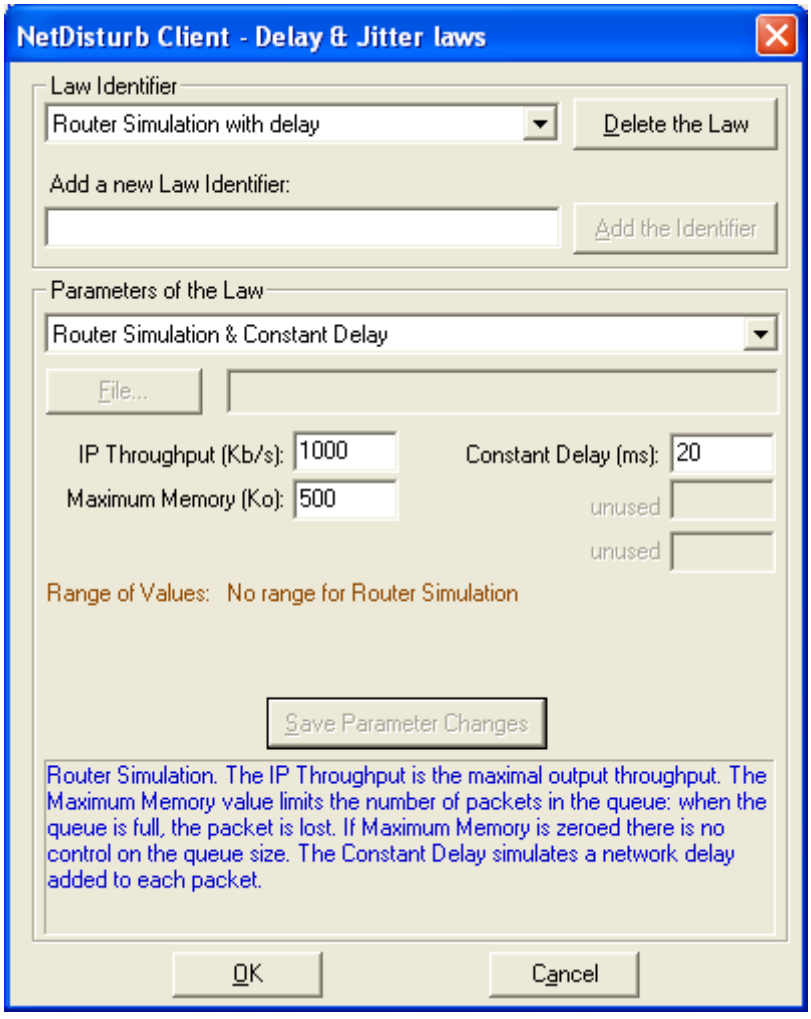
If T1 < T then this second packet is queued with a delay defined as: T0 + D1 – T1
If T1 > or = T then this second packet is sent immediately on the outgoing interface.

Then the new value T is calculated for the third packet: T = T0 + D1 + D2 (with D2 = 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.

### 6.4.4.8 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 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.

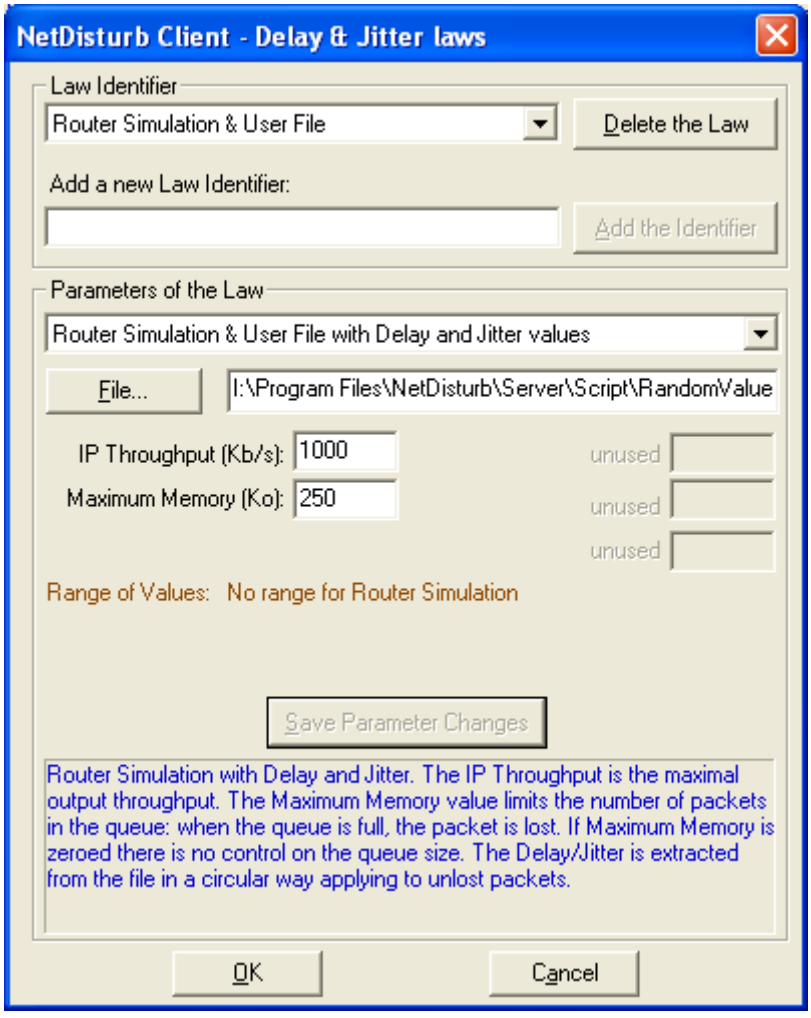
The example displayed below illustrates the 3 parameters used by the “Router Simulation & Constant Delay” law: IP Throughput, Constant Delay and Maximum memory.



#### 6.4.4.9 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

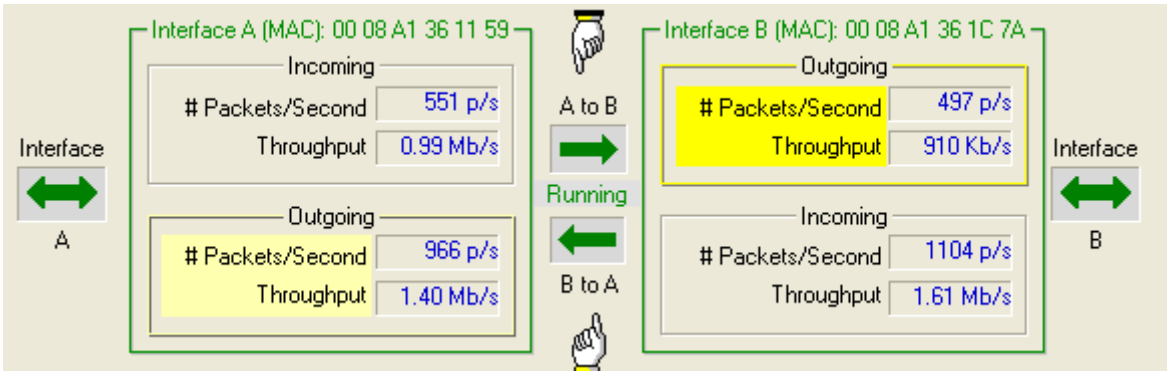
The example displayed below illustrates the 3 parameters used by the "Router Simulation & Constant Delay" law: IP Throughput, Maximum memory and the user file name containing Constant Delay & Jitter values.




## 6.5 Client application 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 is composed

of one receiving area (incoming) and one sending area (outgoing). The GUI displays the following statistics:



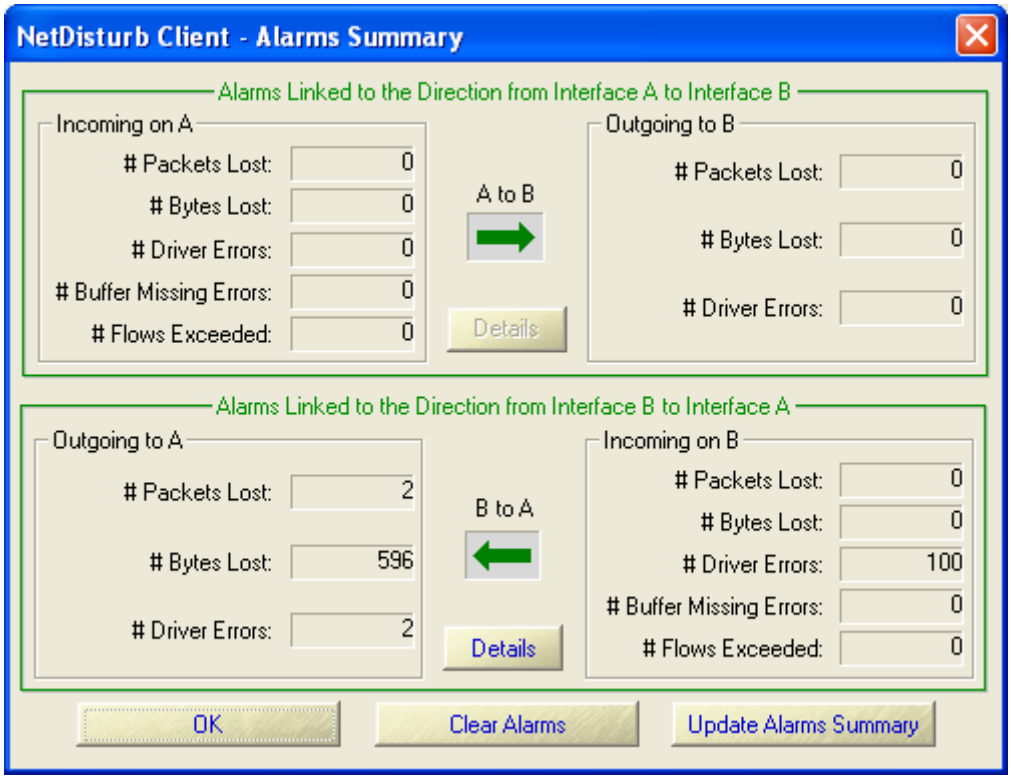

- # Packets/Second: This field presents the instant throughput in packets by second on the IP Flow.
- Throughput: This field displays the instant throughput in bits/Kbits/Mbits per second, according to the sampling period defined in the application configuration.

## 6.6 Errors detected with the 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.

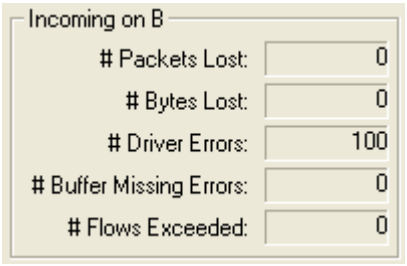

Click on the 

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



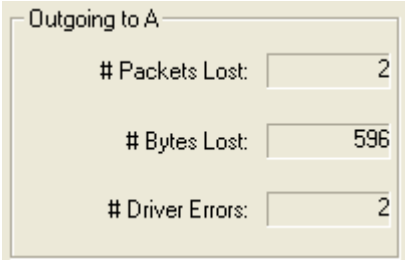

Alarms are classified per direction: **A to B** and **B to A**.

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




<u>On incoming direction</u>:

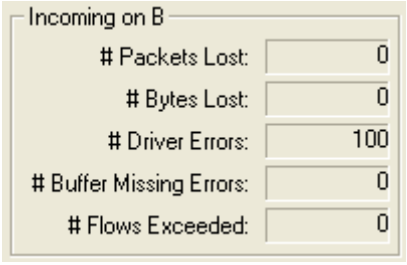
- Number of packets lost
- Number of bytes lost
- Number of errors returned by the Driver of the Interface
- Number of buffers that were missing to keep packets
- Number of ignored flows (when the multi-flows option is in use).




<u>On outgoing direction</u>:

- 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




- **#Packet Lost**
  Number of packets lost due to memory allocation errors or interface access errors.

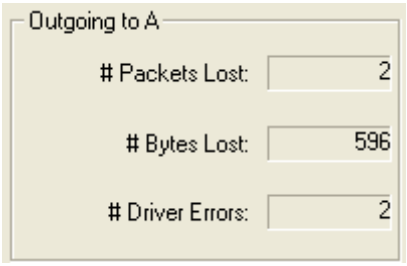
- **#Bytes Lost**
  Number of bytes lost (total packet size including MAC header) due to memory allocation errors or interface access errors.

- **#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 the NetDisturb driver failed, this counter is increased. You can increase the number of buffers allocated by the 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 flows).

### 6.6.2 Details for outgoing errors




- **#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.

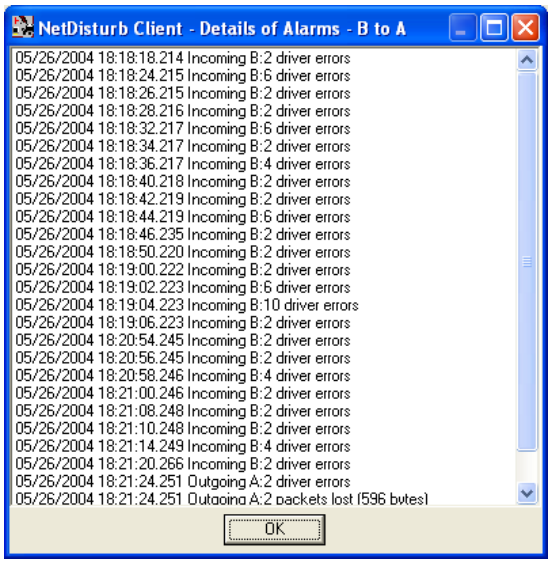
- **#Driver Errors**
  This error counter is the number of alarms returned by the NIC Driver indicating that some errors have occurred from the started time of the NIC. Errors can be due to one of the following reasons:
  - CRC error
  - NIC or Driver Buffer overrun error

### 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 interrogate the 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 

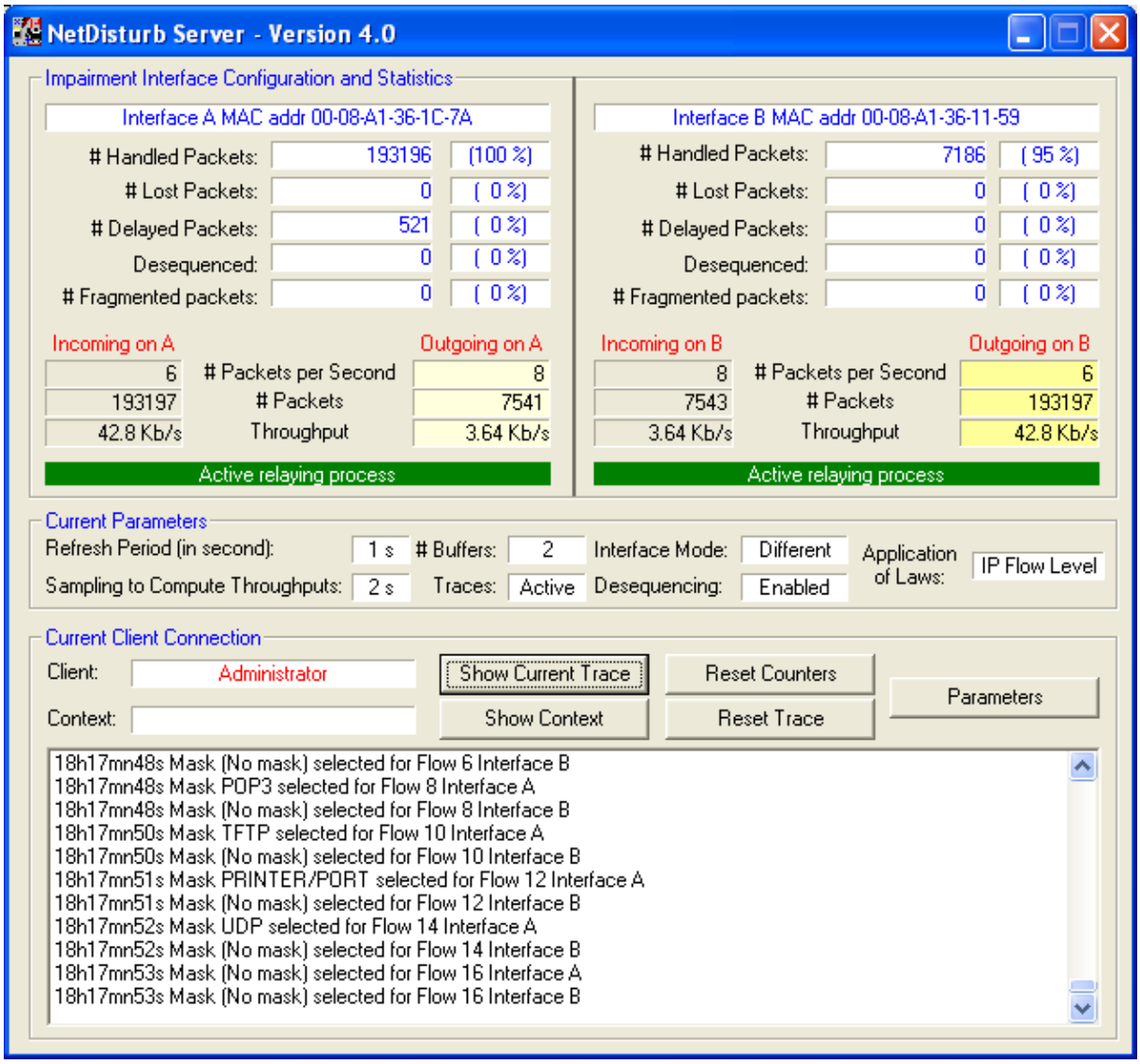
until new errors occur.

# Part 7 Using NetDisturb Server application

NetDisturb Server application is aimed to link the NetDisturb driver and the NetDisturb Client application and:

- ⇨ 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 the password for Administrator connections.

NetDisturb Server application window is composed of three sections:



### ❖ Perturbation or impairment Configuration

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 transmitted without mask comparison because NetDisturb don't handle IP packets 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)** | No packet handled by the NetDisturb driver (physical cut off of the Ethernet link). |
| **Active relaying process (green color)** | The driver is running, relayed packets are processed following the selected masks, and they are lost and delayed following the selected laws. |

### ❖ Current parameters


This section reminds the current configuration; it includes:

1. The refresh period to display statistics of the NetDisturb Server.
2. The sampling period used to calculate the throughput displayed by NetDisturb Server.
3. The number of buffers when the application of laws is TCP/UDP connection.
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 application of laws: it can be IP Flow level or TCP/UDP connections.

### ❖ Client connection

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

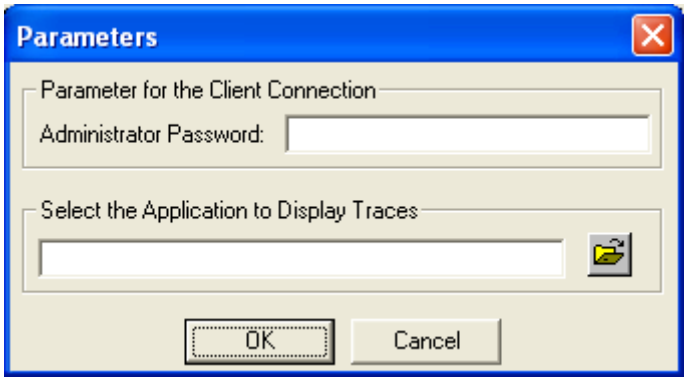
- **"Show Current Traces"** allows opening the trace file in order to examine the commands entered by the Client. The visualization application name must be configured in the parameters of the Server application.

- **"Reset Counters"** allows resetting the Server application User Interfaces counters. This action has no incident on Client application. 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 the Server application. The available parameters are the administrator password and the viewer for the traces.




- This section also displays the name of the last opened context.

# Part 8 Annexes

## 8.1 Default context values

| | |
|---|---|
| • Refreshing time for statistics display | 1 s |
| • Sampling period for throughput computing | 2 s |
| • Relaying process | No relay |
| • Mode | Internet |
| • Traces | Active |
| • Buffer number | 2 |
| • Compression | Disabled |
| • Flow mode | IP Flow Mode |
| • For the 16 definable masks | |
| Mask | No mask |
| Loss law | *No loss* |
| Delay & Jitter law | *No delay & no Jitter* |
| • Other IP Flows | |
| Loss law | *No loss* |
| Delay & Jitter law | *No delay & no Jitter* |

## 8.2 NetDisturb Registry values

***Warning:***

*This part contents description of parameters for the NetDisturb applications and 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 before any change.*

You need administrator rights access to change the registry database. The system 'regedit.exe' application 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 Client part

This part is the client part of the registry. Some parameters refer to dialog with the NetDisturb Server and you should be changed accordingly with the server.

#### 8.2.1.1 Configuration parameters

Key : `HKEY_LOCAL_MACHINE\SOFTWARE\ZTI\NetDisturbClient`

| Name | Type | Value |
|---|---|---|
| AcroReadInfo | REG_SZ | 20040602 |
| AcroReadTimer | REG_DWORD | 0x0000001F (31) |
| HELP_MENU | REG_DWORD | 0x00000006 |
| IPAddress | REG_SZ | Server IP Address<br>(default:127.0.0.1) |
| ServerPath | REG_SZ | Full server path to the script sub directory<br>(There is no default value but a typical value is:<br>C:\Program Files\NetDisturb\Server\Script\) |
| TCPPort | REG_SZ | RPC port number used to dialog with the Server part<br>(default: 2020) |
| TraceLevel | REG_DWORD | Trace level generated by the Client (see note)<br>(default: 0) |
| TraceFileName | REG_SZ | File name where traces are saved in, when the TraceLevel flag is set (*see note*).<br>(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 (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 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 Server part

Key : `HKEY_LOCAL_MACHINE\SOFTWARE\ZTI\NetDisturbServer`

| Name | Type | Value |
|---|---|---|
| ApplicationName | REG_SZ | Trace viewer |
| IHMRefresh | REG_DWORD | Period of refresh, in second.<br>(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<br>(default: empty) |
| Sampling | REG_DWORD | Sampling period to compute throughput<br>(default: 2) |
| TCPPort | REG_SZ | RPC port number used to dialog with the Client part<br>(default: 2020) |
| TraceLevel | REG_DWORD | Trace level generated by the Server (see note)<br>(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 to the standard application debug mechanism (dbmon).
- 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 Server trace window
  - Example:
    If TraceLevel = 1001 means Error level of traces shown into the window trace.

### 8.2.3 Registry Driver part

This part is for information ONLY
but it could be changed with the help of the ZTI Support Team.

Key: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\NetDisturb`

Key (Windows NT only):
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\Disturb`

| Name | Type | Value |
|---|---|---|
| DisplayName | REG_SZ | Name of the NetDisturb Driver<br>(Default: NetDisturb Impairment) |
| ErrorControl | REG_DWORD | Widows System parameter (Set to 1) |
| ImagePath | REG_SZ | Disturb.sys location<br>Default:system32\Drivers\disturb.sys |
| Start | REG_DWORD | Widows System parameter (Set to 3) |
| Type | REG_DWORD | Widows System parameter (Set to 1) |

***WARNING:***

*The sub-key 'parameters' contains the level of trace provided by NetDisturb. A non-null trace level decreases the system performance: it should be set only in conjunction with the help of the ZTI Support Team.*

| Name | Type | Value |
|---|---|---|
| TraceLevel | REG_DWORD | Level of trace from the NetDisturb Driver<br>(default: 0 = no trace). |

**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 Driver debug mechanism (e.g. windbg).
- Flag values are shown in **hexadecimal**:
  - `0001` Error level (system errors)
  - `0002` Error level (internal errors)
  - `0004` Important level
  - `0008` Information level
  - `0010` Data level: dump some part of the frame received (decrease the total system performance)
  - `0100` Verbose level (1)
  - `0200` Verbose level (2)
  - `0400` Add timestamp to trace (not recommended)
  - `0800` Show the input parameter (internal use only)
  - `1000` Dump the internal time to send packet (internal use only)
  - `2000` Show the input parameter (internal use only)
  - Example:
    If TraceLevel = 13 means System and Internal Error level of traces with dump of frame headers send to the Driver debug mechanism.

## 8.3 Mathematical laws

### 8.3.1 Uniform Law

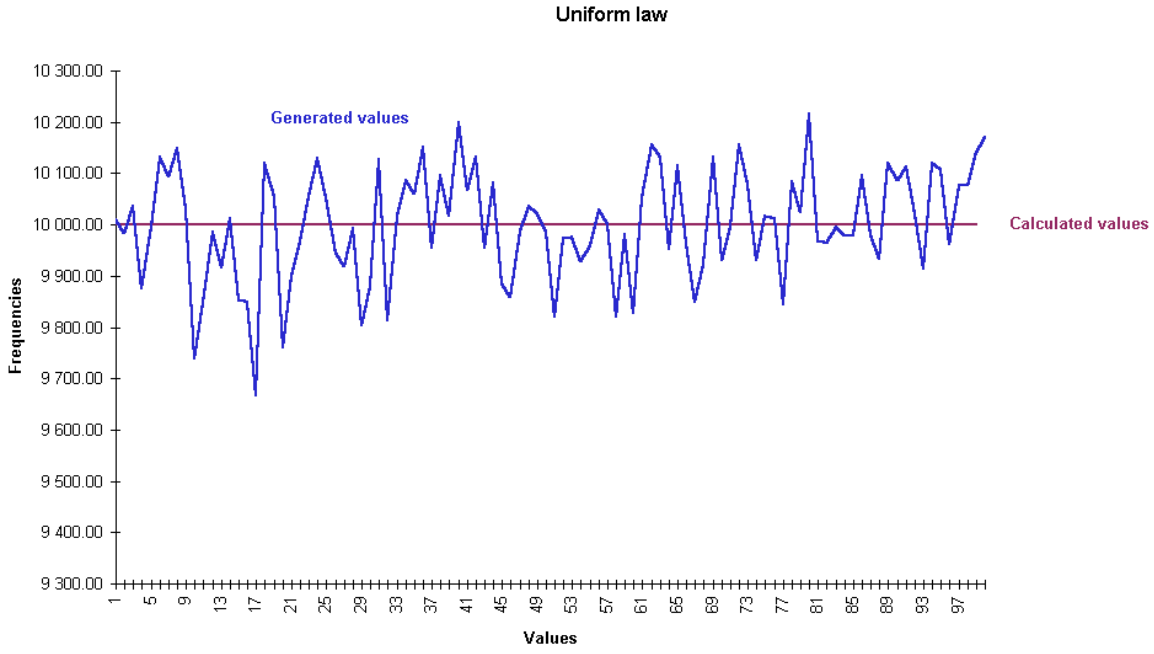
❖ *Presentation:*
Uniform law has two parameters: α and β. It generates a random number included uniformly between α and β. If α is equal to β, the generated number is always α = β.

❖ *Mathematical function:*
Uniform law on $(\alpha, \beta)$ range

$f(x) = 1/(\beta - \alpha)$ if $\alpha < x < \beta$
$f(x) = 0$ 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 intents 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 the NetDisturb Driver (see the “Loss laws configuration” paragraph for more details).

### 8.3.3 Exponential Law

❖ *Presentation*

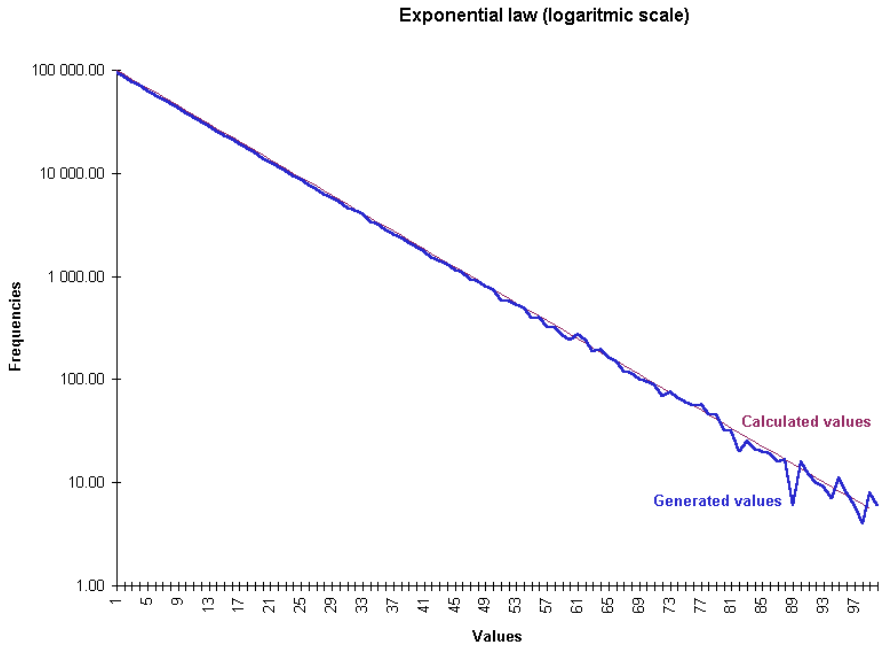
Exponential Law has only one parameter: λ.
The more λ is small, the more the power of 10 of the generated number is high.

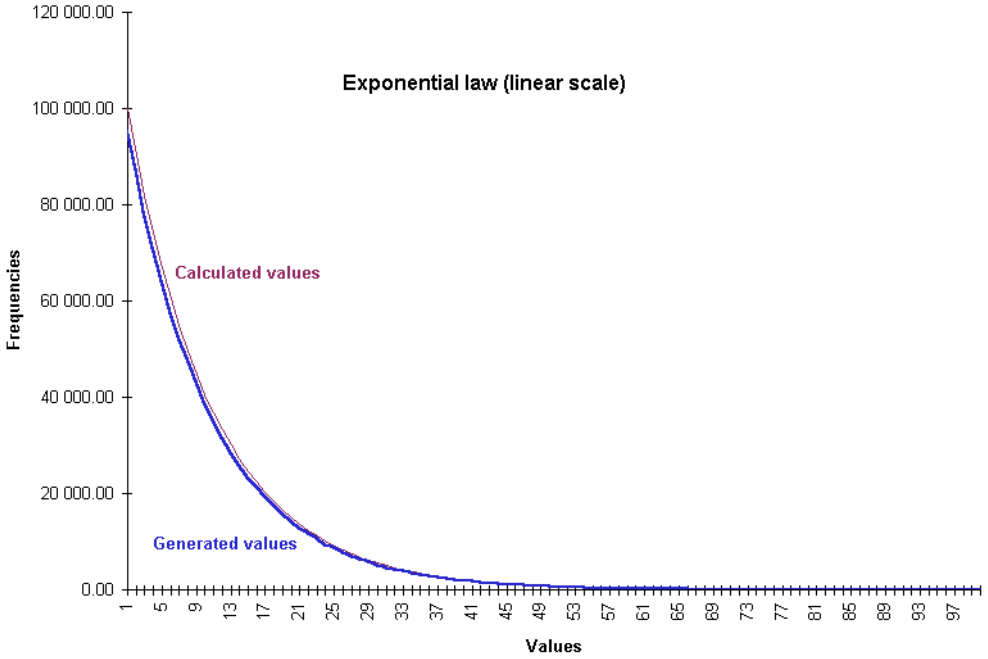
❖ *Mathematical function:*
Exponential law $(\lambda > 0)$

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

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

The factor 1000000 is because the figure intents 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:*

| Values | Delay law results |
|---|---|
| λ = 1 | 10 ms |
| λ = 0,1 | 100 ms |
| λ = 0,01 | 1 s |
| λ = 0,001 | 10 s |
| λ = 0,0001 | 1 mn 43 |
| λ = 0,00001 | 17 mn 19 |
| λ = 0,000001 | 2 h 53 |
| -- Precision limit of λ -- | |