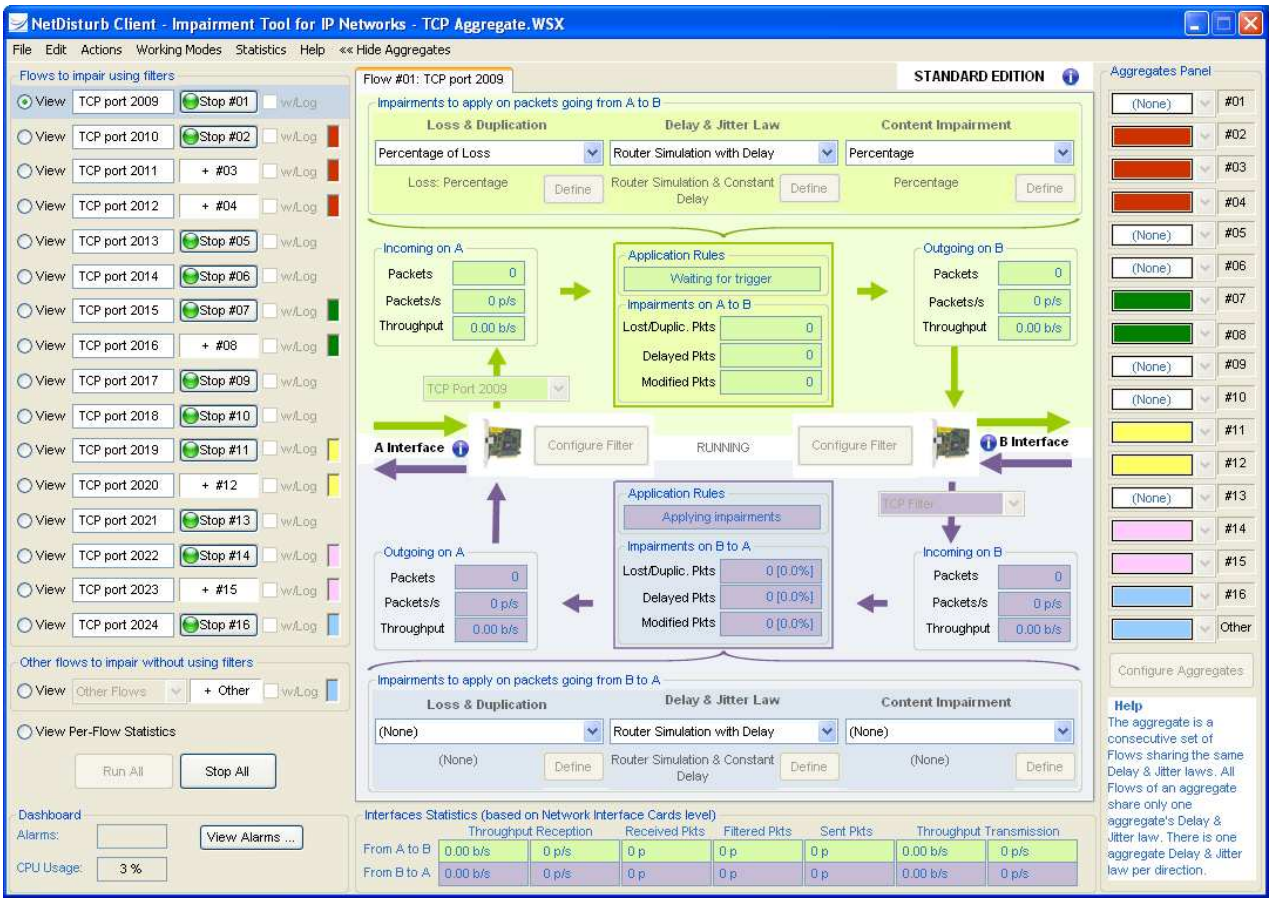
NetDisturb Standard

NetDisturb Enhanced

Version 4.7

Impairment Emulator Software for IP Networks (IPv4 & IPv6)



User Guide

ZTI / 1 boulevard d'Armor / BP 20254 / 22302 Lannion Cedex / France

Phone: +33 2 9648 4343 / Fax: +33 2 9648 1485 / Email: contact@zti-telecom.com / www.zti-telecom.com

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.

The elaboration of this guide has been made to be as accurate as possible. We hope that you will find all the information required to use our software in a convenient way. Failing to do so, do not hesitate to contact us at support@zti-telecom.com.

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

To contact us:

ZTI
1 boulevard d'Armor
BP 20254
22302 Lannion Cedex
France

Phone: +33 2 9648 4343
Fax: +33 2 9648 1485
Web: http://www.zti-telecom.com/or http://www.zti.fr/
Email: contact@zti-telecom.com (marketing & sales)
support@zti-telecom.com (technical support)

Copyrights

Software License Agreement

This is an agreement between you (legal entity or physical person) and ZTI.

COPYRIGHT

The enclosed Software and documentation (here after called the Products) remains the property of ZTI.
French copyright laws and international treaties protect this product.
ZTI grants you the right to use the products according to the following:

USE OF THE SOFTWARE

You may:

- Install the software on the hard disk of your system in accordance with the software protection described in the next paragraph.
- Make one backup copy of the software provided that this copy is not used or installed on any computer.
- Use the Products correctly.

In accordance with copyright and patent laws, the Licensee undertakes:

- To use the Products only for its own use
- Not to modify the Products
- Not to make illegal copy of the Products
- Not to give, rent, sublicense or sale the Products
- To protect and respect ZTI and its Products reputation.

SOFTWARE PROTECTION

NetDisturb software is licensed on a workstation basis. You will need to purchase a separate license for each machine that you install it on. Each licensed copy of the software installed on a workstation has:
o a unique Site Code that requires the corresponding unique Site Key to be entered
o or a unique USB Software Protection key, to be plugged before
to run the software.

LIMITED WARRANTY

The Software is supplied without any express or implied warranty regarding the performances or results obtained by the use of the Products.
ZTI warrants that the software media (i.e. CD-ROM) will be free of material defects for a ninety (90) days period following your purchase. The limited warranty applies to the media and not to the information contained on it. If the media does not comply with this limited warranty, the only remedy is the replacement of the media software
In no event, ZTI will be liable for any kind of direct or indirect damages caused by the Products.

COURT OF LAW

French laws will govern this agreement.
The court of Saint-Brieuc (France) shall finally settle all disputes arising out of or in connection with this Agreement.

For further information, please contact: ZTI customer support department.

ZTI
1 boulevard d'Armor
BP 20254
22302 Lannion Cedex
France

Phone: +33 2 9648 4343
Fax: +33 2 9648 1485
Email: support@zti-telecom.com or support@zti.fr
Web: http://www.zti-telecom.com or http://www.zti.fr

Table of contents

Part 0 Preface

0.1 Organization of this manual

This user guide is aimed at helping you to discover and use **NetDisturb**. This manual is organized as follows:

- **Part 1**: Product Overview

Briefly describes the key features of the **NetDisturb** software.

- **Part 2**: What's new in **NetDisturb** version 4.7

Is a general overview of new features, main improvements provided with **NetDisturb** version 4.7.

- **Part 3**: Install **NetDisturb**

Presents the product requirements, how to install the software downloaded from the Internet or from the CD-ROM, provides important information to upgrade from previous versions and explains how to choose the most suitable **NetDisturb** package.

- **Part 4**: How to handle your license?

Describes how to proceed for the license transfer

- **Part 5**: Uninstall **NetDisturb**

Describes how to uninstall the software.

- **Part 6**: Run **NetDisturb**

Describes how to run the **NetDisturb** Server and **NetDisturb** Client.

- **Part 7**: Using the **NetDisturb** Client

Describes how to use the **NetDisturb** Client.

- **Part 8**: Using the **NetDisturb** Command Line Interface

Describes how to use the **NetDisturb** Command Line Interface (CLI), including the commands and their parameters.

- **Part 9**: Using the **NetDisturb** Server

Describes how to use the **NetDisturb** Server.

- **Part 10**: Annexes

Describes additional information about the mathematical laws used by **NetDisturb**, the default context value and the parameters saved in the Registry database.

In this document, you will find the following symbols: They mean:

	***Warning***		Zoom or Advice		*Note or Remark*

0.2 Minimum System Requirements

To appropriately operate **NetDisturb** you need the following minimum system requirements:

- Windows 2000, XP or Server 2003
- Pentium processor with 512 MB memory at least
- Two identical Ethernet NICs are recommended: Ethernet, Fast Ethernet, or Gigabit Ethernet network interface card.
- 1024 x 768 display, DPI setting = Normal size (96 DPI) and Font size = Normal
- 20 MB free hard disk space

*Acrobat Reader is needed to display the **NetDisturb** Help. If Acrobat reader hasn't been installed, a warning message is displayed to inform that the help file can't be opened.*

0.3 Technical Support

ZTI Technical Support can assist you with all your technical problems from installation to troubleshooting.
Before contacting our Technical Support, please read the relevant sections of the product documentation and the "Read Me First" file.

Before contacting our technical support, make sure you record the following information:

- Product name and version.
- Trial License or unlimited licensed product.
- System configuration.
- Problem details: settings, error messages...
- If the problem is persistent, give the details of how to create the problem.

You can contact Technical Support by:

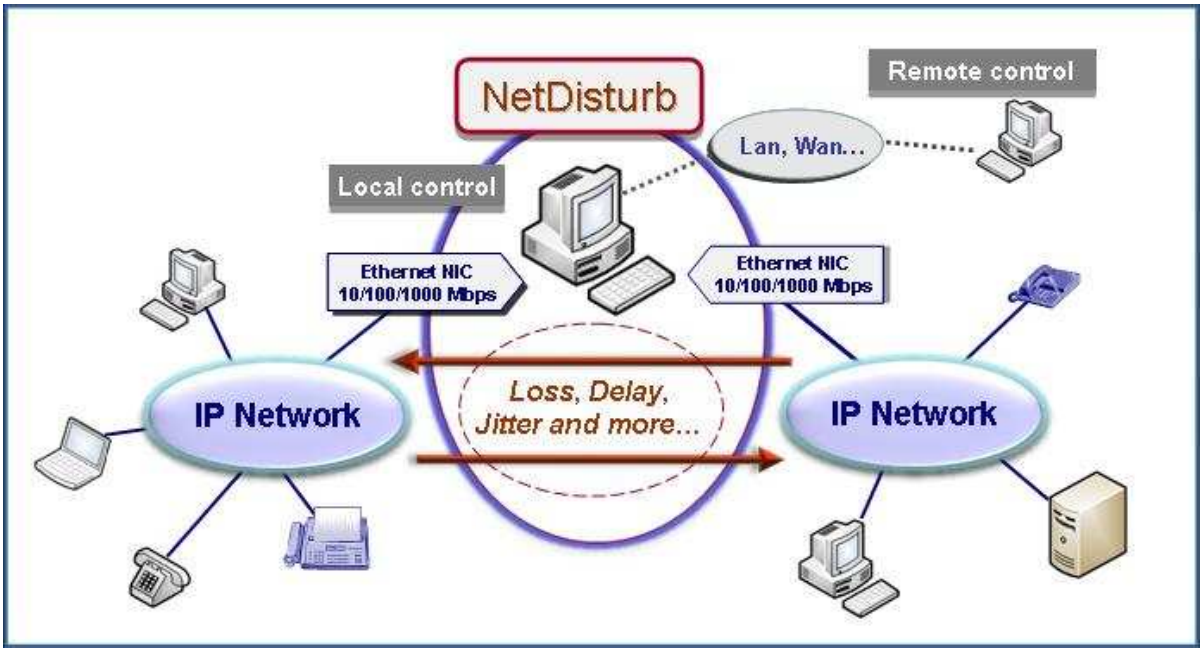
Email	Send as many details as possible to support@zti-telecom.com or support@zti.fr
Fax	Send as many details as possible to +33 2 9648 1485
Telephone	Telephone support is available from 09:00 am to 07:00 pm (GMT Time +01:00 or +02:00), Monday to Friday. Call on +33 2 9648 4343

Part 1 NetDisturb Overview

NetDisturb is an IP network emulator software that can generate impairments over IP networks (IPv4 and IPv6) such as: latency, delay, jitter, bandwidth limitation, loss, duplication and modification of the packets.

NetDisturb allows disturbing flows over an IP network helping to study the behavior of applications, devices or services in a disturbed network environment.

NetDisturb is inserted between two Ethernet segments acting as a bridge and operates bi-directional packet transfer on Ethernet, Fast Ethernet and Gigabit network interface cards.



1.1 Product Requirements

* Platform: Pentium PC running 32 bits version of Windows 2000, XP or Server 2003 with Microsoft TCP/IP installed and at least 512 MB Ram. 20 MB free hard disk space.
* Hyper-threading, multi core and PC multiprocessors are also supported.
* Two Identical Network Interfaces Cards (NIC) are recommended: Ethernet, Fast Ethernet, or Gigabit Ethernet.
* Display resolution: at least 1024 x 768 (more readable: 1152 x 768 and sup.), DPI setting = Normal size (96 DPI) and Font size = Normal.

1.2 Typical Applications

No need to buy expensive hardware, use NetDisturb software as hundreds customers around the world!

- *Development assistance and debug of automatons for IP equipments:* particularly on Set-Top Boxes operating in cable or telecom environments.
- *Performance & Acceptance Tests:* Qualify and evaluate the behavior of IP equipments (phone, fax, gateway, set-top box, IMS core, call server, application server, residential gateway, ADSL wireless router, and more…) and applications (audio and video streaming) on IP networks.
- *Configuration and control of IP Equipments for product verification and test:* Define different QoS levels in an Intranet or Internet environment to configure terminals, gateways and routers.
- *Test Laboratories:* NetDisturb provides repeatable QoS on different flows using configuration mode and values (loss, duplicate, delay, packet content impairment) defined by the user, and so re-create real world problems in the lab.
- *Applications test:* NetDisturb allows testing applications such as Voice over IP, Fax over IP, streaming audio and video, IPTV, VoD, real time applications and services, and other distributed applications.
- *Emulation of symmetric or asymmetric network conditions found on the Internet and enterprise networks (LAN, MAN, WAN):* latency, jitter, packet loss, bandwidth limitations, and more… to test IP applications (VoIP, streaming audio & video, etc.), services and products sensitive to various real conditions.

1.3 Key Features

What are the major features of NetDisturb V4.7?
With NetDisturb 4.7, two software editions are available: **Standard** and **Enhanced**

Common Key features for Standard and Enhanced Editions

- Simultaneous support of **IPv4** and **IPv6**
- Client-Server Architecture based on the SOAP mechanism which uses the HTTP protocol and the XML format for the exchanges between the client and the server.
- NetDisturb is an **Ethernet Bridge** to avoid any network configuration.
- Use of standard Ethernet Network Interface Cards up to **1 Gbps**
- Symmetric or Asymmetric **Bandwidth limitation** with router simulation
- Very easy to use and intuitive Graphical User Interface
- 16 configurable flows per direction
- **Aggregates** of IP flows can be defined (set of IP flows sharing the same Delay & Jitter Law)
- User-defined rules for disturbances: pattern trigger, starting time after delay or number of packets received, stop impairments after number of received packets or elapsed time, loops, and more…
- Predefined filter parameters based on the main protocol header fields (MAC, MPLS, VLAN, IP, TCP and UDP headers) or user-defined pattern filter
- **Unidirectional** or **bi-directional** packet impairments
- Impairments: Latency, Loss, Duplication, bandwidth limitation, Delay and Jitter, Content Impairment (mathematical laws and user-defined files)
- Change the impairment law **on-the-fly** for a flow
- Ability to **impair the remaining network traffic** that could be either only the IP packets or all the Ethernet frames.
- **Connections per IP flow**: impairments are applied to the IP flow or to each connection of the IP flow

- Ethernet / Internet modes (out-of-sequence packets)
- Command Line Interface (CLI) to use NetDisturb in test beds
- Ability to handle Ethernet Jumbo frames (payload up to 17976 bytes)
- Statistics display and export detailed statistics into a file
- Accuracy = **1 millisecond resolution**

Specific Key features for the Enhanced Edition

- Impairments based on protocol primitives:
  - ARP (ARP Operation Code)
  - DHCP (DHCP Message Type)
  - DNS (DNS Message Type, DNS message Operation)
  - FTP (FTP Command, FTP Returned Status)
  - FTP-DATA
  - HTTP (HTTP Method, HTTP Returned Status)
  - NTP
  - RTP (Audio Payload Type, Video Payload Type, DTMF)
  - SIP (SIP Method, SIP From, SIP To, SIP Returned status)

- RTP and FTP data flow automatic discovery.
- Detailed event log window per flow viewing the events and application of the impairments according to the user-defined rules.

1.4 Comparison between Standard and Enhanced Editions

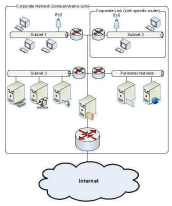
The table below summarizes the main differences between NetDisturb Standard edition and NetDisturb Enhanced edition.

Features	NetDisturb Standard	NetDisturb Enhanced
Impairment of IPv4 and IPv6 packets, ARPs and Ethernet frames	**Yes**	**Yes**
Filter parameters to define a flow: • Activity rules: - Start/Stop after a time limit or a packet counter or a pattern trigger - Loop to reapply the rule with delay between each iteration • Packet filters: source address, destination address, source port, destination port, protocol, DSCP DiffServ (ToS), MPLS, VLAN, , MAC address… • User-defined pattern filter based on Ethernet packet content	**Yes**	**Yes**
16 user-defined flows to impair using filters and other flows to impair without using filters	**Yes**	**Yes**
Dynamically modify impairments on-the-fly per flow in each direction when running	**Yes**	**Yes**
Aggregates of flows (set of flows sharing the same delay and/or jitter laws)	**Yes**	**Yes**
View Per-Flow statistics and NICs statistics	**Yes**	**Yes**
Accuracy = 1 millisecond	**Yes**	**Yes**
Standard impairments: drop/loss, duplicate, delay (latency), jitter, bandwidth limiting, congestion, packet error, bit error, reorder, burst errors Delay from 1 millisecond up to 10 sec in each direction Emulate bandwidth up to 1Gbps	**Yes**	**Yes**
Impairments by using the IP protocol field	**Yes**	**Yes**
Definition of flows to disturb based on protocol primitives:		
• ARP (ARP Operation Code)	No	**Yes**
• DHCP (DHCP Message Type)	No	**Yes**
• DNS (DNS Message Type, DNS Message Operation)	No	**Yes**
• FTP (FTP Command, FTP Returned Status)	No	**Yes**
• FTP-DATA	No	**Yes**
• HTTP (HTTP Method, HTTP Returned Status,)	No	**Yes**
• NTP	No	**Yes**
• RTP (Audio Payload Type, Video Payload Type, DTMF)	No	**Yes**
• SIP (SIP Method, SIP From, SIP To, SIP Returned Status)	No	**Yes**
Detailed events log per flow	No	**Yes**

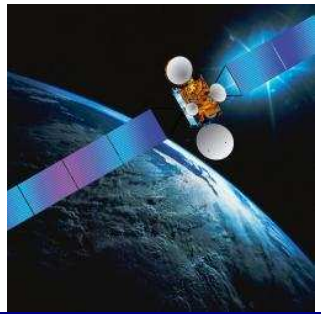
1.5 Examples of Use

The following examples illustrate a subset of use cases implemented in various projects.

Simulation of packet loss rate for a corporate network



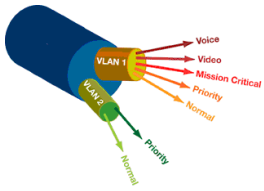
The modeling of packet loss rate of a banking network has generated a loss rate file with 1.3 million values. Before the deployment of new applications on the network, NetDisturb Standard Edition simulates the network to test these applications by using this external file containing loss rates to recreate the actual conditions of exploitation.



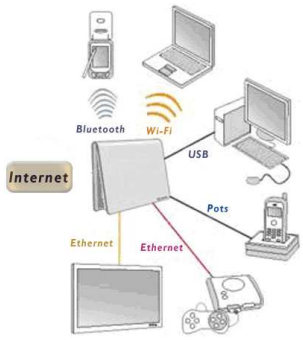
Simulation of a satellite link (with a 2 Mbps downlink and a 512 Kbps uplink throughput) for workstations of a branch office that generate TCP and UDP flows.

NetDisturb Standard Edition simulates the satellite link with limited uplink and downlink bandwidth. An aggregate is defined to submit all TCP and UDP flows to a function of delay - to reflect the delay of several hundreds of milliseconds introduced with the satellite link.

Application of disturbances on VLANs encapsulated over MPLS frames.



NetDisturb Standard Edition generates losses and delays of packets for specific VLANs implemented in a very large MPLS core network.



Tests of robustness for application protocols used in Triple Play Set-Top Box over DSL with NetDisturb Enhanced Edition

VoIP use case: for example, verify that the SIP REGISTER or the SIP INVITE message is retransmitted in case of no answer and then apply a loss and delay for RTP packets of the SIP session.

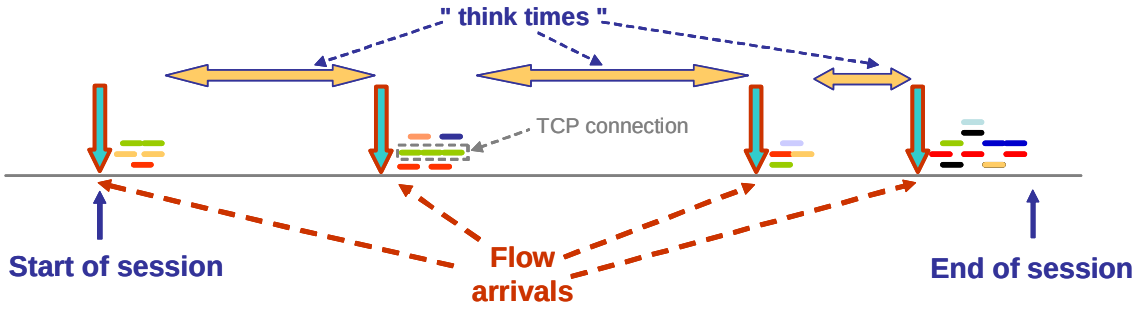
DHCP use case: for example, check that the OFFER message is lost following a transmitted DISCOVER message to validate automatic DHCP retransmission.

Test Video over IP using RTP with NetDisturb Enhanced Edition

NetDisturb generates impairments (loss, delay, duplication, modification of packets…) for the testing of codecs integrated in gateways, servers, STB and more…
.

1.6 NetDisturb handles and impairs flows

NetDisturb is based on the notion of flows.
A flow is a set of packets with a set of common packet properties, and can be unidirectional or bi-directional.
Flows are part of sessions (successions of flows and "think times") related to some homogeneous user activity (e-commerce, mail, MP3 file, web, etc.).



An IP flow is described by using an n-tuple.
In the typical case, the following 5-tuple is used: IP addresses (source and destination), protocol and port numbers (source and destination).
An IP flow is composed of connections (such as TCP connections to make FTP transfer by example).

To define the n-tuple for a flow, NetDisturb uses the notion of filter. A filter is the combination of the following optional parameters:

Ethernet header
- Destination MAC address
- Source MAC address
- Ethernet Packet Length
- IP Version (IPv4 or IPv6)
- Other protocols (ARP)

List of VLAN-ID (Ethernet frames 802.1Q)

List of MPLS-ID

IP Header
- Destination IP address (IPv4 or IPv6)
- Destination IP Mask (bit mask for IPv6)
- Source IP address (IPv4 or IPv6)
- Source IP Mask (bit mask for IPv6)
- Protocol (ICMP, TCP, UDP…)
- Differentiated Services Code Point (DSCP) / ToS Byte

List of Ports (for TCP or UDP packets)
- Destination port list
- Source port list

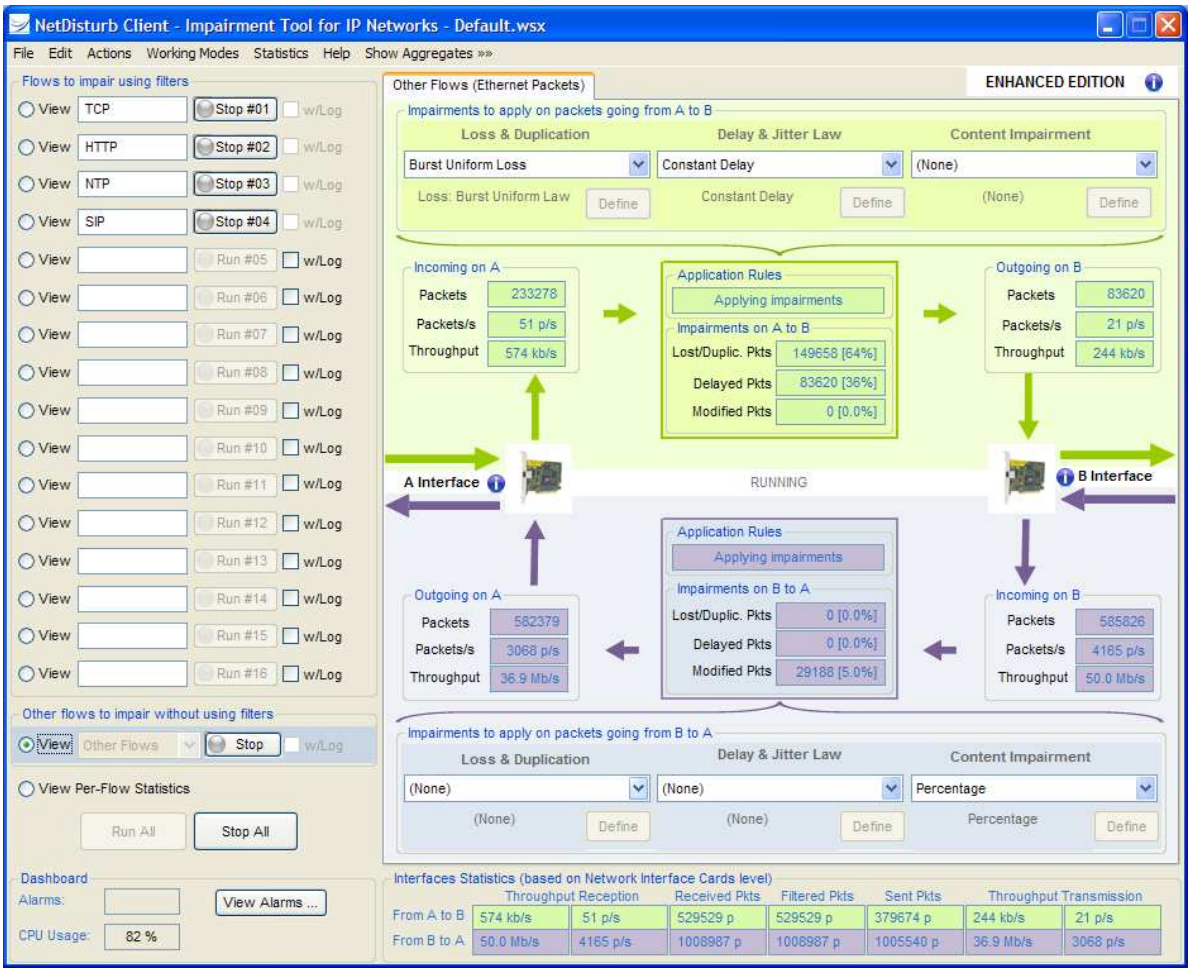
Protocol primitives (only for Enhanced version): ARP, DHCP, DNS, FTP, FTP-DATA, HTTP, NTP, RTP and SIP.

User-defined Pattern Parameter (search for a defined pattern with an offset in the Ethernet frame content)

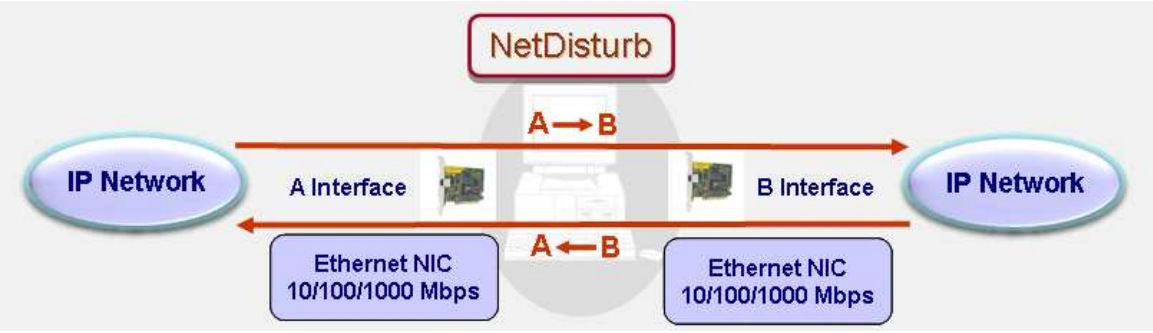
User-defined rules can be associated with the filter to condition the applying of the impairments.

With NetDisturb you can define up to 16 filters, i.e. 16 flows. An additional item named "Other Flows" is in charge to handle all flows (IP or not) that have not been user defined. For this item no filter can be defined, but impairments can be applied.

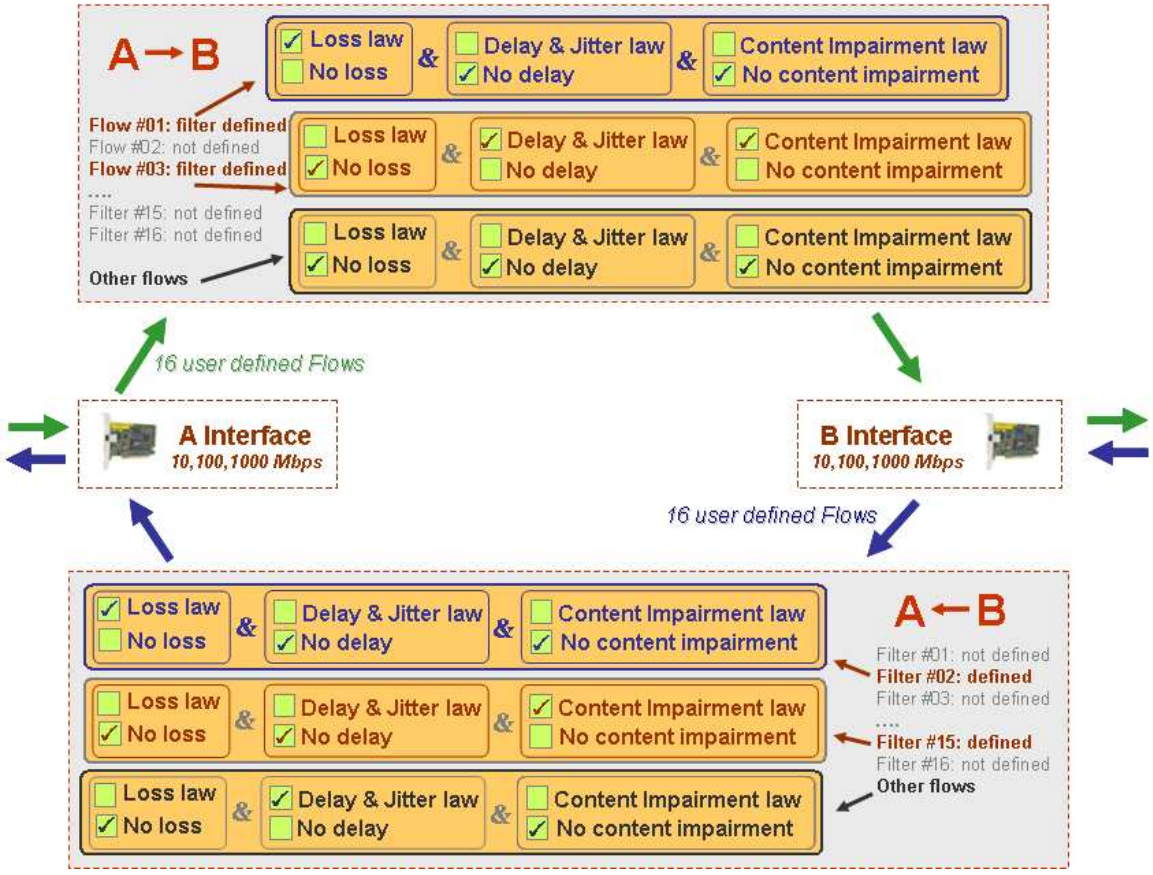
NetDisturb manages up to 10,000 connections – all flows included.
The client window below illustrates the management of flows by NetDisturb.



The graphical user interface represents the two NIC cards used by NetDisturb as "A Interface" and "B Interface" as illustrated below.



For each direction **A → B** or **B → A**, 16 flows can be defined by the user. And for each flow, loss or duplication, delay and jitter, and content impairment laws can be applied as shown in the figure below.



In the above example, NetDisturb has been configured with the following parameters:

Direction A → B

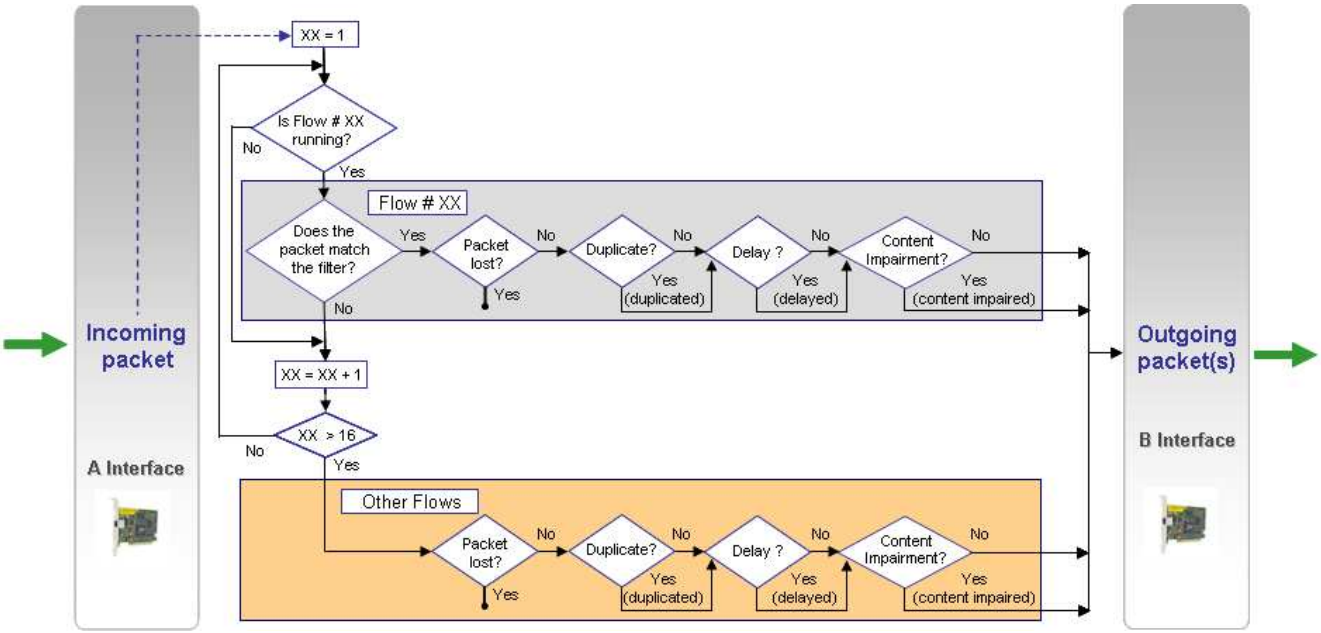
- The **Filter #01** defines the "Flow #01", and a loss law is applied to the packets of this flow,
- The **Filter #03** defines the "Flow #03", a Jitter law and a content impairment law are applied to the packets of this flow,
- As no loss, no delay and no content impairment laws are applied to the 'Other flows', all non-matching packets with the Filters #01 and #03 are relayed directly from A to B.

Direction B → A

- The **Filter #02** defines the "Flow #02", and a loss law is applied to the packets of this flow,
- The **Filter #15** defines the "Flow #15", a content impairment law is applied to the packets of this flow,
- As a delay law is applied to the **'Other flows'**, all non-matching packets with the filters #02 and #15 are delayed from B to A.

1.7 How does it work?

We illustrate how NetDisturb handles incoming packets with the following figure from the A to B interface.



Depending on the active user-defined flows, NetDisturb checks the incoming packet against the filter of the flow before applying loss, delay or content impairment treatments.
When this packet matches the filter of a flow (Flow #xx for example), then NetDisturb identifies whether this packet must be lost/duplicated and/or delayed, and/or its content must be impaired.
If this packet does not match any filter, NetDisturb applies the treatments for the 'Other Flows' and based on the laws defined i.e. lost/duplicated, delayed and content impairment.
For each packet received on an interface, NetDisturb analyzes in order the filters from 1 to 16 before considering this packet belongs to the "Other Flows".

So NetDisturb can apply impairments on the flows defined by the user either unidirectional (**A → B** or **B → A**) or bi-directional (the same or different impairments are being applied for both directions: **A → B** and **B → A**).

1.8 Filter characteristics and user-defined impairment rules for the flow

Two types of parameters can be used to define the filter for a flow:

- Predefined Parameters with the following options:
  - ARP
  - VLAN
  - MPLS
  - IP (TCP/UDP)
  - Protocol primitives (only for Enhanced version): ARP, DHCP, DNS, FTP, FTP-DATA, HTTP, NTP, RTP and SIP.
- And/Or User-defined Pattern Parameter (search for a defined pattern with an offset in the Ethernet frame content)

One of the features of NetDisturb is the definition of optional rules to link the launch of the impairments for a flow with an event or not.

Definition of the optional rules to apply impairments for the flow:
- Start when finding a pattern (with an optional offset) in the packet [**Trigger**]
- Delay before applying impairments (number of packets or elapsed time)
- Stop impairments after a number of received packets or elapsed time
- Reapply n times (n=0 means infinite) the previous conditions with a delay (elapsed time or number of received packets) between each cycle

Thus, the flow can be impaired continuously or impaired following user-defined rules with activity cycles.

If selected, notice that the **Trigger** is an intermediate step after the frame has been classified in a flow and before the frame is impaired.

For example, when NetDisturb is running a flow with user-defined rules including a trigger, several states are possible:

⇨ Waiting for the Trigger: the impairments do not apply. This state is the initial state of the Trigger.

⇨ Delay before applying impairments: the impairments still do not apply because a delay is defined before applying the impairments. This state changes to the state "Applying impairments" when the activation condition is reached. All packets or frames are relayed without treatment.

⇨ Applying impairments: the impairments are applying.

⇨ Delay before next cycle running: the impairments still do not apply because a delay is defined before reapplying the impairments. All packets or frames are relayed without treatment. This is available only when cycles are defined.

⇨ No more impairment: the impairments don't apply anymore. All packets or frames are relayed without treatment.

A Trigger can remain active permanently when no duration limit is defined.

1.9 Apply Impairments to Applicative Protocols with NetDisturb Enhanced Edition

Two editions of NetDisturb software are available: Standard Edition and Enhanced Edition.
The Enhanced Edition allows defining filters including protocol primitives whose list is detailed below. So you can define precisely the exact primitive of the protocol to disturb if needed.

ARP
- ARP request
- ARP reply
- RARP request
- RARP reply
- DRARP request
- DRARP reply
- DRARP error
- InARP request
- InARP reply

DHCP
- DHCPDISCOVER (BOOTP request)
- DHCPOFFER (BOOTP reply)
- DHCPREQUEST (BOOTP request)
- DHCPACK (BOOTP reply)
- DHCPNACK (BOOTP reply)
- DHCPDECLINE (BOOTP request)
- DHCPRELEASE (BOOTP request)
- DHCPINFORM (BOOTP request)

DNS
DNS Message Type
- Query
- Response

DNS Message Operation
- QUERY
- IQUERY
- NOTIFY
- STATUS
- UPDATE

FTP
FTP Returned STATUS
- OK (200)
- Not Found (404)
- 1xx Series
- 2xx Series
- 3xx Series
- 4xx Series
- 5xx Series

FTP Command
- ABOR
- ACCT
- ALLO
- APPE
- CDUP
- CWD
- DELE
- EPRT
- EPSV
- FEAT
- HELP
- LIST
- MKD
- MODE
- NLST
- NOOP
- OPTS

FTP Command (cont.)
- PASS
- PASV
- PORT
- PWD
- QUIT
- REIN
- REST
- RETR
- RMD
- RNFR
- RNTO
- SITE
- SMNT
- STAT
- STOR
- STOU
- STRU
- SYST
- TYPE
- USER

FTP DATA

HTTP
HTTP Returned STATUS
- OK (200)
- Not Found (404)
- Moved (301)
- 1xx Codes
- 2xx Codes
- 3xx Codes
- 4xx Codes
- 5xx Codes

HTTP Method
- OPTIONS
- GET
- HEAD
- POST
- PUT
- DELETE
- TRACE
- CONNECT

NTP

RTP
Audio Payload Type
- 0 PCMU
- 3 GSM
- 4 G723
- 5 DVI4
- 6 DVI4
- 7 LPC
- 8 PCMA
- 9 G722
- 10 L16
- 11 L16

Audio Payload Type (cont.)
- 12 QCELP
- 13 CN
- 14 MPA
- 15 G728
- 16 DVI4 (11,025 Hz)
- 17 DVI4 (22,050 Hz)
- 18 G729

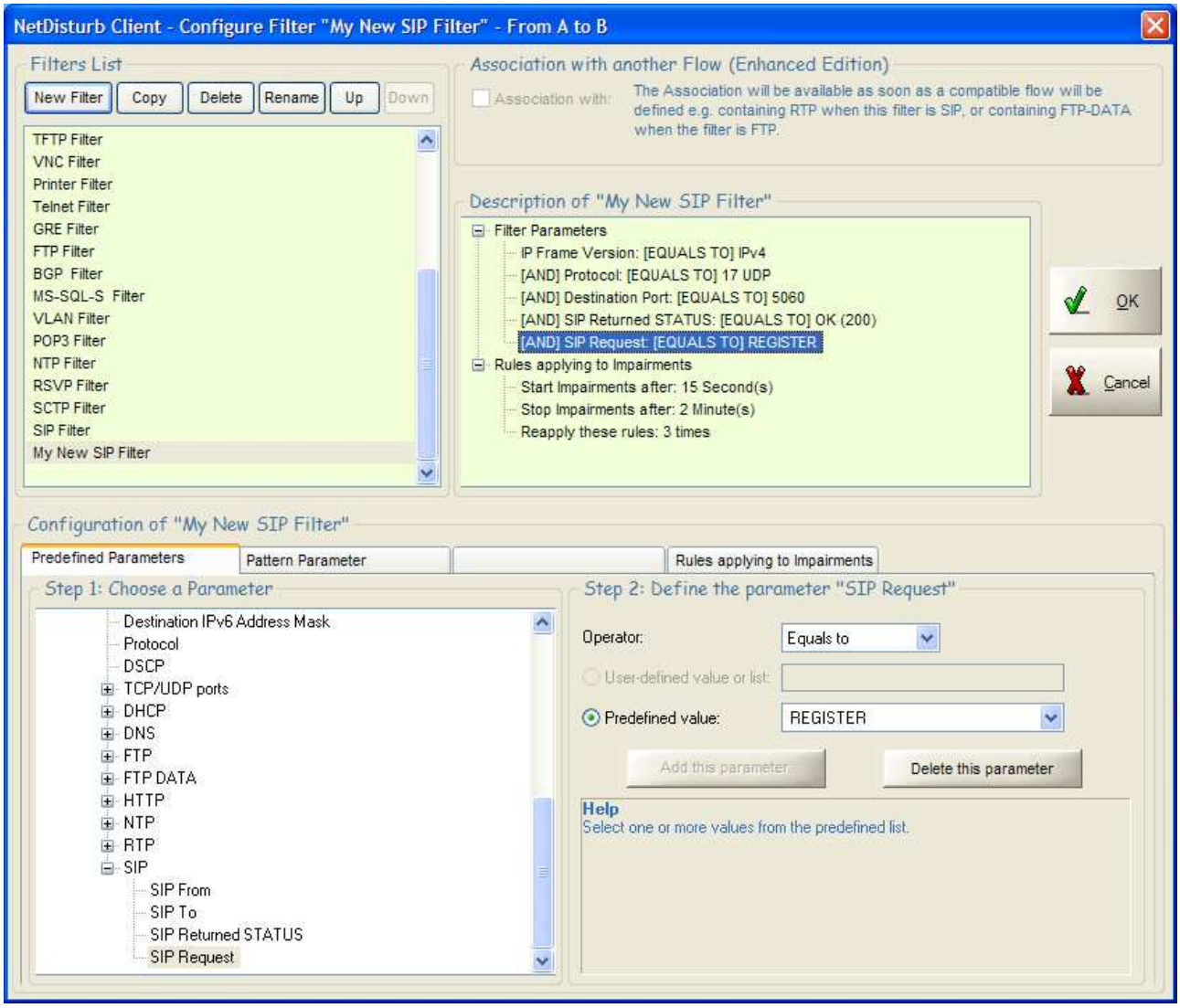
Video Payload Type
- 25 CelB
- 26 JPEG
- 28 nv
- 31 H261
- 32 MPV
- 33 MP2T
- 34 H263

DTMF
RTP (SIP From)
RTP (SIP To)

SIP
SIP From
SIP To
SIP Returned STATUS
- OK (200)
- Trying (100)
- Ringing (180)
- Moved (301)
- 1xx Codes
- 2xx Codes
- 3xx Codes
- 4xx Codes
- 5xx Codes
- 6xx Codes

SIP Request
- INVITE
- ACK
- BYE
- CANCEL
- OPTIONS
- REGISTER
- PRACK
- SUBSCRIBE
- NOTIFY
- PUBLISH
- INFO
- REFER
- MESSAGE
- UPDATE

The following screenshot illustrates for example the parameters of a user-defined filter ("My New SIP Filter") for a SIP message ("REGISTER") that we want to disturb. This filter can be used for example to study the retransmission mechanism when a SIP REGISTER is lost by using NetDisturb with a Set-Top Box.



1.10 List of impairments

Pre-defined Loss and Duplication laws:

- Loss: Constant Law
  Parameter: number of packets
- Loss: Uniform Law
  Parameters: alpha, beta, threshold
- Loss: Burst Uniform Law
  Parameters: alpha, beta, threshold(n), threshold(n + x), depth
- Loss: File (Loss Values)
  Parameters: file name, threshold
- Loss: Percentage
  Parameter: percentage

- Loss: 1 Packet out of N
  Parameter: range (N)
- Loss: Percentage & Duration (time-limited losses percentage)
  Parameter: percentage, duration
- Loss: File (Percentage & Duration)
  Parameter: file name
- Duplication: Percentage (send n times the received packet)
  Parameters: percentage, Min ≤ n ≤ Max
- Duplication: 1 Packet out of M (duplicate 1 packet n times every M received packets).
  Parameters: range (M), Min ≤ n ≤ Max
- Duplication: Uniform Law
  Parameters: alpha, beta, threshold
- Loss (1 out of N) then Duplication (1 out of M): the loss law (1 Packet out of N) is used first before the duplication law (1 Packet out of M)

Pre-defined Delay & Jitter laws:

- Constant Delay
  Parameter = constant delay
- Constant Delay & Exponential Jitter
  Parameters: constant delay, λ
- Constant Delay & Uniform Jitter
  Parameters: constant delay, alpha, beta
- Constant Delay & File (Jitter)
  Parameters: constant delay, user file
- File (Packet Sending Minimum Cadences)
  Parameter: user file
- Router Simulation & Constant Delay
  Parameters: IP throughput, max memory, constant delay
- Router Simulation & File (Packet Sending Minimum Cadences)
  Parameters: IP throughput, max memory, user file
- Constant Delay & File (Throughput & Duration)
  Parameters: constant delay, user file

Pre-defined Content impairment laws:

- 1 Packet out of N
  Parameter: range (N)
- Percentage
  Parameter: percentage
- Normal Law (Laplace-Gauss)
  Parameters: average, standard deviation, threshold
- Uniform Law
  Parameters: alpha, beta, threshold

1.11 Working modes and flow aggregation

Two important features of NetDisturb allow you to define how disturbances will apply to the flow of packets:

- the working mode
- the aggregation of flows

1.11.1 Two Working Modes

NetDisturb offers two working modes by applying impairments:

- Enable/Disable out-of-sequence packets in a flow,
- Impairment laws apply to the IP flow or to each TCP/UDP connection of the IP flow.

These modes are used together.

For example, NetDisturb set with the following modes simulates the Internet network with disturbed flows:

- Enable out-of-sequence packets in a flow
- Impairment laws apply to the IP flow

.

Another example: to disturb VoIP communications in the same way on an Ethernet network, use NetDisturb with the following modes:

- Disable out-of-sequence packets in a IP flow
- Impairment laws apply to each TCP/UDP connection of the IP flow

.

Enable/Disable out-of-sequence Packets

Impairment may introduce changes in the packet sequence – for example by introducing different delays for the packets of a flow.

One of the Ethernet characteristics is to keep packets received in order. Internet hasn't got this constraint regarding the packet order: some packets can use one route while others use another one, with the consequence the receiver may get packets unordered.

NetDisturb is able to simulate the Internet network (enable out-of-sequence packets) or to react as Ethernet does (disable out-of-sequence packets).

Impairment laws apply to the IP flow or to each TCP/UDP connection of the IP flow

NetDisturb is able to dispatch IP packets 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.

Assuming the impairment has been defined with a loss law: lose the third packet for 10 packets received, the results depends on the way this law handles the packets:

- *Impairment laws to be applied to the IP flow*

When this option is selected, every received packet matching the filter for this flow is considered to belong to the same flow. Processing is carried out in "continue". With the previous example of loss law (lose the 3rd packet on 10 received), NetDisturb will lose the 3rd packet for ten received packets whatever the TCP/UDP connection belongs to.

- *Impairment laws to be applied to each TCP/UDP connection of the IP flow*

When this option is selected, NetDisturb analyses each received packet in order to associate this packet to a TCP or UDP connection already existing by using these parameters: protocol, IP addresses and port numbers. If the connection doesn't exist, a new one is created. With the previous example of loss law (lose the 3rd packet on 10 received), NetDisturb will lose the 3rd packet for ten received packets of each TCP or UDP connection. Up to 10,000 connections can be handled simultaneously by NetDisturb.

The option "Impairment laws to be applied to each TCP/UDP connection of the IP flow" is not available for the flows using a filter based on applicative protocol primitives.

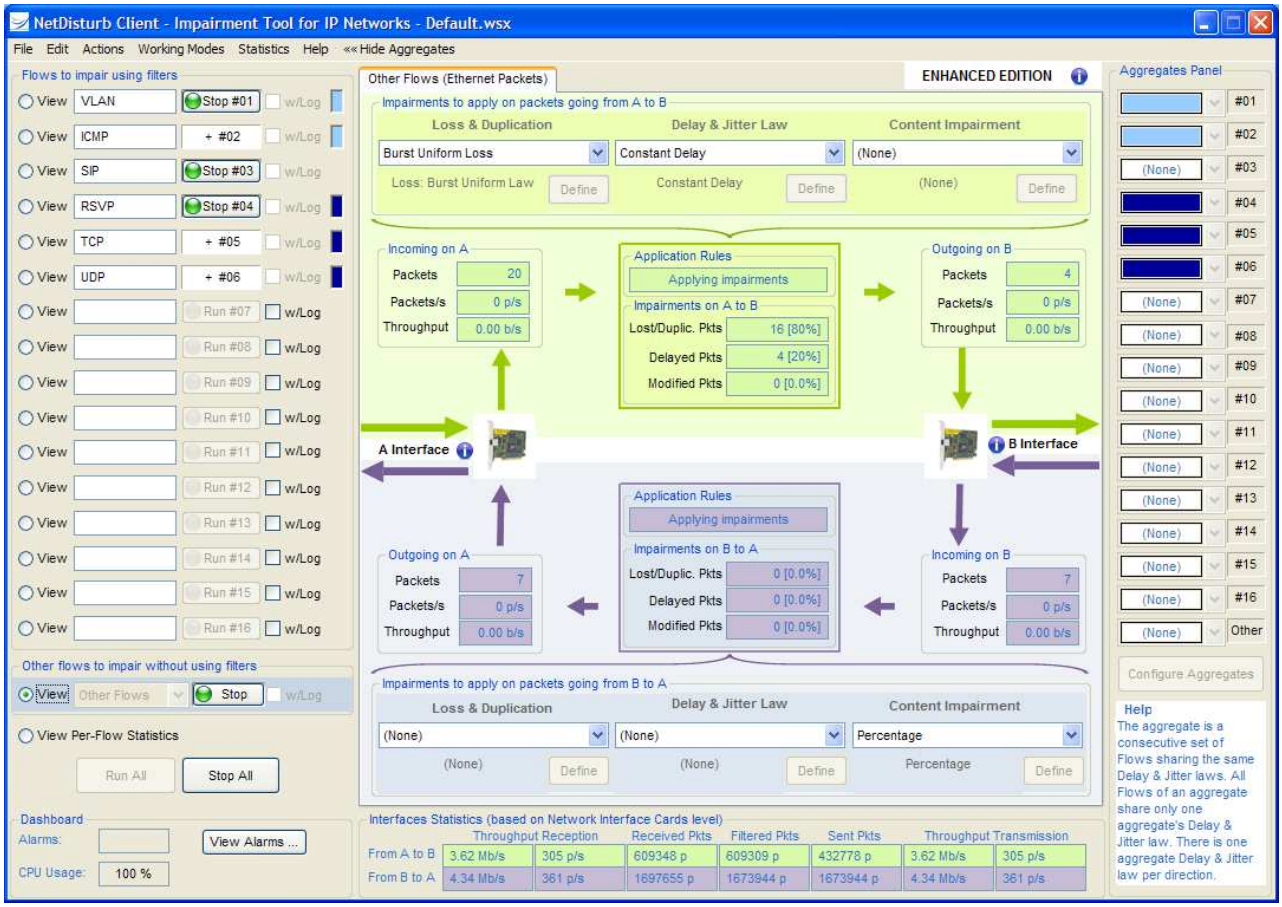
.

1.11.2 Flow Aggregation

An aggregate is a consecutive set of flows sharing the same Delay & Jitter Laws. All flows of an aggregate share only one aggregate's Delay & Jitter law (with one law per direction).

This feature is particularly useful for the following cases: satellite simulation, VPN, routing, bandwidth limitation…
Up to 8 aggregates for all 16 flows can be defined.
The flow order in the aggregate defines the priority of packets to delay. While the top flow packets get the highest priority, the other flow packets are queuing until there are no higher priority packets.
In the example illustrated below, two aggregates have been defined:

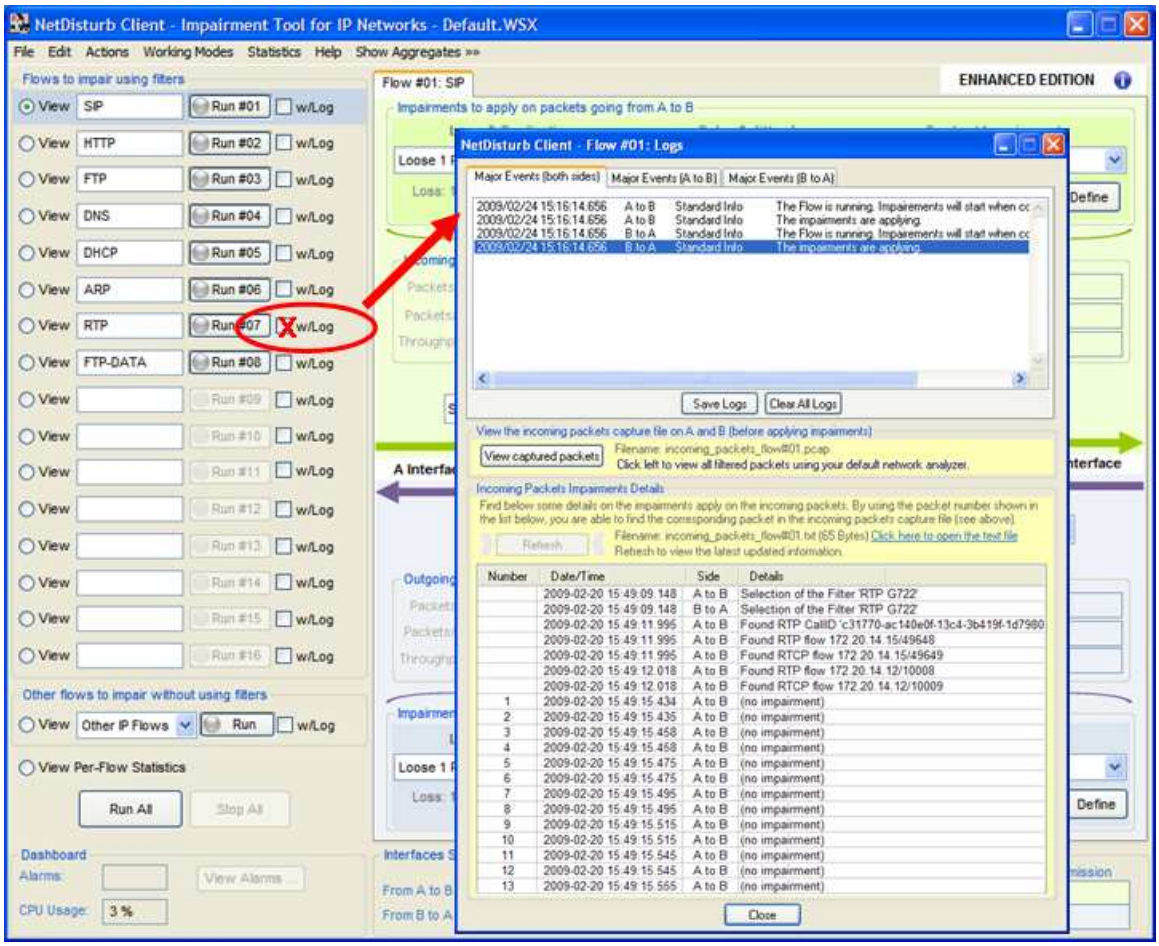
- The light blue colored aggregate collects two flows (#01 and #02)
- The dark blue colored aggregate collects the flows #04, #05 and #06.



1.12 Traces and logs (Enhanced Edition only)

Once a filter is defined for a flow, it's possible to trace the events and packets to impair with NetDisturb Enhanced Edition.

The following screenshot shows the log window displayed after running the flow when the option ☐ **w/Log** has been checked for the flow.



For each flow with the checked log option, all incoming packets for the two interfaces **A** and **B** are saved into a capture file.

By using the opened log window when the flow is started by pressing the corresponding Run #xx button, you can:

- Display the major events for both directions (**A → B** and **B → A**).
- View the captured packets of the flow (for both directions) before applying impairments by using your default network analyzer launched automatically (for example: Wireshark/Ethereal).
- View the impairment applied for each packet of the flow (for both directions): (no impairment) or (lost) or (delayed) or (modified)…

NetDisturb generates two files per flow when the w/Log option is checked:

- incoming_packets_flow#xx.pcap for the flow No. xx (this capture file contains all incoming packets for the two interfaces and can be viewed with a network analyzer such as Wireshark).
- incoming_packets_flow#xx.txt for the flow No. xx (this text file contains the description of the impairment applied for each incoming packet for the two interfaces that is numbered and time-stamped by NetDisturb).

You can then examine very precisely by using these two files what incoming packet is concerned and the nature of the applied impairment.

1.13 Statistics & Alarms

Different statistics are calculated and displayed by NetDisturb:

- Detailed Statistics for each Flow (and for both directions)
- Summary table of Per-flow statistics
- Interfaces Statistics (based on Network Interface Card level) and Alarms

These statistics can be saved into a file for a later use.

Detailed statistics for each Flow

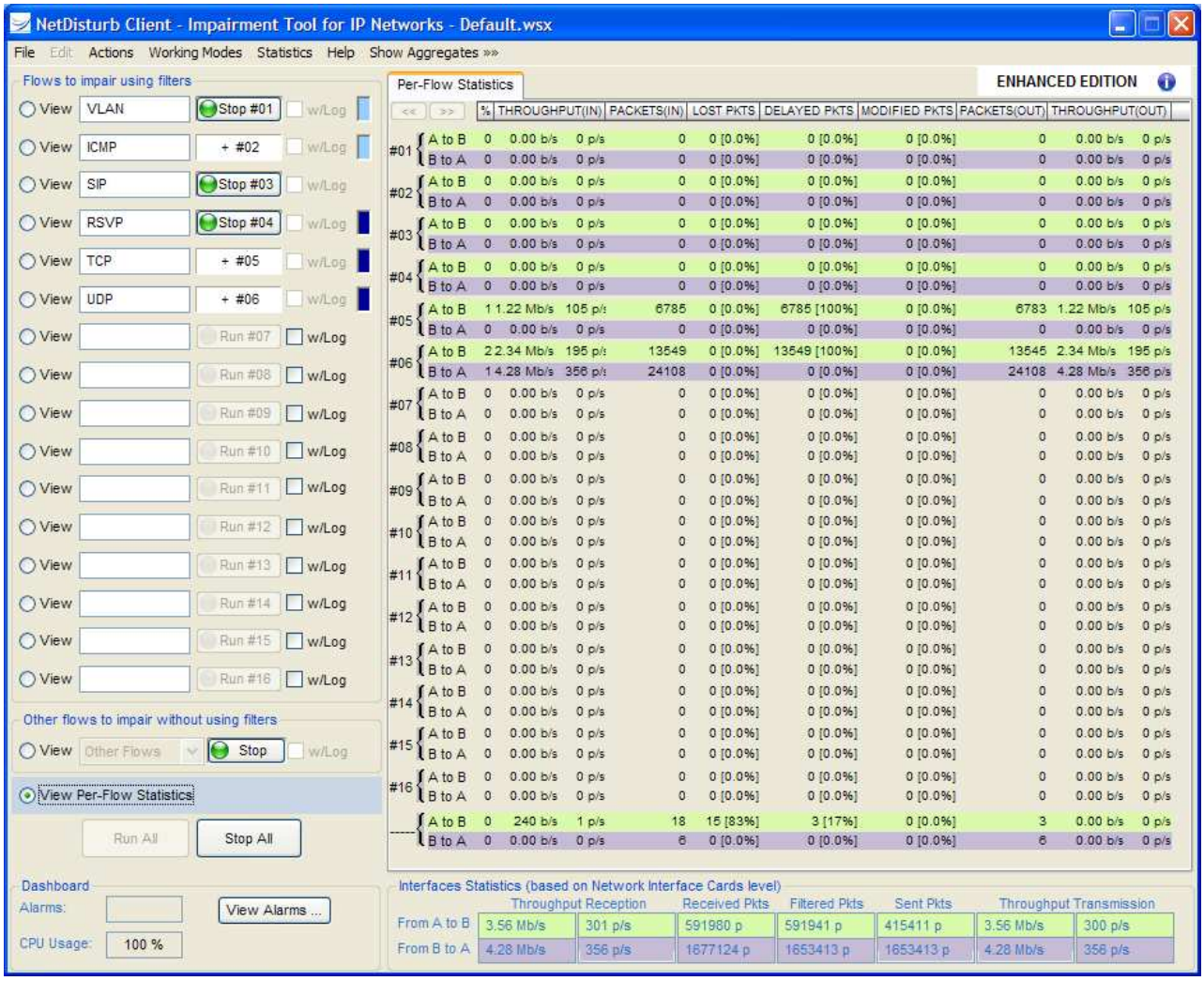
For each direction (A → B or B → A) NetDisturb displays:

- ① For the incoming interface: the number of received packets matching the filter, the number of received packets per second and the throughput
- ② For the impairments:
  - The number and percentage of lost or duplicated packets
  - The number and percentage of delayed packets
  - The number and percentage of modified packets
- ③ For the outgoing interface: the number of sent packets, the number of sent packets per second and the throughput

Summary table of Per-Flow statistics

The View Per-Flow statistics displays for each flow and for each direction:

- The incoming throughput and number of received packets per second
- The number of packets matching the filter
- The number of lost/duplicated packets
- The number of delayed packets
- The number of modified packets
- The outgoing throughput and the number of sent packets per second

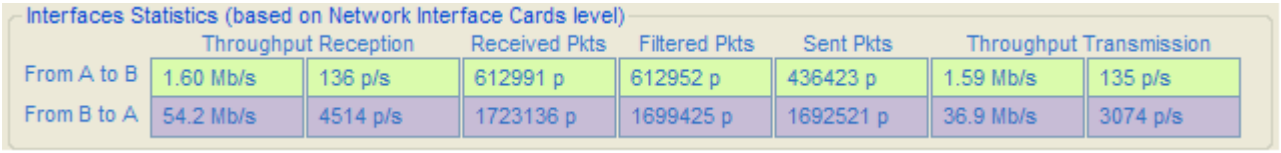


View Per-Flow Statistics

Interfaces Statistics

At the bottom of the Client window, the Interface Statistics displays the following parameters for both NICs (A → B or B → A):

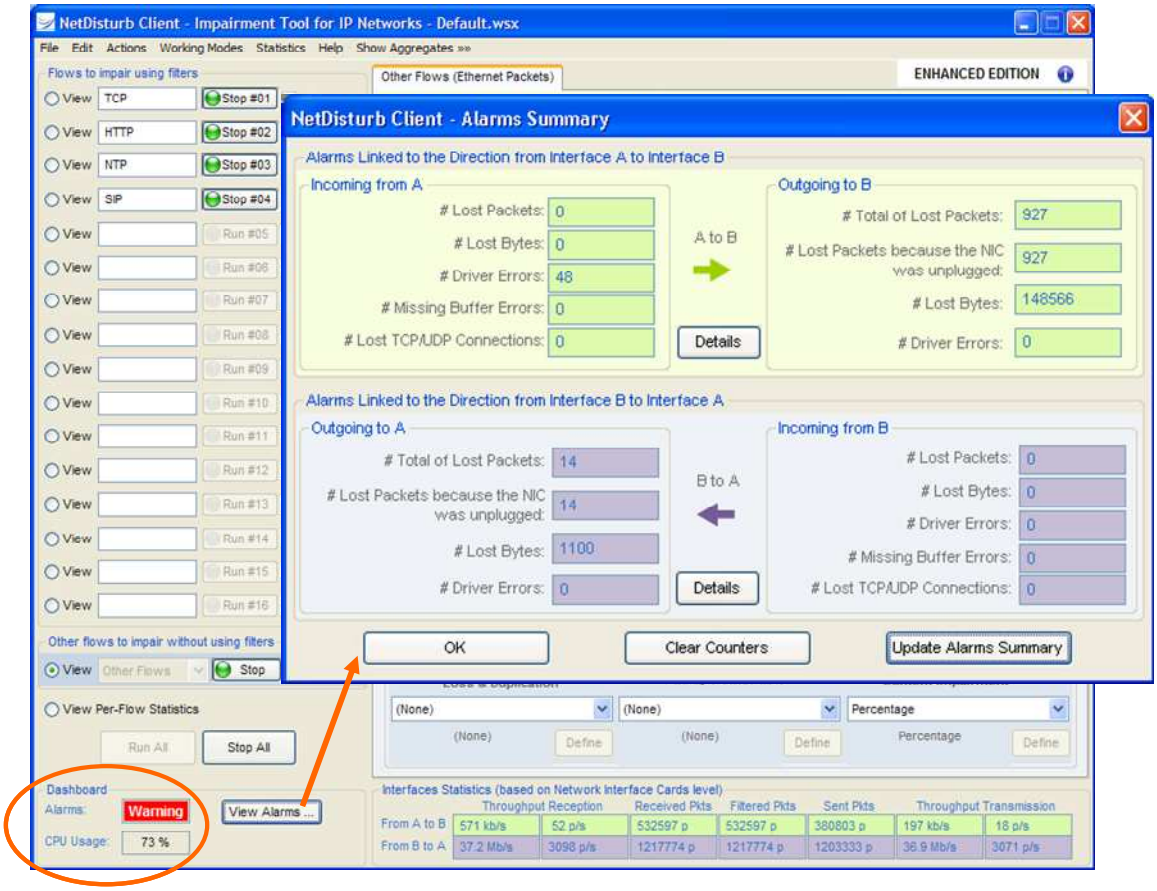
- Throughput and number of received packets per second
- Number of received packets
- Number of filtered packets
- Number of sent packets
- Throughput and number of sent packets per second



Alarms

The alarms encountered by the NetDisturb driver can be displayed by the user and are classified per direction for both interfaces:

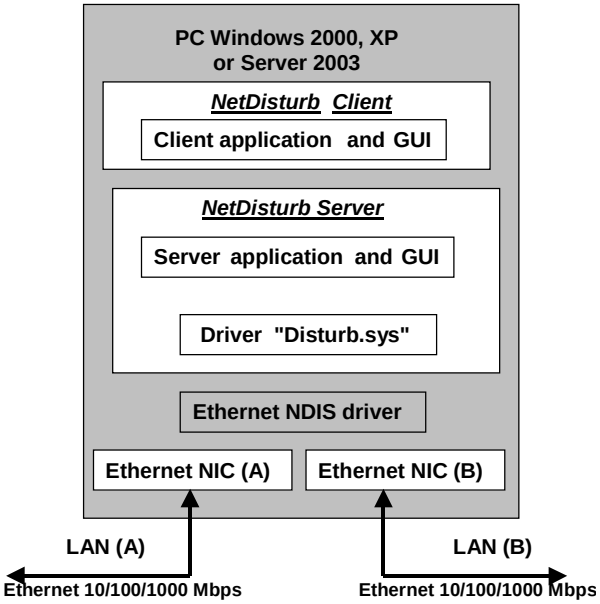
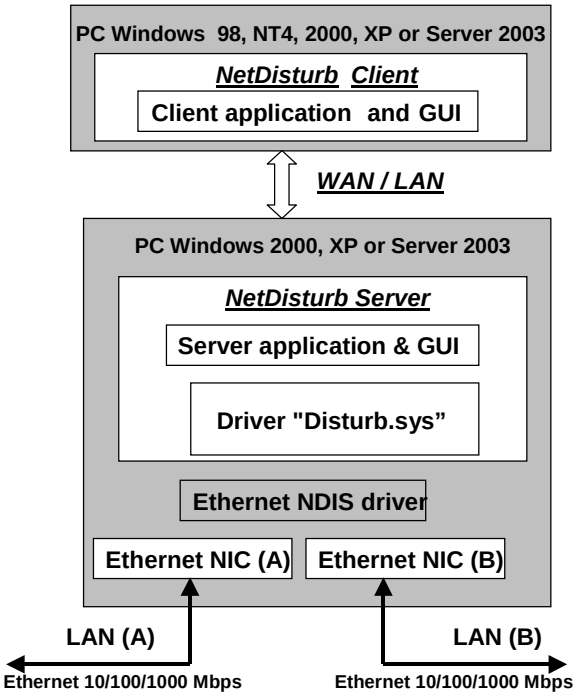
Incoming direction	*Outgoing direction*
• Number of lost packets • Number of lost bytes • Number of errors returned by the Network Interface Card driver • Number of missing buffers to keep packets • Number of lost TCP/UDP connections due to the upper limit of connections handled by NetDisturb	• Total number of lost packets • Number of lost packets due to the unplugged Network Interface Card • Number of lost bytes • Number of errors returned by the Network Interface Card driver



1.14 Configurations

Based on Client-Server architecture, NetDisturb software is made of two parts: NetDisturb Server and NetDisturb Client. NetDisturb Server handles the impairment characteristics and the Client manages the Server using a simple graphical interface.
This allows two configurations where the Server and the Client parts may be installed on the same PC (local control), or the Server is located on one PC and the Client is located on a second PC (remote control). In this second configuration, the Client dialogs with the Server by using a Wan (for example: PSTN or ISDN) or a LAN link.

Note: It is recommended for better performances to use two identical Ethernet Cards for NetDisturb Server.

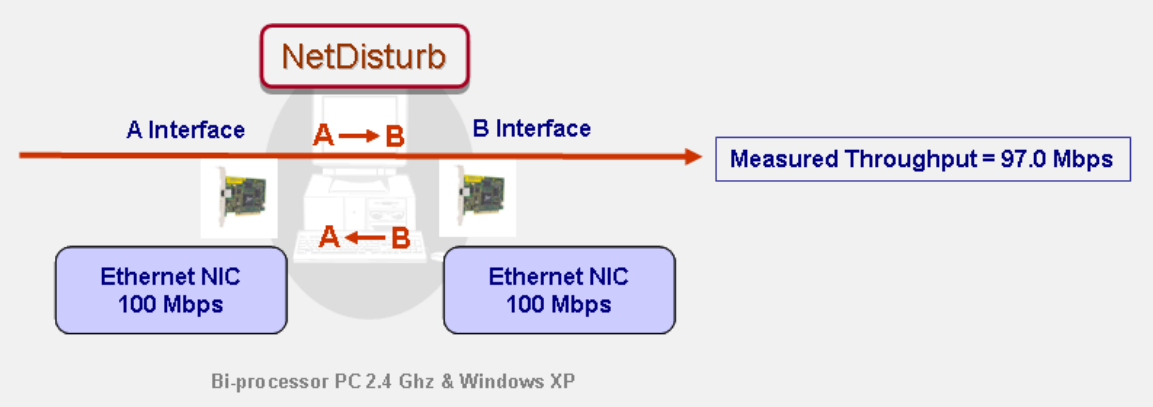
Configuration No 1	Configuration No 2
	
Client and Server on the same PC	*Client and Server on two different PCs*

The Disturb.sys driver is located in the kernel of the operating system and is installed above the NIC drivers. This driver is used by NetDisturb to handle the exchanges with the NICs.

1.15 Performances

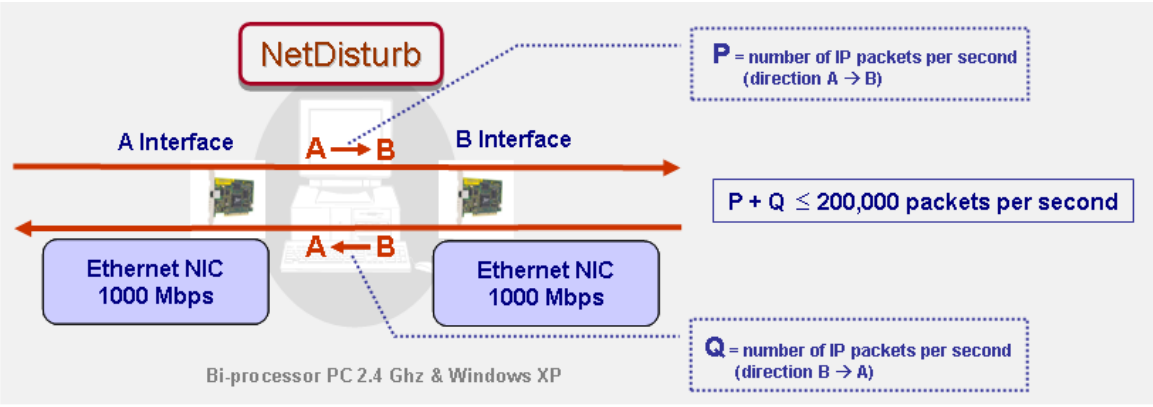
To illustrate the key performances of NetDisturb, 2 examples are presented hereafter (by using an Intel Xeon 5140 2.33 GHz with windows XP SP2).

Example 1: use of 2 Fast Ethernet NICs



NetDisturb is configured with 16 IP flows (no loss and no delay for each flow).
With Fast Ethernet NICs, the throughput measured is 97 Mbps in one direction.

Example 2: use of 2 Gigabit Ethernet NICs



Measured incoming and outgoing throughput up to 980 Mbps
By using 2 Gigabit NICs, NetDisturb can handle up to 200,000 packets per second with 16 IP flows defined (for both directions).
Please refer for more detailed information to the "NetDisturb Performance Characteristics on Gigabits Networks" document.

These two examples show some performances of NetDisturb. This will avoid heavy investments in expensive hardware solutions.

Part 2 What's new in NetDisturb V4.7?

This part is a general overview of new features and improvements provided with **NetDisturb** version 4.7 and important information to upgrade from previous versions.

More details regarding features and improvements included in the different versions of **NetDisturb** can be found in the version.txt file located in the installation directory (default settings: C:\Program Files\NetDisturb).

The new features and improvements provided with **NetDisturb** version 4.7 are listed below:

- ⇨ Two editions are available: **NetDisturb** Standard Edition and **NetDisturb** Enhanced Edition.
- ⇨ New Graphical User Interface: more intuitive, even easier to use and enriched with new features
- ⇨ The definition of a filter to characterize a flow replaces the notion of mask used in earlier versions. This includes at least one of the two ways to describe the frames matching filter:
  - The use of predefined frame fields content (MAC and IP addresses, protocol, port, etc.)
  - The use of a byte pattern comparison that should be true to match the filter.
  - An optional set of rules allows starting and limiting the impairment based on the content, the time or the number of packets.
- ⇨ More detailed statistics for each flow updated in real time for each direction A->B or B->A: number of incoming packets, number of incoming packets per second, incoming throughput, number of impaired packets (lost/duplicated, delayed or modified), number of outgoing packets, number of outgoing packets per second, outgoing throughput.

- ⇨ Features added with the **NetDisturb** Enhanced Edition:
  - Definition of flows to disturb based on protocol primitives
    - ARP (ARP Operation Code)
    - DHCP (DHCP Message Type)
    - DNS (DNS Message Type, DNS Message Operation)
    - FTP (FTP Command, FTP Returned Status)
    - FTP-DATA
    - HTTP (HTTP Method, HTTP Returned Status,)
    - NTP
    - RTP (Audio Payload Type, Video Payload Type, DTMF)
    - SIP (SIP Method, SIP From, SIP To, SIP Returned Status)
  - Detailed event log per flow (to view the impairment applied for each packet of the flow)

The contexts created with versions 4.2, 4.3 RC3, 4.4, 4.5 and 4.6 are reused automatically. When saved, they get the new NetDisturb V4.7 file format.

Part 3 Install NetDisturb

NetDisturb requires less than 20 MB of free disk-space. The installation procedure is a standard installation program for Windows 2000, XP and Windows Server 2003.

** To run **NetDisturb** your computer's screen resolution must be at least 1024x768 (more readable: 1152 x 768 and sup.), the DPI setting should be set up with the "Normal size (96 DPI)" value and the Font size should be set up with the "Normal" value.*

** To install **NetDisturb** under Windows 2000, XP or Server 2003**, you must log on with administrators rights**.*

3.1 Forewords before upgrading from versions 4.2, 4.3, 4.4, 4.5 and 4.6

*When upgrading from a previous version of **NetDisturb** and if you don't have the USB license dongle, do not uninstall the previous version to keep your existing license.*

When upgrading from an older **NetDisturb** version, the installation procedure of **NetDisturb** moves the user's files and the context files, located in the previous default **NetDisturb Server** directory, into **NetDisturb Client** directory. All files related to a context (defined using the extension .txt and .wsx) are copied, but the files installed with **NetDisturb** version 4.7 will overwrite those files**.**

3.2 Forewords before upgrading from versions 4.1 and under

You don't need to uninstall the previous version of **NetDisturb** to keep your license scheme. However, this license will not enable you to use **NetDisturb** version 4.7, because the license date of version 4.1 and under is too old. You should contact ZTI (contact@zti-telecom.com) to get back a new unlimited license when upgrading to version 4.7.

3.3 How to install the software downloaded from the Internet

The installation procedure is a standard installation program.

- If you have downloaded the **NetDisturb**.**zip** file from the website, you must first unzip this file in a temporary directory. It contains the Setup_NetDisturb.exe file and the related documentation.
- Then run "Setup_NetDisturb.exe" from the temporary directory to launch the setup procedure.

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

3.4 How to install the software from the CD-ROM

The installation procedure is a standard installation program. On the CD-ROM, you will find the "Setup_NetDisturb.exe" file.

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

3.5 How to install the NetDisturb Client only (from the CD-ROM)

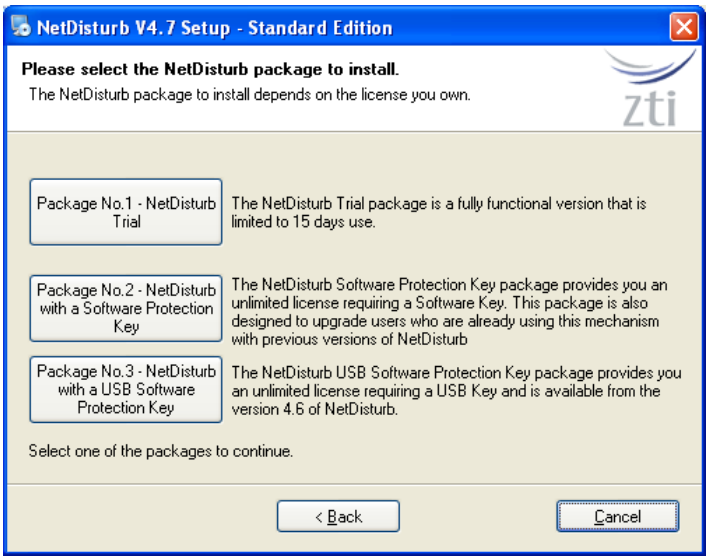
On the CD-ROM, a second setup allows installing the **NetDisturb** Client on a machine. This is useful if you need to install the **NetDisturb** Server and the **NetDisturb** Client on two different machines.

To install the **NetDisturb** Client (Windows 98, 2000, XP or Server 2003), run "Setup_NetDisturbClient.exe" and follow the setup instructions to proceed with the installation.

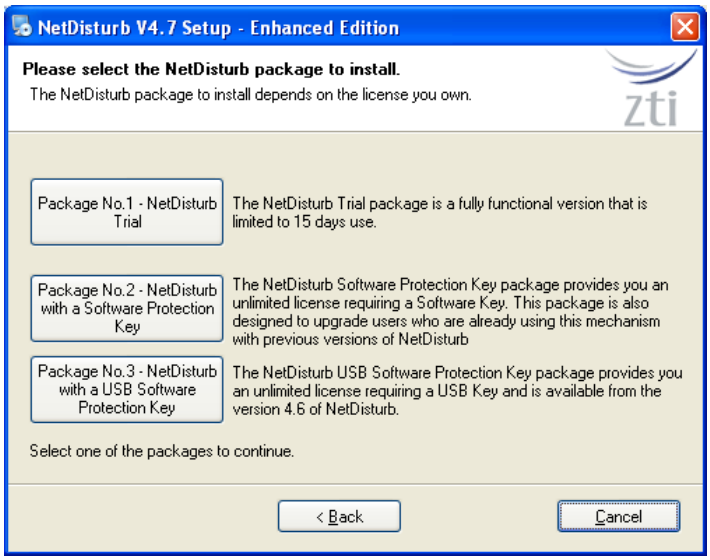
3.6 During the installation

Follow the instructions until reaching the **NetDisturb** package selection window.

NetDisturb Standard Edition



NetDisturb Enhanced Edition



3.6.1 NetDisturb packages in a few words

To use the **NetDisturb** software, there are 3 license schemes:

- **Package No.1 - NetDisturb Trial**: the Trial package allows you using **NetDisturb** during 15 days after the first run. When the trial period has expired, the license should be purchased.
- **Package No.2 - NetDisturb with a Software Protection Key**: this package is for users owning a Software License key and for the users of the previous versions of **NetDisturb**. It keeps your current installation and files, without additional requirement.
- **Package No.3 - NetDisturb with a USB Software Protection Key**: this package requires a USB dongle containing the **NetDisturb** license. The USB Software Protection Key is provided with **NetDisturb** from version 4.6. This package allows the installation of **NetDisturb** on several PCs but the only PC able to run **NetDisturb** is the one having the USB dongle plugged in.

As previous user, you may be interested to move to a USB Software Protection Key: please contact your distributor or ZTI to get more details about the license migration program (see paragraph 4.3 NetDisturb & USB Software Protection Key for more details).

This software is licensed on a per workstation basis. This means that you will need to get a separate license for each machine you will run it on. The license may be a software license key or the USB Software Protection key.

The USB Software Protection key contains only the license information. *The **NetDisturb** software is available on a separate CD-ROM.*

3.6.2 Which package should I install?

Depending on your needs, please find here below the package most suitable for you.

3.6.2.1 I want to evaluate NetDisturb

In that case, choose the Package No.1 *"NetDisturb Trial"*.
You will be able to use **NetDisturb** during 15 days only.

3.6.2.2 I already use NetDisturb…

*This paragraph is dedicated to the users owning a previous version of **NetDisturb.***

… and I want to upgrade and keep my permanent license

In that case, choose the Package No.2 *"NetDisturb with a Software Protection Key"*. Your installation will be upgraded and your existing permanent Software Protection Key will be kept.

… and I want to upgrade and use the USB Software Protection Key I bought

In that case, choose the Package No.3 *"NetDisturb with a USB Software Protection Key"*. Plug the USB dongle before launching **NetDisturb.**

3.6.2.3 I just bought NetDisturb…

*This paragraph is related to the users purchasing **NetDisturb V4.7***

… and I chose the Electronic Software Delivery (ESD)

In that case, choose the Package No.2 *"NetDisturb with a Software Protection Key".* When you launch the software for the first time, press the "Enter" key when the ZTI logo appears. Then, get the site code and email it to us with your details and your purchase order reference at contact@zti-telecom.com. We will send you back the site key enabling your permanent license. More details about the way to proceed are available in paragraph *"4.2.1 Installation of the Software Protection Key".*

… and I received the CD-ROM & USB Software Protection Key

In that case, choose the Package No.3 *"NetDisturb with a USB Software Protection Key"*. Plug the USB dongle before running **NetDisturb.**

… and I will receive CD-ROM & USB Software Protection Key in a few days

In that case, choose the Package No.2 *"NetDisturb with a Software Protection Key".* You will get a fully functional but time-limited Software Protection Key.

3.7 What has been installed on my computer?

The default settings install **NetDisturb** software components in the following directory:

C:\Program Files**NetDisturb** with the following subdirectories:
C:\Program Files\ **NetDisturb** \Client
C:\Program Files\ **NetDisturb** \Driver
C:\Program Files\ **NetDisturb** \Server

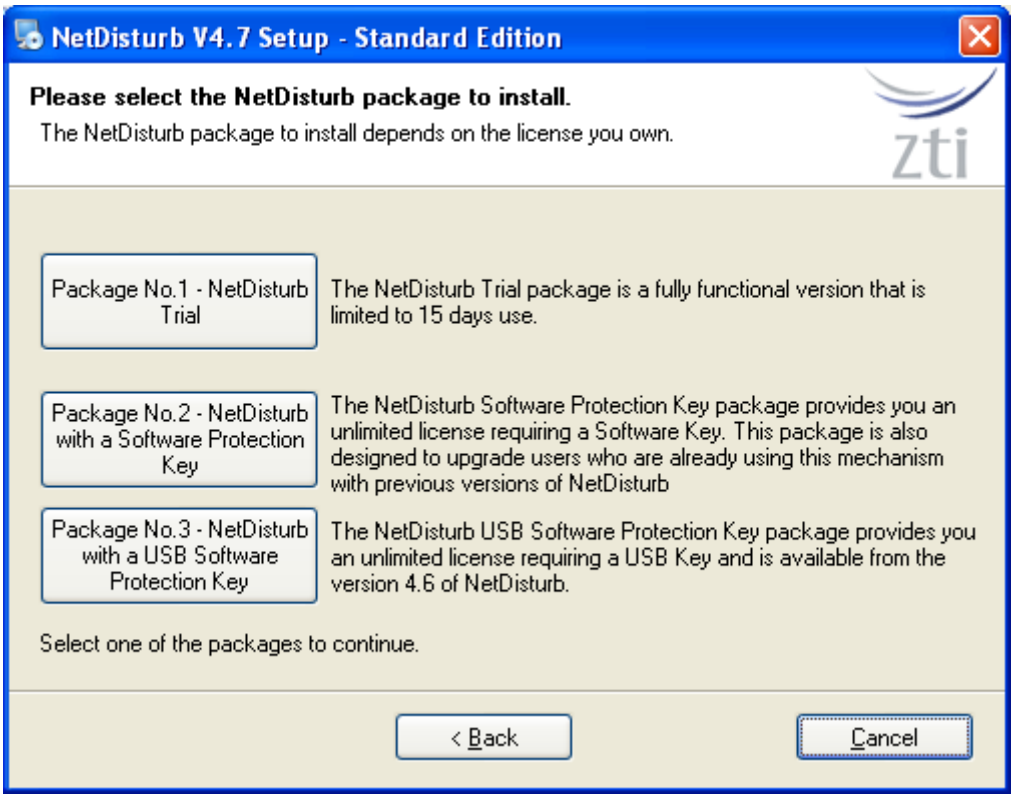
And the following Shortcuts are created:

Start ▶ All Programs ▶ **NetDisturb**

- **NetDisturb** *(start both Server and Client)*
- **NetDisturb Client Only**
- **NetDisturb Server Only**
- **Read Me First**
- **Uninstall NetDisturb**
- **User Guide**
- **USB Key Viewer** *(USB Software Protection Key version only)*

3.8 How to reinstall another package?

If you already have installed one of the **NetDisturb V4.6** packages, click Setup_NetDisturb.exe and select, in the window below, the new package you want to install.



3.9 How to transfer the software to another computer?

For the users having the NetDisturb USB dongle: install the software on the target machine by using the Package No.3 ("NetDisturb with a USB Software Protection Key"), and then plug the USB dongle before running the software on this machine.

For the users having only the Software Protection Key, install the software on the target machine by using the Package No.2 ("NetDisturb with a Software Protection Key"), and then refer to paragraph *"**4.2.2 Software Protection Key Transfers**"* to know how to transfer the Software Protection Key.

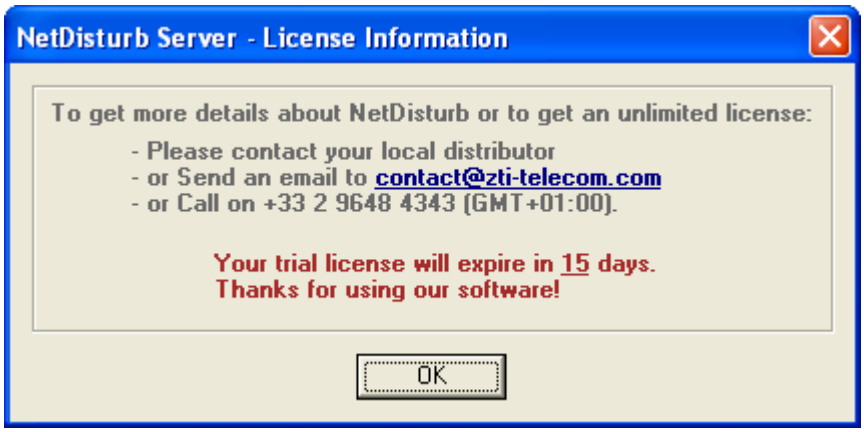
Part 4 How to handle your license?

4.1 NetDisturb Trial

You don't need any license to install the **NetDisturb Trial package**. After the first run of **NetDisturb Server,** the **NetDisturb Trial package** can be used during 15 days.

4.1.1 NetDisturb Server License Information window

When you run **NetDisturb Server,** the information about your trial license is displayed, as shown below.



You are now able to use **NetDisturb** during the next 15 days.

4.1.2 End of the fifteen-day trial period

Once the trial period is over, you can't use **NetDisturb** anymore, see below:

When you press the **OK** button, **NetDisturb** will stop running.

To continue to use **NetDisturb please contact you local distributor or ZTI** to get an unlimited license.

4.2 NetDisturb & Software Protection Key

Licensed users of **NetDisturb** that are already using the Software Protection Key should not need to refer to the section 4.2.1. To transfer the owned Software Protection Key to another PC or to another directory, please go directly to section 4.2.2.

4.2.1 Installation of the Software Protection Key

*This software is licensed on a per workstation basis. This means that you will need to get a separate license for each machine you will install it on. Each licensed copy of the software installed on a system has a unique **Site Code** that requires a corresponding unique **Site Key** to work.*
A period of 15 days is automatically enabled at the first installation of the software. If you try to install the software again, the Software Protection Key will disable the trial period.

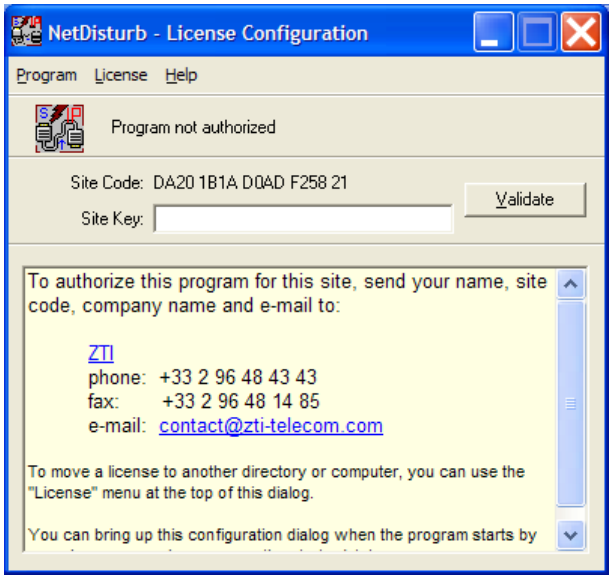
If you want to configure your Software Protection Key before the time-limited period end, press **Enter** just after launching the **NetDisturb** when the following message is displayed:

Then, you will see the following Software Protection Key configuration window:

*At the end of the trial period when you launch **NetDisturb**, the same Software Protection Key configuration window appears, but saying "Program not authorized" instead of showing the remaining days of use.*

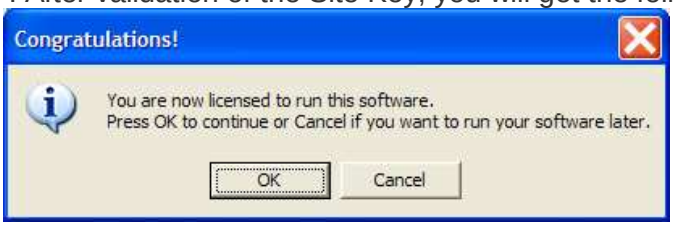
To get the **Site Key** and obtain a permanent license, please send an email to contact@zti-telecom.com or contact@zti.fr with the following information:

- The **Site Code** (you can copy and paste the Site Code displayed in the license window)
- The name of the software: **NetDisturb**
- The OS used
- Your details
- The purchase order's number and date of purchase



We will then email you the **Site Key**. You can now close the license's window.

After you have received the email with the **Site Key**, open the Software Protection Key configuration window again by pressing the Enter key as explained before. Copy the Site Key in and then click "Validate". After validation of the Site Key, you will get the following message:



- Important: one **Site Code** is associated with one **Site Key**, and only one. A **Site Code** is unique for each PC installed. For security reasons, as soon as you validate a **Site Key** (trial or unlimited), the Software License program generates a new **Site Code** automatically.
- For any question or further information, please contact our technical support:
  Email: support@zti-telecom.com or support@zti.fr
  Phone: +33 2 9648 4343
  Fax: +33 2 9648 1485

*When you launch **NetDisturb** with a permanent Software Protection Key, you will see the following window:*

4.2.2 Software Protection Key Transfers

A Software Protection Key transfer is not a duplication of any type. Please contact ZTI or your authorized distributor for site Software Protection Key information and for several Software Protection Keys purchase.

Software Protection Keys can be transferred using one of the following methods:

⇨ **Direct transfer:** move the Software Protection Key to another directory of the same PC or between two PCs linked to the same network.

⇨ **Transfer by media:** move the Software Protection Key from a source PC to a target PC by using a floppy disk or USB key.

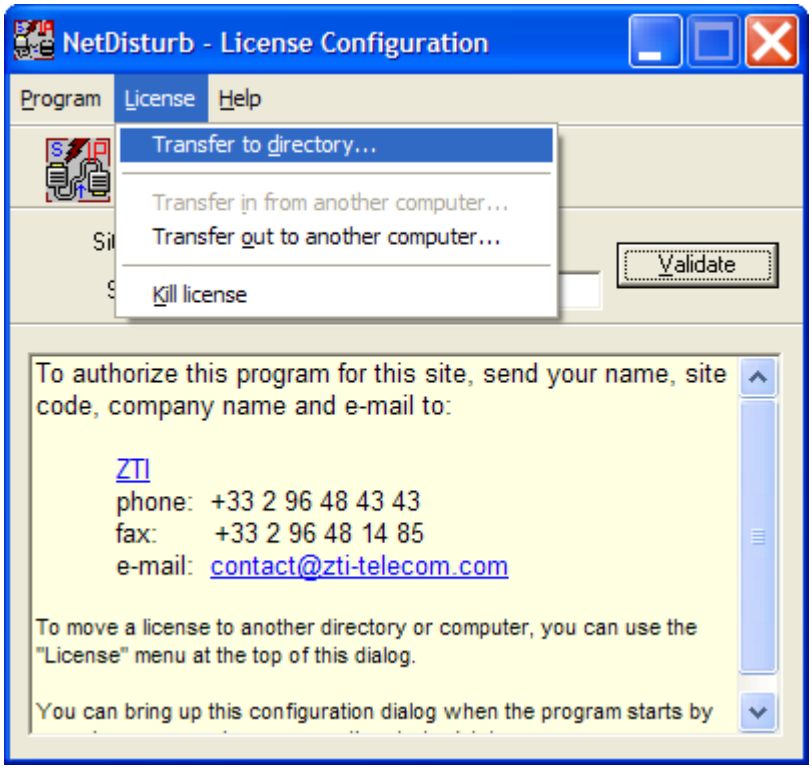
4.2.2.1 Direct Transfer: move the Software Protection Key from one local directory to another

This transfer mechanism must be used to move a Software Protection Key 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 **NetDisturb** folder) to the target directory.
  For example from "C:\Program Files\NetDisturb" to "C:\Temp\NetDisturb"

- Then run the program from its original directory (*from "C:\Program Files\NetDisturb"*). When the Software Protection Key configuration window appears, press **Enter** and select "License > Transfer to directory …" in the License menu as shown below:



- Provide the path name of the target program (*for example C:\Temp\NetDisturb\Server\NetDisturbServer.exe*)
- The Software Protection Key is now transferred to the new directory.

4.2.2.2 Transfer by Media (USB key) from a source PC to a target PC

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

To transfer the Software Protection Key from the source PC (PC #1) to the target PC (PC #2), proceed as described in the following order:

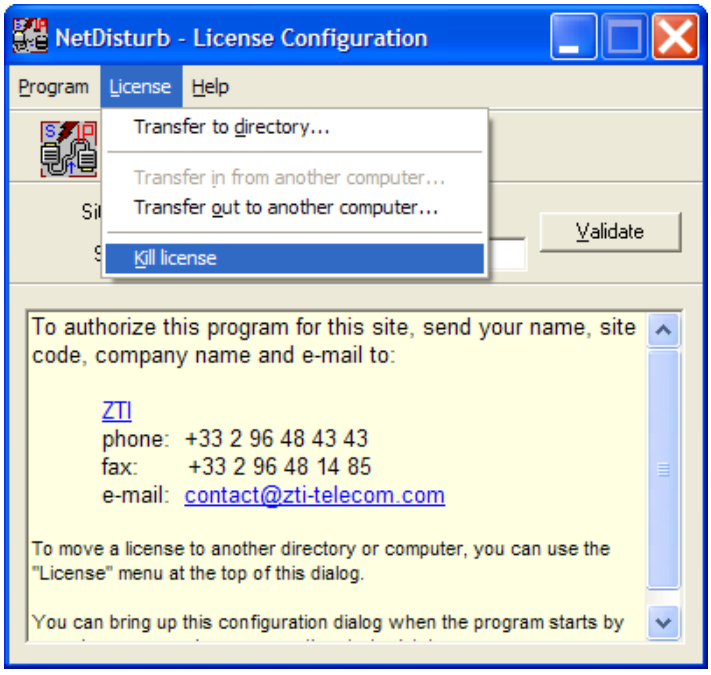
1) First install the program on the target PC (PC #2).

2) Run the software on PC # 2 and kill the time-limited Software Protection Key in order to get an unauthorized license on this PC.

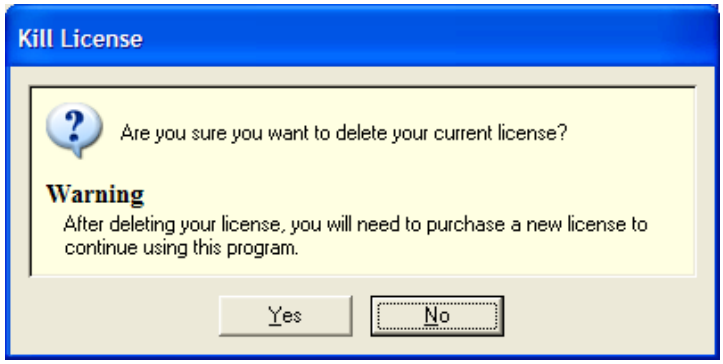
If the "Transfer in from another computer …" item of the license menu is disabled, you must kill the Software Protection Key.

How to kill the Software Protection Key?

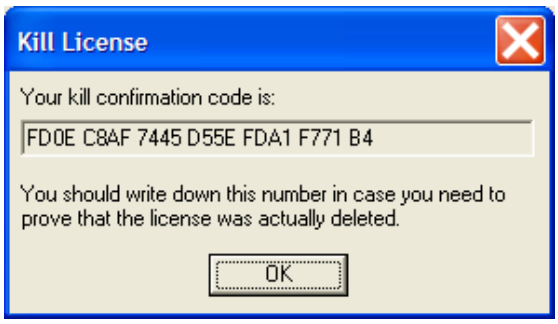
When the Software Protection Key configuration window appears, press **Enter** and select “License > Kill license” in the license menu.



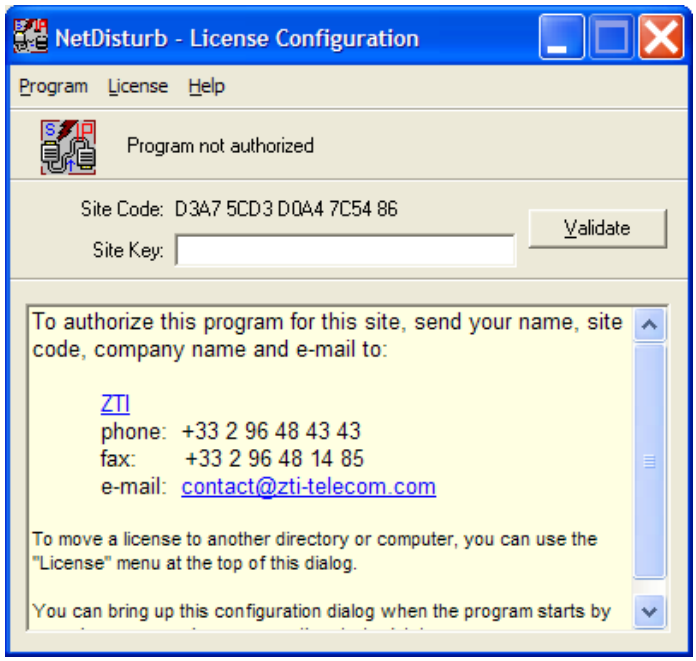
A message box will appear:



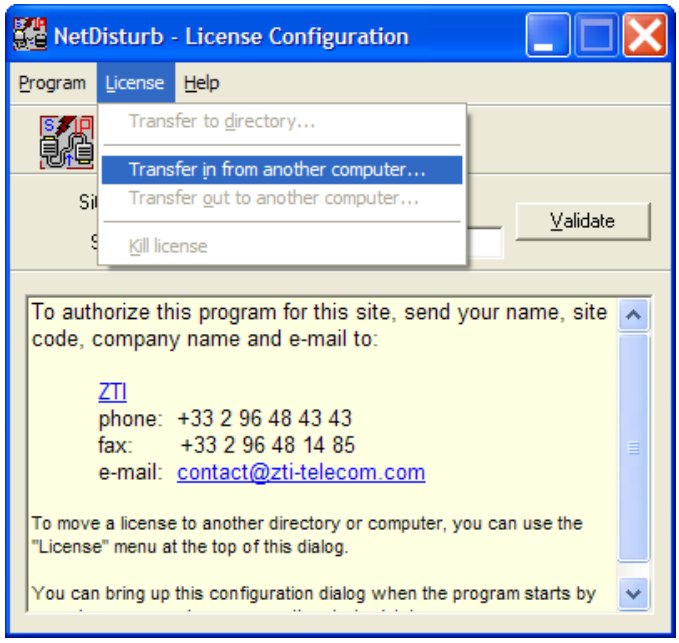
Press 'Yes' to kill the Software Protection Key and a confirmation code is displayed:



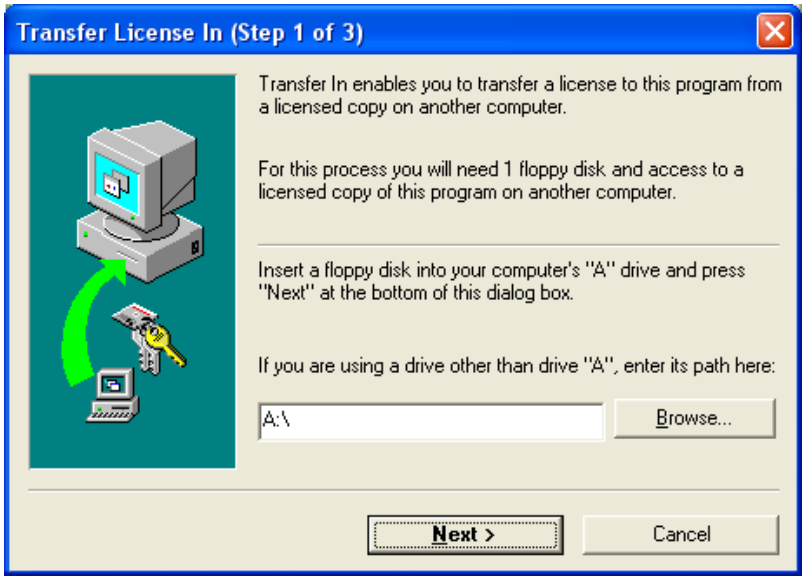
Click 'OK' and the Software Protection Key window displays now "Program not authorized":



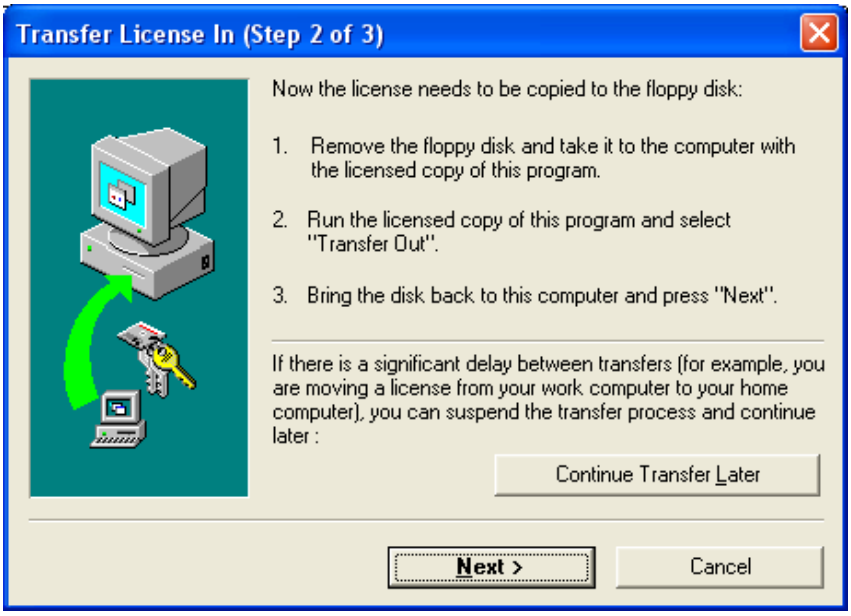
3) Select “License > Transfer in from another computer …” from in the Software Protection Key License menu:



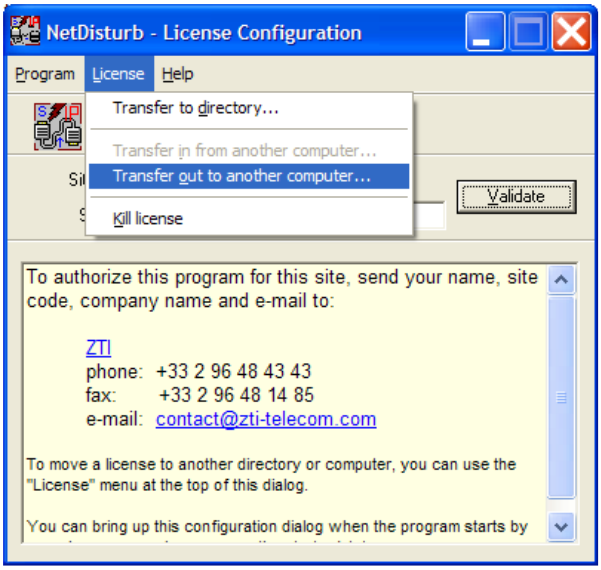
The "Transfer License In (Step 1 of 3)" window is displayed:



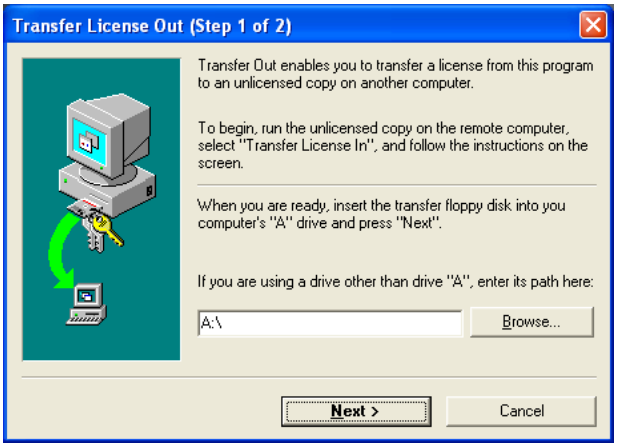
4) Insert a floppy disk or use a USB key as requested in step 1 of 3 and specify the path. Then press “Next >”: the "Transfer License In (Step 2 of 3)" window is displayed:



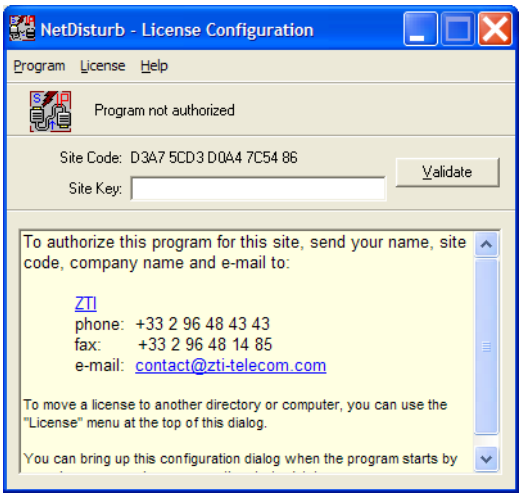
5) Go to the source PC (PC #1) and insert the media (USB key or floppy disk). Then start the program on PC #1. When the license configuration window appears, press **Enter** and select “License > Transfer out to another computer …” as shown below:



The following window is displayed:



Input the media path (USB key or floppy disk) and then press "Next >". When the license is put on the media, you get the “Program not authorized” message:



*You can check that the Software Protection Key is not available anymore on the source PC since the **NetDisturb** software license is on a workstation basis.*
Contact us to get information for a Site Software Protection Key (contact@zti.fr or contact@zti-telecom.com).

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 permanent Software Protection Key is now transferred from the source PC to the target PC, and you get the following message:

Click Finish to continue.

4.3 NetDisturb & USB Software Protection Key

The USB Software Protection Key is the most flexible way to transfer your license to any other PC. Plug it in the computer you want to use **NetDisturb** on.

If you are a user of a previous version of **NetDisturb (version 4.5 and under)** and if you are interested with the USB Software Protection Key, please contact ZTI Sales Offices (Email: sales@zti-telecom.com).

Part 5 Uninstall NetDisturb

To uninstall **NetDisturb,** please select “Uninstall NetDisturb” by using the shortcut:

Start ▶ Programs ▶ NetDisturb

All installed components of **NetDisturb** will be removed including the **NetDisturb** driver.

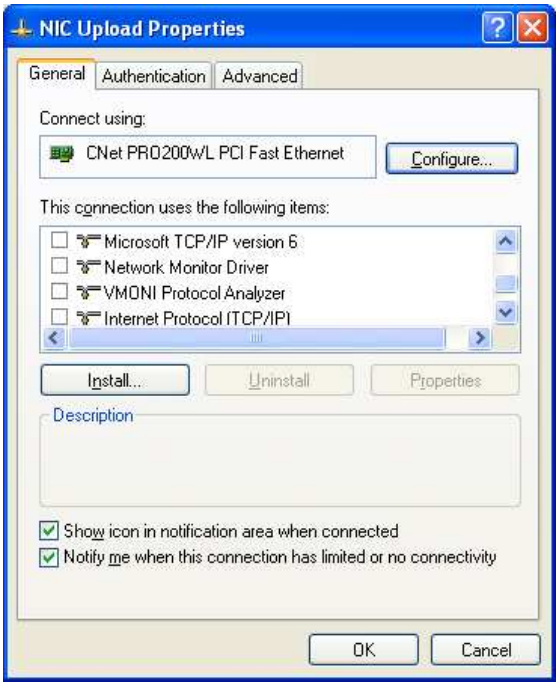
Part 6 Run NetDisturb

6.1 IMPORTANT STEP: I must configure the NICs that will be used and unselect all protocols before running NetDisturb

The setup procedure realizes the installation of the **NetDisturb** driver transparently. It will be installed positioned on top of each Ethernet or wireless NIC if the driver of the NIC is NDIS compatible. The **NetDisturb** driver sets in the kernel of Windows 2000, XP or Server 2003 and handles the exchanges between two NICs. The **NetDisturb** driver linked to the selected NICs is available and transparent. It doesn't appear in the protocol list.

Now there is an important manual operation to do before using NetDisturb:

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



Example of NIC with all protocols unchecked

6.2 Launch NetDisturb

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

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

To run the software in this order, click on:

Start ▶ All Programs ▶ **NetDisturb** ▶ **NetDisturb** (start both Server and Client)

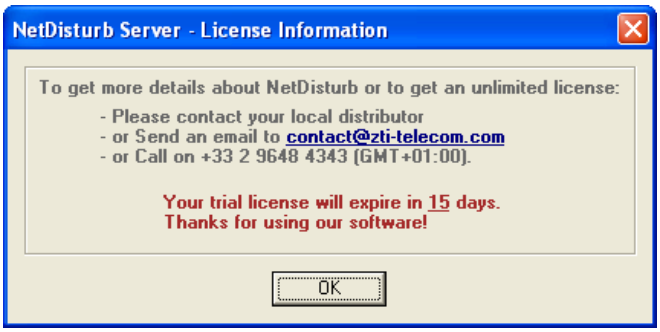
6.3 First Run

1) The NetDisturb Server startup

NetDisturb Server is started automatically when using the **NetDisturb** shortcut (start both Server and Client).

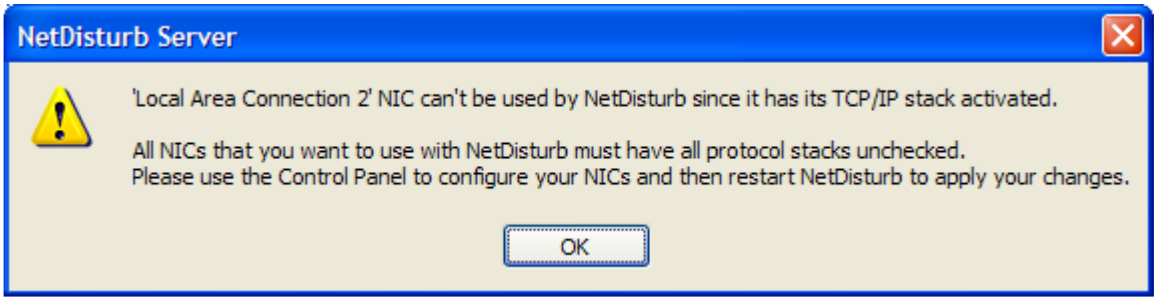
*You may also start the server independently, for instance when you are using a remote configuration where **NetDisturb Server** doesn't run on the same PC as **NetDisturb Client**.*
*To start the **NetDisturb Server** alone, use the Windows start menu:*
Start ▶ All Programs ▶ **NetDisturb** ▶ **NetDisturb Server**

After a few seconds and depending on your license, you will get one of the following license windows:

15-day trial version license	***Permanent Software License***
	

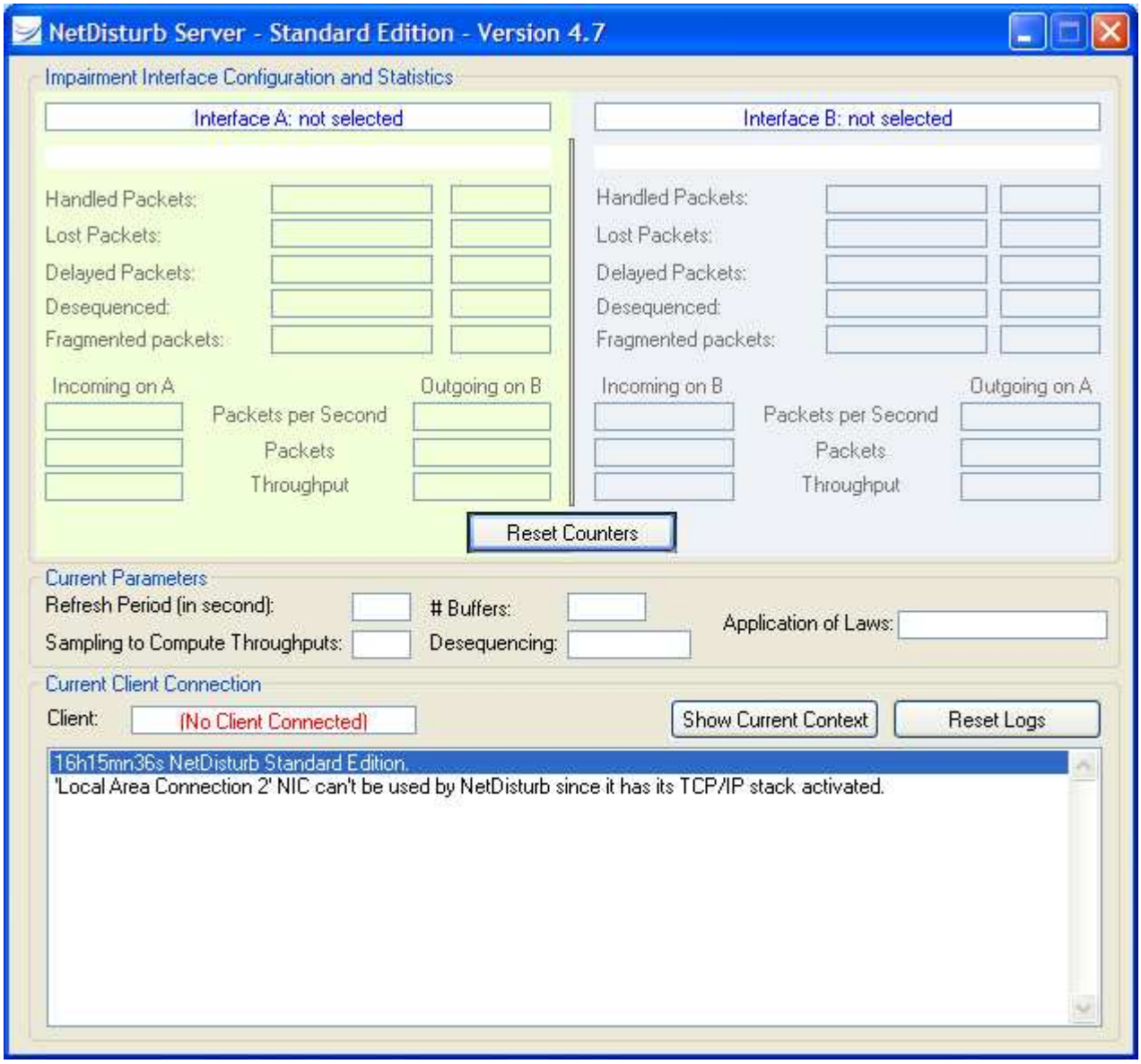
USB Software Protection key
When you use a USB Software Protection key, there is no window displayed!

If **NetDisturb** has detected some configuration issues, a list of NICs, which can't be used by **NetDisturb** will be displayed as shown in the warning message below:



Click on OK to validate (you will configure later).

The next window displayed is **NetDisturb Server**



We recommend closing **NetDisturb Server** and then to configure the NICs usable by **NetDisturb** as described in paragraph 6.1 if you didn't configure the NICs before.

2) NetDisturb Client startup

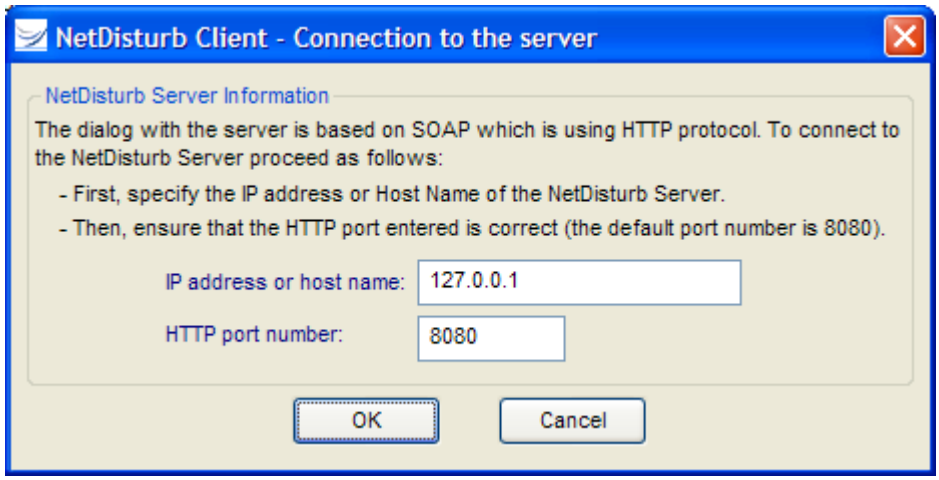
NetDisturb Client is started automatically when using the **NetDisturb** shortcut.
The default connection parameters used to exchange between **NetDisturb Client** and **NetDisturb Server** are:

- **NetDisturb Server IP address or Host Name = 127.0.0.1**

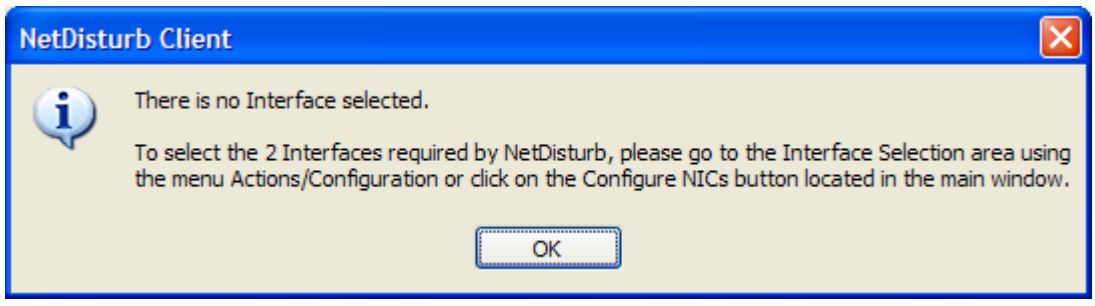
  (127.0.0.1 = default local IP address if the **NetDisturb Server** and the **NetDisturb Client** are installed on the same machine).

- **HTTP Port Number** = 8080

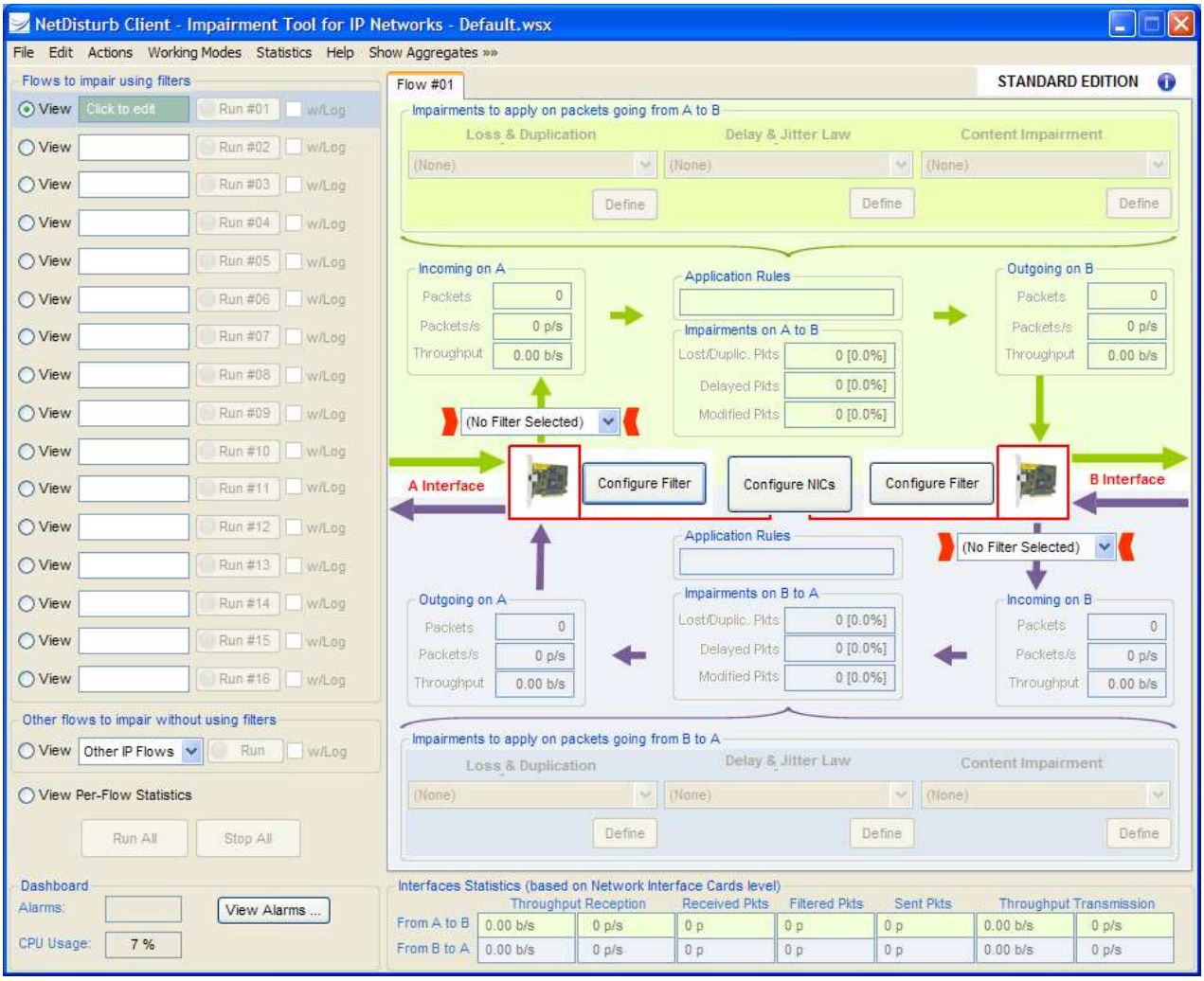
*You may also start the **NetDisturb Client**'s part alone, to connect to a remote **NetDisturb Server.***
*To start the **NetDisturb Client** alone, use the Windows start menu:*
Start ▶ All Programs ▶ **NetDisturb** ▶ **NetDisturb** Client
*When **NetDisturb Client** starts, it will ask you to enter the parameters to connect to the **NetDisturb Server** machine:*



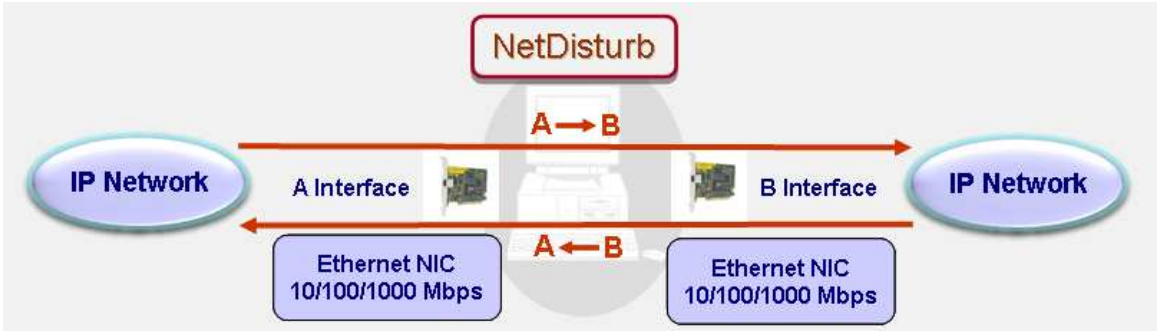
*On the first run, there is no Interface defined. **NetDisturb Client** will tell you how to configure those 2 interfaces.*



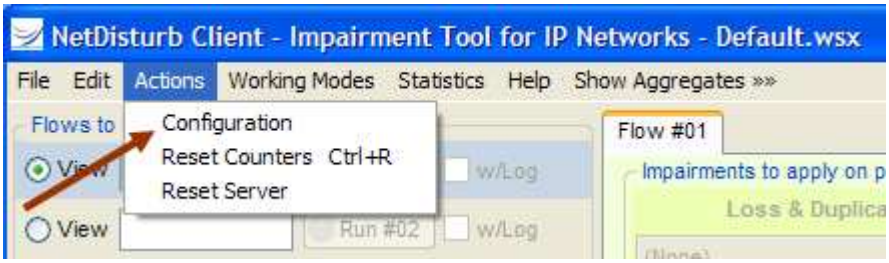
Click “OK” and the **NetDisturb Client** main window will appear:



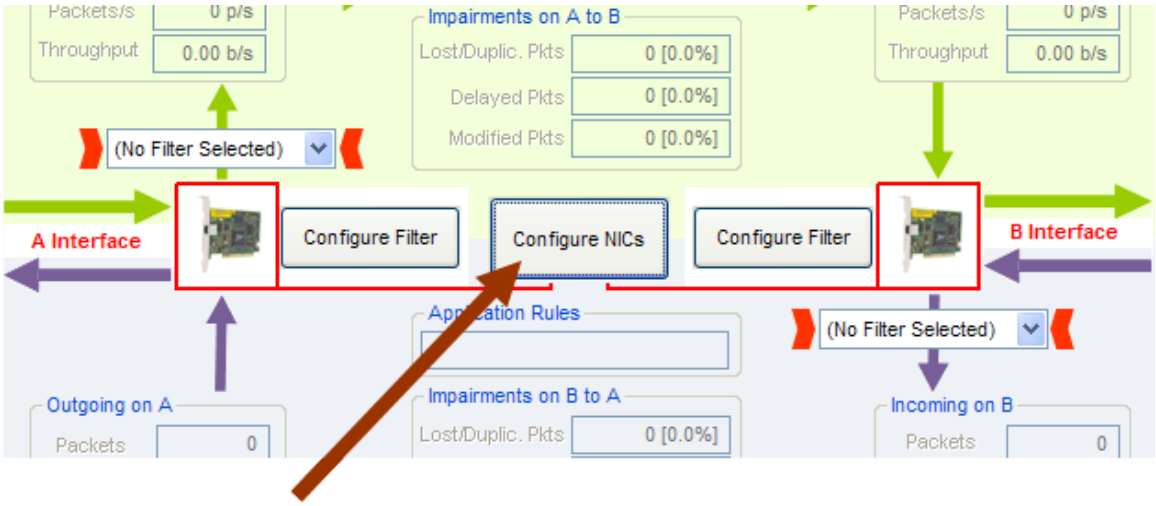
Then, you need to select the NICs (interface A and interface B) that the **NetDisturb** Server is going to use.



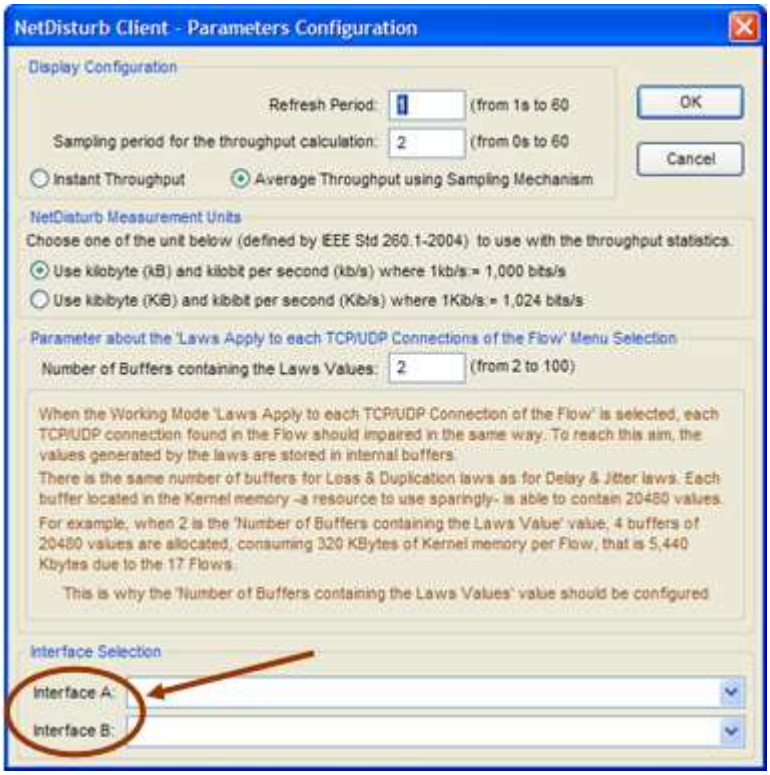
Select “Configuration” in the Actions menu:



or click on the "Configure NICs" button located in the main window:



Then the parameters configuration window is displayed:

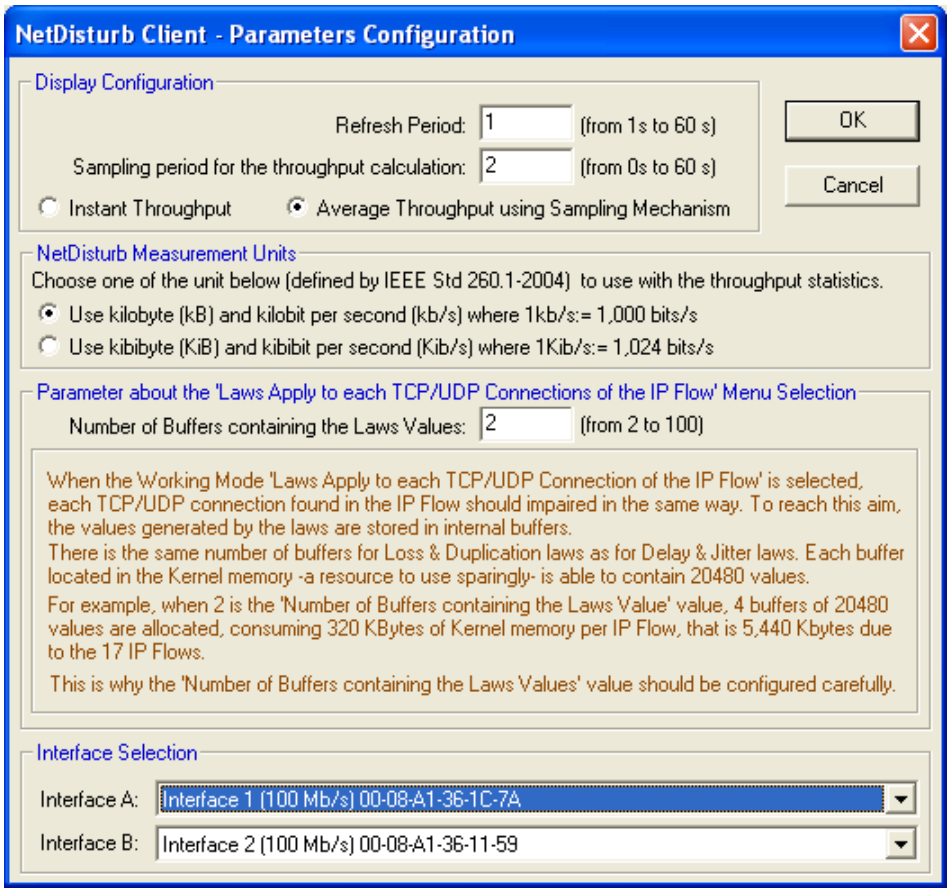


At the bottom of this window in the "Interface Selection" part, select one NIC for Interface A and another NIC for Interface B, and then confirm with “OK”.

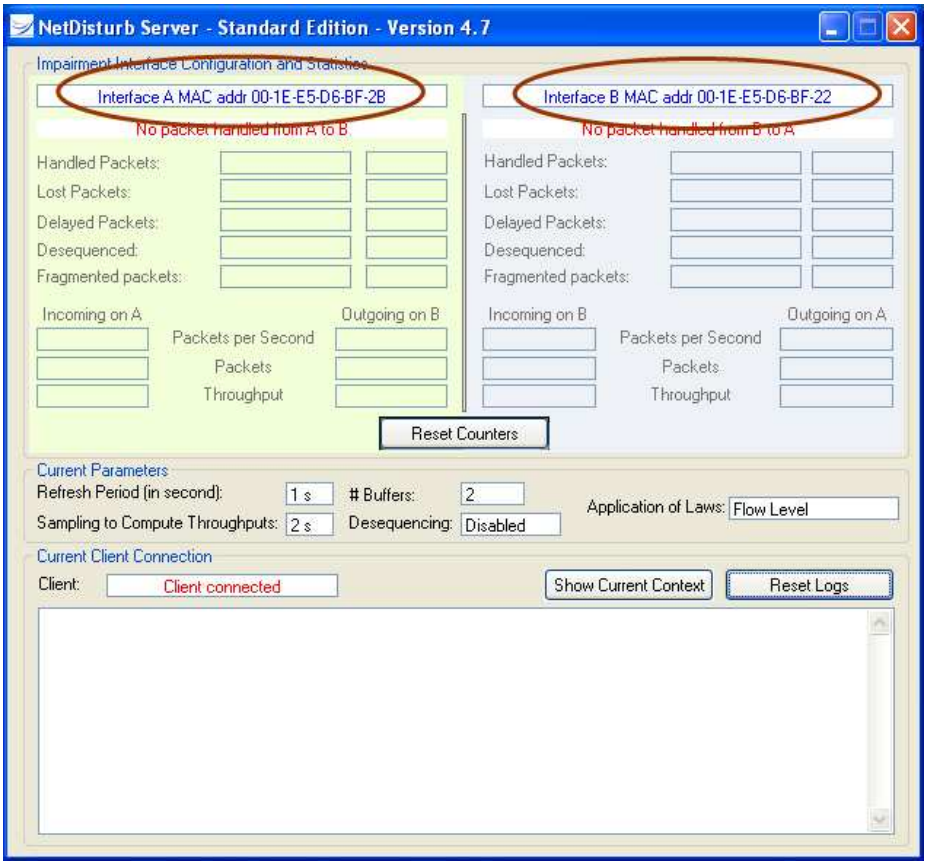
You should see in the combo-box (Interface A or Interface B) all available and operational NICs. If you don't see any NICs, please follow the steps below:

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

Then you should see your installed NICs in the Interface A and B combo-boxes (see the example below):

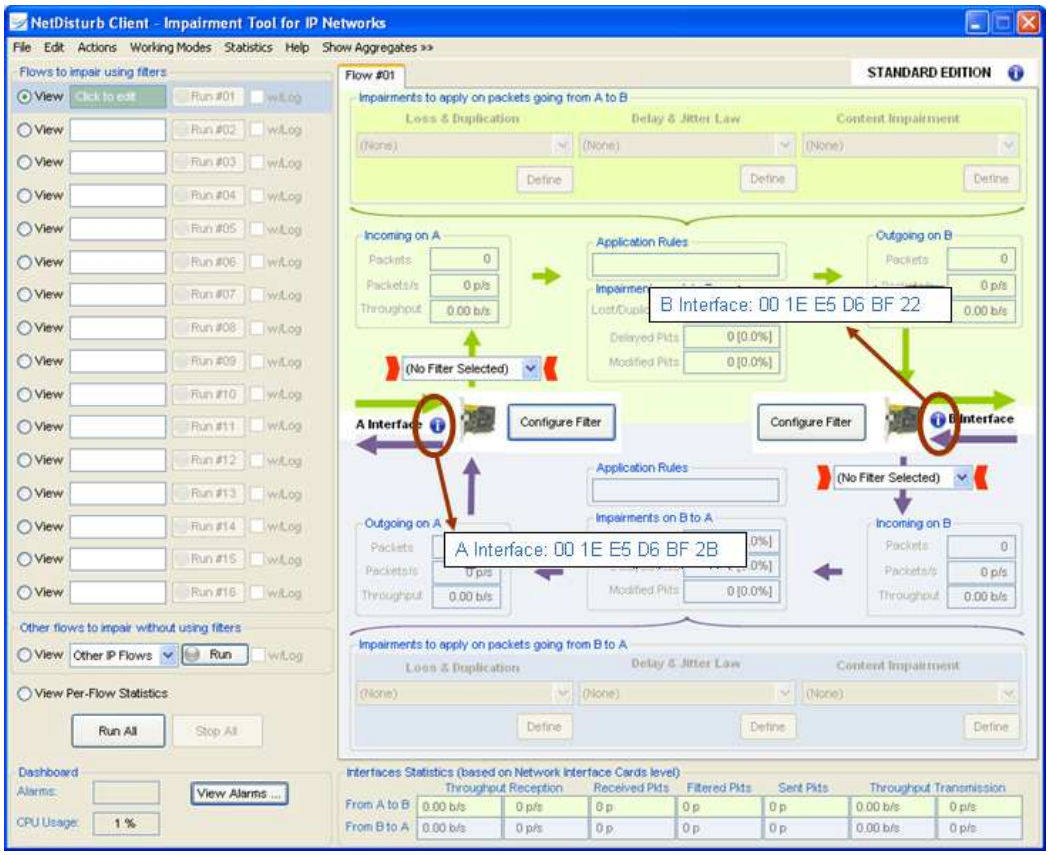


As soon as the configuration is done, the **NetDisturb** Server recognizes "Interface A" and "Interface B" as shown below.



NetDisturb Server *configured with two Ethernet NICs (A and B)*

The MAC Addresses of the selected interfaces are also displayed in the **NetDisturb** Client window by clicking on the ⓘ symbol of each interface:

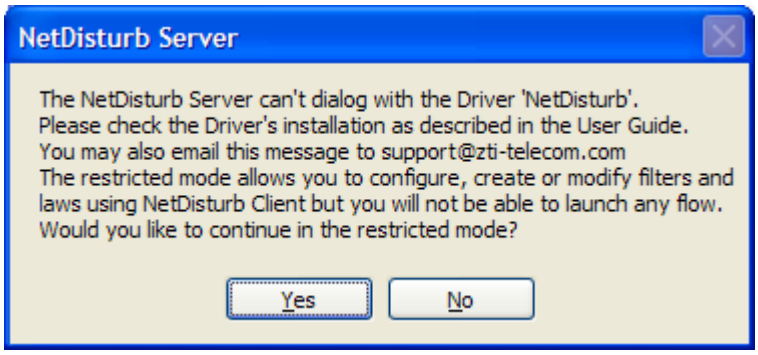


NetDisturb Client *with two Ethernet NICs configured*

6.4 Detailed Description of the Server and Client Startup

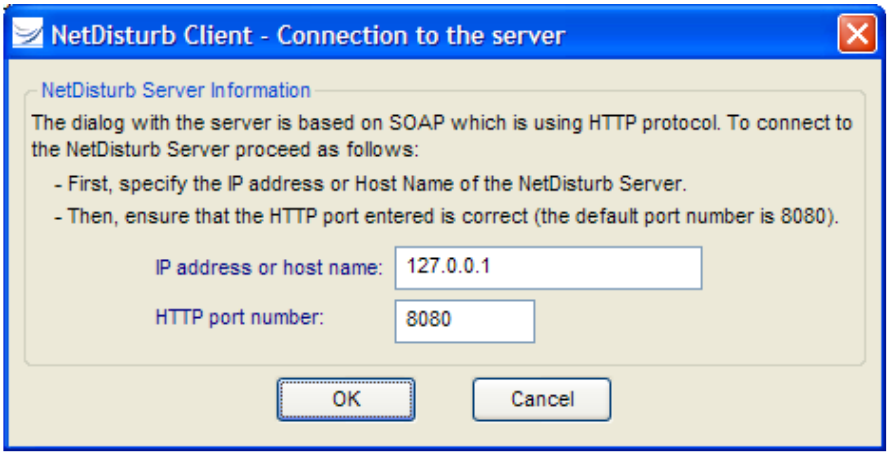
6.4.1 The NetDisturb Server Startup Modes

The level of provided functionalities depends on the availability or not of the **NetDisturb** driver. If the **NetDisturb** driver is lacking, a message warns the user. In that case it is possible to continue in the “restricted mode” where only a few functions are available.



6.4.2 The NetDisturb Client Startup Options

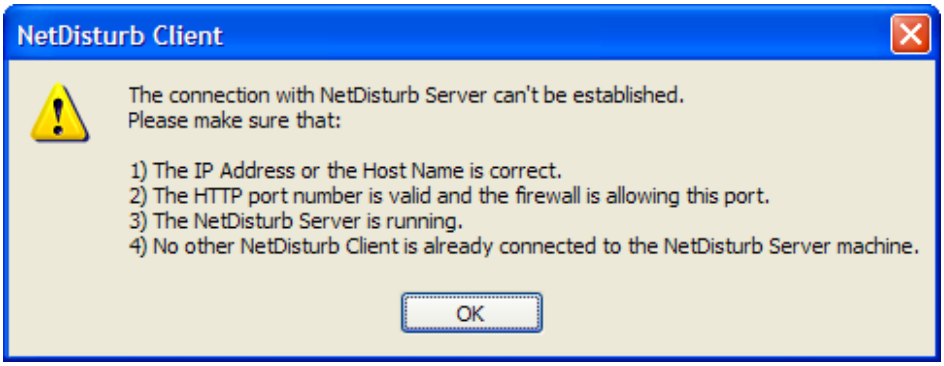
When starting the **NetDisturb Client**, the Connection to Server parameters window is displayed.



This parameters window is made of two sections:
The **NetDisturb** Client needs the following information in order to connect to the **NetDisturb** Server:

- The **NetDisturb** Server IP address
- The **NetDisturb** Server HTTP port number

In case of a connection failure (if one of the parameters is invalid), an error window pops up. To go back to the identification window, just click on the OK button.



Part 7 Using the NetDisturb Client

The **NetDisturb** Client is the main **NetDisturb** User Interface.
With **NetDisturb** Client you can:

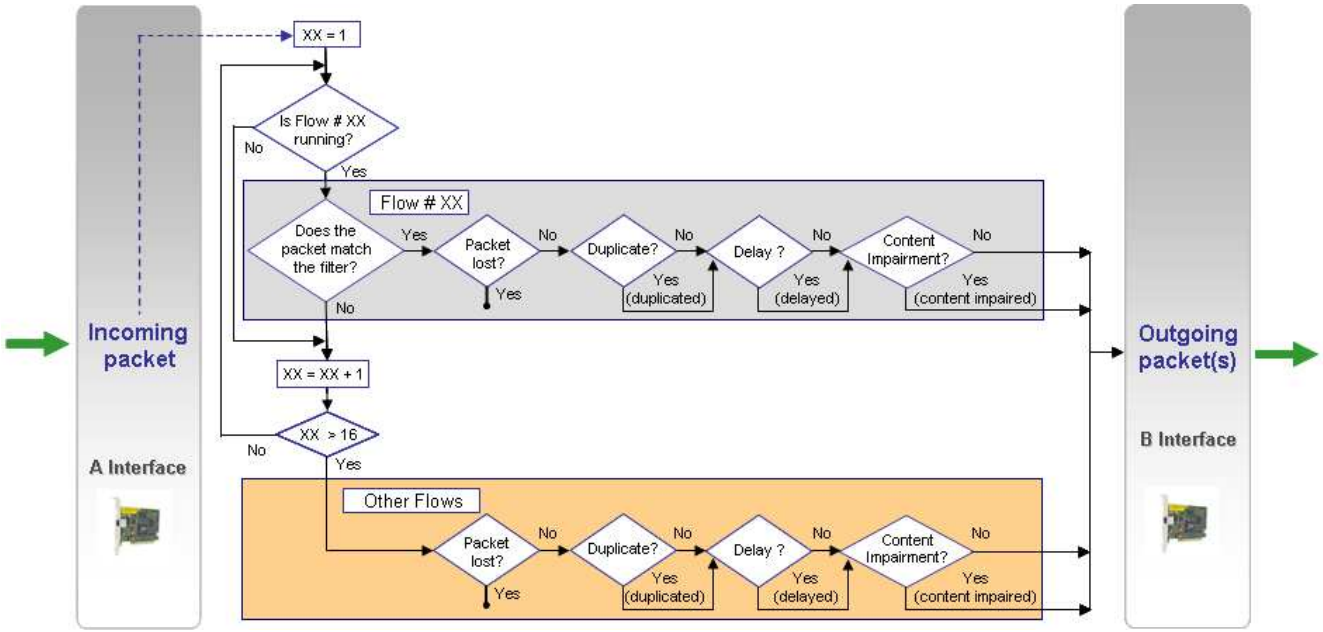
- ⇨ Select packet stream to process and configure impairments to apply,
- ⇨ Run / Stop traffic following the configured impairments,
- ⇨ Open, save… contexts,
- ⇨ Configure the **NetDisturb** Server and **NetDisturb** driver.

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

*To use **NetDisturb**:*
⇨ ***First run NetDisturb Server***
⇨ ***Then run NetDisturb Client***

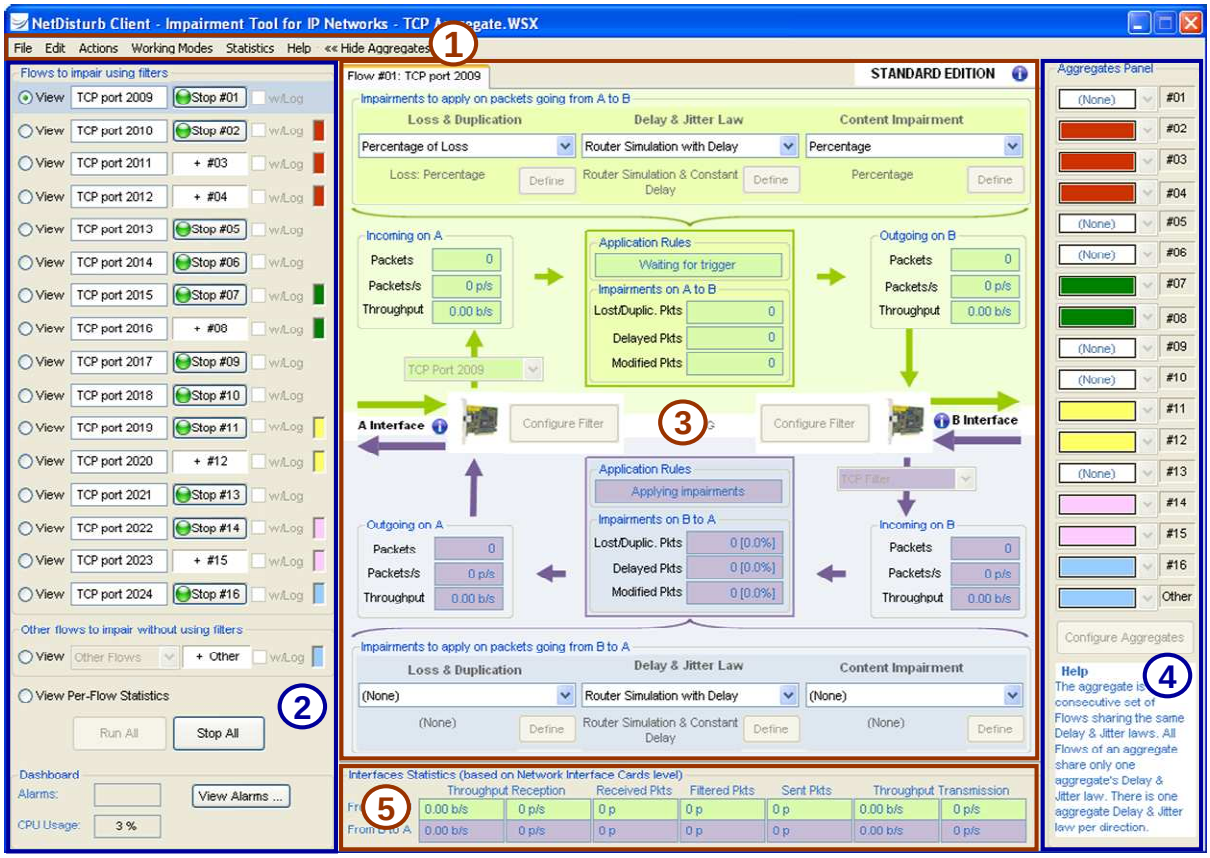
7.1 The NetDisturb Client Main Window

The **NetDisturb** Client main window is displayed after client identification. Traffic and impairment representation on the 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 five areas:



- **(1)** The menu is a standard application menu.
  The items of the menu are detailed in paragraph 7.2 Menu Description.

- **(2)** This area contains several objects:

  ▪ 'Flows to impair using filters' area with for each flow from 01 to 16:
  * View button: to display the characteristics of the selected flow in **(3)**
  * Text box: to enter the name of the flow
  * "Run #xx / Stop #xx" button: to start and stop the flow
  * "w/Log" checkbox: to trace the packets and events per flow (Enhanced Edition only)
  * Colored plot: to indicate if the flow belongs to an aggregate

  ▪ The 'Other Flows to impair without using filters' object allows applying specific loss, delay laws and content impairment laws to non-previously filtered packets

  ▪ The "View-Per-Flow Statistics" magnify summarizes the flows #01 to #16 and the other flows impaired without using the filters.

  ▪ "Run All" and "Stop All" buttons: to start and stop all flows at the same time.

  ▪ ▪ "Dashboard": It includes 'Alarms' returned by the NIC drivers or by the NetDisturb driver when memory errors occur. The CPU usage value is provided for information.

  These areas are explained in paragraph 7.3.

- **(3)** This central-part shows traffic statistics for each Flow #01 to #16 or the 'Other IP Flows'. It is used to create, delete and modify loss/duplication laws, delay/jitter laws, content impairment laws or IP filters.

- **(4)** The 'Aggregates' area allows defining up to 8 aggregates (an aggregate is a consecutive set of IP flows sharing the same Delay & Jitter law). An aggregate is defined with a color and a Delay & Jitter law can be defined for each direction (A → B and/or B→ A).

- **(5)** The total synthesis area is a reference area where statistics information is presented.

7.2 Menu Description

7.2.1 File Menu

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

A context file contains:
- The impairment parameters (selected filter & laws),
- The configuration values.

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

7.2.1.1 File/New

This command opens a new default context (no impairment parameters).

7.2.1.2 File/Open

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

7.2.1.3 File/Save

This command allows saving the parameters and laws in a context file (.WSX file). The contexts saved by this version can't be used by an older version of **NetDisturb**.

7.2.1.4 File/Save as…

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

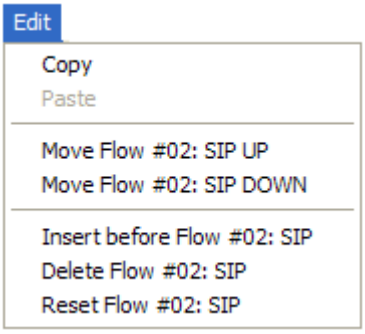
7.2.1.5 File/Recent Files

The 4 most recent files used are displayed at this place.

7.2.1.6 File/Exit

This command stops the **NetDisturb** Client. If changes where made you get the opportunity to save them in a context file.

7.2.2 Edit Menu



The edit menu helps to handle the IP Flows.

7.2.2.1 Edit/Copy

The Copy item makes a copy of the current Flow into memory for further use. Copy includes the current selected filter, Loss & Duplication Law, Delay & Jitter Law and Content Impairment Law for the both directions. The Flow mnemonic is also concerned.

7.2.2.2 Edit/Paste

The Paste item changes the current Flow parameters by the previously memorized Flow parameters (use of the previous Copy command). It applies to the Filter, the Loss & Duplication Law, the Delay & Jitter Law and Content Impairment Law for the both directions, and to the Flow mnemonic name.

7.2.2.3 Edit/Move xxx Up

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

7.2.2.4 Edit/Move xxx Down

The Move Down item moves the flow location to one position down. The Move Down item includes the item's mnemonic on which the operation applies. For example 'Move Flow #04 Down' switches Flow #04 with Flow #05, where the content of Flow #04 is moved into the fifth position, while the content of Flow #05 is moved into the fourth position. The Flow mnemonic is also concerned.

7.2.2.5 Edit/Insert before xxx

The 'Insert before …' item makes a room available at current item location, whose mnemonic is added. The items located after the current item move one position down; this includes the current

item. The current item becomes empty. The 16th item is lost. If the current item is the 16th, no change appends to the 15th previous but the current – the 16th - is reset.

7.2.2.6 Edit/Delete xxx

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

7.2.2.7 Edit/Reset xxx

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

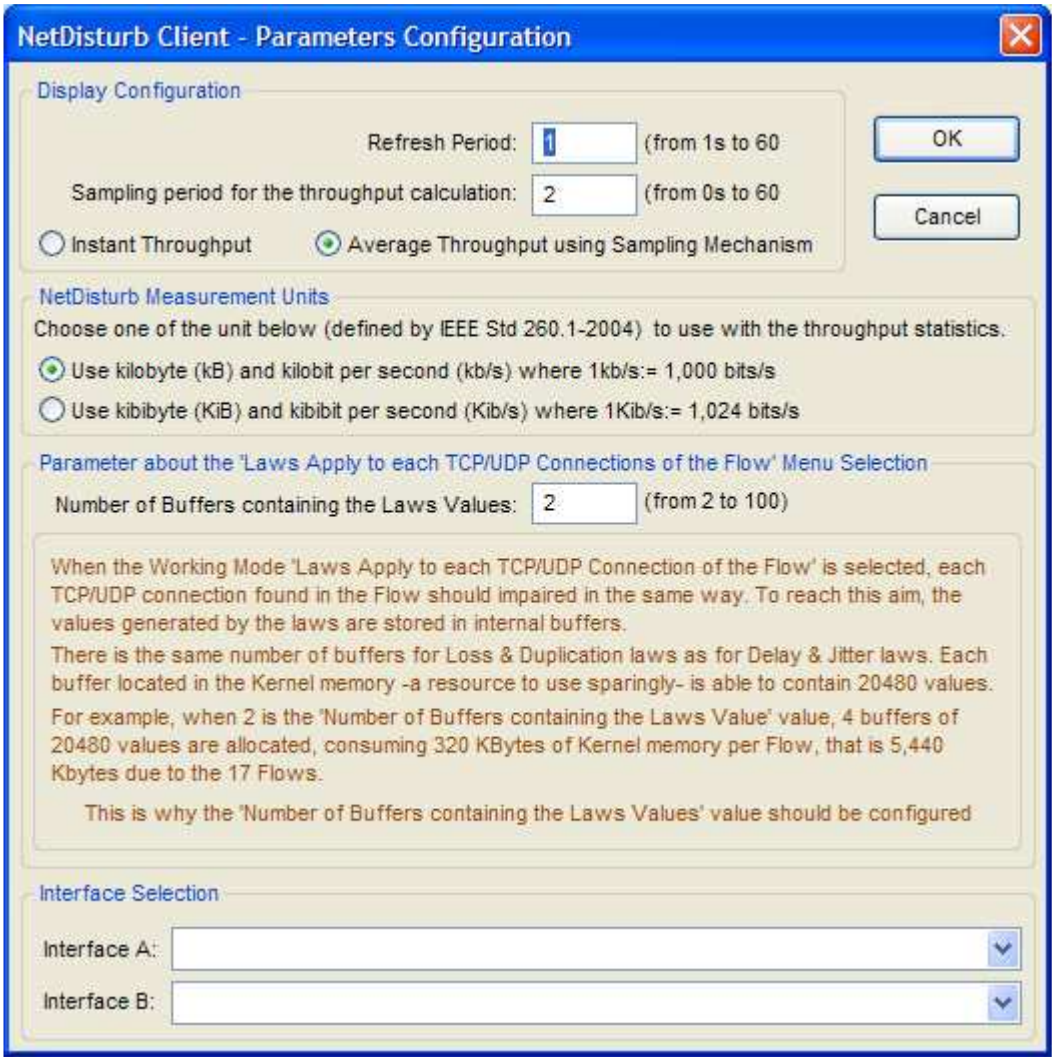
7.2.2.8 Edit menu and the Aggregates

The aggregate configuration of a Flow is not changed by an action from the Edit menu.

7.2.3 Actions Menu

7.2.3.1 Actions/Configuration

Select the "Configuration" item in the Actions menu to display the Parameters Configuration window:



This window is divided in four parts: Display configuration, Measurement Units, Parameter about the 'Laws apply to each TCP/UDP connection of the Flow' selection and Interface Selection.

⇨ Display configuration

From this section you can:

- Define the refresh period for the display of GUI's counters
- Define the sampling period for the throughput calculation
- Define the way the throughput will be processed (instant or average). The average throughput is based on the latest x seconds statistics (x is the sampling period). Instant computing means computing with value of the latest second.

*Define an average throughput with a sampling period of 0 allows obtaining an average throughput on the whole period of the **NetDisturb** use (since the last Reset).*

⇨ Parameters applying to measurement units

- Use kilobit: in this case a kilobit/s (kb/s) is equal to 1,000 bits/s.

Display	Meaning
10 b/s	10 bits per second
1 kb/s	1 Kilo bits per second (1,000 b/s)
1 Mb/s	1 Mega bits per second (1,000,000 b/s)
1 Gb/s	1 Giga bits per second (1,000,000,000 b/s)
1 Tb/s	1 Tera bits per second (1,000,000,000,000 b/s)
1.23^65	1.23 x 10^65 bits per second

- Use kibibit: in this case a kibibit/s (Kib/s) is equal to 1,024 bits/s.

Display	Meaning
10 b/s	10 bits per second
1 Kib/s	1 Kibibits per second (1,024 b/s)
1 Mib/s	1 Mibibits per second (1,048,576 b/s)
1 Gib/s	1 Gibibits per second (1,073,741,824 b/s)
1 Tib/s	1 Tibibits per second (1,099,511,627,776 b/s)
1.23^65	1.23 x 10^65 bits per second

⇨ Parameter about the 'Laws apply to each TCP/UDP connection of the Flow' selection

This parameter (number of buffers containing the law values) is used when the following working mode is selected: "Laws apply to each TCP/UDP connection of the Flow" (see paragraph 7.2.4.2), i.e. each TCP/UDP connection found in the Flow should be impaired in the same way. To reach this goal, the values generated by the laws are stored in internal buffers. There is the same number of buffers for the Loss & Duplication laws as for the Delay & Jitter laws. Each buffer located in the kernel memory of the NetDisturb Server machine – a resource to use sparingly, is able to contain 20,480 values.

*The number of buffers defines the number of values (delay or loss) kept by the **NetDisturb** driver and used for each Connection of a Flow.*
One buffer contains 20,480 values and the minimum number of buffers is 2.
*With this working mode, the **NetDisturb** Server generates delay and loss values as much as the **NetDisturb** driver can keep.*
*When the **NetDisturb** driver detects a new flow, it gets its own pointer to loose and delay values exclusive of the 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.*

Content Impairment Laws are not concerned by the working modes.

⇨ Interface selection

This section allows selecting the Ethernet NICs to use for the interfaces A and B.

7.2.3.2 Actions/Reset Counter

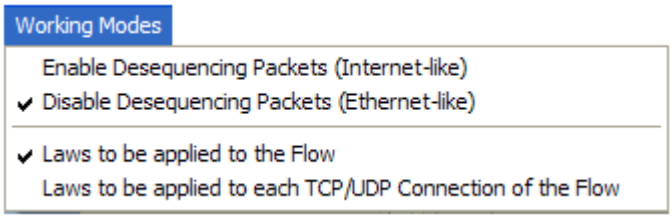
The Reset Counter impacts both the local Client and Server counters. All statistical counters and percentages are set to 0.

7.2.3.3 Actions/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 you should restart the **NetDisturb** Server and Client manually.

To stop and free pending packets, you should reset the server.
When you stop the Flow, pending packets remain in the output queue.

7.2.4 Working Modes Menu



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

The **NetDisturb** driver analyzes the IP packets to split them into the 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 for example.

7.2.4.1 Working Modes :: Enable & Disable Out-of-Sequence 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.
The **NetDisturb** Driver can simulate an Internet network or can react as Ethernet does.

How **NetDisturb** creates an out-of-sequence case?

It may append a delay applied 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.

In such case, what's happening when the Disable Out-of-Sequence Packets is selected?

When a packet should be sent before previous ones and the Out-of-Sequence option is disabled, the packets remain in order. The delay of the older packets is changed to take into account the delay of this new packet i.e. all older packets in the queue get the same *time-to-send* value that the new packet. When the *time-to-send* is reached, all packets are sent in order, creating a burst of packets when the queue is big.

7.2.4.2 Working Modes :: Laws apply to the Flow or to each TCP/UDP Connection of the Flow

- Laws to be applied to the Flow

  When the 'Laws Apply to the Flow' option is selected, every packet matching the Filter requirements is considered belonging to the same flow. Processing is carried out in "continue". When you define to loose 1 packet on 3, the third received packet is lost, whatever the TCP/UDP connection it belongs to.

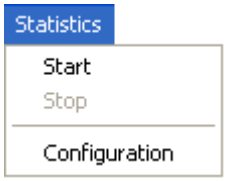
- Laws to be applied to each TCP/UDP connection of the Flow

  When this option is selected the **NetDisturb** driver analyses each IP packet trying to put the IP packet into a TCP or UDP connection by using the following parameters: protocol, IP addresses and port numbers. If the connection doesn't exist, a new one is created.

  Let's take the same example as above: loose 1 packet on 3.
  In that case, the third packet of each TCP or UDP connection will be lost.
  Up to 10,000 connections can be handled simultaneously.

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

7.2.5 Statistics Menu



The **NetDisturb** Client statistics can be saved in a text file. The values saved are shown in the 'View Per-Flow Statistics' (see 7.3 for more details). They are saved at the same rate they are visually refreshed.

You can select the configuration dialog box to save the statistics of each Flow in the statistics file.

7.2.5.1 Statistics/Start

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

Each following record gets the format:

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

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

The throughput values are expressed in Kbps or Kibibit per second (more information is available in paragraph 7.2.3.1 Actions/Configuration).

7.2.5.2 Statistics/Stop

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

7.2.5.3 Statistics/Configuration

This option allows defining various configuration parameters.

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

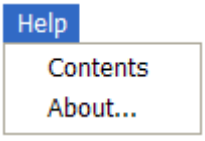
- **(1)** Filename: The filename edit box contains the target file name where statistics will be written. If the file still exists, it will be overwritten.

- **(2)** Tick the Flow(s) to Export: This section is used to select Flows to include into the statistics file. Flow #01 to Flow #16, plus the "Other IP Flows" can be selected. The Total Synthesis **(3)** refers to the bottom part of the Client Windows (Part 7 in the detailed description 7.1).

- **(3)** Include the Total Synthesis: This option is used to add the total synthesis items into the data saved.

- **(4)** Tick the related Statistics to export: This section is used to select the statistic items to save.

7.2.6 Help Menu



7.2.6.1 Help/Contents

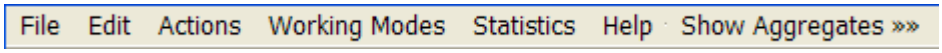
This command opens the **NetDisturb** User Guide as a PDF file. So you need a PDF reader to view the contents.

7.2.6.2 Help/About

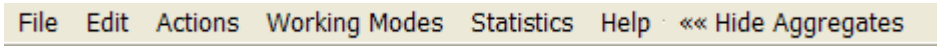
This command displays the version number and copyright of the software.

7.2.7 Hide or Show Aggregates Menu

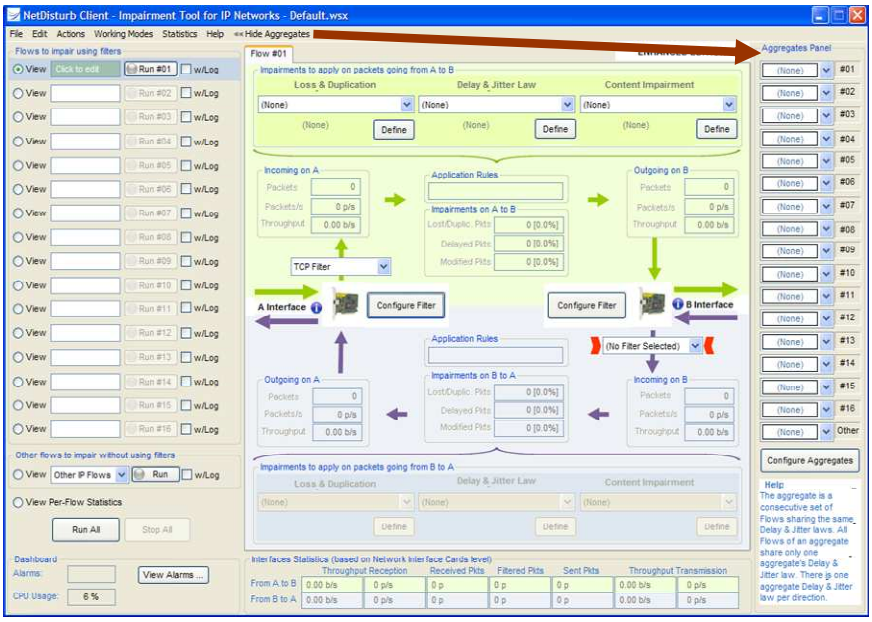
This menu has two states:



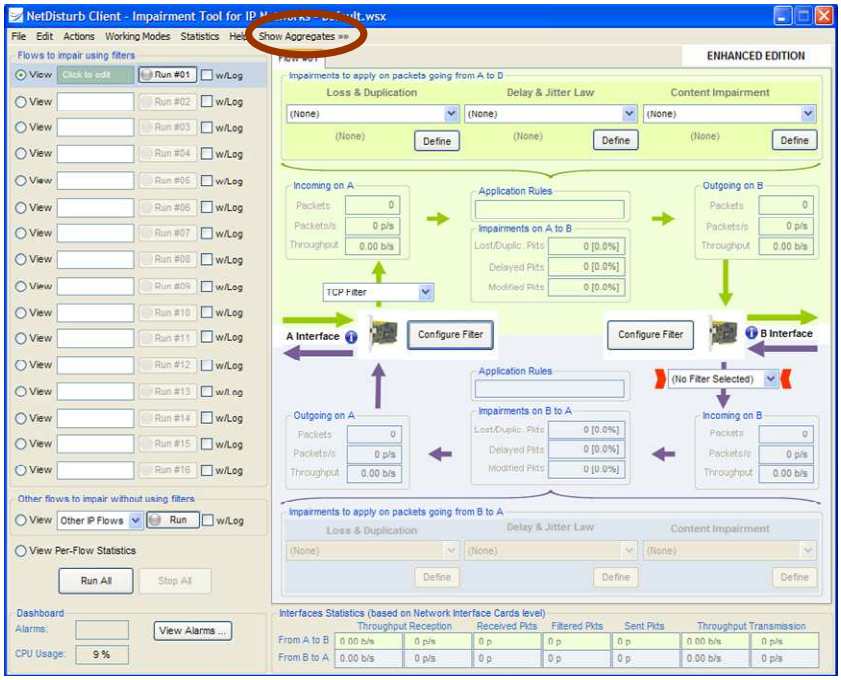
Or



By clicking on the 'Show Aggregates' menu, the **NetDisturb** Client window is enlarged on the right and shows the aggregates area:



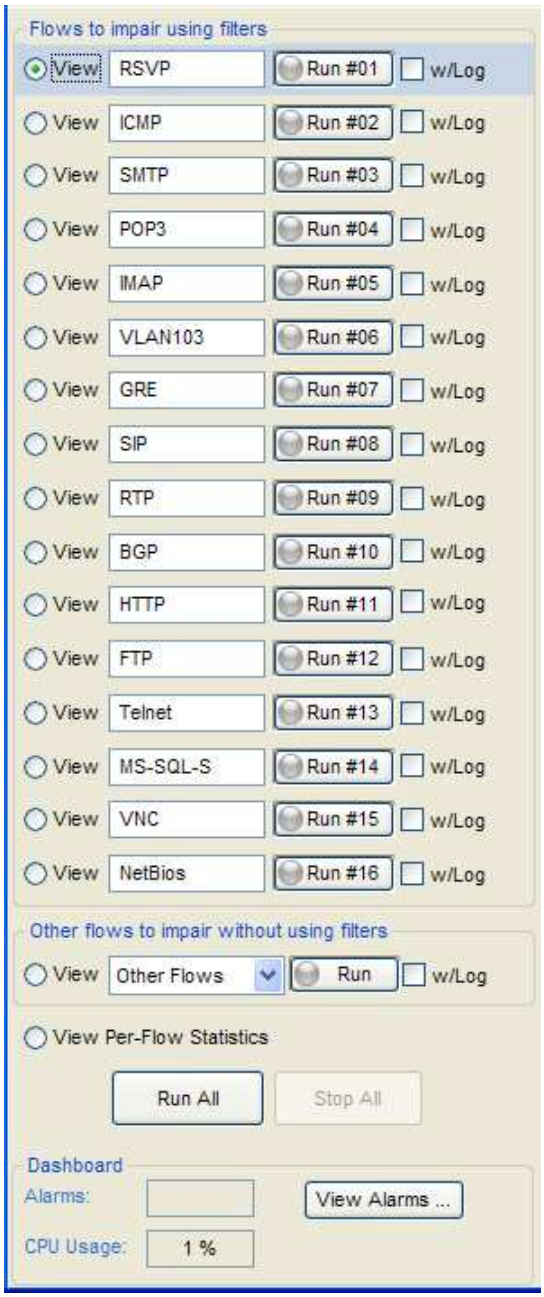
By clicking on the 'Hide Aggregates' menu, the **NetDisturb** Client window is reduced by hiding the aggregates area:



7.3 The Flows

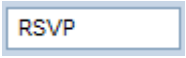
This section describes the left part area of **NetDisturb** Client user interface.

7.3.1 General Description

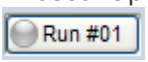


Flows to impair using filters

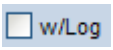
This button is used to access the details configuration and statistics of a specific Flow.



This edit area is used to name the flow with a mnemonic that helps to remember impairment parameters or filter used. Up to 16 flows with filters can be defined.



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



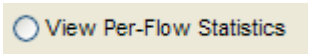
(Enhanced Edition only)

Once a filter is defined for a flow, it's possible to trace the events and packets to impair when the flow is running if this option is checked.

Other flows to impair without using filters

The "Other Flows"/"Other IP Flows" object is in charge to handle the remaining traffic that wasn't filtered by the previous Flows. It can't be renamed: its specific characteristics are described in paragraph 7.3.2.

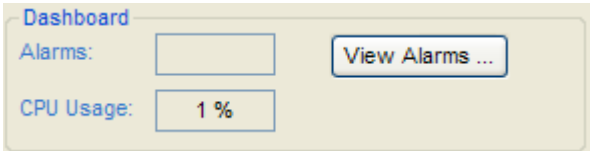
View Per-Flow Statistics



When selecting this button, you can get an abstract of the activity of all flows. Details can be found in paragraph 7.3.3

Bottom buttons

The 'Run All' button starts all Flows, except the Flows that don't have a filter defined.
The 'Stop All' button stops all running Flows.



Alarms: this error counter is the number of alarms returned by the NIC driver indicating that some errors (CRC errors, NIC or driver buffer overrun) have occurred from the started time of the NIC. When pressed, the "**View Alarms…**" button displays a pop-up window with alarm details.
CPU Usage: indicates the level of processor activities.

7.3.2 Other Flows to impair without using filters

This object is in charge to handle the remaining traffic. This is why there is no need to have a filter for this object. The remaining traffic (not filtered by the Flows from #01 to #16) could be one of the following:

The traffic considered is the IP frames that haven't been filtered by IP Flows #01 to #16. Only the IP Frames are eligible when this option is selected.

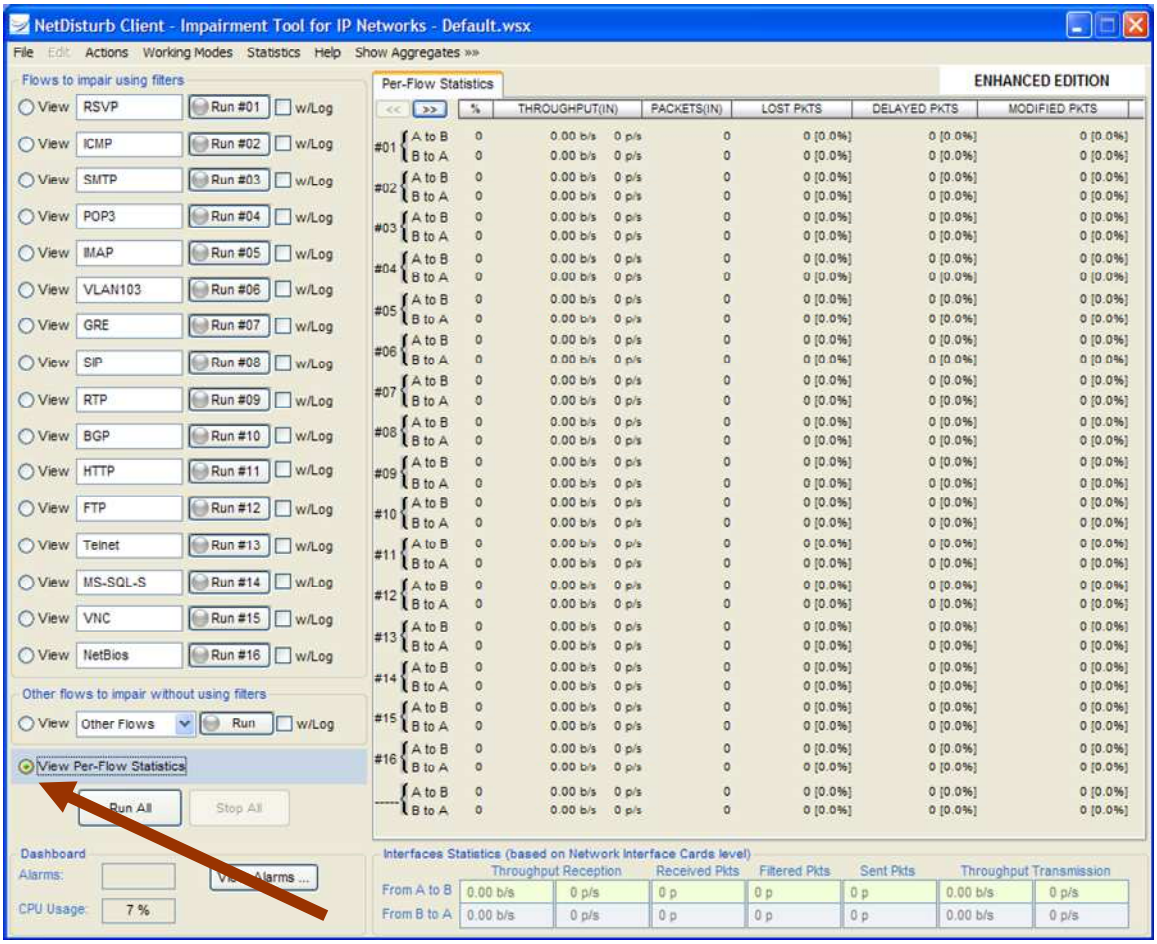
The traffic considered consists in all Ethernet frames that haven't been filtered by IP Flows #01 to #16. The IP frames as well as all the other Ethernet frames (such as IPX or MPLS frames) will be filtered when this option is selected.

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

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

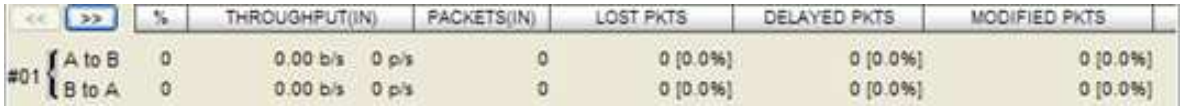
7.3.3 View Per-Flow Statistics

To get this view you have to press the **View Per-Flow Statistics** button.



On this screenshot no Flow is running.

Detailed Description:



<< >> The two arrows allow scrolling the statistics synthesis window in order to view the hidden statistics. In order to change the order of the columns, simply drag and drop them. These columns can be also resized.

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

%: This column shows the percentage of packets from A to B or from B to A which correspond to the selected filter criteria regarding the total number of packets treated by NetDisturb (respectively from A to B or from B to A).

THROUGHPUT(IN) or Incoming Throughput: This column shows the instant or average throughput, depending on the Display Configuration chosen (more details are available in paragraph 7.2.3.1 Actions/Configuration).
The Incoming Throughput shown in the upper line refers to data received by the 'Interface A' applying the IP Filter (or 'Interface B' for the second line respectively).

PACKETS(IN) or Incoming Packets: This column presents the number of packets received. It is a cumulated value.

LOST PKTS or Lost Packets: This column presents the number of packets lost, and the percentage of those packets regarding the global number of packets filtered, for the relevant direction. In case of duplication, this counter shows the number of generated packets by the duplication process.

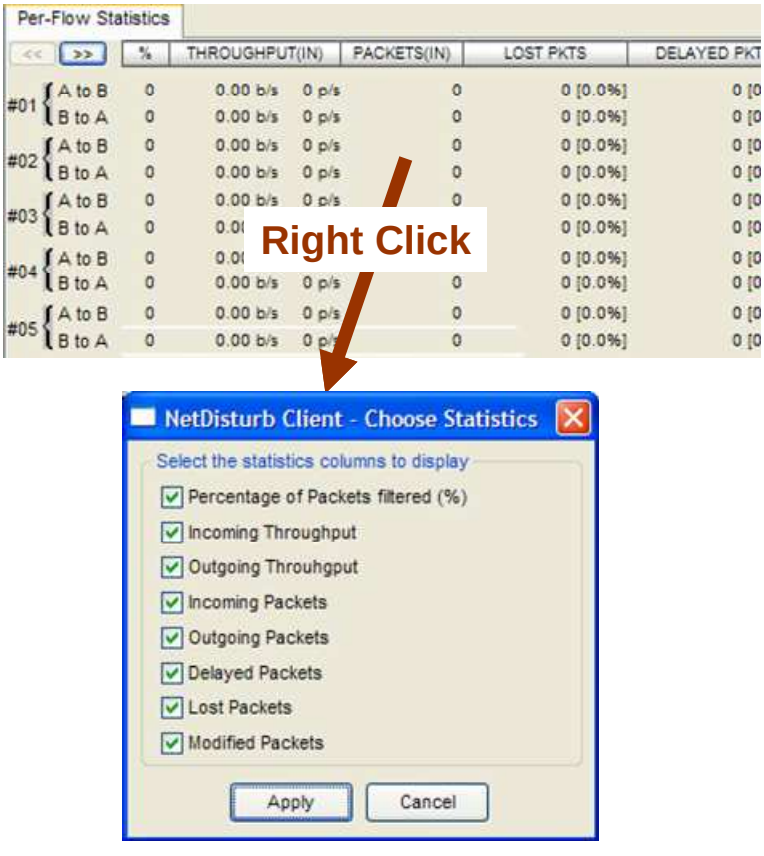
DELAYED PKTS or Delayed Packets: This column presents the number of delayed packets, and the percentage of those packets regarding the global number of packets filtered (***Incoming Packets*** column), for the relevant direction.

MODIFIED PKTS or Modified Packets: This column presents the number of packets of which the content has been impaired, and the percentage of those packets regarding the global number of packets filtered (***Incoming Packets*** column), for the relevant direction.

PACKETS(OUT) or Outgoing Packets: This column presents the number of packets sent from one interface to the other. It is the number of packets filtered (column ***Incoming Packets***) minus the number of packets lost (***Lost Packets*** column), for the relevant direction.

THROUGHPUT(OUT) or Outgoing Throughput: This column shows the instant or average throughput, depending on the Display Configuration chosen (more details are available in paragraph 7.2.3.1 Actions/Configuration). The Outgoing Throughput column shown in the upper line refers to data sent to the Interface B (or Interface A for the second line respectively).

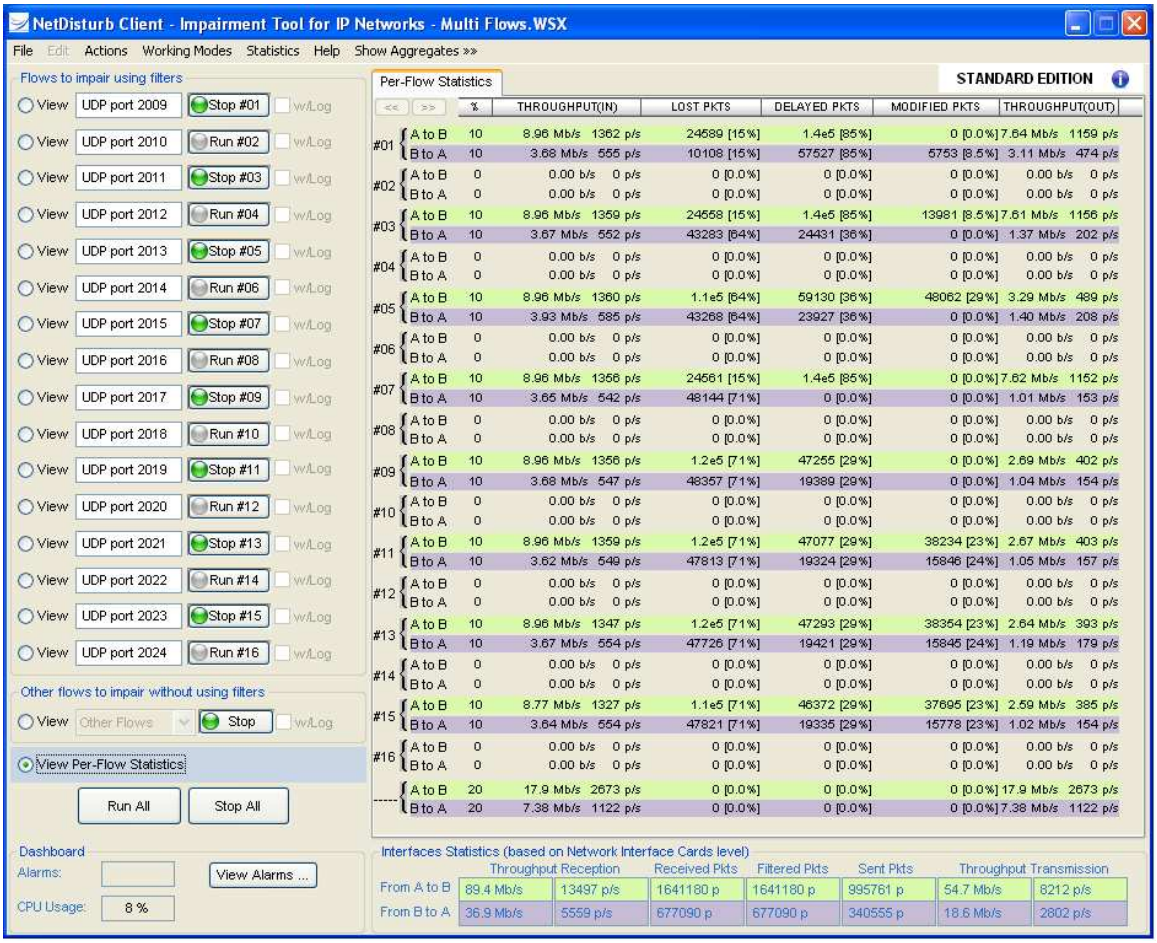
By default, all of the statistical columns are displayed. The NetDisturb Client offers the possibility to hide the non-mandatory columns. To access to the configuration window showed below, **right click** on the statistical area to open it. When a column is selected, this one is inserted at the end of the tab.



The display preferences (order, size and visibility) of the statistical columns are saved into the context file

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

- The green color is related to the A➔B direction
- The gray color is related to the B➔A direction

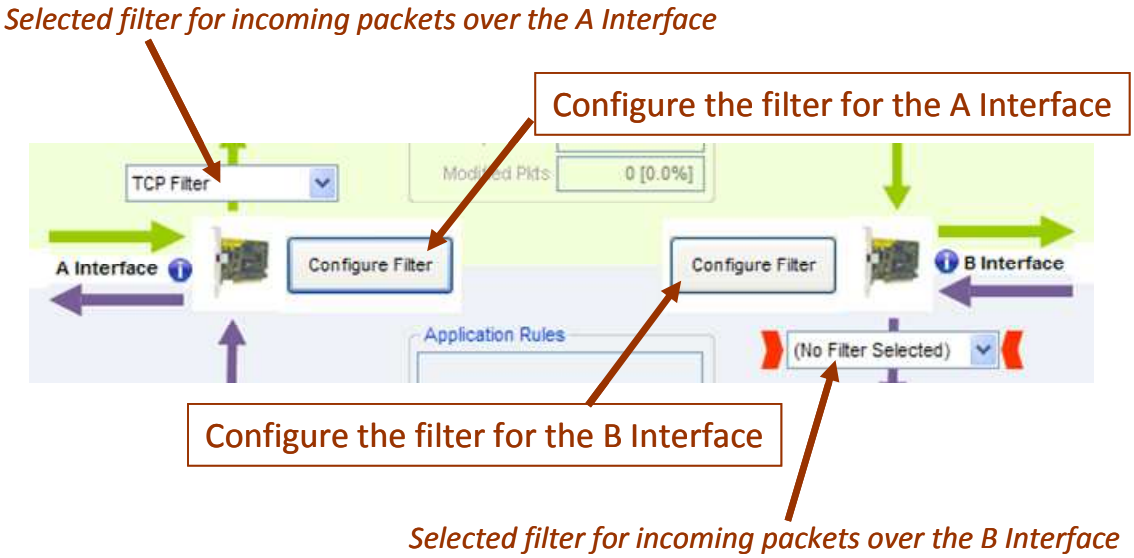


7.4 The Impairment Parameters and associated Commands

The impairment parameters are defined by using a **Loss & Duplication law** and/or a **Delay & Jitter law** and/or a **Content Impairment law**. 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.

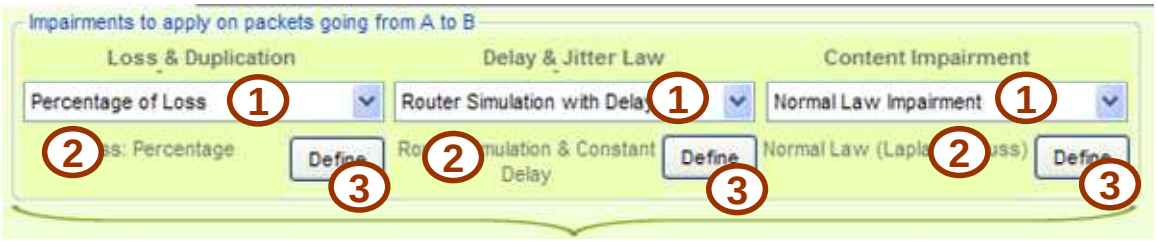
The "**Configure Filter**" button allows specifying the parameters for the incoming packets of the Flow, and there is one button per direction:

- Direction **A ➡ B**: use the left "**Configure Filter**" button to configure the parameters of the filter to use over the A interface
- Direction **B ➡ A**: use the right "**Configure Filter**" button to configure the parameters of the filter to use over the B interface



The **Filter** allows selecting packets to process and eventually the rules to apply the impairments.

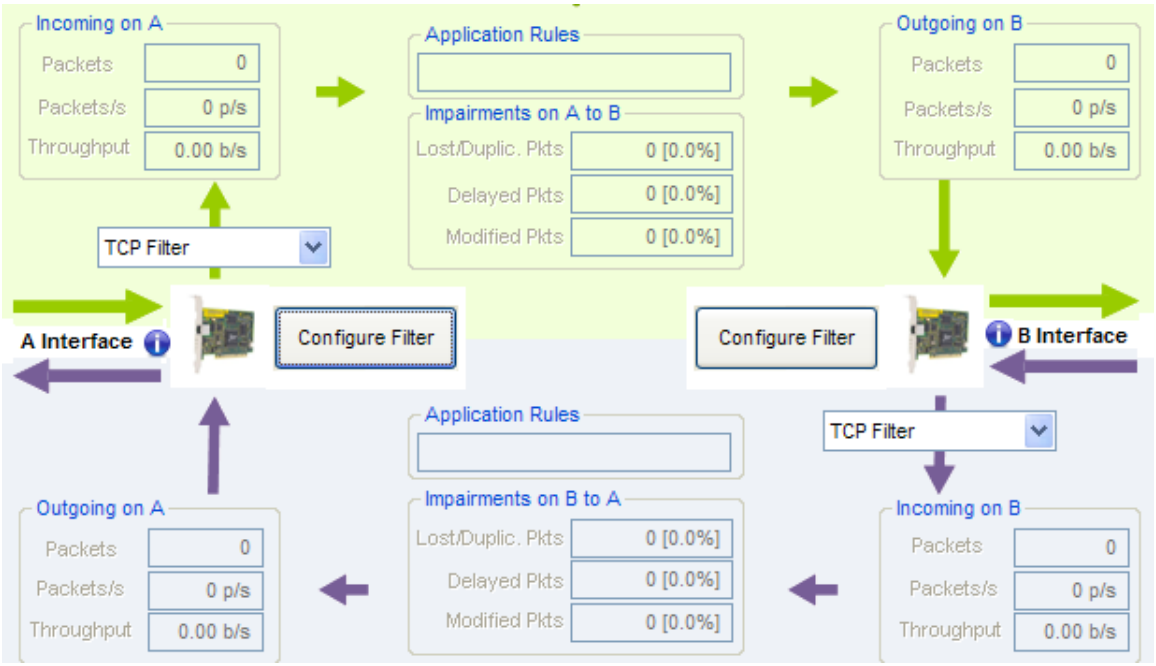
Once a filter is defined for a direction (A ➡ B or B ➡ A), the impairments can be defined by using the objects presented below:



Each section for the impairment law is composed of 3 objects:

- **(1)** The combo-box allows selecting the defined law
- **(2)** The resume of the law selected in the combo-box
- **(3)** The Define button allows defining and modifying the impairment law.

The center part (shown below) displays statistical counters for the two interfaces:

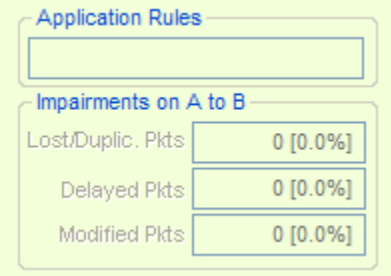


- **Incoming on A (or Incoming on B)**

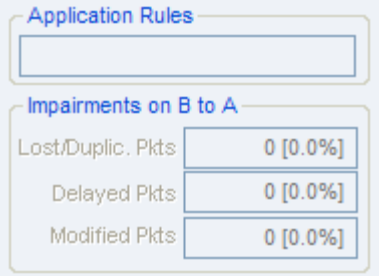
In the upper left for the A interface (bottom right corner for the B interface), the "Incoming on A" (or " Incoming on B") object displays:

- number of incoming **Packets** matching the Filter for the interface
- number of incoming **Packets/s** matching the Filter for the interface
- the incoming **Throughput**

- **Application Rules and Statistics for the Impairments**



Direction A ➡ B



Direction B ➡ A

When the Flow is running, the following information is displayed and refreshed:

- **Application Rules**: The possible status are the following:
  - Waiting for trigger
  - Delay before impairments
  - Applying impairments
  - Delay before next cycle
  - No more impairment
  - No impairments law selected

- **Impairments on A to B (or B to A)**:

  • **Lost/Duplic. Pkts counter (Lost / Duplicated Packets)**
  With a loss law, this counter displays the number of lost packets and the ratio of packets lost on the number of filtered packets for the current Flow.
  With a duplication law, this counter displays the number of generated packets by the duplication process and the ratio of generated packets on the number of filtered packets for the current Flow.
  In the case of the "Loss (1 out of N) then Duplicate (1 out of M)" law, it displays the number of lost packets added to the number of generated packets by the duplication process.

  • **Delayed Pkts counter (Delayed Packets)**
  The number of delayed packets and the percentage of delayed packets on number of filtered & no lost packets are displayed with this counter.

  • **Modified Pkts counter (Modified Packets)**
  The number of modified packets and the percentage of modified packets on number of filtered & no lost packets are displayed.

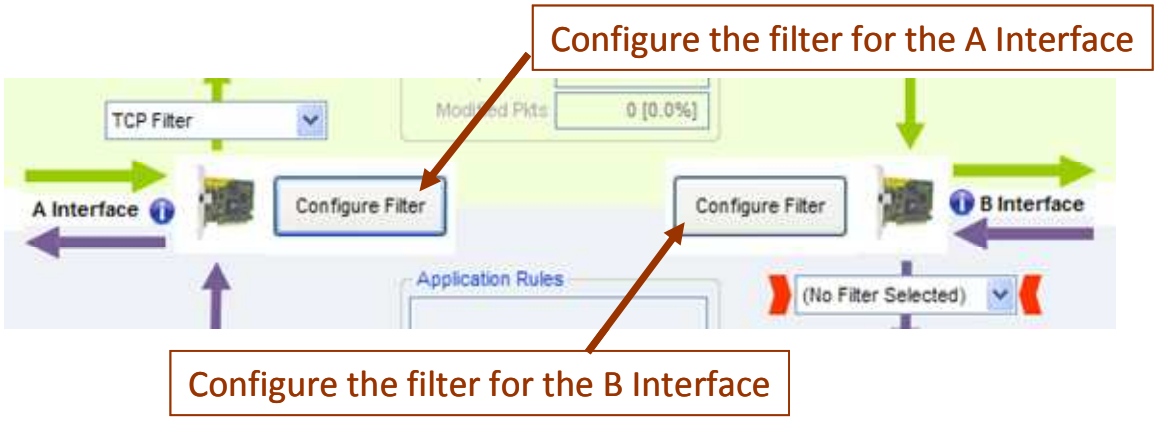
Once created a new Filter or a new Law, it will be available to be applied to both directions (A ➔ B or B ➔ A).

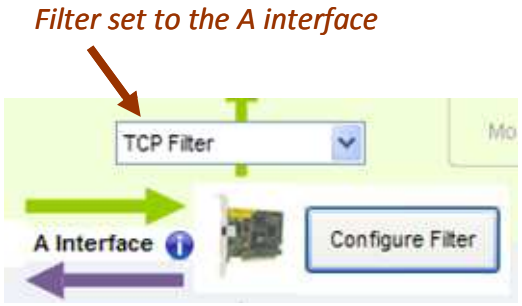
7.4.1 Selection of a Filter or Impairment Law

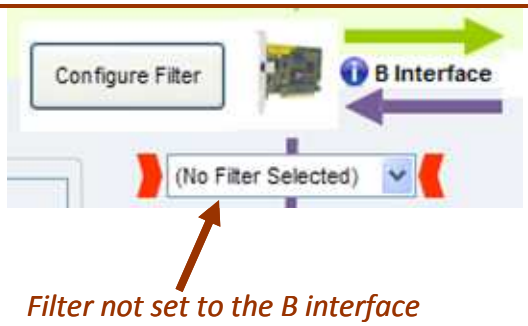
To change the selection of the filter or the law, select the requested filter or law from the list displayed in the related combo-box. The filter or the law is automatically selected.

7.4.2 The Filter Configuration

To configure a filter for a flow, press the **Configure Filter** button as shown below.







Red stripes near the combo-box are displayed when there is no filter set for the interface

A Filter is a set of parameters to select the packets that would be impaired for the flow.

With NetDisturb you can define up to 16 filters, i.e. 16 flows. An additional item named "Other Flows" is in charge to handle all flows (IP or not) that have not been user defined. For this item no filter can be defined, but impairments can be applied.

A Filter is composed of a combination of several items – ***Predefined Parameters***, where each one of them is optional (except the Frame Type), and it's possible to add a user-defined **Pattern Parameter** and **Rules** to apply the impairments.

Predefined Parameters

Ethernet header

- Source MAC address
- Destination MAC address
- Ethernet Packet Length
- IP Frame Version (IPv4 or IPv6)
- ARP Frame

ARP Operation (Enhanced Edition only)

List of VLAN-ID (Ethernet frames 802.1Q)

List of MPLS-ID

IP Header
- Source IPv4 address
- Source IPv4 address mask
- Destination IPv4 address
- Destination IPv4 address mask
- Source IPv6 address
- Source IPv6 address mask
- Destination IPv6 address
- Destination IPv6 address mask
- Protocol (ICMP, TCP, UDP, GRE, …)
- Differentiated Services Code Point (DSCP) / ToS Byte

List of Ports (for TCP or UDP packets)
- Source port list
- Destination port list

Protocol primitives (only for Enhanced version): ARP, DHCP, DNS, FTP, FTP-DATA, HTTP, NTP, RTP and SIP.

Pattern Parameter

The Pattern Parameter is a user-defined filter based on the Ethernet packet content (search for a defined pattern with an offset in the Ethernet frame content).
The pattern parameter is composed of:
- Offset (decimal value)
- Pattern (hexadecimal string)
- Result (hexadecimal string)

The analysis starts at the Offset position of the Ethernet frame, where the content ANDed with the Pattern (up to the pattern length) should be equal to the Result.

The Pattern Parameter can be used alone or in addition to predefined parameters.

Rules applying to Impairments

User-defined rules may be associated with the filter to condition the applying of the impairments:

- Start when finding a Trigger (a trigger is defined with 3 parameters: Offset, Pattern, Result) and impair or not the frame that has triggered
- Delay before applying impairments: number of packets or elapsed time expressed in milliseconds or seconds or minutes or hours
- Stop impairments after: number of packets or elapsed time expressed in milliseconds or seconds or minutes or hours

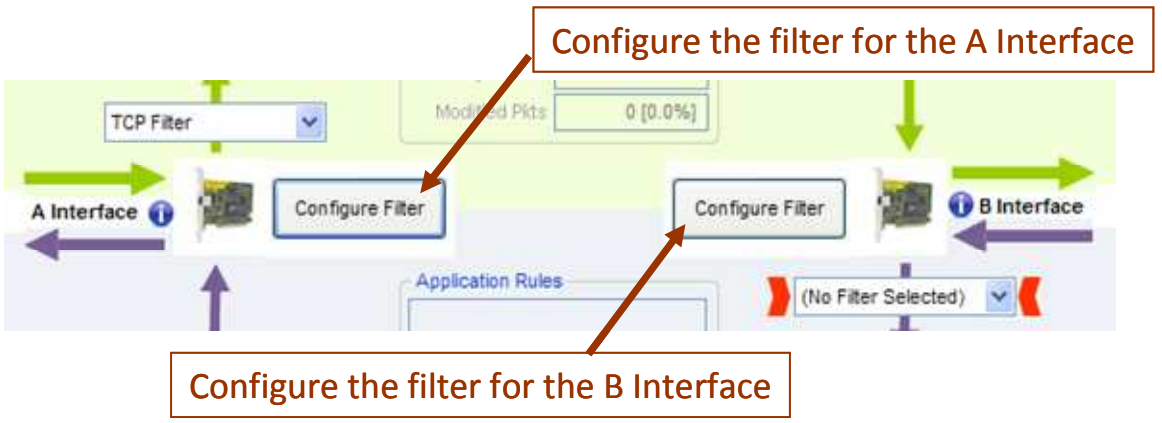
- Define a loop for the rules above with 2 parameters:
    - Create a loop and apply it n times
    - Pause between each loop (expressed in number of packets or elapsed time in milliseconds or seconds or minutes or hours)

By default, the following Filters are included with the default context named **Default.wsx**:

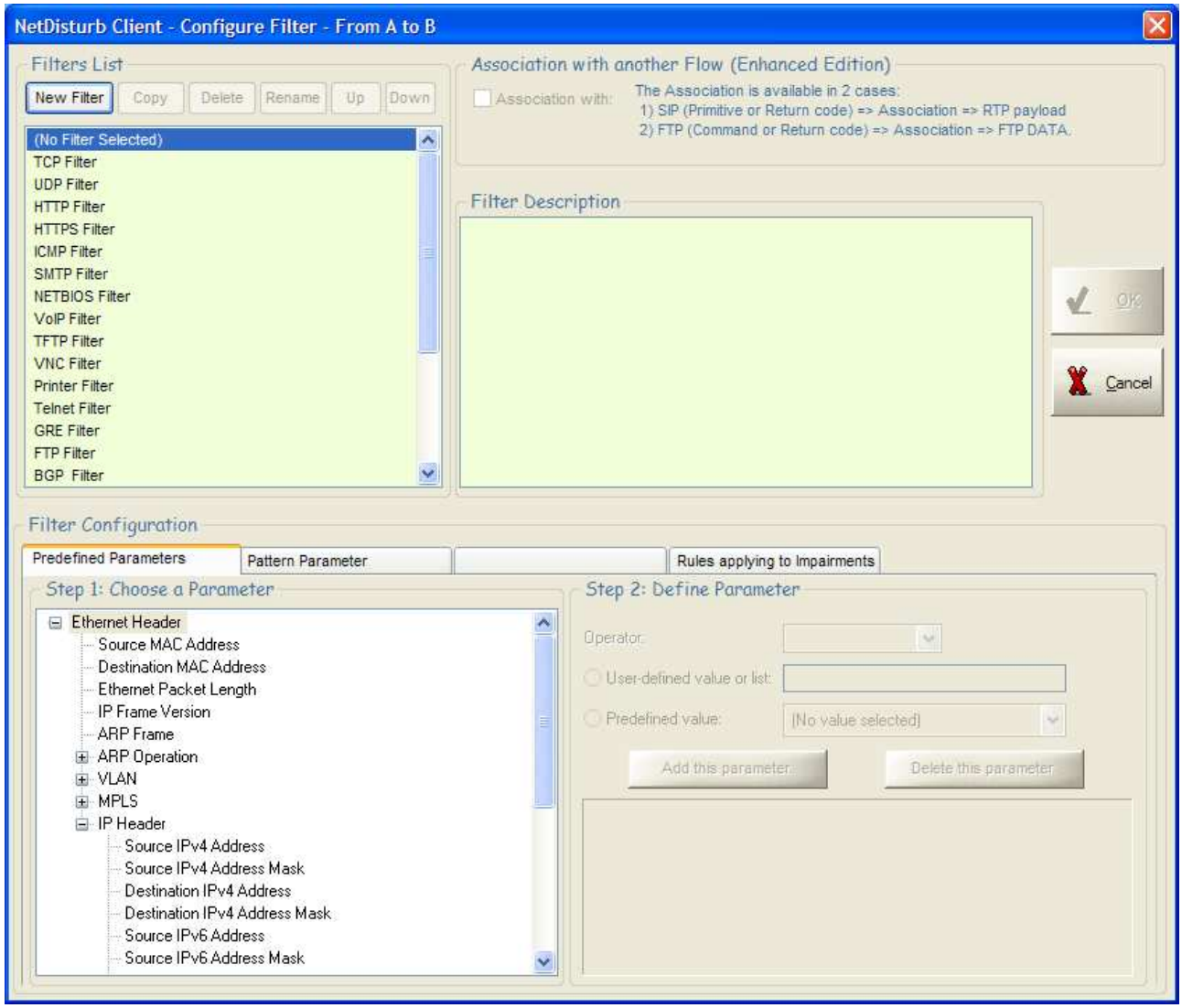
Name of the Filter	Description
(None)	This filter disables the Flow because no packet can match a Filter without selection criteria.
TCP Filter	This filter considers only IP packets with a protocol set to TCP.
UDP Filter	This filter considers only IP packets with the UDP protocol.
HTTP Filter	This filter considers IP packets with the TCP protocol and the destination ports 80 or 8080.
HTTPS Filter	This filter considers IP packets with the TCP protocol and the destination port 443.
ICMP Filter	This filter considers only IP packets with ICMP (01) protocol.
SMTP Filter	This filter considers IP packets with the TCP protocol and the destination port 25.
NETBIOS Filter	This filter considers IP packets with the TCP protocol and destination ports 137, 138 or 139.
VoIP Filter	This filter considers IP packets with the UDP protocol and the destination port 1250.
TFTP Filter	This filter considers IP packets with the UDP protocol and the destination port 69.
VNC Filter	This filter considers IP packets with the TCP protocol and destination port 5900.
Printer Filter	This filter considers IP packets with the TCP protocol and destination port 9100.
TELNET Filter	This filter considers IP packets with the TCP protocol and the destination port 23.
GRE Filter	This filter considers IP packets with the GRE (x2F) protocol.
FTP Filter	This filter considers IP packets with the TCP protocol and the destination ports 20 or 21.
BGP Filter	This filter considers IP packets with the TCP protocol and destination port 179.
MS-SQL-S Filter	This filter considers IP packets with the destination port 1433.
VLAN Filter	This filter considers IP packets when the VLAN ID is included between 1 and 5.
POP3 Filter	This filter considers IP packets with the TCP protocol and the destination port 110.
NTP Filter	This filter considers IP packets with the UDP protocol and the destination port 123.
RSVP Filter	This filter considers IP packets with the RSVP (x2E) protocol.
SCTP Filter	This filter considers IP packets with the SCTP (x84) protocol.
SIP Filter	This filter considers IP packets with the following parameters: UDP protocol, destination port = 5060, SIP returned status = OK, SIP Request = INVITE.
RTP Audio filter	This filter considers IP packets with the following parameters: UDP protocol, payload type = 9 (G.722)
RTP Video filter	This filter considers IP packets with the following parameters: UDP protocol, payload type = 31 (H.261)

Supplementary filters may be added depending of the product release.

To define or edit an existing Filter, press the **Configure Filter** button as indicated below:



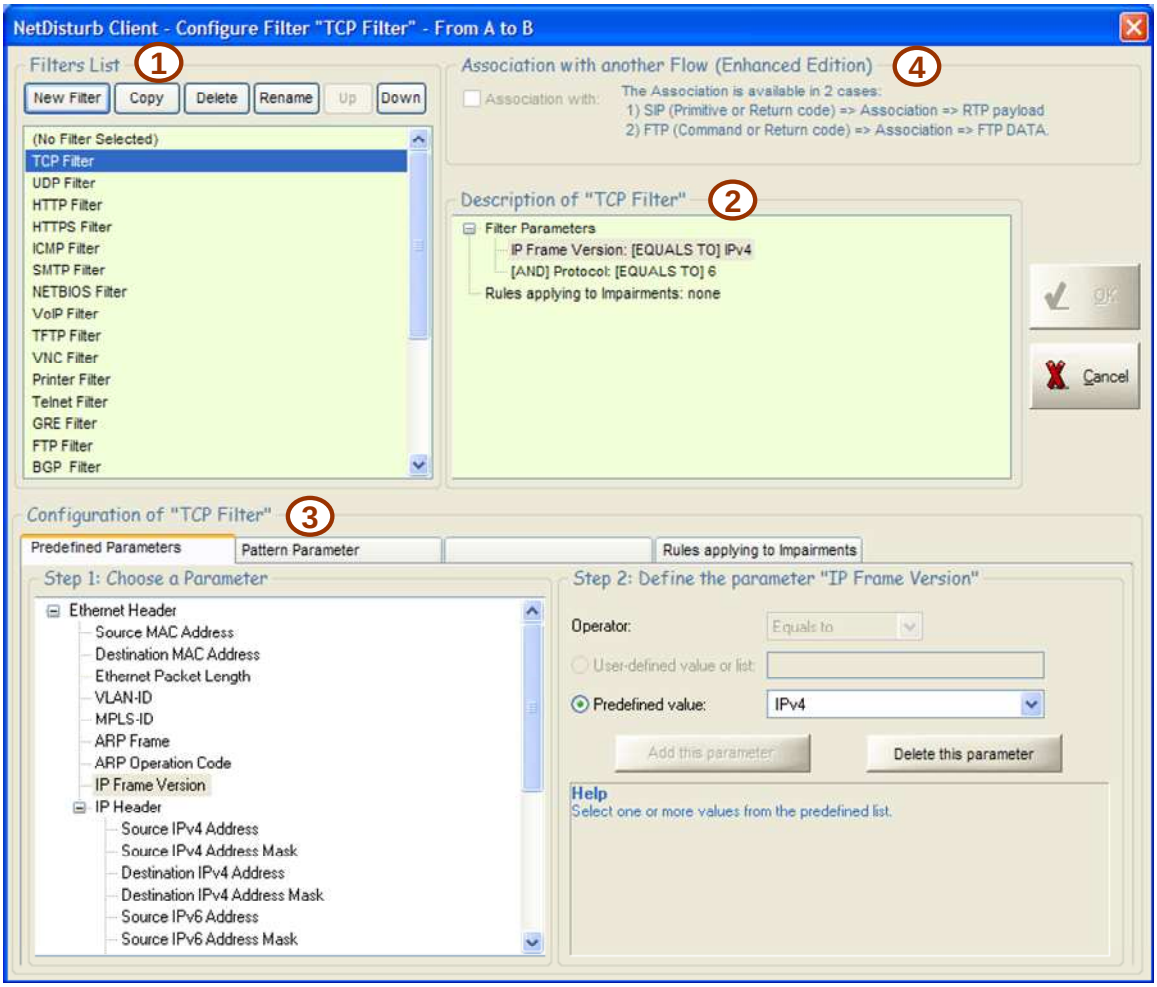
Then the following window will appear:



This window allows creating a new Filter or modifying an existing one.

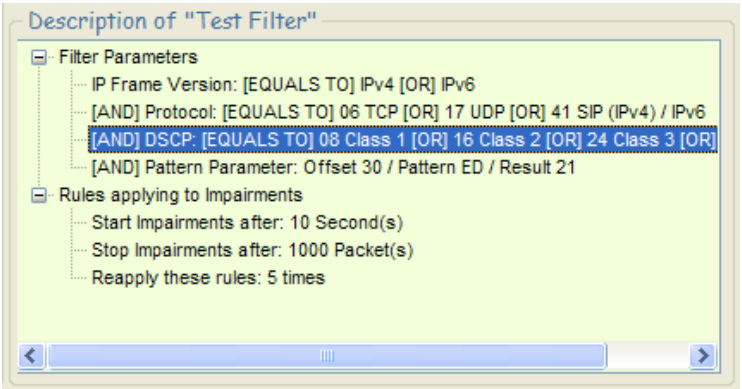
If "(None)" is selected, only the **New Filter** button is enabled and the tabs to define the parameters are disabled.

If you select a preexisting Filter in the current list-box, then the parameters of this Filter can be viewed and the first "Predefined Parameters" tab is set as in the example below:



This window is composed of several areas:

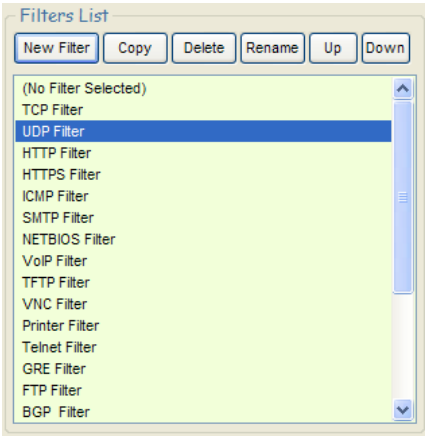
- **(1) Filters List**: List of the defined Filters: a list-box displays the defined Filters and five buttons allow managing the Filters: **New Filter**, **Copy**, **Delete**, **Rename**, **Up** and **Down**.
- **(2) Filter Description**: the list-box displays the detailed characteristics of the Filter and the specific impairment rules if specified, as shown in the example below:



- **(3) Filter Configuration**: three tabs allow defining the parameters of the selected Filter.
  - Predefined Parameters (to specify one or several parameters)
  - Pattern Parameter (optionally: to specify if a pattern must be defined)
  - Rules applying to Impairments (optionally: to specify if impairment rules must be defined)

- **(4) Association with another Flow** (Enhanced Edition only): available in 2 cases (SIP and FTP) to correlate control and data flows by example.

7.4.2.1 Filters List



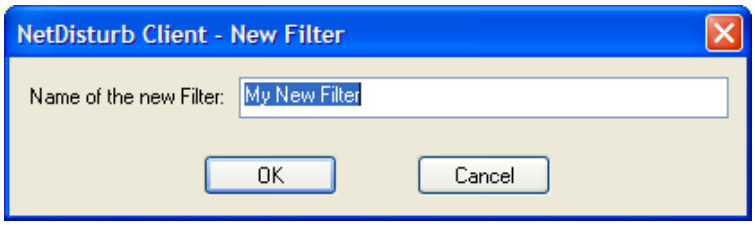
The list-box displays the names of the filters defined in the current context.

To manage the list, add or modify or delete a filter, six buttons are available:

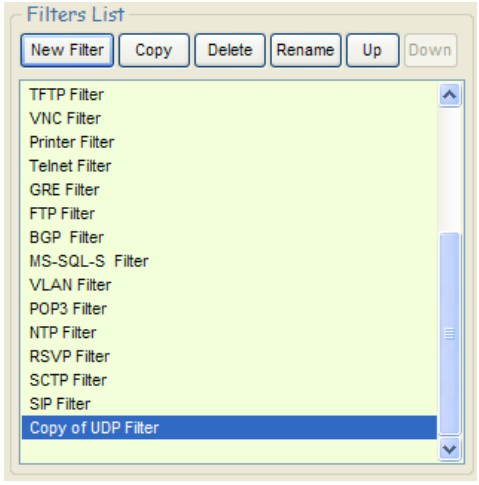
- New Filter
- Copy
- Delete
- Rename
- Up
- Down

New Filter: this button should be used to add a new Filter in the list.

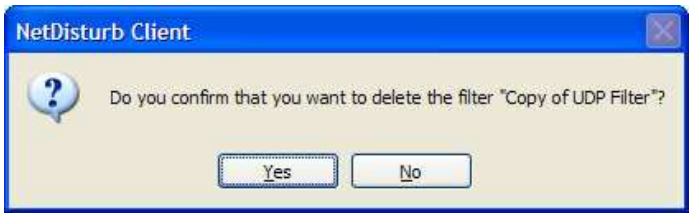
After pressing this button, a new window is displayed to enter a filter name. Then press OK to validate.
The new entry is added at the end of the list-box.



Copy: this button copies the current selected Filter at the end of the list with a new name. The following example shows the new list-box after copying the existing UDP Filter:



Delete: this button should be used to remove a Filter from the current list.
First select in the list-box the Filter to delete and then press the Delete button. A confirmation window is then displayed:



Rename: this button should be used to change the Filter name.

Up: to move up the selected Filter of the list one position to the top.

Down: to move down the selected Filter of the list one position to the bottom.

7.4.2.2 Three tabs to define and configure the parameters of the Filter

Once a Filter has been created, you can define or modify the parameters of the Filter and the related rules by using the following tabs:

- (Tab 1: Predefined Parameters) Optional: Simplest way to define the filter.
- (Tab 2: Pattern Parameter) Optional: Filter based on the Ethernet packet content
- (Tab 3: Rules applying to Impairments) Optionally: to apply specific impairment rules

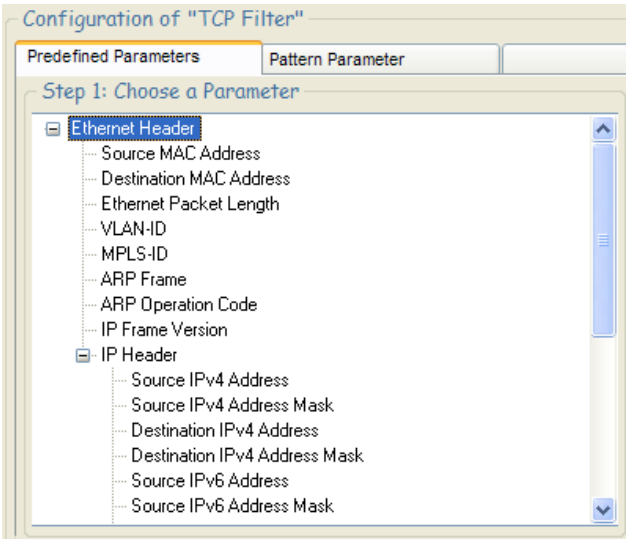
A Filter is defined by the combination of four types of parameters: Frame Type, MAC header, IP header and Ports. In the Enhanced Edition, application protocol parameters may be added.

Each parameter of a Filter is optional, but at least one predefined parameter or the Pattern parameter should be set. When a parameter is set then the parameter **has to** be present in the frame to match the Filter.

Each Filter is defined in reference to a direction in order to identify which interface the source and destination addresses belongs to. If the processes are also applied to the other direction, the **NetDisturb** driver reverses automatically the source and destination addresses and ports.

7.4.2.2.1 Filter: the "Predefined Parameters" tab

This tab allows defining the needed parameters for the Filter with the following structure:



- Source MAC Address
- Destination MAC Address
- Ethernet Packet Length
- VLAN-ID
- MPLS-ID
- ARP Frame
- ARP Operation Code *(Enhanced Edition only)*
- IP Frame Version
- IP Header:
  - Source IPv4 Address
  - Source IPv4 Address Mask
  - Destination IPv4 Address
  - Destination IPv4 Address Mask
  - Source IPv6 Address
  - Source IPv6 Address Mask
  - Destination IPv6 Address
  - Destination IPv6 Address Mask
  - Protocol
  - DSCP
  - TCP/UDP Ports
  - FTP DATA *(Enhanced Edition only)*
  - NTP *(Enhanced Edition only)*
  - DHCP *(Enhanced Edition only)*
  - DNS *(Enhanced Edition only)*
  - FTP *(Enhanced Edition only)*
  - HTTP *(Enhanced Edition only)*
  - RTP *(Enhanced Edition only)*
  - SIP *(Enhanced Edition only)*

(Enhanced Edition only) means that the parameter can't be used with NetDisturb Standard Edition.

7.4.2.2.1.1 List of Values

Some parameters in the Filter can be a list of values. To match the Filter, the packet should include one value from the list. The syntax of the list allows a set of individual values or ranges of values. Both individual values and ranges can be mixed. **Values are expressed in decimal**.
The separator between individual values or range of values is the (;) semicolon character. The syntax used is very near the syntax of the printer for a set of pages.

Individual Value
An individual value is one and only one value. Example: 135

List of Individual Values
A list of values is multiple individual values, each value separated by a semi-coma.
Example: 25;80;110;435

Range of Values
A range of values is a set of values indicated by the first and the last of the range (first and last included). The first value is separated from the last value by a dash.
Example: 2009-2020;3000-3100

Complex List
Here is an example including individual values and range of values.

List:	**12; 13; 25-30; 50-100; 120**
Values matching:	12, 13, 25 to 30 included, 50 to 100 included, and 120
Values not matching:	< 12, 14 to 24, 31 to 49, 101 to 119, > 121

7.4.2.2.1.2 Description of the parameters

Source Mac Address	
Operator:	Equals to Doesn't equal to
User-defined value or list:	enter the MAC address with the following format: **XX:XX:XX:XX:XX:XX** (12 hexadecimal digits grouped by 2 and separated by the colon character).

Example: Source Mac Address **doesn't equal to 00:80:C8:81:37:66**
The IP packets having a MAC source address different of **00:80:C8:81:37:66** will belong to this IP flow.

Destination Mac Address	
Operator:	Equals to Doesn't equal to
User-defined value or list:	Enter the MAC address with the following format: **XX:XX:XX:XX:XX:XX** (12 hexadecimal digits grouped by 2 and separated by the colon character).

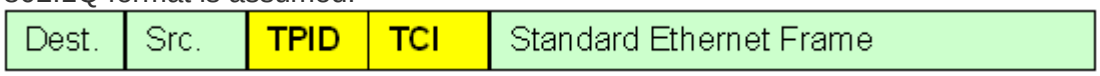
Example: Destination Mac Address **equals to 00:0B:DB:95:3D:BF**
The IP packets having a MAC destination address equals to **00:80:C8:81:37:66** will belong to this IP flow.

*The reference for the Source and Destination MAC addresses depends on the original Interface selection. In case the **Configure Filter** button from the Interface A was pressed, the direction from Interface A to Interface B is the reference direction. If the Filter is re-edited from the Interface B, then the Source and Destination MAC addresses are inverted automatically by the **NetDisturb** Client to match the new direction.*

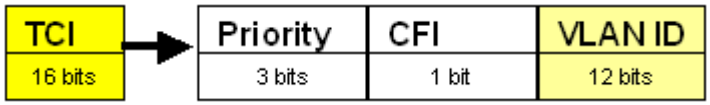
Ethernet Packet Length	
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify the Ethernet packet length from 64 bytes up to 1,514 bytes. The length may be: • a range of values (i.e. 64-128 means a length from 64 to 128 bytes) • Individual values separated by a semicolon (i.e. 62;160;364) • A mix of the two previous cases (i.e. 64;128-1294;1514)

VLAN-ID	
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify values from 0 up to 4,095. As ID List, you can enter: • A range of values (i.e. 120-250 means from 120 to 250) • Individual values separated by a semicolon (i.e. 500;600) • A mix of the two previous cases (i.e. 500;550-560;599)

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:



MPLS-ID	
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify values from 0 up to 1,048,575. As ID List, you can enter: • a range of values (i.e. 120-250 means from 120 to 250) • Individual values separated by a semicolon (i.e. 500;600) • A mix of the two previous cases (i.e. 500;550-560;599)

ARP Frame	
Operator:	*None*
Predefined value:	ARP Frame. If the ARP frame type is selected, only the following parameters can be defined: • Source MAC Address • Destination MAC Address • Ethernet Packet Length • ARP Operation Code *(Enhanced Edition only)*

ARP Operation Code	*(Enhanced Edition only)*
Operator:	Equals to Doesn't equal to
Predefined value:	9 predefined values can be used such as: • 01 ARP Request • 02 ARP Reply • 03 RARP Request • 04 RARP Reply • 05 DRARP Request • 06 DRARP Reply • 07 DRARP Error • 08 InARP Request • 09 InARP Reply *Note: several values can be used.*

IP Frame Version	
Operator:	*None*
Predefined value:	Specify the IP version to consider. The version may be: • IPv4 • IPv6 • IPv4 or IPv6

Important note for IPv4 addresses and masks:
*The reference for the Source and Destination IP addresses and masks depends on the original Interface selection. In case the **Configure Filter** button from the Interface A was pressed, the direction from Interface A to Interface B is the reference direction.*
*When the Filter is re-edited from the Interface B, the Source and Destination IP addresses and masks are inverted automatically by the **NetDisturb** Client to match the new direction.*

Source IPv4 Address	
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify the IPv4 source address respecting this format: ddd.ddd.ddd.ddd where d is a value from 0 to 9. Example: 192.168.0.1

Source IPv4 Address Mask	
Operator:	*None*
User-defined value or list:	Specify the IPv4 mask respecting this format: ddd.ddd.ddd.ddd where d is a value from 0 to 9. Example: 255.255.255.0 This mask is used in conjunction with the IPv4 source address you defined and with the IP address of the received packet.

Destination IPv4 Address	
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify the IPv4 destination address respecting this format: ddd.ddd.ddd.ddd where d is a value from 0 to 9. Example: 192.168.0.25

Destination IPv4 Address Mask	
Operator:	*None*
User-defined value or list:	Specify the IPv4 mask respecting this format: ddd.ddd.ddd.ddd where d is a value from 0 to 9. Example: 255.255.255.0 This mask is used in conjunction with the IPv4 destination address you defined and with the IP address of the received packet.

Important note for IPv6 addresses and masks:
*The reference for the Source and Destination IP addresses and masks depends on the original Interface selection. In case the **Configure Filter** button from the Interface A was pressed, the direction from Interface A to Interface B is the reference direction.*
*When the Filter is re-edited from the Interface B, the Source and Destination IP addresses and masks are inverted automatically by the **NetDisturb** Client to match the new direction.*

Source IPv6 Address	
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify the IPv6 source address respecting this format: dddd::ddd:dddd where d is a hexadecimal value from 0 to F. For example: FE80::211:43FF:FE03:1959

Source IPv6 Address Mask	
Operator:	*None*
User-defined value or list:	Specify the IPv6 mask respecting this format: nn (bit mask) where n is a decimal value from 0 to 9. The bit mask refers to the high bits of the address used for comparison with the IP address of the received packet. For example: 48

Destination IPv6 Address	
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify the IPv6 destination address respecting this format: dddd::ddd:dddd where d is a hexadecimal value from 0 to F. For example: FE80::211:43FF:FE03:1959

Destination IPv6 Address Mask	
Operator:	*None*
User-defined value or list:	Specify the IPv6 mask respecting this format: nn (bit mask) where n is a decimal value from 0 to 9. The bit mask refers to the high bits of the address used for comparison with the IP address of the received packet. For example: 48

Protocol	
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify a protocol value from 0 to 255 You may define a set of protocols with: • A range of values (i.e. 120-250 means from 120 to 250) • Individual values separated by a semicolon (i.e. 6;17) • A mix of the two previous cases (i.e. 6-15;17;21)
Predefined value:	You can select one or more predefined values among 38 of the combo-box such as: - 01 ICMP (IPv4) - 02 IGMP (IPv4) - 04 IPinIP - 06 TCP - 08 EGP - and more…

DSCP	
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify a DSCP value from 0 to 63 You may define a list with: • A range of values (i.e. 12-25 means from 12 to 25) • Individual values separated by a semicolon (i.e. 50;60) • A mix of the two previous cases (i.e. 10;25-36;49)
Predefined value:	You can select one or more predefined values among 21 of the combo-box such as: - 00 DEFAULT PHB (Per-Hop Behavior) - 08 Class 1 - 10 Class 1 Gold (AF11) - 12 Class 1 Silver (AF12) - 14 Class 1 Bronze (AF13) - and more…

TCP/UDP ports :: Source Port	
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify a port number value from 1 to 65,535 or a port list. A list of ports may be: • A range of values (i.e. 20-25 means from port 20 to 25) • Individual values separated by a semicolon (i.e. 7;9;80) • Denied individual values if the symbol != is used before the value (i.e. !=21) • A range of values and individual values (i.e. 7;9;20-25;80;435) • A range of values with denied individual values (i.e. 10-50;!=20;!21 which means ports from 10 to 50 without 20 or 21)

*The reference for the Source and Destination ports depends on the original Interface selection. In case the **Configure Filter** button from the Interface A was pressed, the direction from Interface A to Interface B is the reference direction. If the Filter is re-edited from the Interface B, then the Source and Destination ports are inverted automatically by the **NetDisturb** Client to match the new direction.*

TCP/UDP ports :: Destination Port	
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify a port number value from 1 to 65,535 or a port list. A list of ports may be: • A range of values (i.e. 20-25 means from port 20 to 25) • Individual values separated by a semicolon (i.e. 7;9;80) • Denied individual values if the symbol != is used before the value (i.e. !=21) • A range of values and individual values (i.e. 7;9;20-25;80;435) • A range of values with denied individual values (i.e. 10-50;!=20;!21 which means ports from 10 to 50 without 20 or 21)

*The reference for the Source and Destination port depends on the original Interface selection. In case the "Configure Filter" button from the Interface A was pressed, the direction from Interface A to Interface B is the reference direction. If the Filter is re-edited from the Interface B, then the Source and Destination ports are inverted automatically by the **NetDisturb** Client to match the new direction.*

DHCP Message Type	***(Enhanced Edition only)***
Operator:	Equals to Doesn't equal to
Predefined value:	You can select one or more predefined values among 8 of the combo-box such as: • DHCPDISCOVER (BOOTP request) • DHCPOFFER (BOOTP reply) • DHCPREQUEST (BOOTP request) • DHCPACK (BOOTP reply) • DHCPNACK (BOOTP reply) • DHCPDECLINE (BOOTP request) • DHCPRELEASE (BOOTP request) • DHCPINFORM (BOOTP request)

DNS Message Type	***(Enhanced Edition only)***
Operator:	Equals to Doesn't equal to
Predefined value:	You can select one or more predefined values of the combo-box such as: • Query • Response

DNS Message Operation	***(Enhanced Edition only)***
Operator:	Equals to Doesn't equal to
Predefined value:	You can select one or more predefined values of the combo-box such as: • QUERY • IQUERY • NOTIFY • STATUS • UPDATE

FTP Returned Status	***(Enhanced Edition only)***
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify a status value from 0 to 65,535 or select one or more predefined values with the combo-box. A list of status values may be: • A range of values (i.e. 120-250 means from 120 to 250) • Individual values separated by a semicolon (i.e. 500;600) • A mix of the two previous cases (i.e. 500;550-560;599)
Predefined value:	You can select one or more predefined values of the combo-box such as: • OK (200) • Not Found (404) • 1xx Series • 2xx Series • 3xx Series • 4xx Series • 5xx Series

FTP Command	***(Enhanced Edition only)***
Operator:	Equals to Doesn't equal to
Predefined value:	You can select one or more predefined values of the combo-box such as: • ABOR • ACCT • ALLO • APPE • CDUP • CWD • DELE • EPRT • EPSV • FEAT • HELP • LIST • MKD • MODE • NLST • NOOP • OPTS • PASS • PASV • PORT • PWD • QUIT • REIN • REST • RETR • RMD • RNFR • RNTO • SITE • SMNT • STAT • STOR • STOU • STRU • SYST • TYPE • USER

FTP Data	***(Enhanced Edition only)***
Operator:	There is no operator
Predefined value:	There is no predefined value. This parameter indicates the filter creates the list of Dynamic FTP data connections and impairs the packets belonging to a connection of this list.

HTTP Returned Status	***(Enhanced Edition only)***
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify a status value from 0 to 65,535 or select one or more predefined values with the combo-box. A list of status value may be: • A range of values (i.e. 120-250 means from 120 to 250) • Individual values separated by a semicolon (i.e. 500;600) • A mix of the two previous cases (i.e. 500;550-560;599)
Predefined value:	You can select one or more predefined values of the combo-box such as: • OK (200) • Not Found (404) • Moved (301) • 1xx Codes • 2xx Codes • 3xx Codes • 4xx Codes • 5xx Codes

HTTP Method	***(Enhanced Edition only)***
Operator:	Equals to Doesn't equal to
Predefined value:	You can select one or more predefined values of the combo-box such as: • OPTIONS • GET • HEAD • POST • PUT • DELETE • TRACE • CONNECT

NTP	***(Enhanced Edition only)***
Operator:	There is no operator
Predefined value:	There is no predefined value. This parameter indicates the filter will match with the port 123 in either source or destination port

RTP Audio Payload Type	*(Enhanced Edition only)*
Operator:	Equals to Doesn't equal to
Predefined value:	You can select one or more predefined values of the combo-box such as: • 0 PCMU • 3 GSM • 4 G723 • 5 DVI4 • 6 DVI4 • 7 LPC • 8 PCMA • 9 G722 • 10 L16 • 11 L16 • 12 QCELP • 13 CN • 14 MPA • 15 G728 • 16 DVI4 (11,025 Hz) • 17 DVI4 (22,050 Hz) • 18 G729

RTP Video Payload Type	*(Enhanced Edition only)*
Operator:	Equals to Doesn't equal to
Predefined value:	You can select one or more predefined values of the combo-box such as: • 25 CelB • 26 JPEG • 28 nv • 31 H261 • 32 MPV • 33 MP2T • 34 H263

RTP DTMF	*(Enhanced Edition only)*
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify a value included in **[0,9]** or in **[A,D]** or # or *****. As DTMF list, you can enter: • A range of values (i.e. **0-5** means from 0 to 5) • Individual values separated by a semicolon (i.e. **1;A;#**) • A mix of the two previous cases (i.e. **0-9;A-D;#;***) Lists such as **0-D** or **1-#** or **A-*** are not allowed.

RTP (SIP From)	*(Enhanced Edition only)*
Operator:	Equals to Doesn't equal to Contain Doesn't contain
User-defined value or list:	Specify an alphanumeric value identifying the ***SIP From*** field. Example: 172.13.25.4@SIPDev Please note that comparison between the value defined and the ***SIP From*** field received depends on the Operator: - The defined value and the ***SIP From*** field are strictly compared when the operator is 'Equal to' or 'Doesn't equal to' i.e. size and content should be the same. - The defined value is a substring searched in ***SIP From*** field when the operator is 'Contain' or 'Doesn't contain'.

RTP (SIP To)	***(Enhanced Edition only)***
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify an alphanumeric value identifying the ***SIP To*** field. Example: 172.13.25.4@SIPDev Please note that comparison between the value defined and the ***SIP To*** field received depends on the Operator: - The defined value and the ***SIP To*** field are strictly compared when the operator is 'Equal to' or 'Doesn't equal to' i.e. size and content should be the same. - The defined value is a substring searched in ***SIP To*** field when the operator is 'Contain' or 'Doesn't contain'.

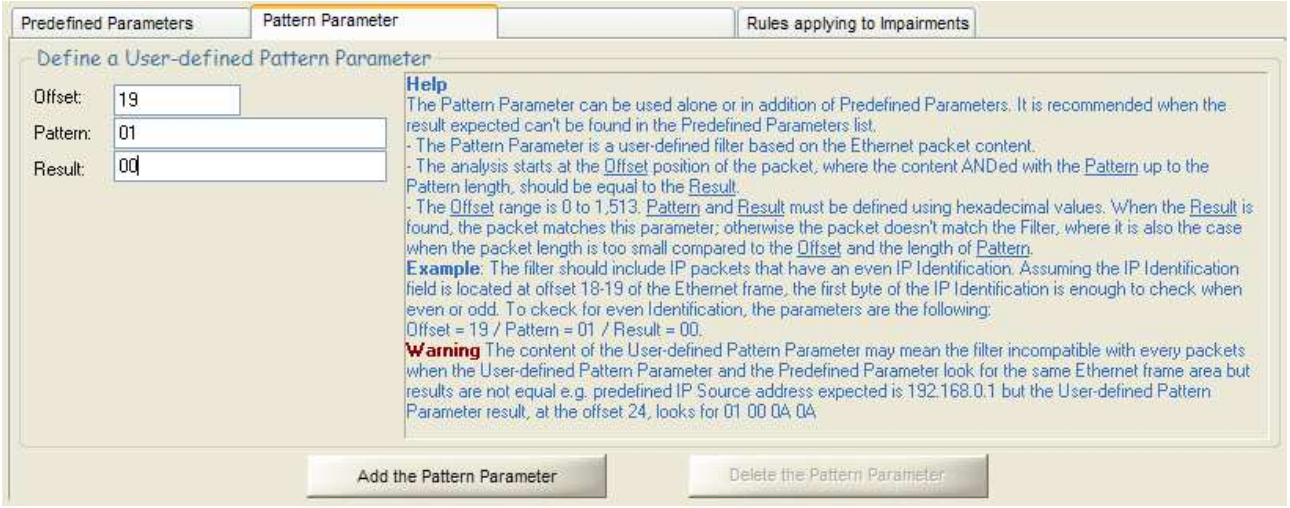
SIP From	***(Enhanced Edition only)***
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify an alphanumeric value identifying the ***SIP From*** field. Example: 172.13.25.4@SIPDev Please note that comparison between the value defined and the ***SIP From*** field received depends on the Operator: - The defined value and the ***SIP From*** field are strictly compared when the operator is 'Equal to' or 'Doesn't equal to' i.e. size and content should be the same. - The defined value is a substring searched in ***SIP From*** field when the operator is 'Contain' or 'Doesn't contain'.

SIP To	***(Enhanced Edition only)***
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify an alphanumeric value identifying the ***SIP To*** field. Example: 172.13.25.4@SIPDev Please note that comparison between the value defined and the ***SIP To*** field received depends on the Operator: - The defined value and the ***SIP To*** field are strictly compared when the operator is 'Equal to' or 'Doesn't equal to' i.e. size and content should be the same. - The defined value is a substring searched in ***SIP To*** field when the operator is 'Contain' or 'Doesn't contain'.

SIP Returned Status	***(Enhanced Edition only)***
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify a status value from 0 to 65,535 or select one or more predefined values with the combo-box. A list of status value may be: • A range of values (i.e. 120-250 means from 120 to 250) • Individual values separated by a semicolon (i.e. 500;600) • A mix of the two previous cases (i.e. 500;550-560;599)
Predefined value:	You can select one or more predefined values of the combo-box such as: • OK (200) • Trying (100) • Ringing (180) • Moved (301) • 1xx Codes • 2xx Codes • 3xx Codes • 4xx Codes • 5xx Codes • 6xx Codes

SIP Request	***(Enhanced Edition only)***
Operator:	Equals to Doesn't equal to
User-defined value or list:	Specify a status value from 0 to 65,535 or select one or more predefined values with the combo-box. A list of status value may be: • A range of values (i.e. 120-250 means from 120 to 250) • Individual values separated by a semicolon (i.e. 500;600) • A mix of the two previous cases (i.e. 500;550-560;599)
Predefined value:	You can select one or more predefined values of the combo-box such as: • INVITE • ACK • BYE • CANCEL • OPTIONS • REGISTER • PRACK • SUBSCRIBE • NOTIFY • PUBLISH • INFO • REFER • MESSAGE • UPDATE

7.4.2.2.2 Filter: the "Pattern Parameter" tab



This tab allows defining a Filter for the flow based on the Ethernet packet content.
The Pattern Parameter can be used alone or in addition with predefined parameters.

We recommend using the **Pattern Parameter** when you can't use a predefined parameter (defined in the **Predefined Parameter** tab).

*Warning: if you have already defined Predefined Parameters and you want using also a pattern parameter, please note that the Filter will consider for the flow the incoming packets matching the Predefined Parameters **AND** the pattern parameter.*

Three user-defined values are used: **Offset**, **Pattern** and **Result**.

The analysis starts at the **Offset** position in the packet – where the content **ANDED** with the **Pattern** up to the pattern length, should be equal to the **Result**.

The **Offset** range is 0 to 1,513. **Pattern** and **Result** must be defined using hexadecimal values.
When the **Result** is found, the packet matches the Pattern Parameter condition.
When the **Result** is not found, the packet doesn't match the pattern Parameter condition – that's also the case when the packet length is too small compared to the **Offset** and the length of the **Pattern**.

Example: Define a filter including IP packets with an even IP identification.
Assuming the IP identification field is located at offset 18-19 of the Ethernet frame, the second byte of the IP identification field is sufficient to check if the even or odd condition is encountered.
To check for an even identification, the parameters are:
Offset = 19
Pattern = 01
Result = 00

7.4.2.2.3 Filter: the "Rules applying to Impairments" tab

This tab is composed of two areas:

- Define the Rules applying to Impairments
- Define a loop for the impairment rules defined above

Define the Rules applying to Impairments

Two conditions can be defined and combined to start the impairments, and one condition to stop:

- Start when finding a Trigger
- Delay before applying impairments (period of time of number of packets)
- Stop impairments after (period of time or number of packets)

Start when finding a Trigger

The Trigger is designed to associate the beginning of the impairment to the content of the Ethernet frames.

Three user-defined values are used: **Offset**, **Pattern** and **Result**.

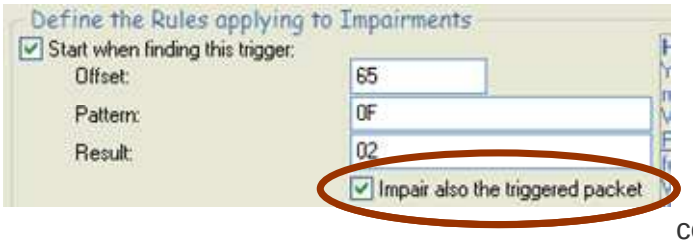
The Trigger is activated when the content of the Ethernet frame matches a given result. To check if the content of the Ethernet frame matches the expected **Result**, a logical AND operation is made between the content of the Ethernet frame and the **Pattern**. The Ethernet frame analysis starts at the given **Offset** value of the frame up to the length of the given **Pattern**. The result of the logical AND operation is compared to the **Result**: the Trigger is activated when both are equal.

When the Trigger is activated, the beginning of the impairment refers to both Interfaces (A to B, B to A).

When a Trigger is set in the Filter of each direction, the activated Trigger starts impairment(s) on both directions.

Impair also the triggered packet

This option allows including or not the Ethernet frame that matches the Result in the list of frames to impair. When this option is checked, the frame that has activated the Trigger is included in the set of frames to impair.
By default, the frame isn't included.



As example, it is useful to let the first frame without impairment when this frame starts the connection to impair i.e. a TCP frame with the SYN flag for any TCP connection. In this case, if the TCP SYN frame had been lost, the connection would not have been able to start so there wouldn't be any frame to impair for this TCP connection.

	NetDisturb *doesn't check if the Trigger is relevant to the parameters of the Filter.*

An example and more explanations on how the Trigger works are given in paragraph 7.4.2.2.4

Delay before applying impairments (period of time or number of packets)

An additional delay or number of packets can be added before **NetDisturb** starts the impairment (with a defined trigger or not).
This delay is expressed in milliseconds, seconds, minutes, hours or number of packets. By default, this delay value is 0, which means that **NetDisturb** starts the impairment immediately.
When this delay is higher than zero, the impairment will start after the given delay. In the meantime, the frames are relayed without being impaired.
A delay greater than zero is needed with some application protocols (i.e. video) – for example: when there is some information to exchange before starting the exchange of the most important frames.

Stop impairments after (period of time or number of packets)

This parameter limits the impairments in the time (expressed in milliseconds, seconds, minutes or hours) or after a number of received packets.

When the impairment stops, the next frames matching the Filter are transferred from the incoming Interface to the outgoing Interface immediately without treatment.

Define a loop for the impairment rules defined above

Two additional conditions can be added to define impairment cycles:

- Create a loop and apply it
- Pause between each loop

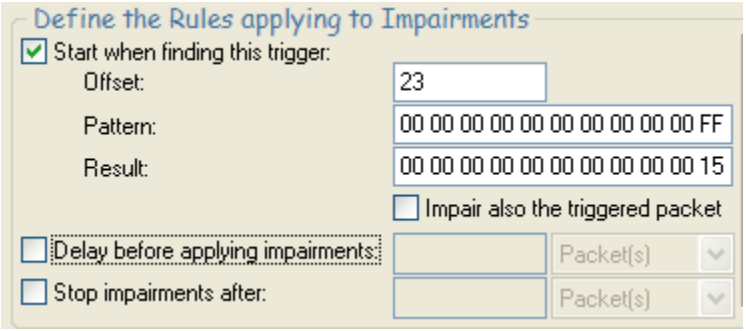
Create a loop and apply it

When a **Number of loops** (value from 0 to 1,000) is specified, the impairment cycle restarts at the beginning of the frame analysis process until the number of loop is reached.
Note: 0 means an infinite loop.

When the **Number of loops** is reached, the impairment(s) stops: the next frames matching the Filter are transferred from the incoming Interface to the outgoing Interface immediately.

Pause between each loop: this parameter introduces a delay between each iteration of the loop. The delay is expressed in number of received packets or a period of time – milliseconds, seconds, minutes or hours.

7.4.2.2.4 Example of using a Trigger



The following example assumes that the impairment should start when a FTP connection is requested. The definition of the pattern is:

- The protocol should be TCP
- The port number should be 21 (FTP)

To define a Trigger that fulfills this requirement, the Pattern analysis starts at the protocol field of the IP Header that is located at the 23rd byte of the Ethernet frame. The port number is located at the 35th byte of the frame. The bytes between the protocol and the port number are not significant.

The definition of this trigger is:

Offset (decimal value) = `23`

Pattern (hexadecimal value) = `FF 00 00 00 00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00 00 00 00 00 00 0F`

Result (hexadecimal value) = `06 00 00 00 00 00 00 00 00 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 01`

The Pattern and the Result parameters should be entered in hexadecimal.

In this example, a VLAN can't be used with these values because it adds 2 bytes before the IP Header. When a VLAN is used the protocol field is the 25th byte of the Ethernet frame.

With this simple Trigger, let's see what's happening with two common Ethernet frames.

The analysis of the Ethernet frames made by NetDisturb is described below. In this example, the first frame is FTP Response frame, the second frame is TCP FIN frame. The part of the frame under analysis is highlighted.

Frame #1 = FTP Response: 221 Good Bye!

Offset	Content
0000	00 11 43 03 a2 18 00 02 55 54 ce 6f 08 00 45 00
0010	00 36 c8 d6 40 00 80 06 af ff c0 a8 00 78 c0 a8
0020	00 23 00 15 09 02 b8 85 7b 14 19 70 dc bf 50 18
0030	fb d2 10 54 00 00 32 32 31 20 47 6f 6f 64 62 79
0040	65 21 0d 0a

The analysis process is the following:

```
Frame part to analyze:      06 af ff c0 a8 00 78 c0 a8 00 23 00 15 09 02 b8 85 7b 14
                            19 70 dc bf 50 18

                                   Logical AND with the Pattern

Pattern:                    FF 00 00 00 00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00
                            00 00 00 00 00 0F


Frame after the AND:        06 00 00 00 00 00 00 00 00 00 00 00 15 00 00 00 00 00 00
                            00 00 00 00 00 08


Result expected:            06 00 00 00 00 00 00 00 00 00 00 00 15 00 00 00 00 00 00
                            00 00 00 00 00 01
```

The Result is not equal to the frame after the AND operation. **The Trigger isn't activated**.

Frame #2 = TCP FIN ACK

Offset	Content
0000	00 11 43 03 a2 18 00 02 55 54 ce 6f 08 00 45 00
0010	00 28 c8 d7 40 00 80 06 b0 0c c0 a8 00 78 c0 a8
0020	00 23 00 15 09 02 b8 85 7b 22 19 70 dc bf 50 11
0030	fb d2 ff 25 00 00 00 00 00 00 00 00

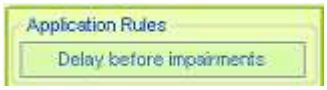
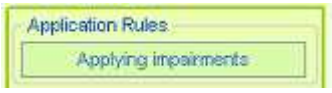
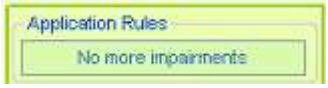
The analysis process is the following:

```
Frame part to analyze:      06 b0 0c c0 a8 00 78 c0 a8 00 23 00 15 09 02 b8 85 7b 22
                            19 70 dc bf 50 11

                                   Logical AND with the Pattern

Pattern:                    FF 00 00 00 00 00 00 00 00 00 00 00 FF 00 00 00 00 00 00
                            00 00 00 00 00 0F


Frame after the AND:        06 00 00 00 00 00 00 00 00 00 00 00 15 00 00 00 00 00 00
                            00 00 00 00 00 01


Result expected:            06 00 00 00 00 00 00 00 00 00 00 00 15 00 00 00 00 00 00
                            00 00 00 00 00 01
```

The Result is equal to the frame after the AND operation. **The Trigger is activated!**

7.4.2.2.5 The Trigger Dynamics

This paragraph gives some examples for the use of Trigger parameters to explain the 5 states of a Trigger:

1. Waiting for the trigger. The Application of Rules gets this state before the trigger has been found. There are 2 cases when a Trigger gets this state: either the IP Flow has just been started or, the end of the pause between each loop has been reached and the Number of Cycles hasn't been reached. In this state, Ethernet frames matching the filter are relayed without impairment.	
2. Delay before applying impairments. The Application of Rules gets this state when the Delay before Impairment has not yet expired. When a trigger has been defined, this state means that an Ethernet frame matching the trigger has been found. In this state, Ethernet frames matching the filter are relayed without impairment.	
3. Applying impairments. The Application of Rules gets this state when the Impairment applies, for one of the following reasons: - There was no trigger and no Delay before Impairment defined. - A Trigger was defined and the Ethernet frame matching it has been found - A Delay before Impairment was defined and this delay has expired - Both of the 2 previous reasons (Trigger & Delay before Impairment) have been reached. In these cases, Ethernet frames matching the filter are impaired.	
4. Delay before next cycle running. The impairments still do not apply because the Stop Impairment condition (delay or number of packets) has been reached and a pause between 2 loops has been defined. This state is available only when cycles are defined. In this state, Ethernet frames matching the filter are relayed without impairment.	
5. No more impairment. The Application of Rules gets this state when the maximum number loops have been reached. This is a permanent state until the Flow is stopped. In this state, Ethernet frames matching the filter are relayed without impairment.	

The Figure 1 illustrates the configuration with only the Trigger defined i.e. Duration of Impairment nor Stop. When the Trigger has been reached, the Impairment remains active until the Flow is stopped.

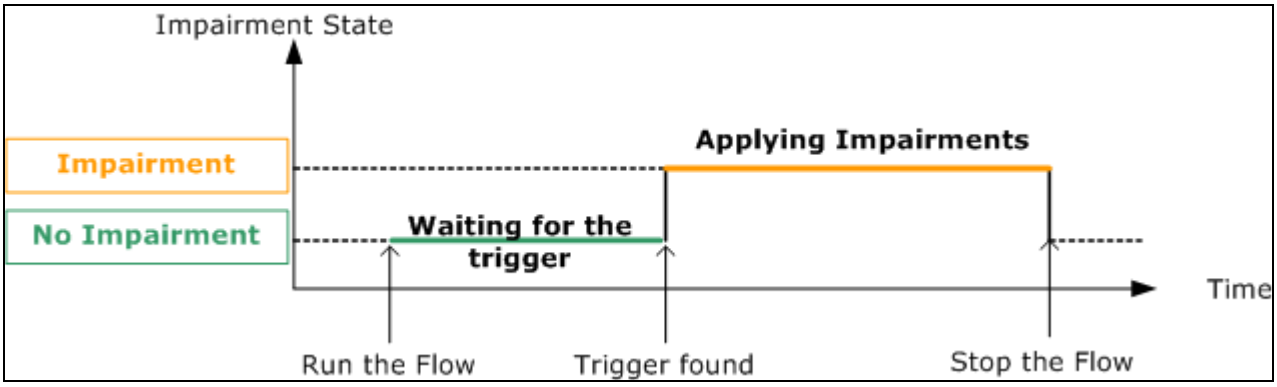


Figure 1 - Impairment Rules with just a Trigger defined (no Delay for applying Impairment nor Stop)

The Figure 2 illustrates the configuration where the Trigger and the Delay before applying Impairments have been defined. The Stop condition is not defined. When the Trigger has been reached, the Impairment(s) starts after the Delay and remains active until the Flow is stopped.

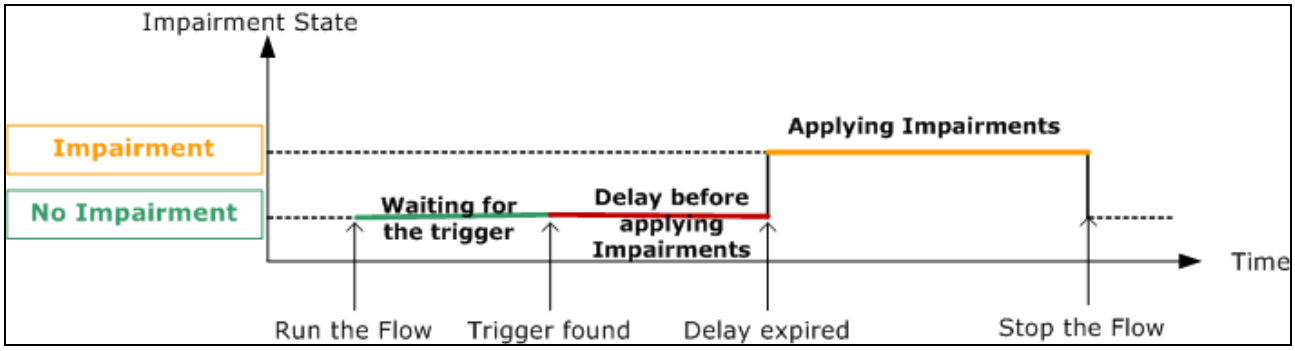


Figure 2 - Impairment Rules with a Trigger and a Delay before applying Impairment

The Figure 3 illustrates the configuration of the Impairment Rules with a Trigger without the Delay before applying Impairments but and a Stop condition set: the Stop condition is the duration of the impairment. There is an unlimited number of Loops.

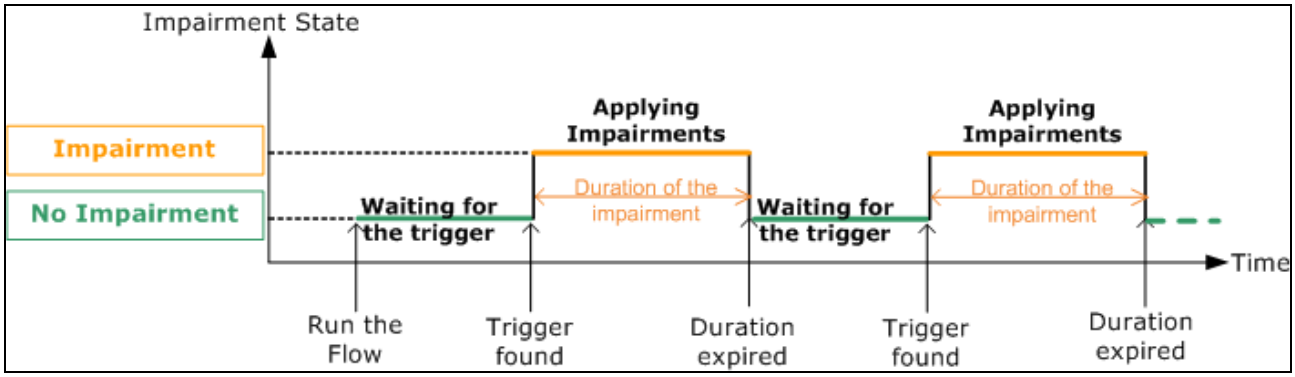


Figure 3 - Impairment Rules with a Trigger, a Stop Impairment Duration and an unlimited number of loops

The **Error! Reference source not found.** illustrates the configuration of Impairment Rules without any trigger but the Stop impairment condition and a number of loops limited to 1.

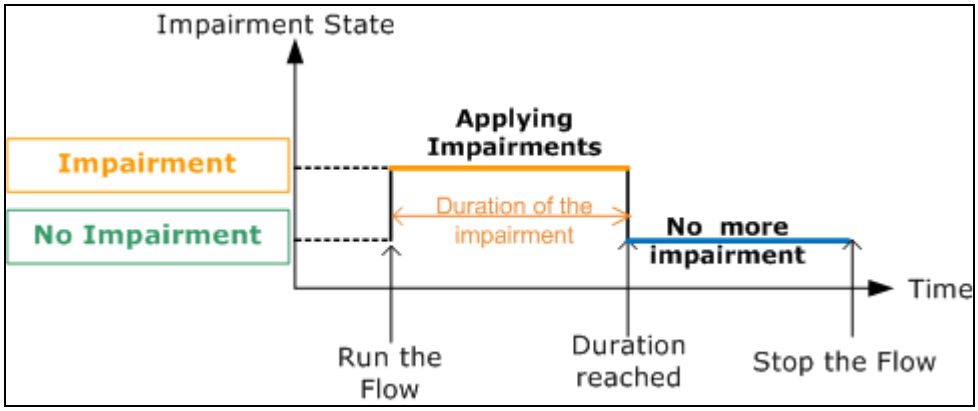


Figure 4 – Impairment Rules with the Impairment Duration and 1 Cycle

The Figure 5 illustrates the configuration of Rules to apply to Impairments with a Delay Applying before the Impairment not zero, the Duration of the Impairment not zero and a Number of Cycles set to 2.

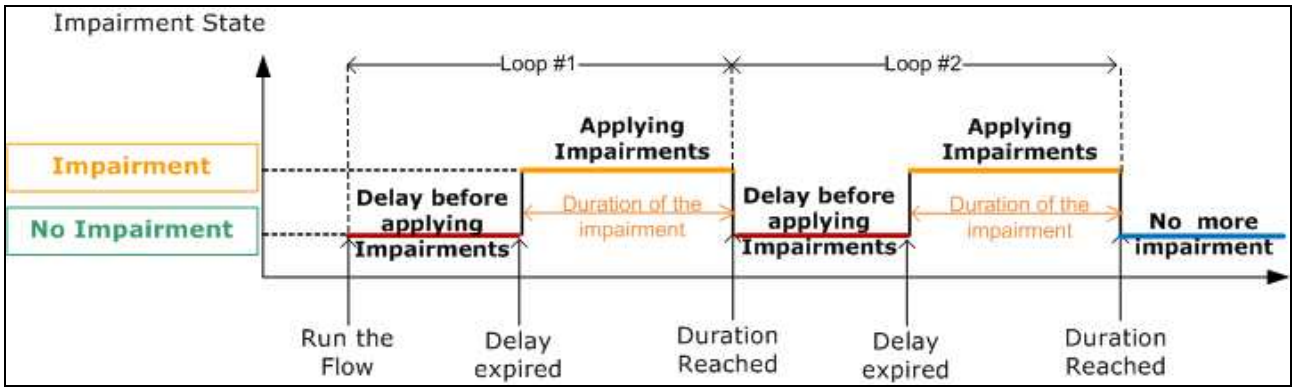


Figure 5 – Impairment Rules with a Delay, Impairment Duration and a limited number of Cycles

7.4.2.3 Association with another Flow (Enhanced Edition only)

The association of a filter with another Flow is used with SIP or FTP filters: these filters contain the required information describing the data flows. The data flows are using RTP or FTP-Data (respectively). The Association with another Flow helps to keep the information included in the SIP or FTP flows to create the list of dynamic connections that will convey the data. The Association with another flow is available with the NetDisturb Enhanced Edition because it requires the application protocol filters that are only available with the NetDisturb Enhanced Edition.

7.4.2.3.1 How NetDisturb handles the frames

The general algorithm used by NetDisturb to handle the Ethernet frames consist in finding the filter a frame is matching. When a filter has been found, NetDisturb stops the search process of a filter and it applies the impairment laws defined for this flow (Loss & Duplication, Delay & Jitter, packet content change) to the packet.

7.4.2.3.2 How NetDisturb discovers the dynamic RTP or FTP-Data connections

The RTP and FTP-Data connection don't use a fix port number and the IP address may be different than the one use with the server. NetDisturb needs to analyze the content of the SIP and

FTP (port 21) connections to discover which IP address and port is going to contain RTP and FTP data. When such couple (port and IP address) has been found, it is added in the list connection of the RTP (or FTP data). For RTP filter, additional parameters (payload type, SIP From or To fields) could be required before the couple is added in this list.

However, the handler of frames described in 7.4.2.3.1 prevents a RTP or FTP-Data flow to get the information from packets matching previous flows. This is why the Association with another flow is needed.

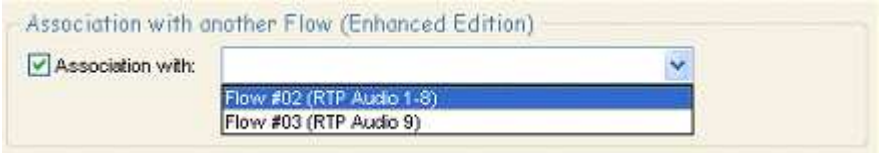
7.4.2.3.3 When to use Association with another Flow

The Association with another Flow is required when the packets of the SIP (or FTP) belongs to a Flow located above the relevant RTP (or FTP-Data respectively) because NetDisturb stops to analyze the frame content as described in paragraph 7.4.2.3.1.
When using SIP, if you are intended to impair both the SIP and the RTP flows that could linked together i.e. the SIP filter contains the information about the RTP flows to impair too, you need to activate the Association with another Flow for the SIP flow to indicate to NetDisturb that such RTP flow could get the content SIP packets. The RTP engine processes the packet before it is lost or changed using the SIP impairment laws defined for that SIP flow.

7.4.2.3.4 When the Association with another Flow is available

The Association with another Flow availability is activated when the filter under definition is SIP or FTP, if RTP or FTP-Data flows respectively still exist. When the filter doesn't belong to SIP or FTP the area is grayed, as shown below.

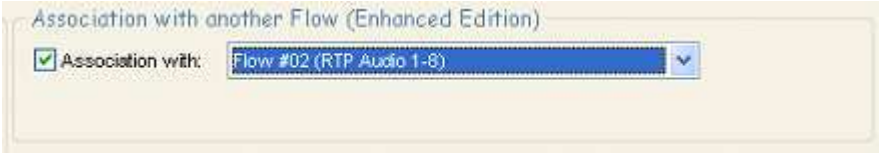
When SIP is going to be defined, the flows that have been created using the RTP parameters are presented in the available flow.



In the way, when FTP is going to be defined, the flows that have been created using the FTP-Data parameter are presented in the available flow.

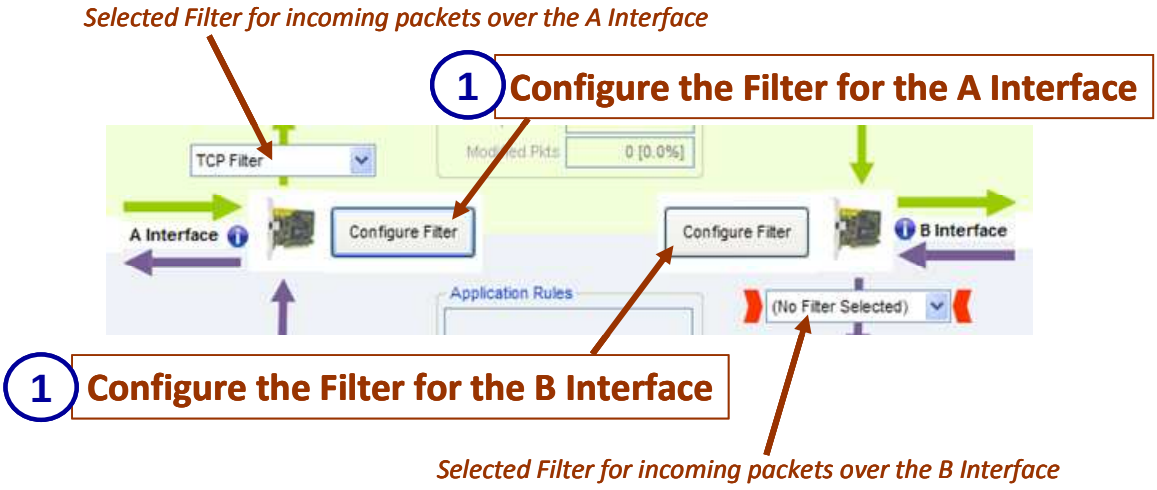
The flow number and the name (if defined) are displayed in the list.

You may associate only one flow to the SIP or FTP data filter.



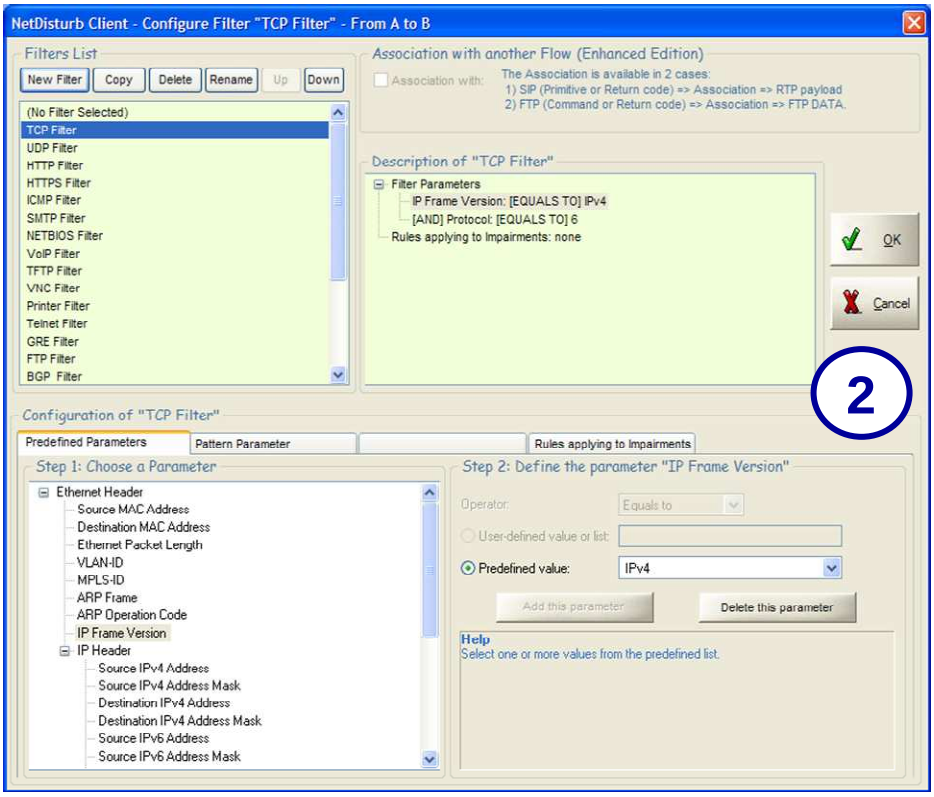
7.4.2.4 How to Create a New Filter with its parameters in a few steps

1) Click on the **Configure Filter** button as shown below:

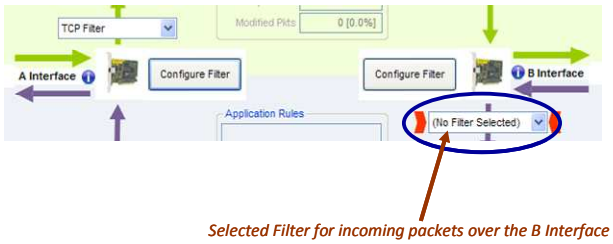


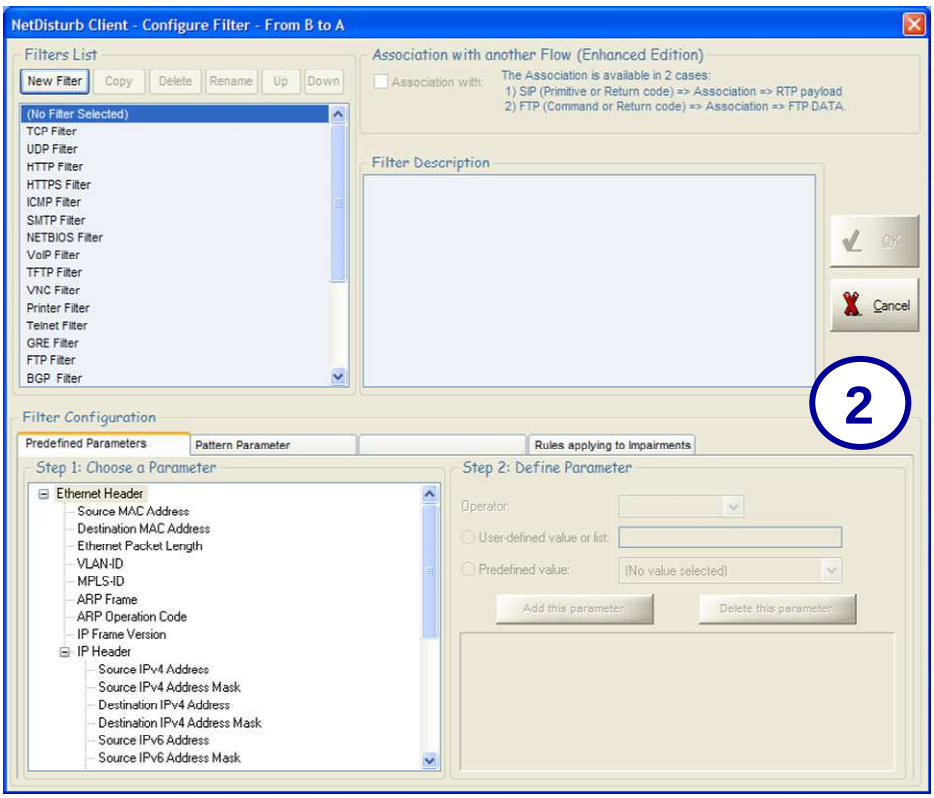
2) Then the **Configure Filter** window is displayed. The title of the window indicates the considered direction (**From A to B** or **From B to A**).

If a Filter was already selected in the combo-box related to the Interface, for example **TCP Filter** on the A interface as shown below, the Configure Filter window opens with the **TCP Filter** already selected.

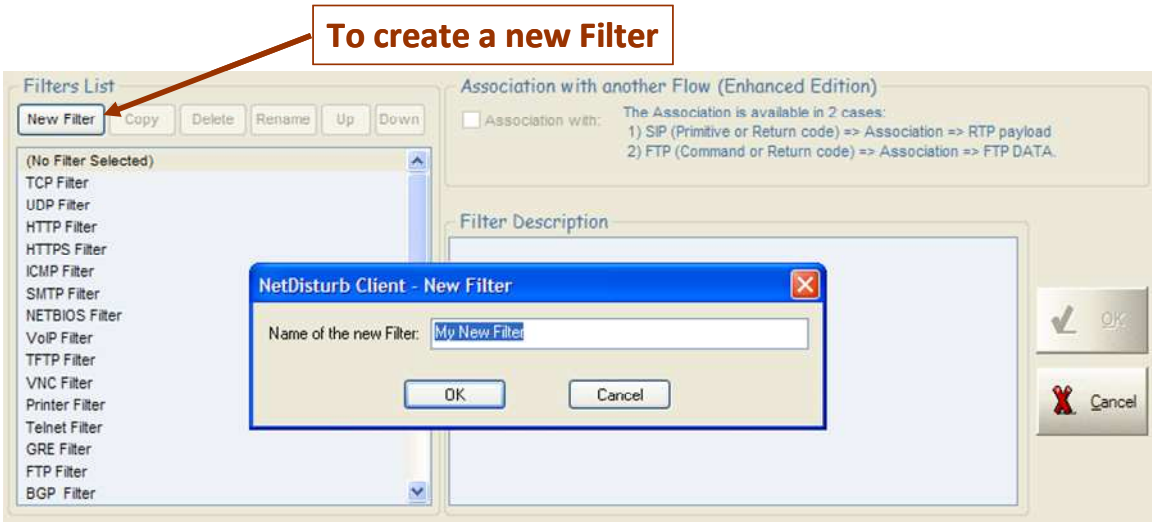


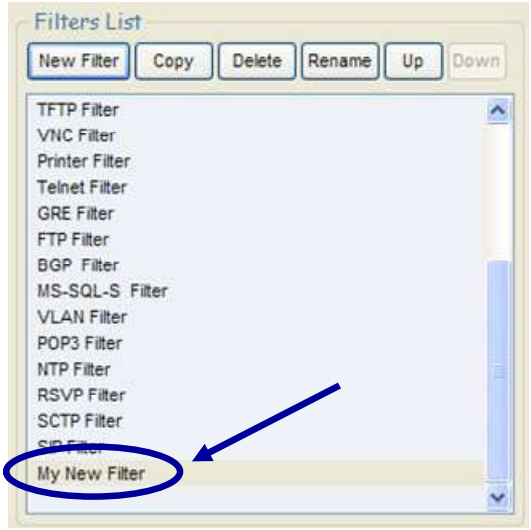
If no Filter was already selected in the combo-box related to the Interface, for example on the B interface as shown below, the Configure Filter window opens with **No Filter Selected**.





3) Then click on the New Filter button and enter the name of the new Filter.



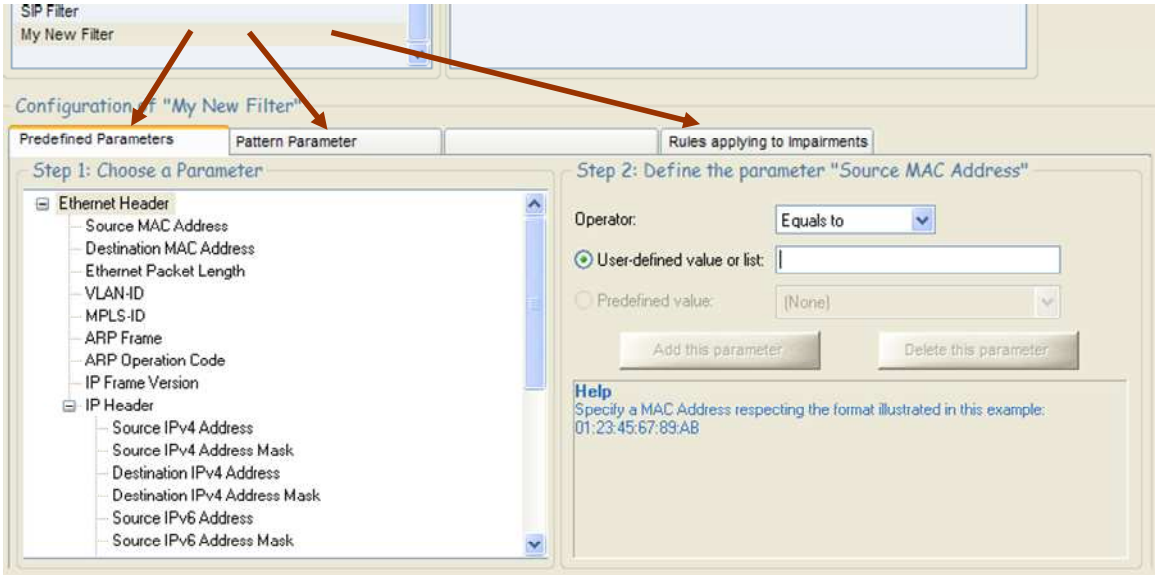


The new Filter is added at the end of the list.

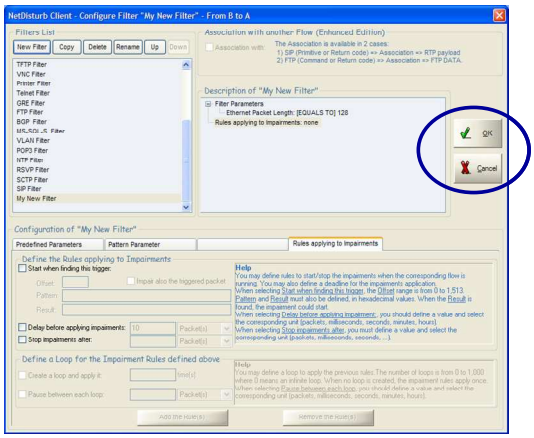
By using the buttons located at the top of the list, you can copy, delete, rename, and move up or down a filter in the list.

4) Once a Filter is defined or selected, then you can enter or modify the parameters by using the tabs:

- Tab 1: Predefined Parameters
- Tab 2: Pattern Parameter
- Tab 3: Rules applying to Impairments



When at least one parameter is defined for a Filter, then you can save the Filter and quit the window by pressing OK.

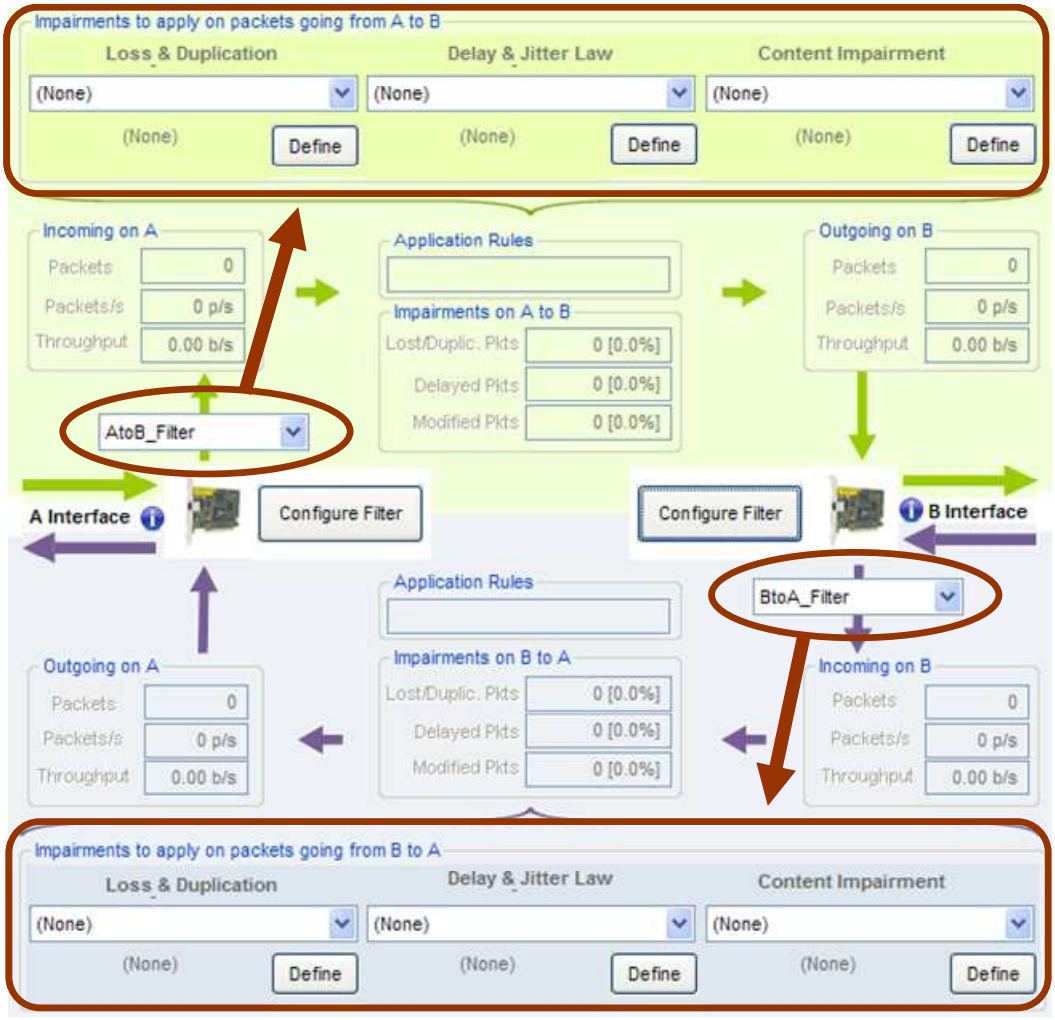


5) Return at step 2 if you want continues to edit or create a new Filter.

6) Press "OK" or "Cancel" to quit the **Configure Filter** window.

7.4.3 Use of Laws to create Impairments

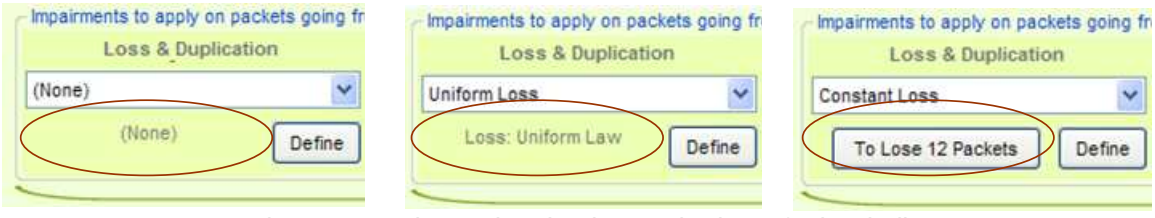
Once a Filter is selected for a direction (A to B or B to A), then the area to access the laws to define impairments is enabled as shown below.



For each direction, 3 types of laws can be defined and used simultaneously:

- Loss & Duplication
- Delay & Jitter
- Content Impairment

The following paragraphs describe each type of law.



Note: the text area located under the combo-box of a law indicates a comment or can contain an action button.

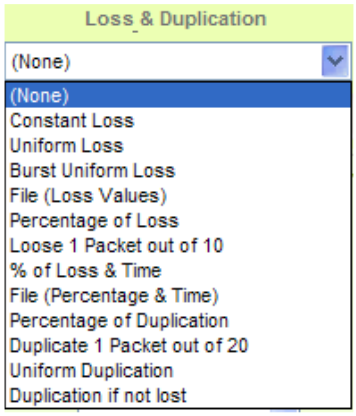
7.4.4 The Loss & Duplication Law Configuration

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

- **NetDisturb** losses the selected IP packets following either the mathematical law configured or a percentage or a 1 out of N law or discrete values extracted from a user file.
- **NetDisturb** is able to duplicate IP packets following either the Uniform mathematical law configured by User or a percentage or a 1 out of M law.
- **NetDisturb** is able to loose packets following a 1 out of N law and then duplicate the non-lost packets following a 1 out of M law.

Up to 100 Loss & Duplication laws can be created.

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



The description of each law is given below.

Combo-box (Law identifier)	(None)	**Description**
(None)	(None)	With this option, no duplication and no loss law apply to the Flow.
Loss Law		
Constant Loss	Loss: Constant Law with the button "To Lose 12 packets"	12 packets are lost each time the user activates this button.
Uniform Loss	Loss: Uniform Law	Domain values [1 to 100] Threshold = 30
Burst Uniform Loss	Loss: Burst Uniform Law	Domain values [10 to 1000] Threshold (n) = 350 Threshold (n+x) = 380 Depth = 2
File (Loss Values)	Loss: File (Loss Values)	Sample file: OnePer100.txt Loss of 1 packet per 100 packets
Percentage of Loss	Loss: Percentage	Percentage: 15
Loose 1 Packet out of 10	Loss: 1 Packet out of N	Range (N): 10
% of Loss & Time	Loss: Percentage & Duration	Period of 30 seconds of loss (up to 10 %) alternating with period of 2 minutes without loss.
File (Percentage & Time)	Loss: File (Percentage & Duration)	Sample file: PercentageLossAndDurationSample.txt Loss up to 50 % with steps of 5% each 10 seconds.

Duplication Law		
Percentage of Duplication	Duplication: Percentage	Percentage = 10 % Minimal Duplication = 1 Maximal Duplication = 3
Duplicate 1 Packet out of 20	Duplication: 1 Packet out of M	Range (N): 20 Minimal Duplication = 1 Maximal Duplication = 3
Uniform Duplication	Duplication: Uniform Law	Alpha: 1 – Beta: 50 Threshold: 10 Minimal Duplication = 1 Maximal Duplication = 1
Duplication if not lost	Loss (1 out of N) then Duplication (1 out of M)	Loss Range (N): 100 Duplication Range (M): 50 Minimal Duplication = 1 Maximal Duplication = 3

7.4.4.1 Loss & Duplication Law and the Working Mode

Working Mode: Laws apply to the IP Flow

When a Loss & Duplication law is selected on a given IP Flow, the law applies to all packets matching the Filter. For each new packet, a new value is extracted from the law or from the file, depending on the type of law selected. These values are stored in a global table by **NetDisturb**. When the table is empty, **NetDisturb** Server provides a new table to 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 may be delayed.

Working Mode: Laws apply to each TCP/UDP connection of the IP Flow

When a Loss & Duplication law is selected for a given IP Flow, the law applies to all packets matching the Filter.

These values are stored in a table maintained by **NetDisturb**.

The **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, the **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 the IP addresses and protocol are only used.

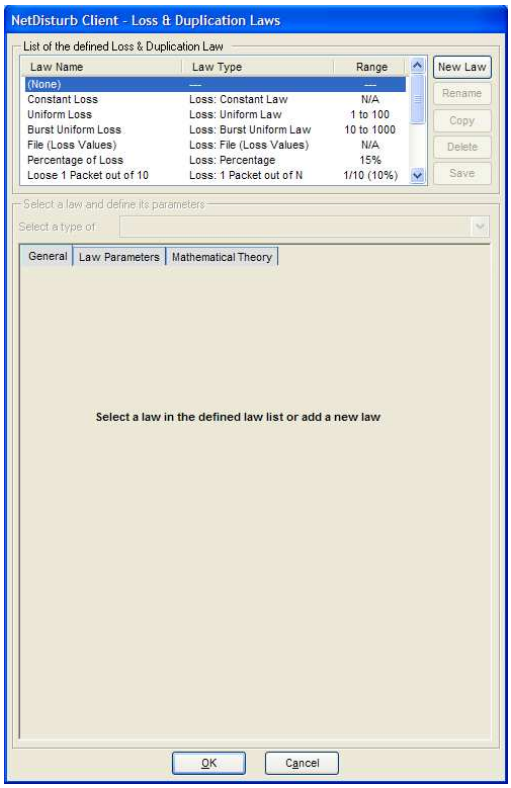
For each packet, a loss value is extracted from the loss value buffer, at the current index of the packet of the given connection. When the end of the table is reached, values extracted restart at the beginning.

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.

7.4.4.2 How to create or edit the Loss & Duplication Law

To create or configure a Loss & Duplication Law click on the “Edit” button at the top or bottom part of the main window.

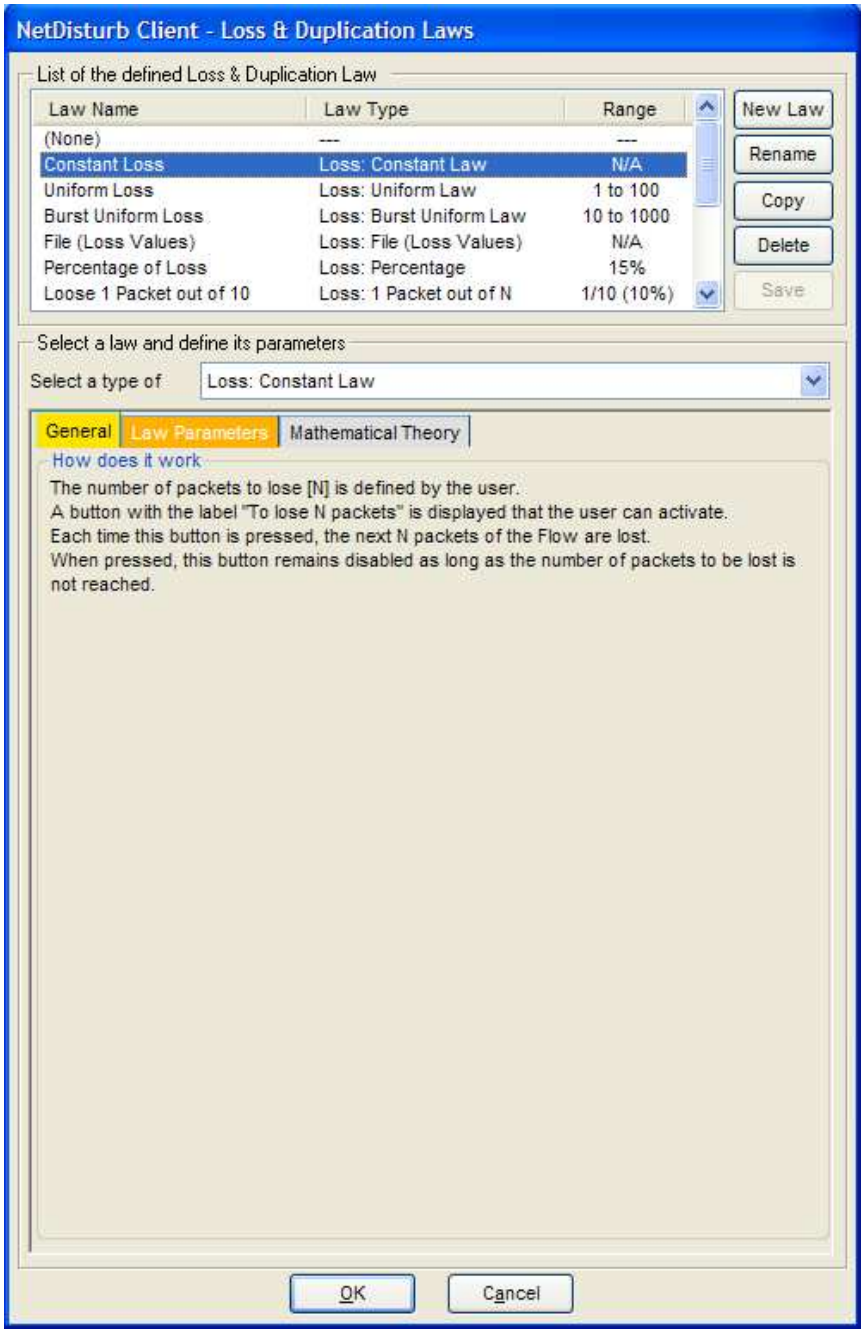
The following window is then displayed:



This window allows creating a new law or modifying an existing one.

If **(None)** is selected, only the New Law button is enabled and the tabs to define the parameters are disabled.

If you select a preexisting law in the current list-box, then the parameters and the details about this law can be viewed and the first "General" tab is enabled.



This window is composed of two areas:

- **List of the defined Loss & Duplication La**w: a list-box displays the defined laws and five buttons allow managing the laws: **New Law**, **Rename**, **Copy**, **Delete** and **Save**.
- **Select a Law and define its parameters:** a list-box displays the loss and duplication laws authorized by the software. Then there are 3 tabs to define and set up the parameters of the selected law.
  - (Tab 1) **General** (explaining how does the impairment law work)
  - (Tab 2) **Law Parameters**
  - (Tab 3) **Mathematical Theory** (only available with Loss & Duplication Laws using a mathematical law)

7.4.4.2.1 List of the Loss & Duplication Laws defined

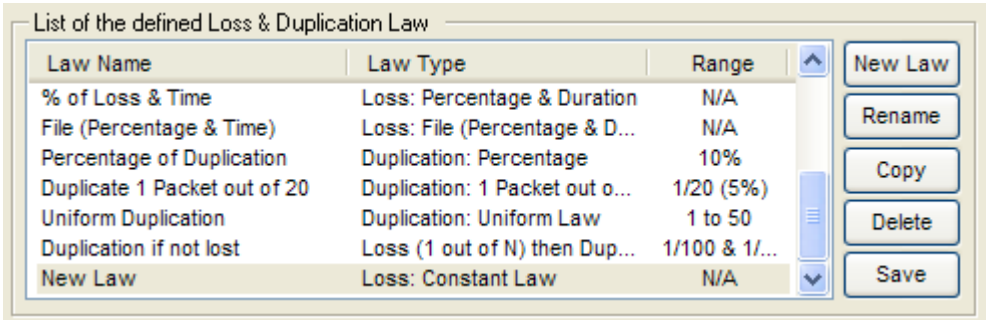
The list-box displays for each defined law the summary of the characteristics, except for (None) corresponding to 'No Loss & Duplication Law' selected:

- Law Name: name of the law
- Law Type: the type of Loss & Duplication law chosen amongst the pre-defined list (more details available in paragraph **Error! Reference source not found.** Select a law and define its parameters)
- Range: range of values generated by the specified laws.

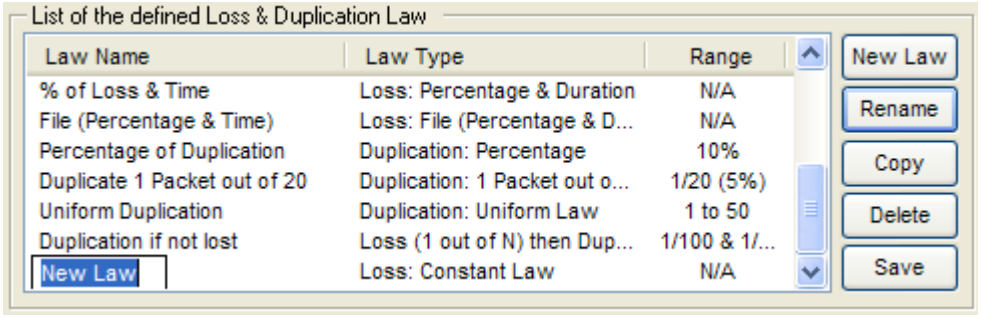
To manage the Law list, various buttons are available:

New Law: this button should be used to add a new Law in the defined Law list.

After pressing the New Law button, a new entry is added at the end of the list-box with 'New Law' as name of the law:

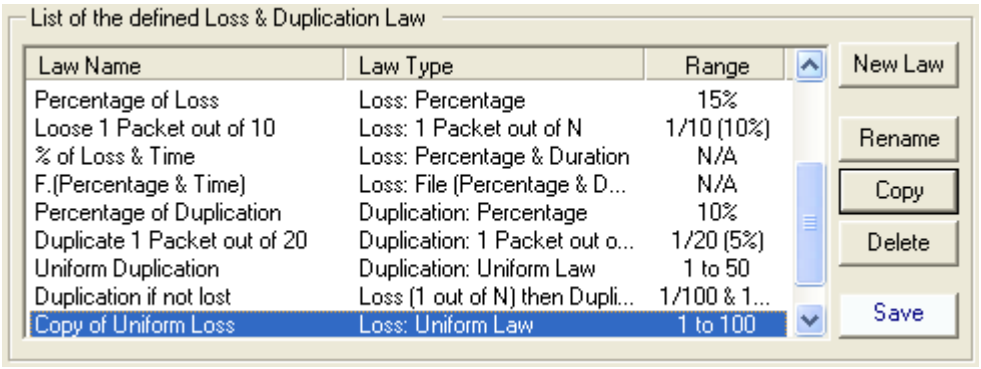


Then click on 'New Law' label to rename this entry or press the Rename button:

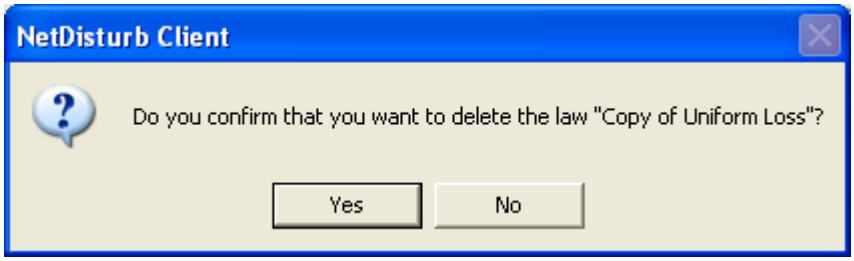


Rename: to rename the Law. This button should be used to change the Law name.

Copy: this button copies the current selected law at the end of the list with a new name. The following example shows the new list-box after copying the existing Uniform Loss law:



Delete: this button should be used to remove a Law from the current list.
First select in the list-box the law to delete and then press the Delete button. A confirmation window is then displayed:



Save: to save all changes related to the laws.

7.4.4.2.2 Select a law and define its parameters

Once a law has been created, then you can define or modify the parameters of the law:

The first step is to choose the law type amongst the list of the pre-defined laws.

Then there are 3 tabs to define and to help the user to set up the parameters of the selected law.

- (Tab 1) **General** (explaining how does the impairment law work)
- (Tab 2) **Law Parameters**
- (Tab 3) **Mathematical Theory** (only available with Loss & Duplication Laws using a mathematical law). This tab gives some details on the theory of the mathematical law used.

⇨ Select a type of law

A combo box allows selecting a law among the following pre-defined laws:

- Loss: Constant law
  Parameter: number of packets
- Loss: Uniform law
  Parameters: alpha, beta, threshold
- Loss: Burst Uniform law
  Parameters: alpha, beta, threshold(n), threshold(n + x), depth
- Loss: File (Loss Values)
  Parameters: filename, threshold

- Loss: Percentage
  Parameter: percentage

- Loss: 1 Packet out of N
  Parameter: range(N)

- Loss: Percentage & Duration (time-limited loss percentage)
  Parameters: percentage, duration

- Loss: File (Percentage & Duration)
  Parameters: percentage, filename

- Duplication: Percentage
  Parameters: percentage, Min ≤ n ≤ Max

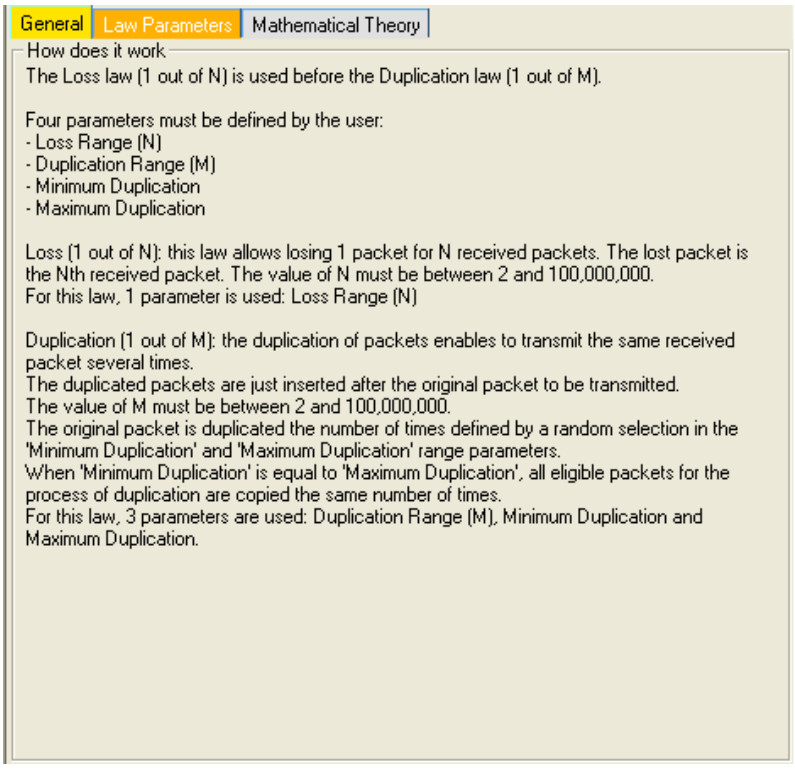
- Duplication: 1 Packet out of M
  Parameters: range(M), Min ≤ n ≤ Max

- Duplication: Uniform Law
  Parameters: alpha, beta, threshold

- Loss (1 out of N) then Duplication (1 out of M): the loss law (1 out of N) is used first before the duplication law (1 out of M)

⇨ The “General” tab (tab 1)

Details on the law type chosen and on the way to choose the parameters are provided on this tab as shown on the figure below:



⇨ The “Law Parameters” tab (tab 2)

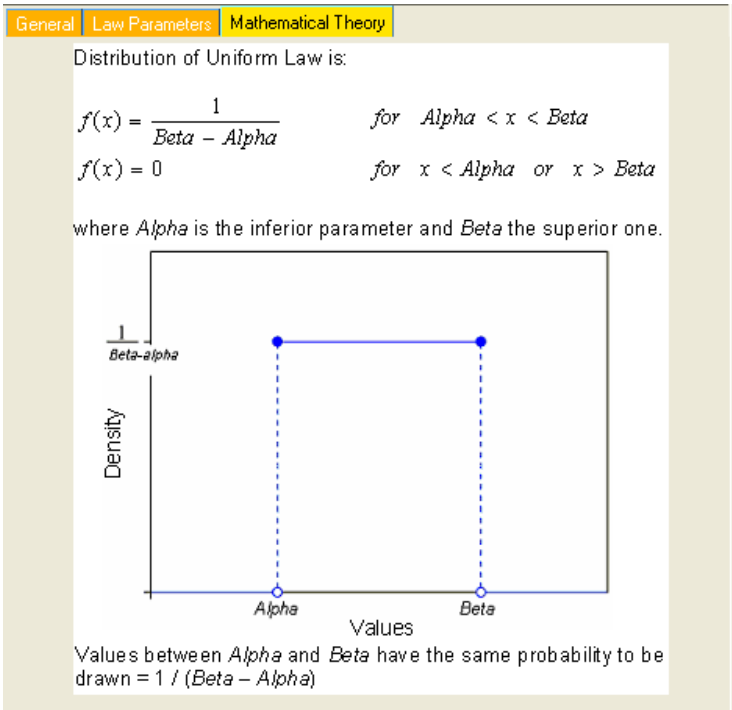
This tab is described for each law type here after.

⇨ The “Mathematical Theory” tab (tab 3)

This tab is available with the following laws only:

- Loss: Uniform Law
- Loss: Burst Uniform Law
- Duplication: Uniform Law

This tab provides the main explanations of the mathematical theory of the law as shown on the figure below:



⇨ Action buttons

The "Loss & Duplication Laws" window handles a temporary list of laws until the user press the OK or Cancel button.

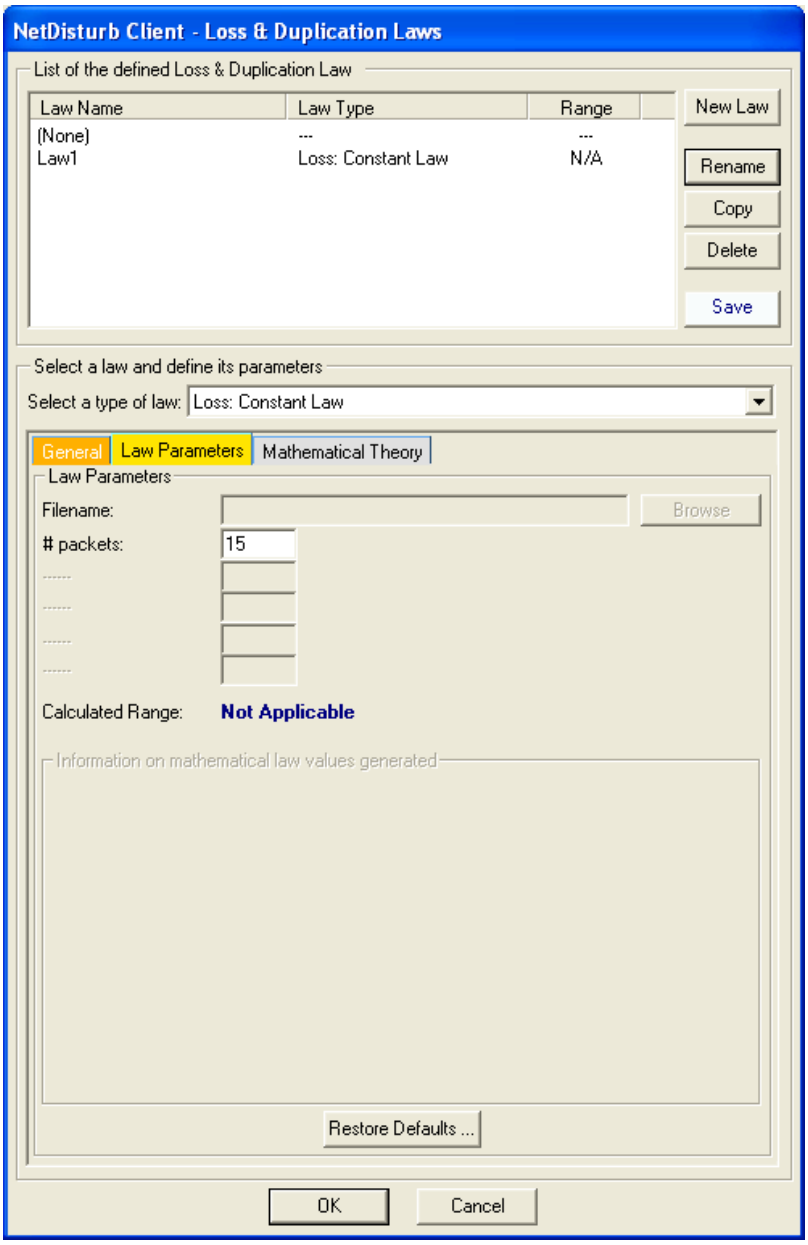
Button	*Action*
Restore Defaults …	Reset all parameters of the current law.
OK	Save all modifications made if you didn't save them before. Moreover, the selected law in the list of the defined laws becomes the selected law in the combo-box of the IP Flow window.
Cancel	Ignore all modifications made if you didn't click on the Save button before. In that case, the last law selected in the combo-box of the IP Flow window is kept.

How to create a new Loss & Duplication Law:

1. Click on the "New Law" button,
2. Then click on the “Rename” button to modify the name of the law.
3. Choose one of the pre-defined law in the combo box
4. Select the "Law Parameters" tab,
5. Enter law parameter(s). The "General" tab and the "Mathematical Theory" tab contain information that can be useful to define the parameters.
6. Press the “Save“ button to save the changes and to continue to create or modify other laws.
7. Press “OK” to quit the “Loss & Duplication Laws” window and to select this new law as the law to be applied on the corresponding Flow.

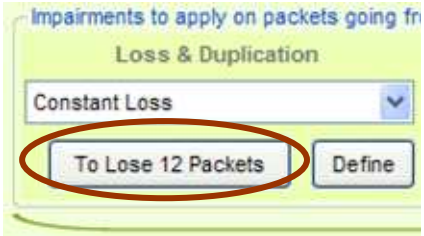
7.4.4.3 Loss: Constant Law

When this law is selected, the **NetDisturb** driver will lose the number of packets defined.



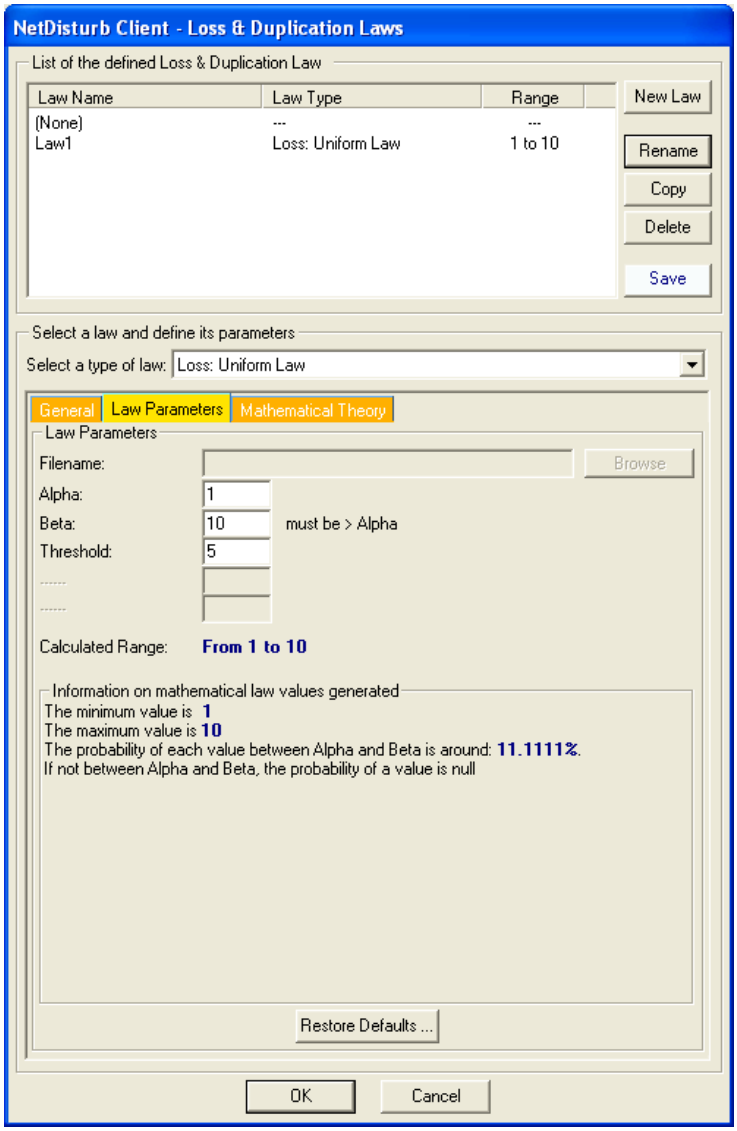
For this law, only one parameter must be defined: **number of packets**

A button with the label "To lose N packets" is displayed that the user can activate. Each time this button is pressed, the next N packets of the flow are lost. When pressed, this button remains disabled as long as the number of packets to be lost is not reached.



7.4.4.4 Loss: Uniform Law

When this law is selected, a uniform distribution of numbers contained between the **Alpha** and **Beta** values 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 7.4.4.1) for each selected packet. If this number is greater or equal than the threshold, then the packet is lost.

The mathematical function used is (see the Uniform Law in Part 10 for more information):

Uniform law on (α, β) range

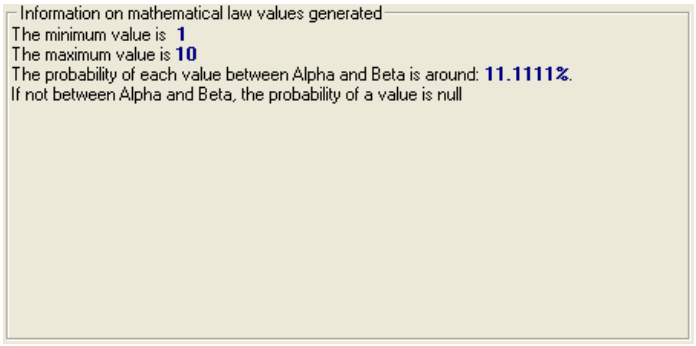
$f(x) = 1/(\beta - \alpha)$ if $\alpha < x < \beta$

$f(x) = 0$ else

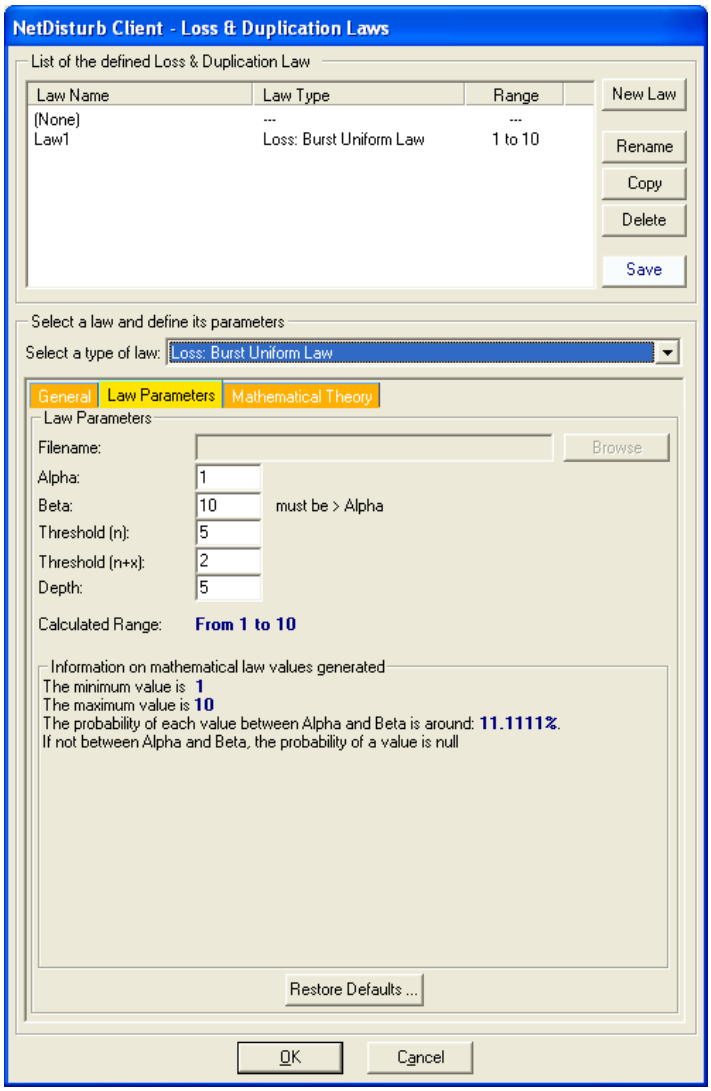
For this law, three parameters are defined:

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

An additional area, called “Information on mathematical law values generated” is available with this law. Here are provided some information about the minimum and maximum values. The mathematical law generates these values using the user-defined parameters. Moreover, the probability of each value that can be generated is also shown.



7.4.4.5 Loss: Burst Uniform Law



When this law is selected, the loss of packets is uniformly distributed with burst of loss enabled. The burst is limited by the **Depth** parameter: this is a set of consecutive packets.

When the law generates a value equal or greater than the **Threshold(n)** parameter, the first packet of the set of packets is lost.

For the next packets of the set, the value of the law is compared to the **Threshold(n+x)** parameter until the law generates the no loss value, or when the number of lost packets equals the **Depth** value.

As for 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 the **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:

- ⇨ The **NetDisturb** driver picks a number from the table for each packet (see also 7.4.4.1)
- ⇨ For the packet n, the **NetDisturb** driver picks one number from the table (current number) and loses this packet 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 used 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).

The mathematical function used is (click on the “Mathematical Theory” tab or see the Uniform Law in Part 10 for more information):

Uniform law on (α, β) range

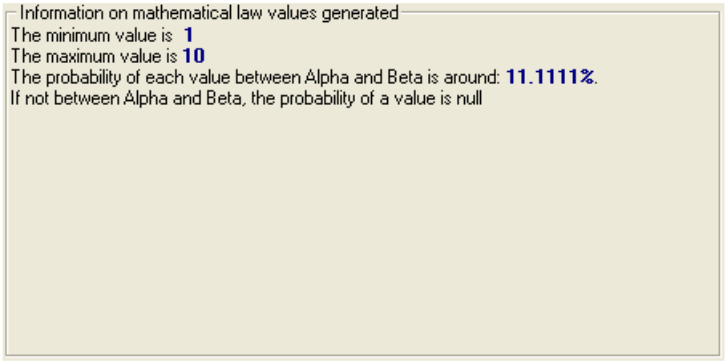
$f(x) = 1/(\beta - \alpha)$ if $\alpha < x < \beta$

$f(x) = 0$ else

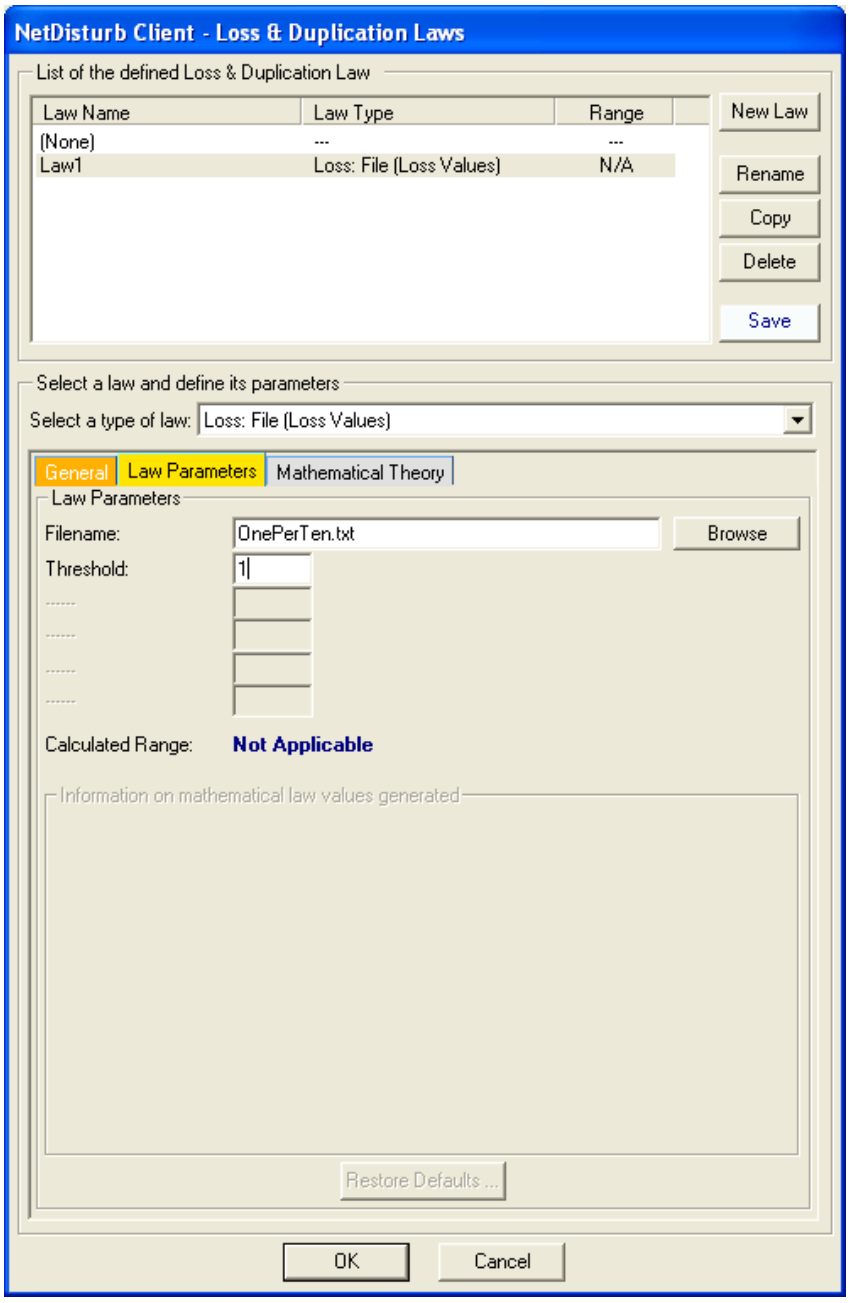
For this law, five parameters are defined:

- **Alpha:** min value of the range
- **Beta:** max value of the range
- **Threshold(n):** first loss factor
- **Threshold(n+x):** second loss factor
- **Depth:** burst limit

An additional area, called “Information on mathematical law values generated” is available with this law. Here are provided some information about the minimum and maximum values. The mathematical law generates these values using the user-defined parameters. Moreover, the probability of each value that can be generated is also shown.



7.4.4.6 Loss: User-defined File



When this law is selected, the loss values are extracted from the user-defined file. This 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.

If a line starts with a sharp (#) character, the rest of the line is ignored i.e. up to the End of Line (CR or CR-LF).

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

If the file size exceeds the 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, the file is read again from the beginning to complete the table.

The **NetDisturb** driver picks a number in the table (see also 7.4.4.1) for each selected packet. If this number is greater or equal than the threshold, then the packet is lost. When the end of the file is reached, the **NetDisturb** driver restarts with the beginning of the file in a circular way.

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

(Content of the OnePerTen.txt file is: `0 0 0 0 0 0 0 0 0 100`)

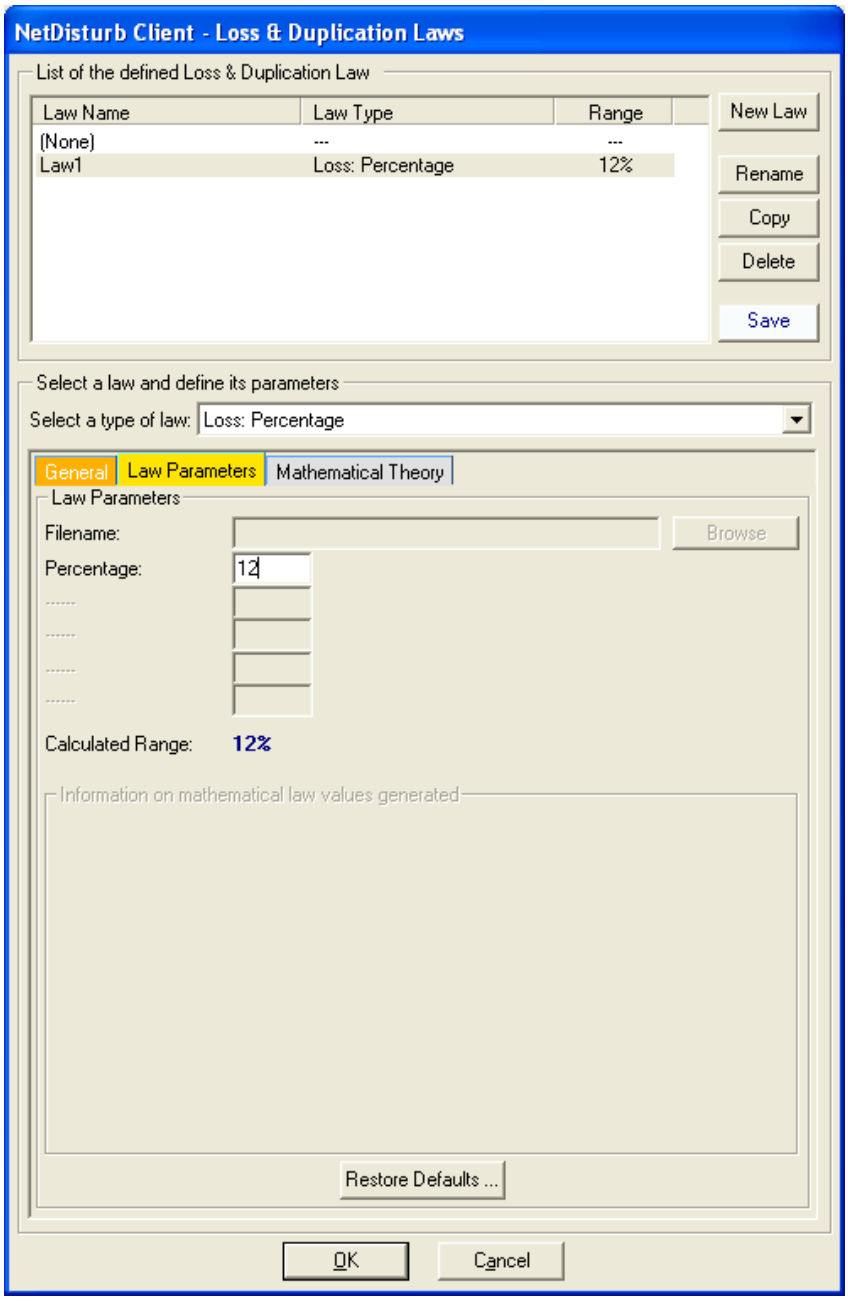
- For any Threshold value greater than 1 and smaller or equal than 100, only the 10th packet is lost.
- If the Threshold value is greater than 100, no packet is lost.
- If the Threshold value is 0, all packets are lost.

Here is another example of the impact of the threshold value.
The 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*

Continue *means the packet is not lost and may be handled by the Delay & Jitter Law if defined and/or may be handled by the Content Impairment Law if also defined.*

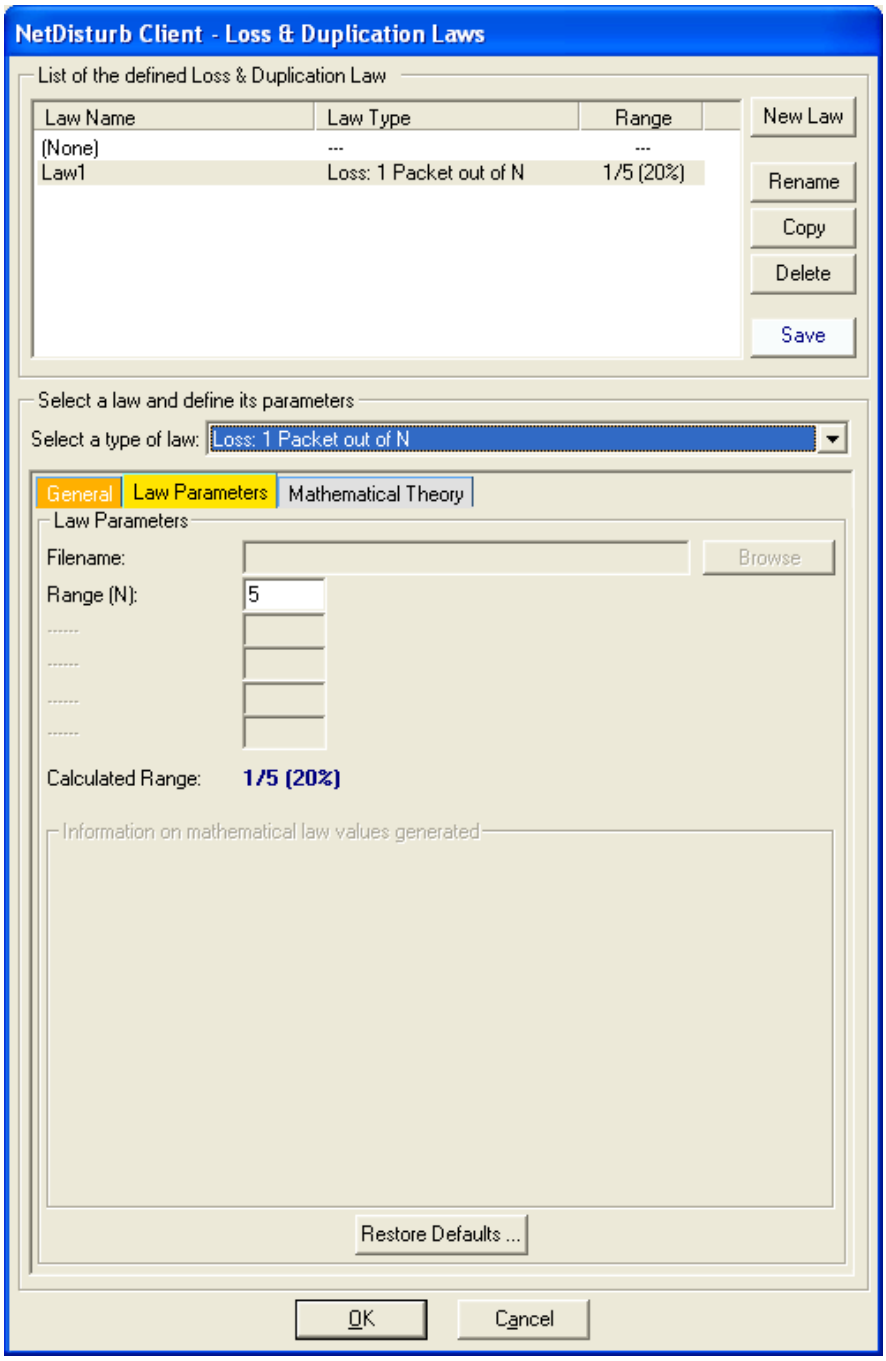
7.4.4.7 Loss: Percentage



When this law is selected, a percentage of packets are lost and the packets to lose are randomly selected.
The percentage of lost packets is calculated on the basis of 100 received packets or a multiple of 100. For this reason, the percentage indicated has to be 1 or 2 consecutive digits, i.e. 12% and 0.00056% are allowed BUT NOT 10.2% or 0.00506%.

If the value of 100% is specified then all the packets are lost.
The value of the percentage must be bounded between 0.00000001% and 100%, and the lost packets are selected in a random way.

7.4.4.8 Loss: 1 Packet out of N

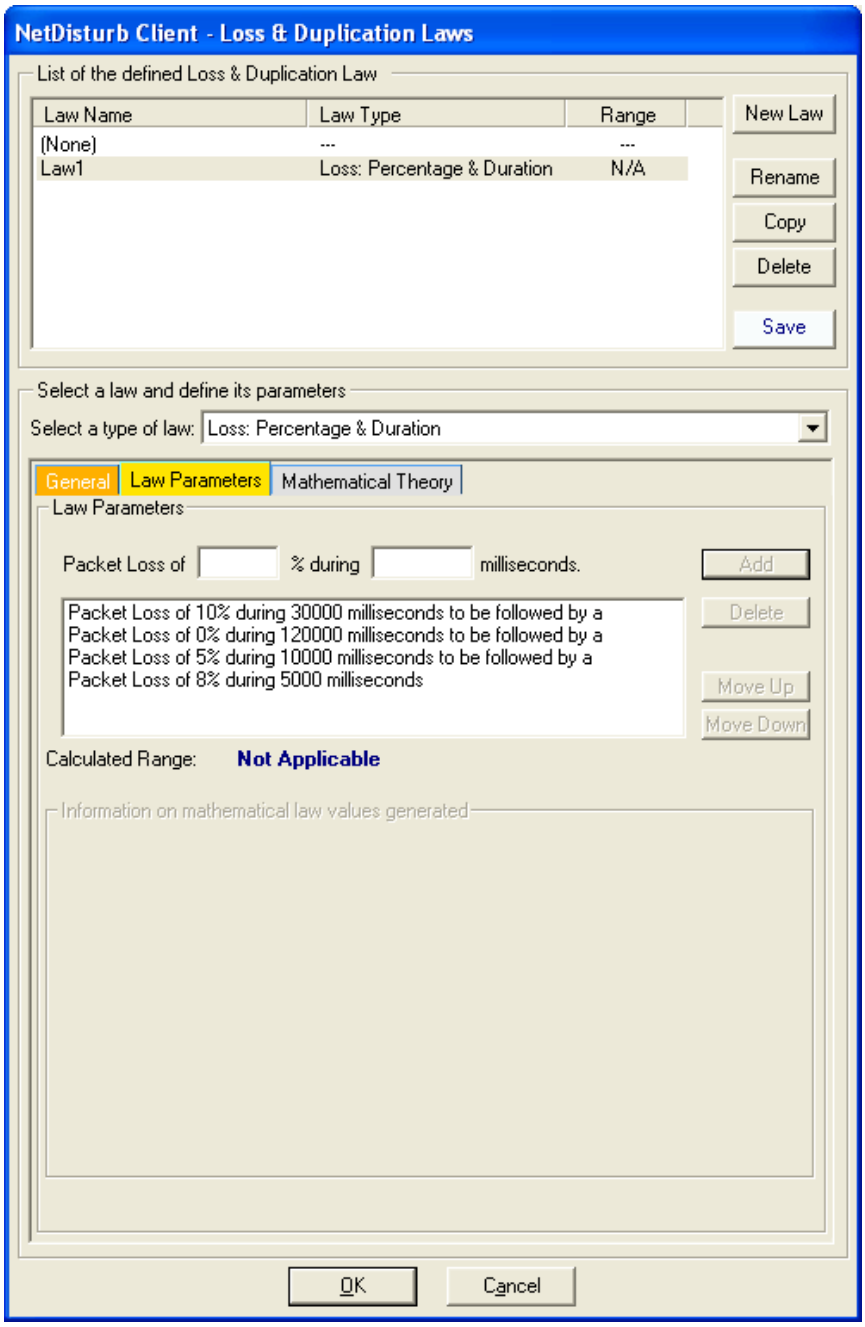


This law allows loosing 1 packet out of N received packets.

The lost packet is the Nth received packet, i.e. considering N is 5, then the 5th, 10th, 15th … packets and so on are lost.

The value of N must be between 2 and 100,000,000.

7.4.4.9 Loss: Percentage & Duration



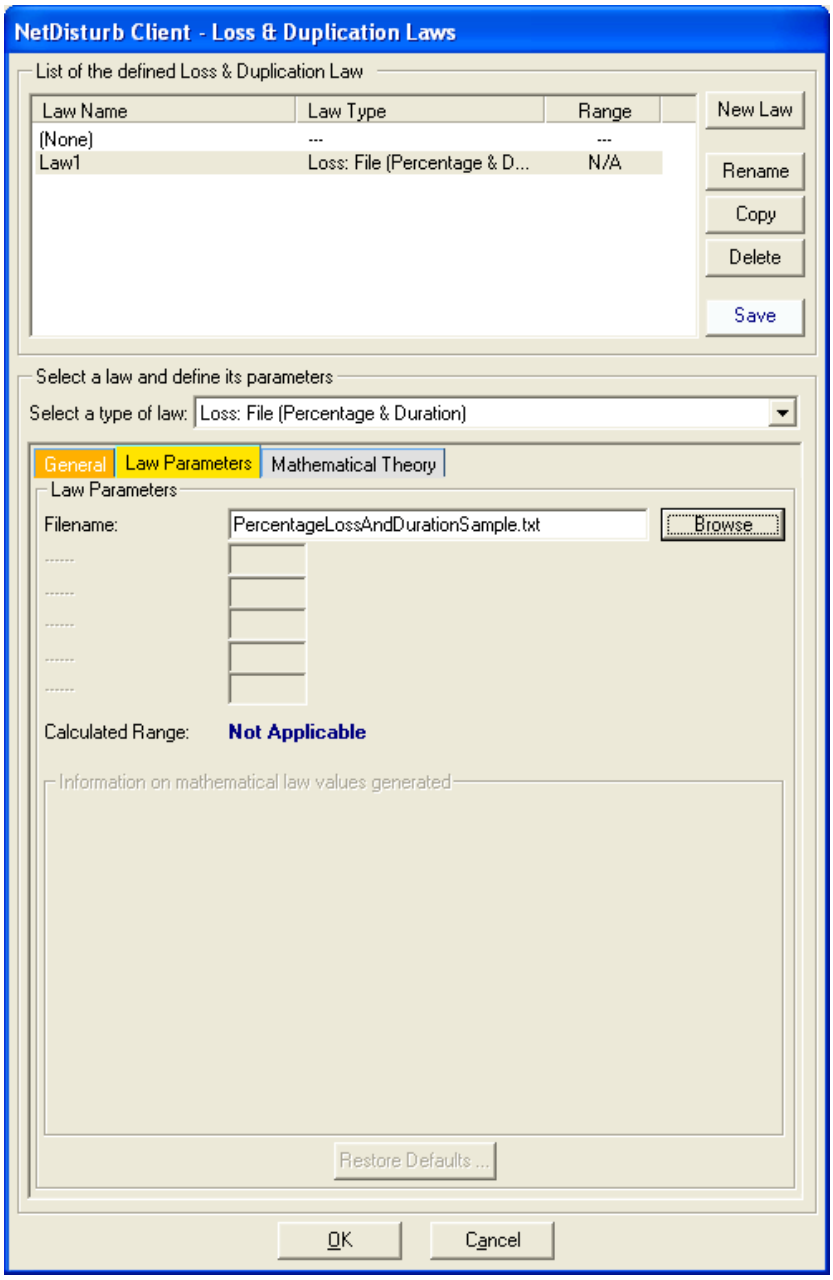
When this law is used, a percentage of packets are lost and the packets to lose are randomly selected. This loss is done for a defined duration.

You can define up to 50 successive doublets: <% Packet loss, Duration> that **NetDisturb** will process.

The percentage of lost packets is calculated on the basis of 100 received packets or a multiple of 100. For this reason, the percentage indicated has to be 1 or 2 consecutive digits, i.e. 12% and 0.00056% are allowed BUT NOT 10.2% or 0.00506%.

If the value of 100% is specified then all the packets are lost.
The value of the percentage must be bounded between 0.00000001% and 100%, and the lost packets are selected in a random way.

7.4.4.10 Loss: File (Percentage & Duration)



When this law is used, the loss and duration values are extracted from the user-defined file. This file must be a text file.

The percentage of lost packets is calculated on the basis of 100 received packets or a multiple of 100. For this reason, the percentage indicated has to be 1 or 2 consecutive digits, i.e. 12% and 0.00056% are allowed BUT NOT 10.2% or 0.00506%.

Duration is expressed with an integer positive number and in milliseconds. Separators used for decoding are End of Line (CR or CR-LF), semicolon, coma, and tab or space characters.
If a line starts with a sharp (#) character, the rest of the line is ignored i.e. up to the End of Line (CR or CR-LF).

To assure performance, the file is read in one shot and stored in memory at law selection time. The values of the file are used to load the table transmitted to the **NetDisturb** driver. In order to not overload the memory resources, maximum read number of loss and duration values is limited to 200 couples of values.

If the file size exceeds the 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, the file is read again from the beginning to complete the table.

The file sample (PercentageLossAndDurationSample.txt) illustrates a gradual loss from 5% to 50%. Each step is applied during 10 seconds, except for the maximal loss value (50%) and the minimal one (0%), which are applied during 20 seconds.

Loss Value extracted	Corresponding Duration Value extracted
5	10000
10	10000
15	10000
20	10000
25	10000
30	10000
35	10000
40	10000
45	10000
50	20000
45	10000
40	10000
35	10000
30	10000
25	10000
20	10000
15	10000
10	10000
5	10000
0	20000

7.4.4.11 General Rules concerning the Duplication of Packets

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

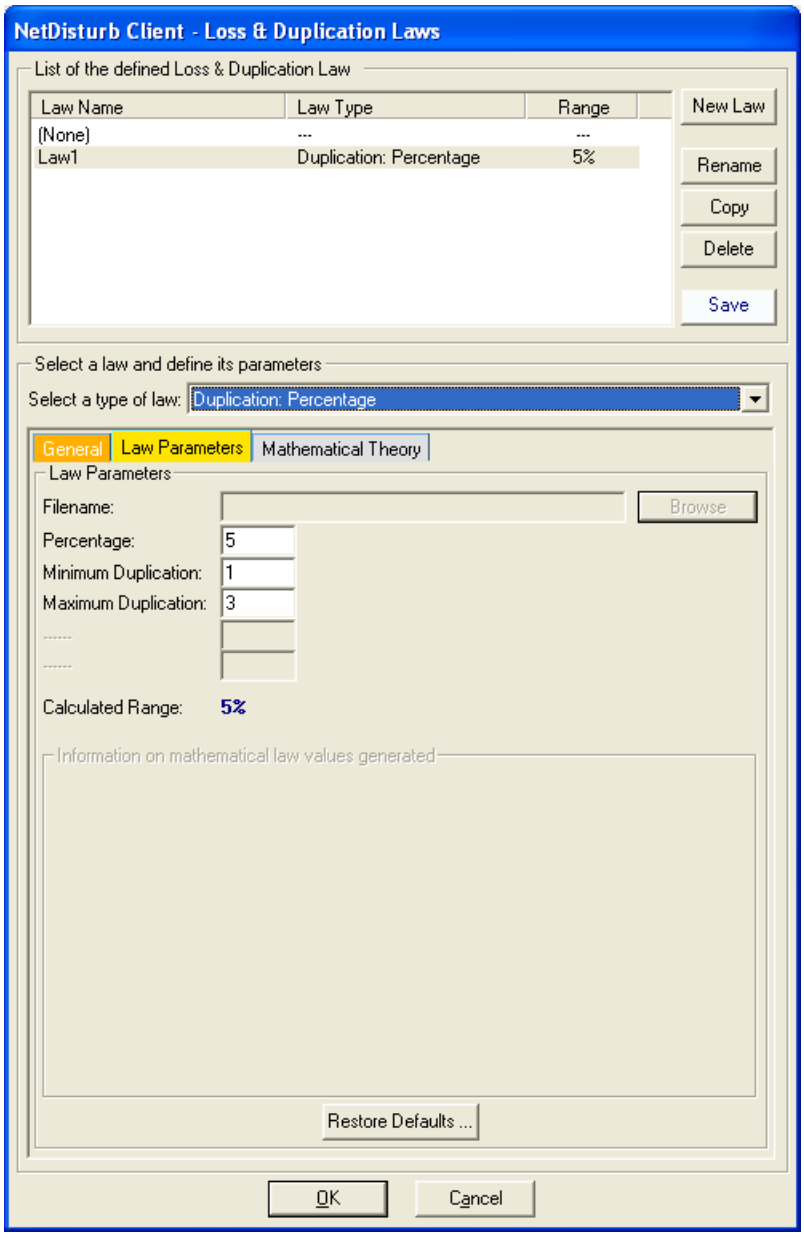
7.4.4.11.1 What does Duplication mean with NetDisturb

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

7.4.4.11.2 How many times is a packet duplicated

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

7.4.4.12 Duplication: Percentage



The duplication of packets enables to transmit the same received packet several times. The duplicated packets are just inserted after the original packet to be transmitted.

The **Percentage** of duplicated packets is calculated on the basis of 100 received packets or a multiple of 100.
For this reason, the percentage indicated has to be 1 or 2 consecutive digits, i.e. 12% and 0.00056% are allowed BUT NOT 10.2% or 0.00506%. If the value of 100% is specified then all the packets are duplicated.
The value of the percentage must be bounded between 0.00000001% and 100%, and the packets to duplicate are selected in a random way.

The original packet can be duplicated for a number of times defined by a random selection in the '**Minimum Duplication**' and '**Maximum Duplication**' range parameters.

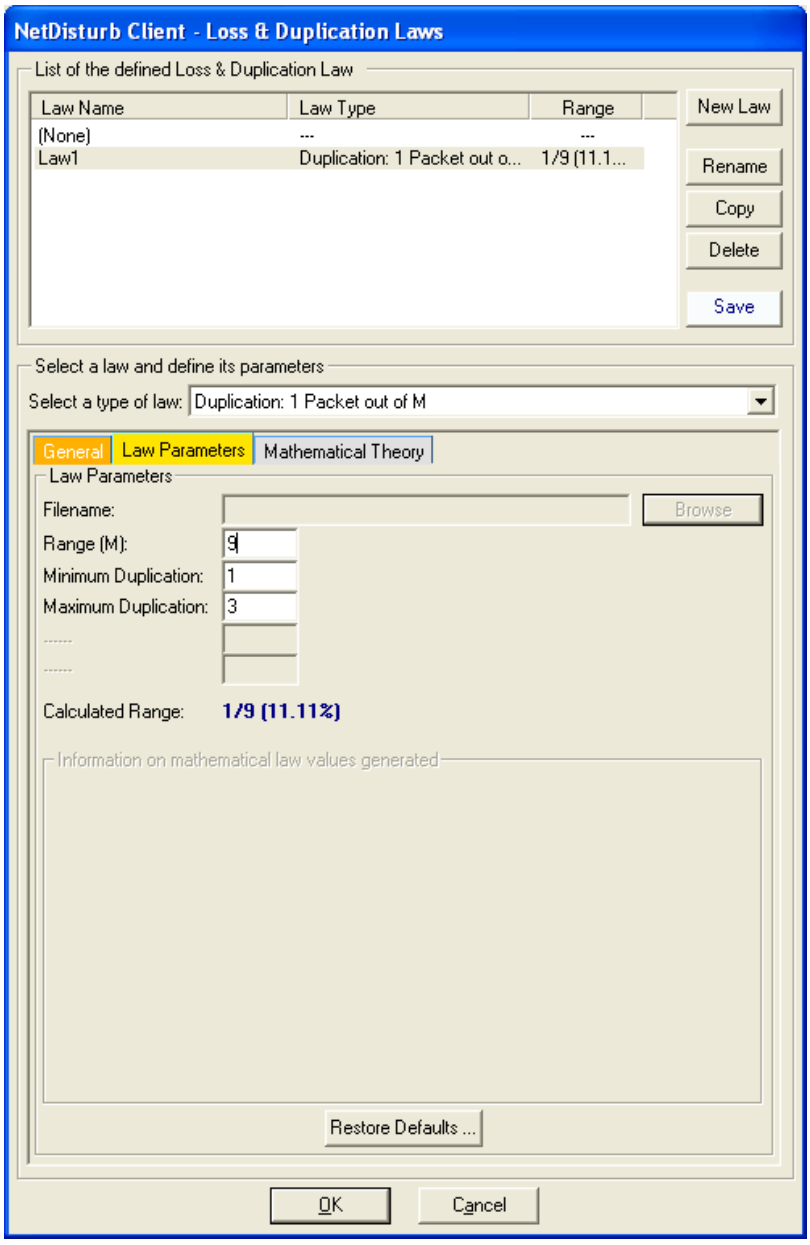
When '**Minimum Duplication**' equals '**Maximum Duplication**', all the eligible packets during the process of duplication are copied the same number of times.

Here are a few examples:

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

See also paragraph 7.4.4.11 for the general rules and terms relevant to the duplication of packets.

7.4.4.13 Duplication: 1 Packet out of M



This duplication of packets enables to transmit the same received packet several times. The duplicated packets are just inserted after the original packet to be transmitted.
This law duplicates 1 packet out of M received packet and the packet to be duplicated is the Mth received packet.

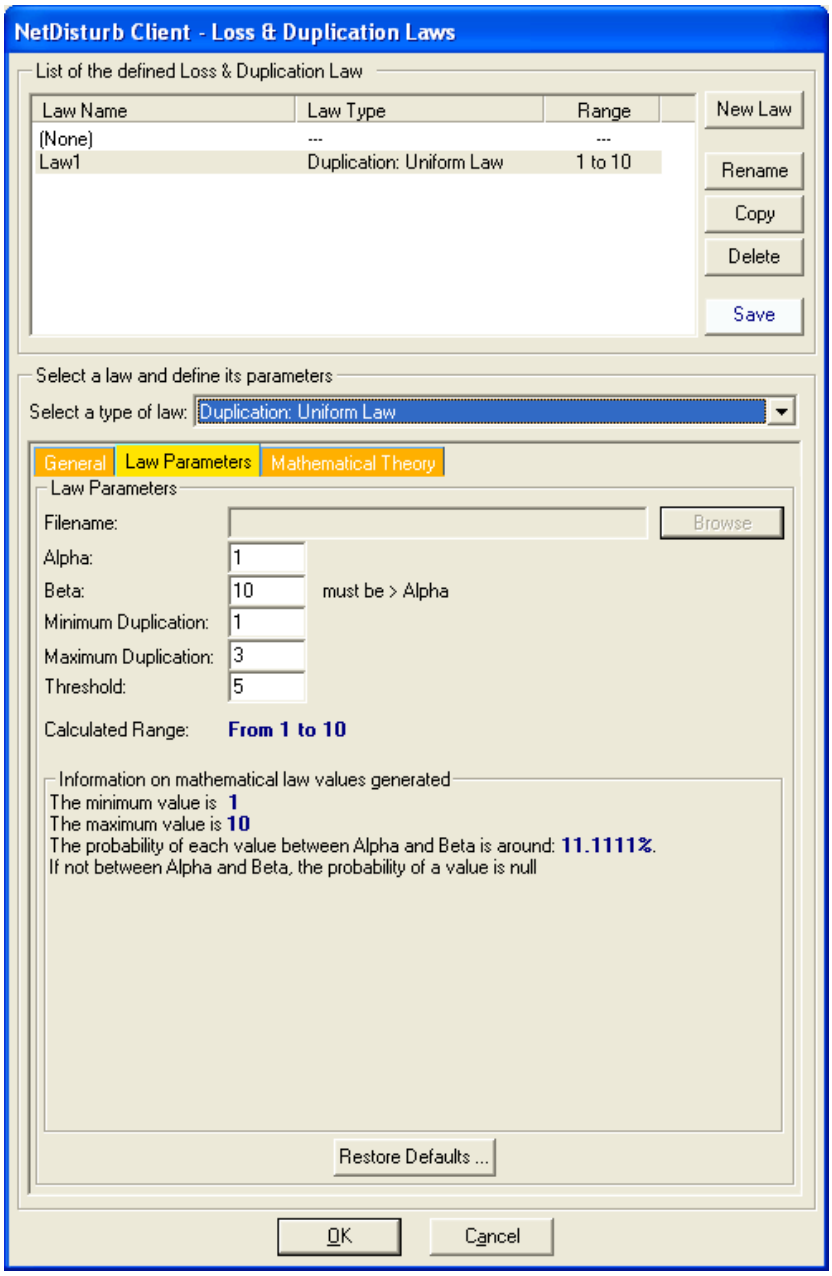
The **Range (M)** parameter indicates which packet is going to be duplicated i.e. considering M is 9, then the 9^{h}, 18th, 27th packet and so on are duplicated.
The value of M must be between 2 and 99,999,999.

The original packet can be copied the number of times defined by a random selection in the '**Minimum Duplication**' and '**Maximum Duplication**' range parameters.

When '**Minimum Duplication**' equals '**Maximum Duplication**', all the eligible packets during the process of duplication are copied the same number of times.

See also paragraph 7.4.4.11 for the general rules and terms relevant to the duplication of packets.

7.4.4.14 Duplication: Uniform Law



The duplication of packets enables to transmit the same received packet several times. The duplicated packets are just inserted after the original packet to be transmitted.
The decision to duplicate a received packet is made by using the uniform law.

If the value calculated by the law is equal or greater than the **Threshold** parameter, then the packet is duplicated.
The original packet is duplicated the number of times defined by a random selection in the '**Minimum Duplication**' and '**Maximum Duplication**' range parameters.

When '**Minimum Duplication**' equals '**Maximum Duplication**', all the eligible packets during the process of duplication are copied the same number of times.

When this law is selected, a uniform distribution of numbers between the **Alpha** and **Beta** values is computed and stored in a table. This table and the **Threshold** value are then transmitted to the **NetDisturb** driver.

The **NetDisturb** driver picks a number in the table for each selected packet. If this number is greater or equal than the **Threshold**, then the packet is duplicated.

The mathematical function used is (click on the “Mathematical Theory” tab or see the Uniform Law in Part 10 for more information):

Uniform law on (α, β) range

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

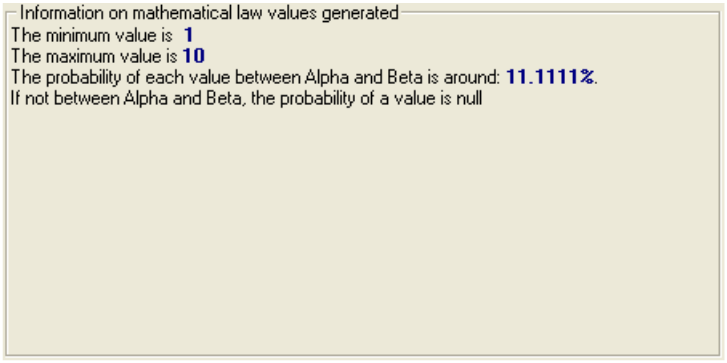
$f(x) = 0$ else

For this law, three parameters are defined:

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

See also paragraph 7.4.4.11 for the general rules and terms relevant to the duplication of packets.

An additional area, called “Information on mathematical law values generated” is available with this law. Here are provided some information about the minimum and maximum values. The mathematical law generates these values using the user-defined parameters.
Moreover, the probability of each value that can be generated is also available.



7.4.4.15 Loss (1 out of N) then Duplication (1 out of M)

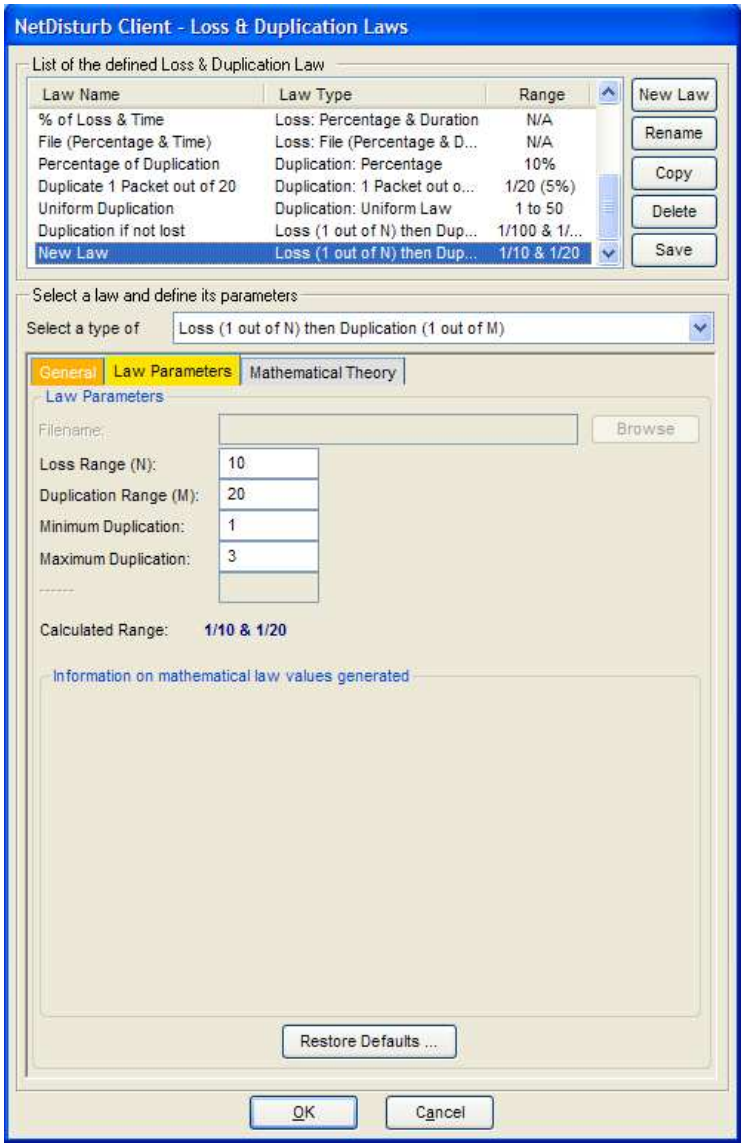
The Loss law (1 out of N) is used before the Duplication law (1 out of M).

Loss (1 out of N): this law allows losing 1 packet for N received packets. The lost packet is the Nth received packet. The value of N must be between 2 and 100,000,000.
For this law, 1 parameter is used: **Loss Range (N).**

*Please refer to paragraph **7.4.4.8 Loss: 1 Packet out of N** for more details.*

Duplication (1 out of M): the duplication of packets enables to transmit the same received packet several times. The duplicated packets are just inserted after the original packet to be transmitted. The value of M must be between 2 and 100,000,000.
The original packet is duplicated the number of times defined by a random selection in the '**Minimum Duplication**' and '**Maximum Duplication**' range parameters.
When '**Minimum Duplication**' equals '**Maximum Duplication**', all the eligible packets for the process of duplication are copied the same number of times.
For this law, 3 parameters are used: **Duplication Range (M)**, **Minimum Duplication** and **Maximum Duplication**.

*Please refer to paragraph **7.4.4.13 Duplication: 1 Packet out of M** for more details.*



Let's take an example of 100 packets received with **Loss Range (N)** = 10 and **Duplication Range (M)** = 20.

The lost packets are the 10th, the 20th, the 30th, the 40th … the 100th.

The duplicated packets are the 22nd (because packet #10 and #20 have been lost), the 44th (because packet #30 and #40 have been lost and because the first packet of the next set of 20 none lost packets is the 23rd), the 66th (because packet #50 and #60 have been lost, and the first packet of this set of 20 packets is the 45th) and the 88th (because packet #70 and #80 have been lost with a 20 packets set starting at 67th).

7.4.5 The Delay & Jitter Law Configuration

NetDisturb can delay the packets following a mathematical law configured by the user or using values extracted from an input file. These values apply to the packets matching to the selected Filter, if a loss law hasn't previously lost the packets.

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.
The **Default.wsx** context file copied by the **NetDisturb** installer contains the following laws:

Combo-box (Law identifier)	Comment area	Description
(None)	(None)	With this option, no delay or jitter is applied to the IP flow.
Constant delay	Constant Delay	A 20 ms delay is applied to IP packets
Exponential jitter	Constant Delay & Exponential Jitter	Delay & Jitter to apply: from 20 to 21 ms. The delay is 20 ms and the jitter varies from 0 to 1 ms.
Uniform jitter	Constant Delay & Uniform Jitter	Delay & Jitter to apply: from 3 to 102 ms. The delay is 2 ms and the jitter varies from 1 to 100 ms.
Constant Delay & File (Jitter)	Constant Delay & File (Jitter)	The file Random_delay.txt contains jitter values to add to the constant 10 ms delay.
File (Minimum Cadences)	File (Packet Sending Minimum Cadences)	The file RandomValues.txt contains values used as Delay & Jitter.
Router Simulation with Delay	Router Simulation & Constant Delay	Constant delay = 20 ms IP Throughput = 1000 Kb/s Max memory = 500 KB
Router Simulation & File (Cadences)	Router Simulation & File (Packet Sending Minimum Cadences)	IP Throughput = 1000 Kb/s Max memory = 250 KB Delay & Jitter values are extracted from a user file (RandomValues.txt).
Delay & File (Throughput, Time)	Constant Delay & File (Throughput, Duration)	Constant delay = 250 ms Throughput values and Duration of the Throughput values are extracted from a user file (ThroughputAndDurationSample.txt).

7.4.5.1 Delay & Jitter Law and the Working Mode

Working Mode: Laws apply to the IP Flow

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

Working Mode: Laws apply to each TCP/UDP connection of the IP Flow

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

These values are stored in a table maintained by the **NetDisturb** driver.

The **NetDisturb** Server provides the table once to the **NetDisturb** driver with values provided by the law or extracted from the file. The **NetDisturb** driver loops on values from this table: when the end of the table is reached, **NetDisturb** driver restarts at the beginning.

If the packet is TCP or UDP, the 5-tuple IP addresses, protocol and ports is used to classify the packet. Else the IP addresses and protocol are only 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, the values extracted restart at the beginning of the table.

7.4.5.2 Delay & Jitter Accuracy

The **NetDisturb** driver accuracy is ±1 millisecond.

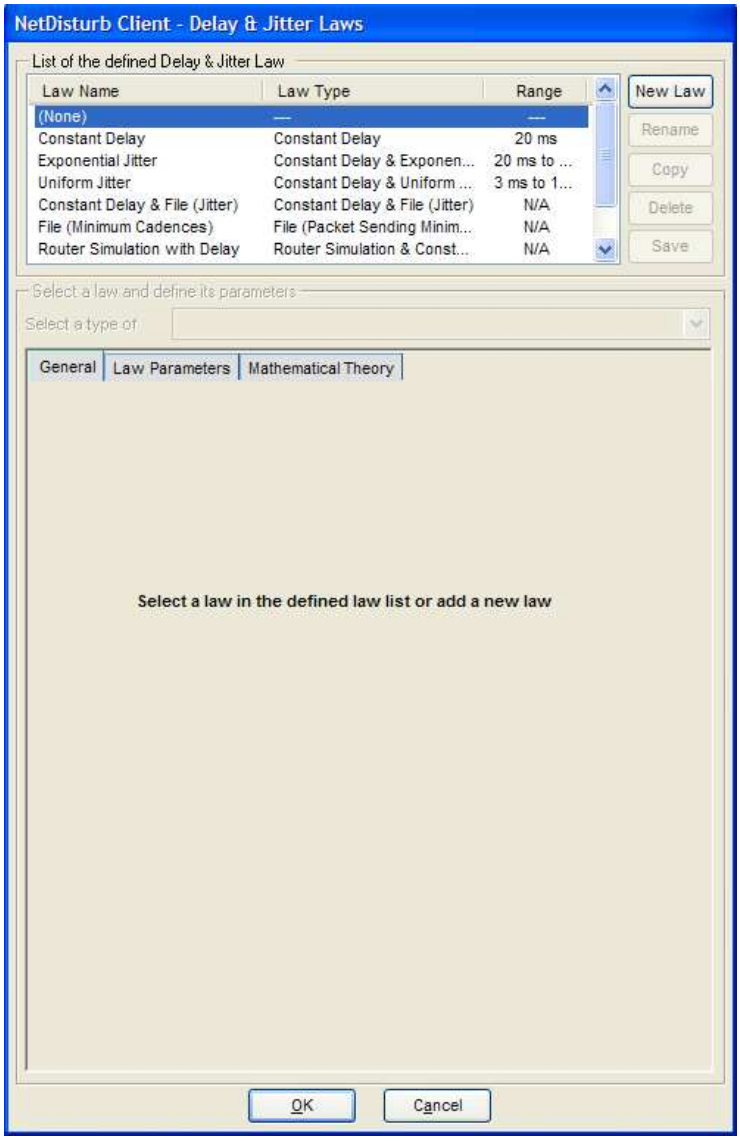
It means that a delay variation of one millisecond between two packets can be taken into account.

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

7.4.5.3 How to create or edit the Delay & Jitter Law

To create or configure a Delay & Jitter Law click on the **Define** button at the top or bottom part of the main window.

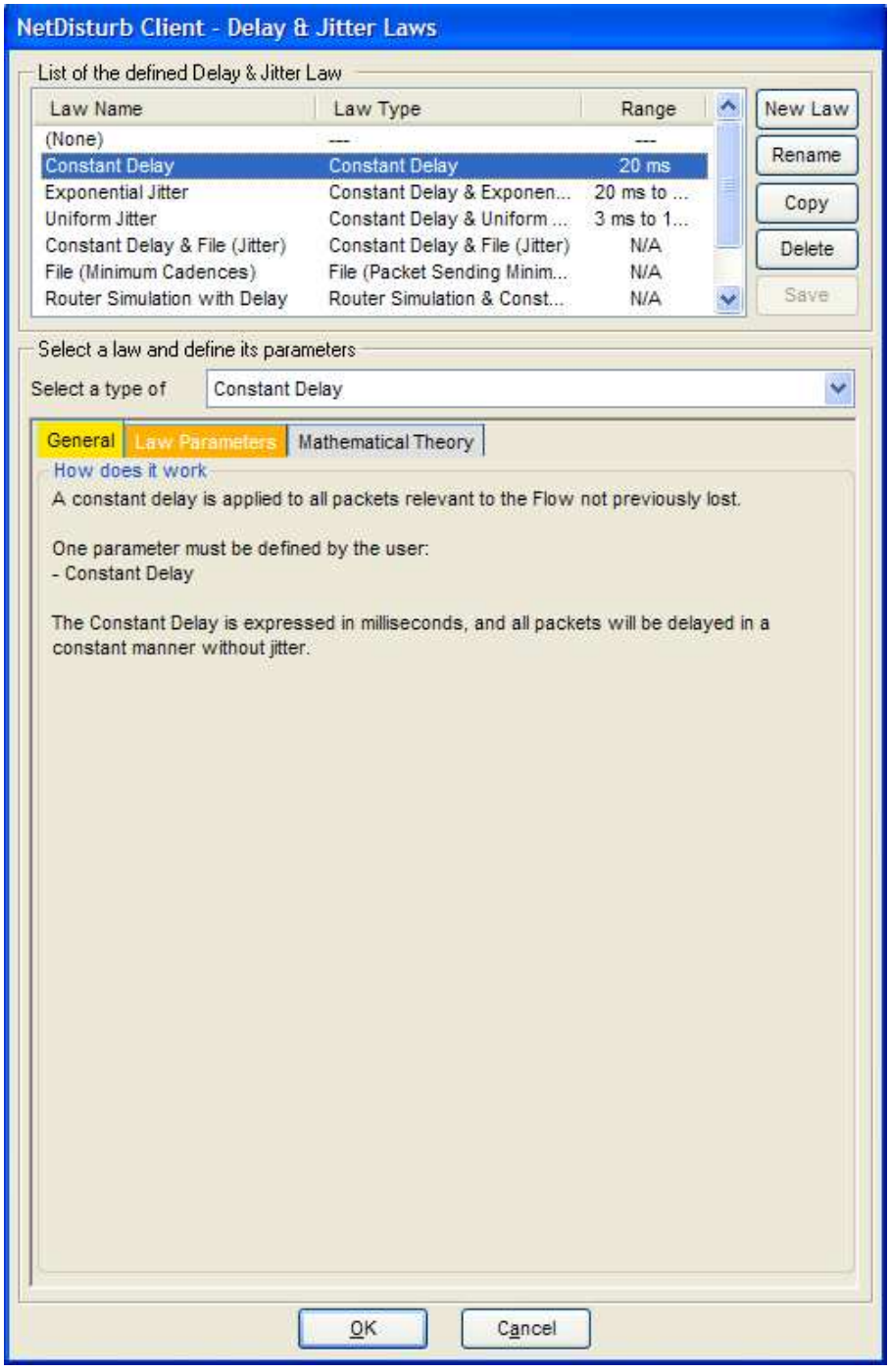
The following window is then displayed:



This window allows creating a new law or modifying an existing one.

If **(None)** is selected, only the **New Law** button is enabled and the tabs to define the parameters are disabled.

If you select a preexisting law in the current list-box, then the parameters and the details about this law can be viewed and the first "General" tab is enabled as in the example below:



This window is composed of two areas:

- **List of the defined Delay & Jitter Law**: a list-box displays the defined laws and five buttons allow managing the laws: **New Law**, **Rename**, **Copy**, **Delete** and **Save**.
- **Select a Law and define its parameters:** a list-box displays the loss and duplication laws authorized by the software. Then there are 3 tabs to define and set up the parameters of the selected law.
  - (Tab 1) **General** (explaining how does the impairment law work)
  - (Tab 2) **Law Parameters**
  - (Tab 3) **Mathematical Theory** (only available with Loss & Duplication Laws using a mathematical law)

7.4.5.3.1 List of the Delay Laws defined

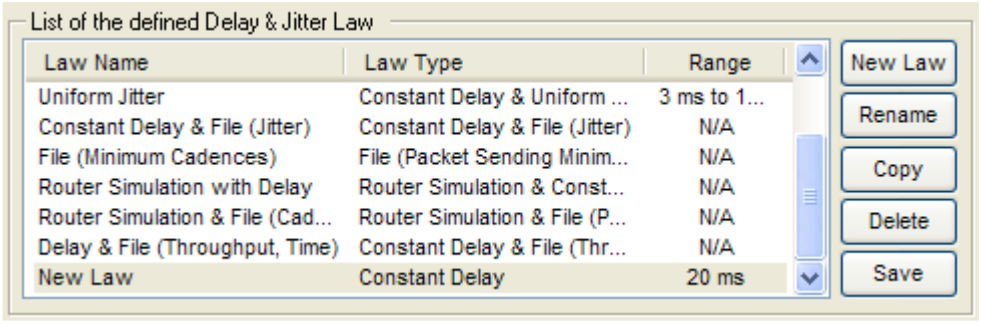
The list-box displays for each defined law the summary of the characteristics, except for (None) corresponding to 'No Delay & Jitter Law' selected:

- Law Name: name of the law
- Law Type: the type of Delay law chosen amongst the pre-defined list (more details available in paragraph 7.4.5.3.2 Select a law and define its parameters)
- Range: range of values generated by the specified laws.

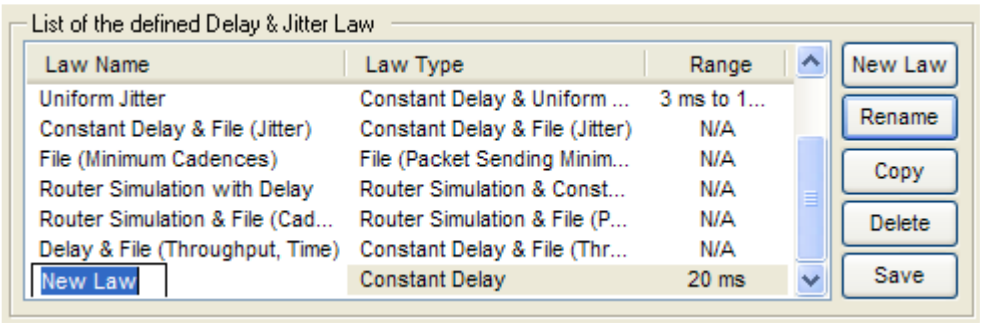
To manage the Law list, various buttons are available:

New Law: this button should be used to add a new Law in the defined Law list.

After pressing the New Law button, a new entry is added at the end of the list-box with 'New Law' as name of the law:

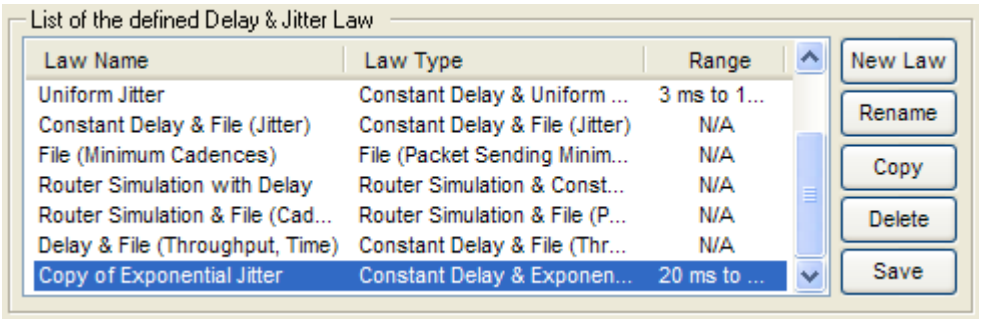


Then click on 'New Law' label to rename this entry or press the Rename button:



Rename: to rename the Law. This button should be used to change the Law name.

Copy: this button copies the current selected law at the end of the list with a new name. The following example shows the new list-box after copying the existing Exponential Jitter law:



Delete: this button should be used to remove a Law from the current list.

First select in the list-box the law to delete and then press the Delete button. A confirmation window is then displayed:

Save: to save all changes related to the laws.

7.4.5.3.2 Select a law and define its parameters

Once a law has been created, then you can define or modify the parameters of the law:

The first step is to choose the law type amongst the list of the pre-defined laws.

Then there are 3 tabs to define and to help the user to set up the parameters of the selected law.

- (Tab 1) **General** (explaining how does the impairment law work)
- (Tab 2) **Law Parameters**
- (Tab 3) **Mathematical Theory** (only available with Delay & Jitter Laws using a mathematical law). This tab gives some details on the theory of the mathematical law used.

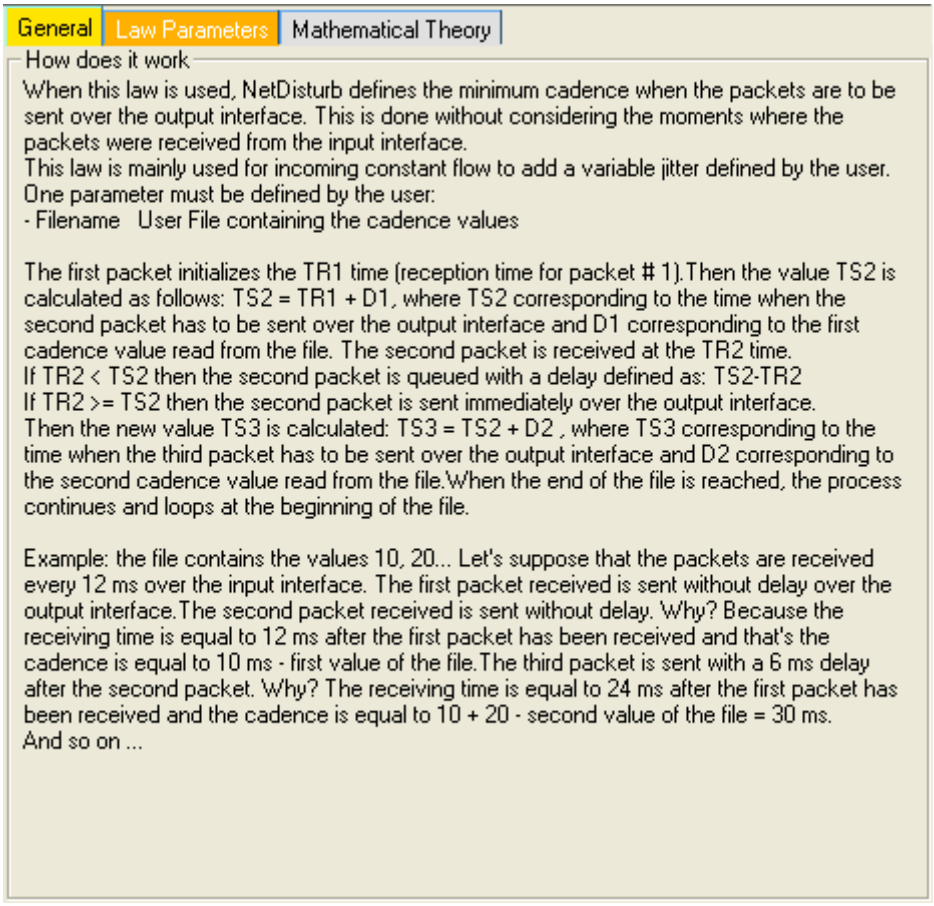
⇨ Select a type of law

A combo box allows selecting a law among the following pre-defined laws:

- Constant Delay
  Parameter = constant delay
- Constant Delay & Exponential Jitter
  Parameters: constant delay, λ
- Constant Delay & Uniform Jitter
  Parameters: constant delay, alpha, beta
- Constant Delay & File (Jitter)
  Parameters: constant delay, filename
- File (Packet Sending Minimum Cadences)
  Parameter: filename
- Router Simulation & Constant Delay
  Parameters: IP throughput, max memory, constant delay
- Router Simulation & File (Packet Sending Minimum Cadences)
  Parameters: IP throughput, max memory, filename
- Constant Delay & File (Throughput & Duration)
  Parameters: constant delay, filename

⇨ The “General” tab (tab 1)

Details on the law type chosen and on the way to choose the parameters are provided on this tab as shown on the figure below:



⇨ The “Law Parameters” tab (tab 2)

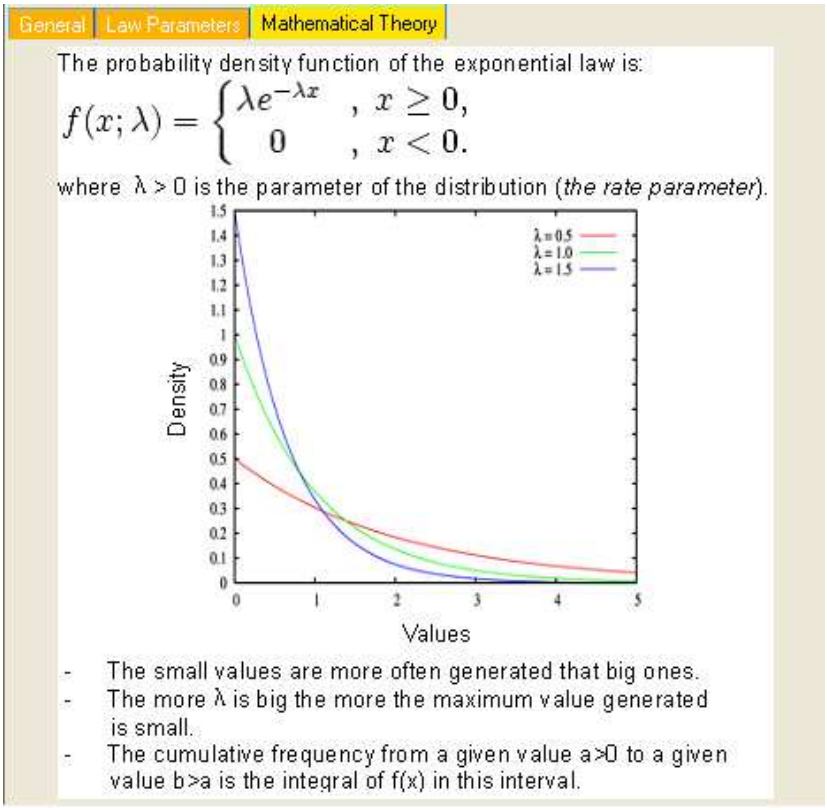
This tab is described for each law type here after.

⇨ The “Mathematical Theory” tab (tab 3)

This tab is available with the following laws only:

- Constant Delay & Exponential Jitter
- Constant Delay & Uniform Jitter

This tab provides the main explanations of the mathematical theory of the law as shown on the figure below (**Constant delay & Exponential Jitter** law by example):



⇨ Action buttons

The "Delay & Jitter Laws" window handles a temporary list of laws until the **OK** or **Cancel** button is pressed.

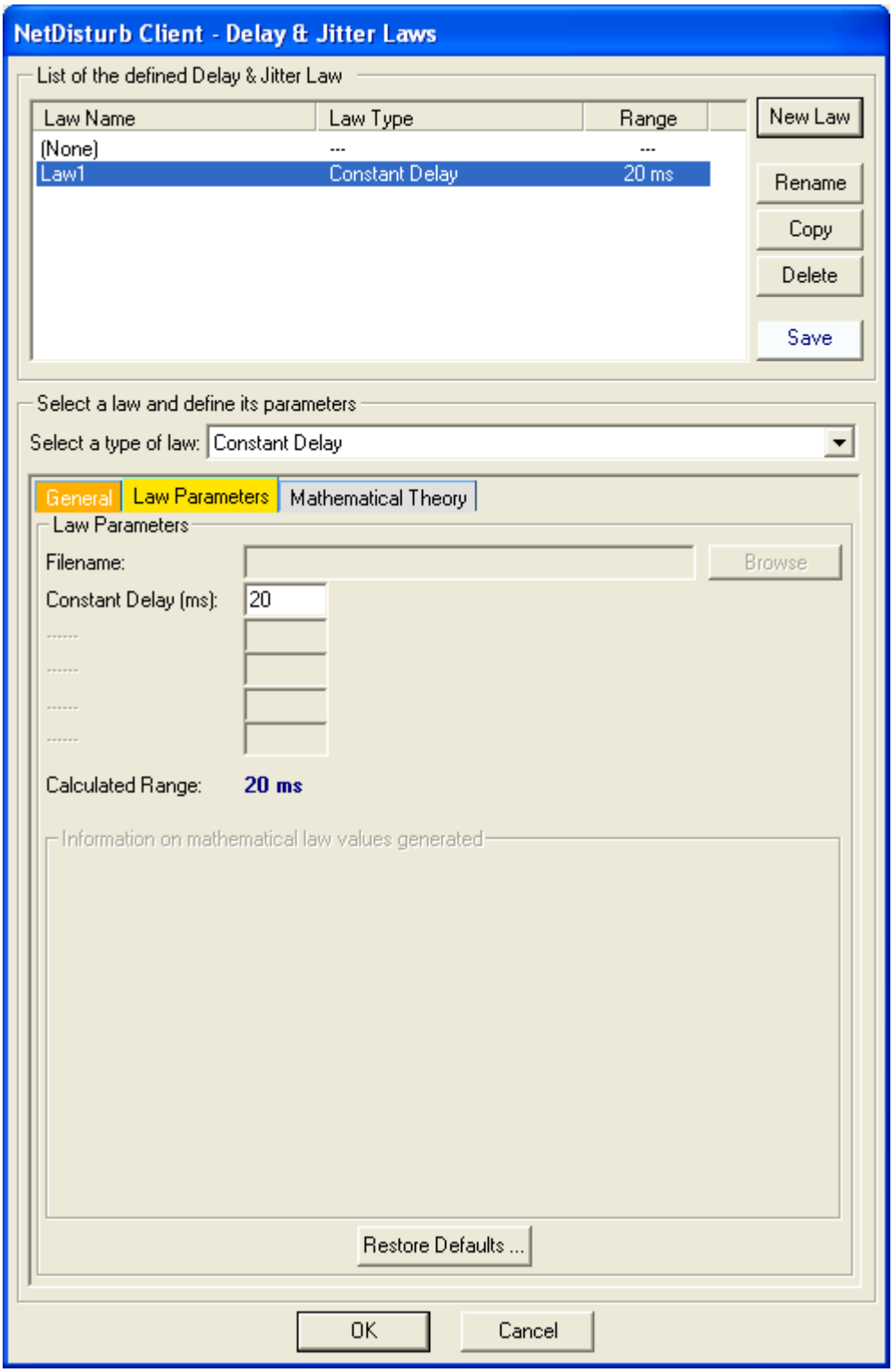
Button	*Action*
Restore Defaults …	Reset all parameters of the current law.
OK	Save all modifications made if you didn't save them before. Moreover, the selected law in the list of the defined laws becomes the selected law in the combo-box of the Flow window.
Cancel	Ignore all modifications made if you didn't click on the Save button before. In that case, the last law selected in the combo-box of the Flow window is kept.

How to create a new Delay & Jitter Law:

1. Click on the "New Law" button,
2. Then click on the “Rename” button to modify the name of the law.
3. Choose one of the pre-defined law in the combo box
4. Select the "Law Parameters" tab,
5. Enter law parameter(s). The "General" tab and the "Mathematical Theory" tab contain information that can be useful to define the parameters.
6. Press the “Save“ button to save the changes and to continue to create or modify other laws.
7. Press “OK” to quit the “Delay & Jitter Laws” window and to select this new law as the law to be applied on the corresponding Flow.

7.4.5.4 Constant Delay

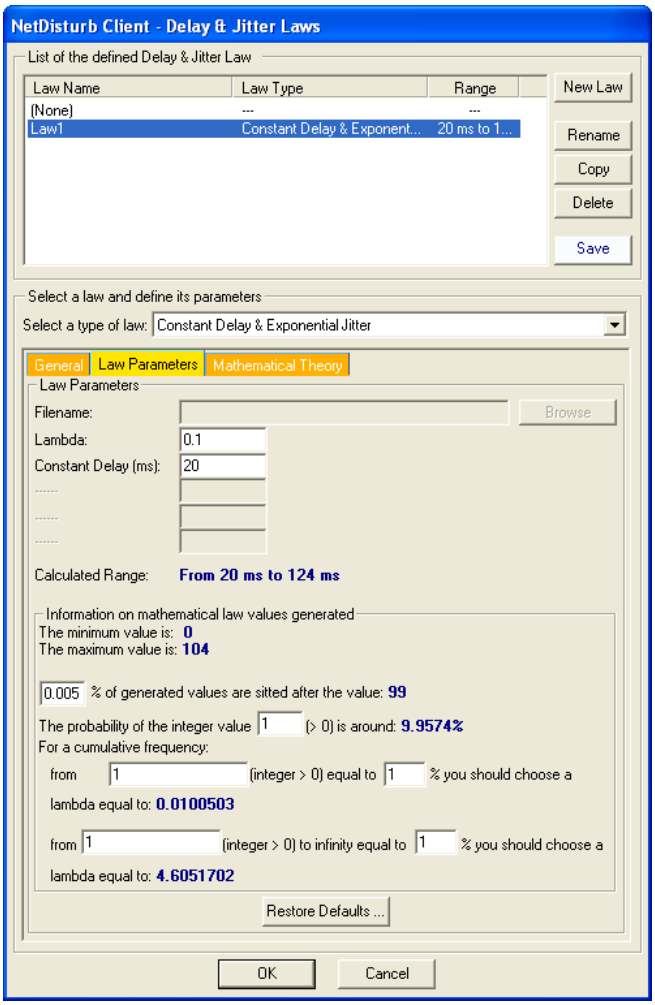
A constant delay is applied to all packets relevant to the IP Flow not previously lost.



The "Constant Delay (ms)" parameter must be defined, and all packets will be delayed in a constant manner.

7.4.5.5 Constant Delay & Exponential Jitter

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



The mathematical function used is (click on the “Mathematical Theory” tab or see the Exponential Law in Part 10 for more information):

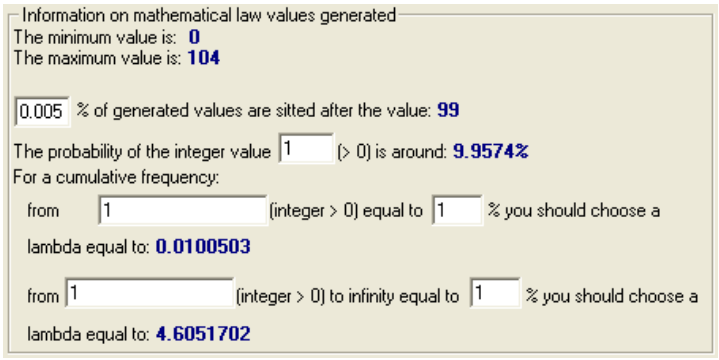
Exponential law $(\lambda > 0)$

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

For this law, one parameter is defined:

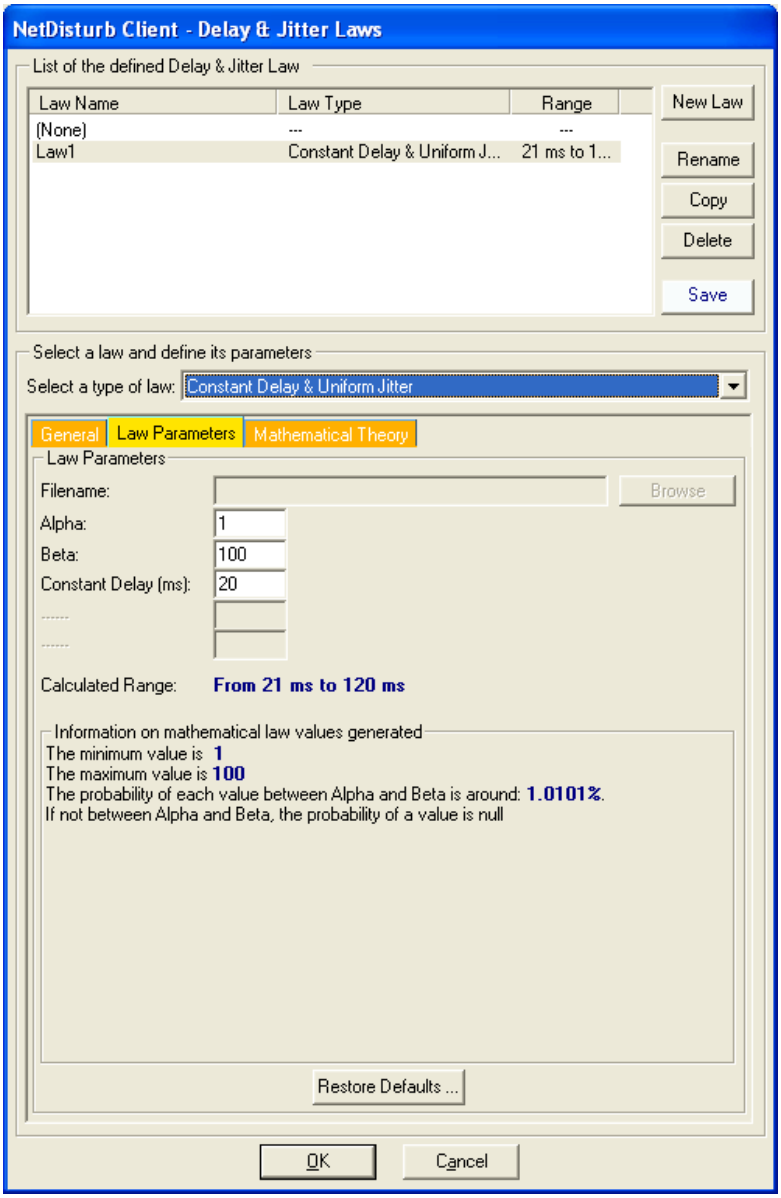
Lambda Parameter of the law

An additional area, called “Information on mathematical law values generated” is available with this law. Here is provided some information about the minimum and maximum values. The mathematical law generates the values using the user-defined parameters. Moreover, the probability of each value that can be generated is also available. In order to help the user to choose the lambda parameter, by giving domain of values and a cumulative frequency, NetDisturb can give you an approximation of the lambda parameter.



7.4.5.6 Constant Delay & Uniform Jitter

When this law is used, a uniform distribution of jitter values is calculated from the **Alpha** and **Beta** parameters.
This distribution is stored in a table. This table is then transmitted to the **NetDisturb** driver, finally coupled with a **Constant Delay** (expressed in ms) that will be added to the calculated jitter.



The mathematical function used is (click on the “Mathematical Theory” tab or see the Uniform Law in Part 10 for more information):

Uniform law on (α, β) range

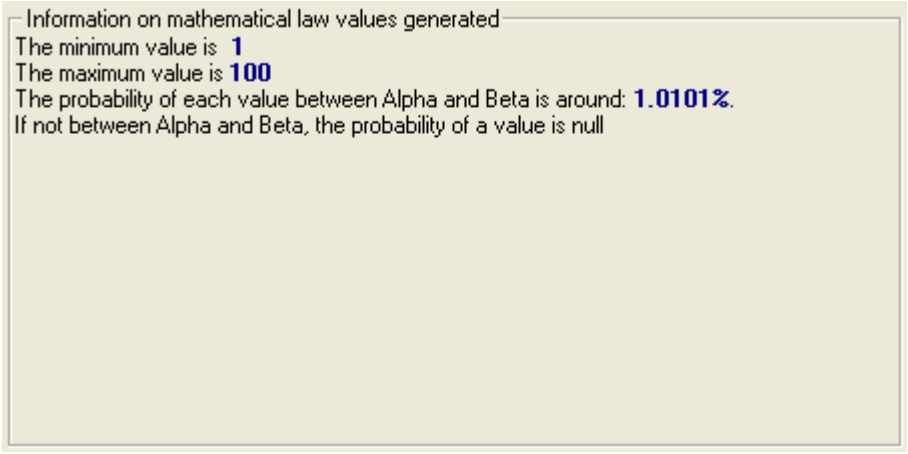
$f(x) = 1/(\beta - \alpha)$ if $\alpha < x < \beta$

$f(x) = 0$ else

For this law, two parameters are defined:

Alpha	min value of the range
Beta	max value of the range

An additional area, called “Information on mathematical law values generated” is available with this law. Here is provided some information about the minimum and maximum values. The mathematical law generates the values using the user-defined parameters. Moreover, the probability of each value that can be generated is also available.



7.4.5.7 Constant Delay & File (Jitter)

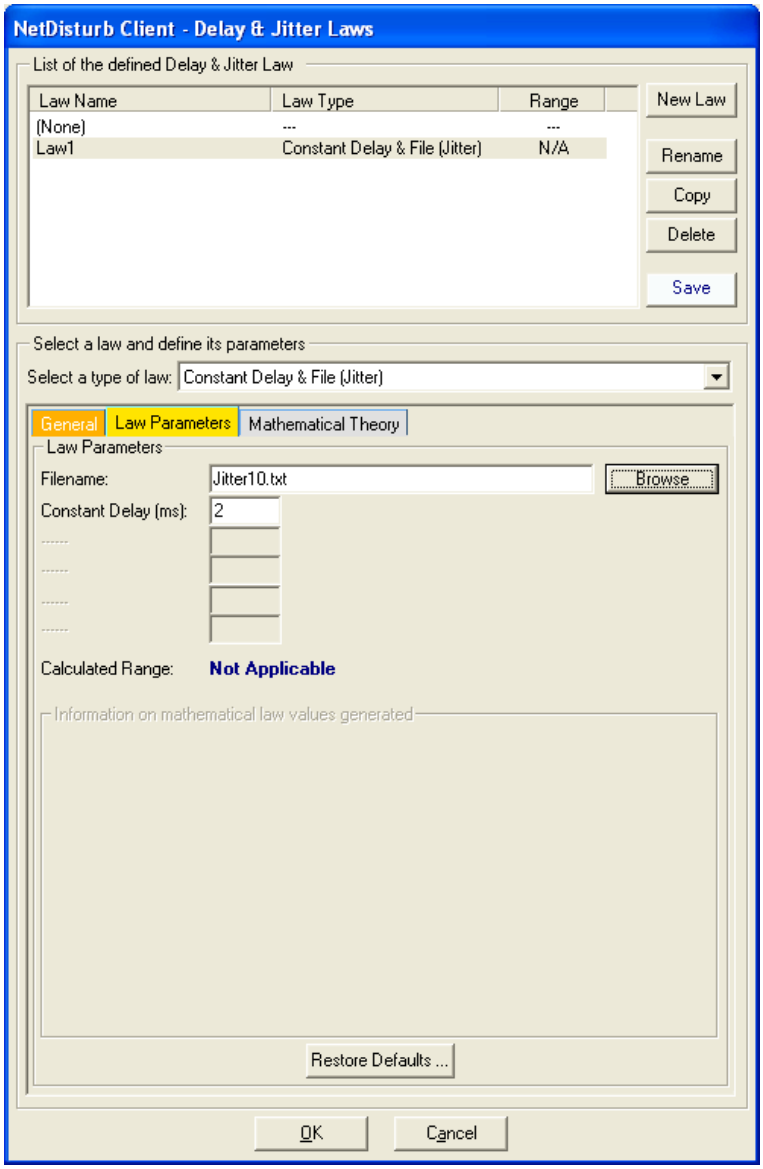
When this law is selected, the delay rate is obtained from a file.

Total delay applied to the packet = Constant Delay (expressed in ms) + delay (read from the file for this packet).

The Jitter values file must be a text file.

Delays are expressed in integer positive numbers. The unit is the millisecond. The separators used for decoding are: end of line (CR or CR-LF), semicolon, coma, and tab or space characters. If a line starts with a sharp (#) character, the rest of the line is ignored i.e. up to the End of Line (CR or CR-LF).

One Jitter value is picked for each packet handled. When the end of the file is reached, the **NetDisturb** driver restarts with the first values of the file.



For performance reasons the file is read in one shot, and stored in memory when the Flow is set in the Run state. The values are used to load the table transmitted to the **NetDisturb** driver. In order to not overload the memory resources, the maximum number of delays read is limited to 40,960.
If the file size exceeds the 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.

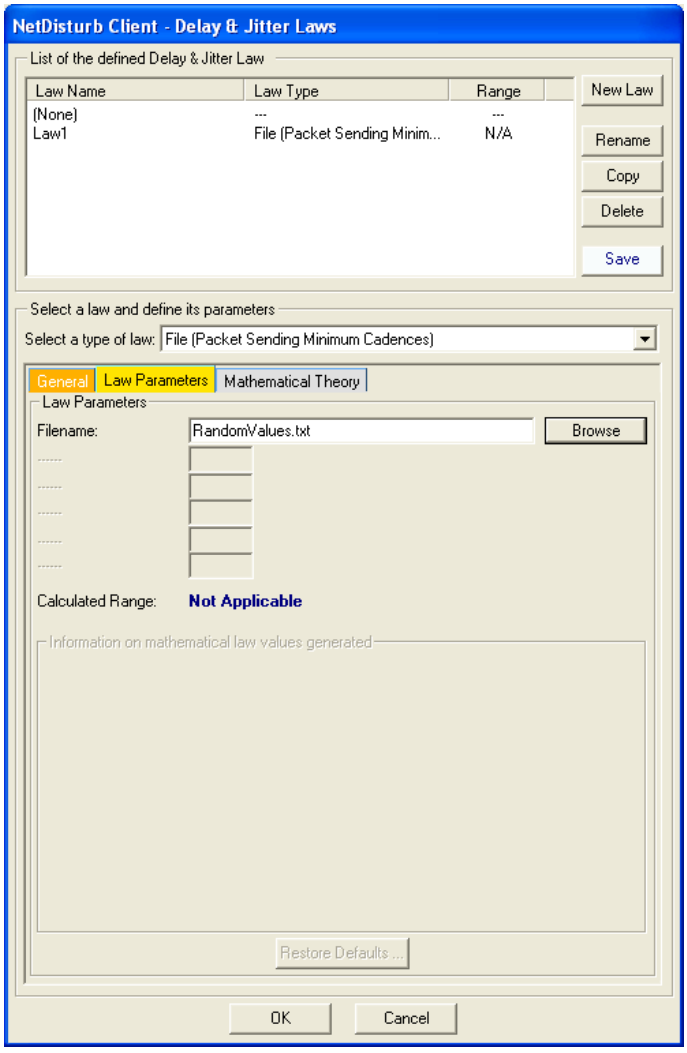
7.4.5.8 File (Packet Sending Minimum Cadences)

When this law is used, **NetDisturb** defines the minimum cadence when the packets are to be sent over the output interface. This is done without considering the moments where the packets were received from the input interface.

This law is mainly used for incoming constant flow to add a variable jitter defined by the user.
The file containing the values must be a text file. Sending times are expressed by integer positive numbers (unit is the millisecond).

The separators used for decoding are: end of line (CR or CR-LF), semicolon, coma, and tab or space characters. If a line starts with a sharp (#) character, the rest of the line is ignored i.e. up to the End of Line (CR or CR-LF).

NetDisturb extracts the values from the file in a circular way and one value is picked for each packet handled.



The first packet initializes the TR1 time (reception time for packet # 1).
Then the value TS2 is calculated as follows: TS2 = TR1 + D1, where TS2 corresponds to the time when the second packet has to be sent over the output interface and D1 corresponds to the first cadence value read from the file. The second packet is received at the TR2 time.

If TR2 < TS2 then the second packet is queued with a delay defined as: TS2-TR2

If TR2 >= TS2 then the second packet is sent immediately over the output interface.

Then the new value TS3 is calculated: TS3 = TS2 + D2, where TS3 corresponds to the time when the third packet has to be sent over the output interface and D2 corresponds to the second cadence value read from the file.
When the end of the file is reached, the process continues and loops at the beginning of the file.

Example: the file contains the values 10, 20...

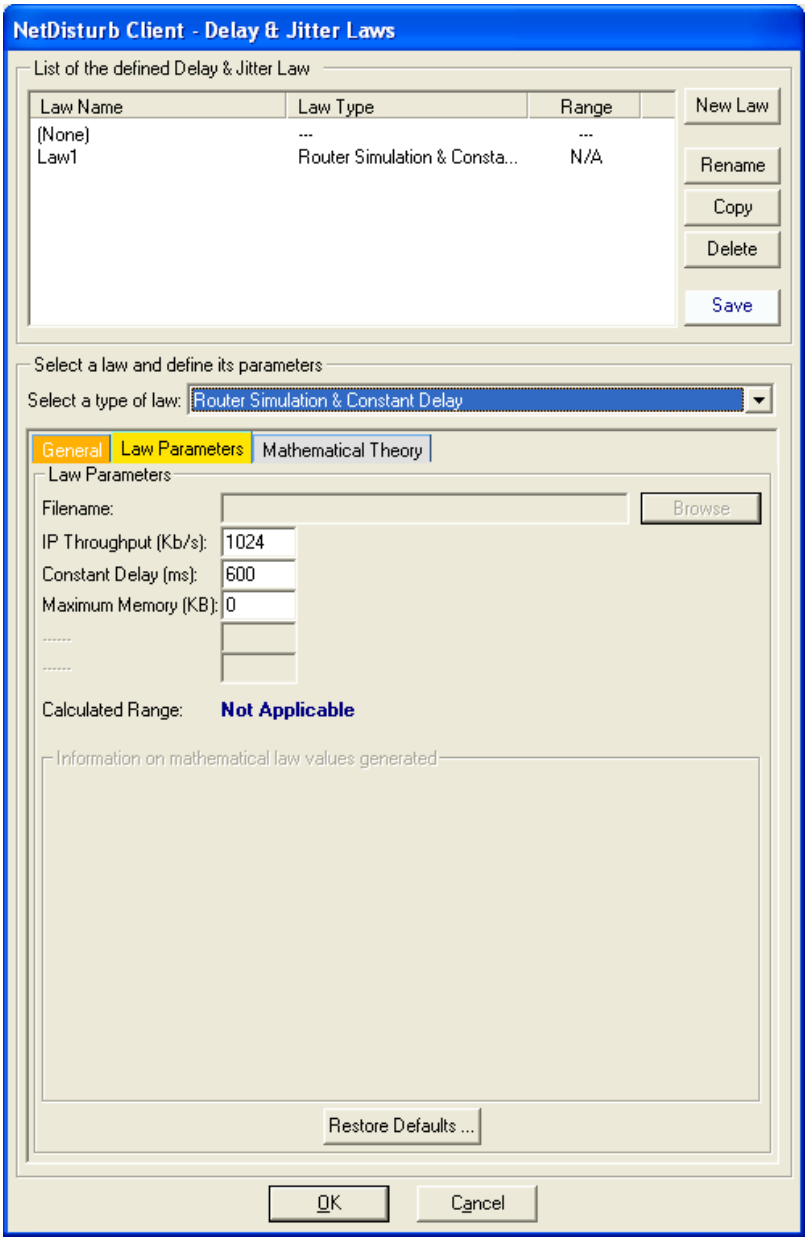
Let's suppose that the packets are received every 12 ms over the input interface. The first packet received is sent without delay over the output interface.
The second packet received is sent without delay. Why? Because the receiving time is equals to 12 ms after the first packet has been received and that's the cadence is equals to 10 ms - first value of the file.
The third packet is sent with a 6 ms delay after the second packet. Why? The receiving time is equal to 24 ms after the first packet has been received and the cadence is equals to 10 + 20 - second value of the file = 30 ms.
And so on...

7.4.5.9 Router Simulation & Constant Delay

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

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

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



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

(continue)

When the Flow is started i.e. when the 'Run' button is pressed, the internal remaining size is the Maximum Memory parameter value.
Each time a packet is received, the internal remaining size parameter is decreased by the packet size. When the remaining size parameter is 0, the queue is marked as full.
Any new packet is lost until the remaining size becomes positive. When the packet is sent, the relevant queue size parameter is increased.

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

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

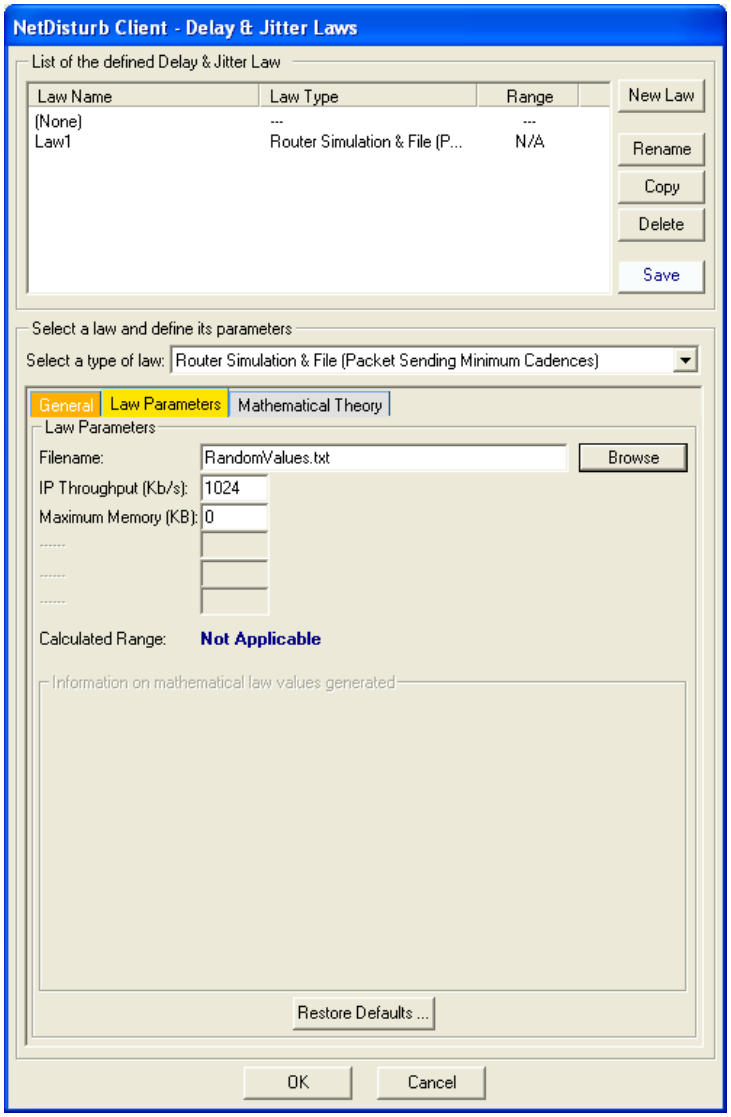
You shouldn't be surprised if packets continue to be sent even if no packet has been received: it is in most cases the **output queue** that is not yet empty.

7.4.5.10 Router Simulation & File (Packet Sending Minimum Cadences)

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 **Maximum Memory** parameter expressed in Kb/s is the output queue size). When the output queue is full, all new incoming packets will not be transmitted to the output interface.
- The minimum cadences (values read from the text file) when the packets are sent over the output interface whatever the moments when the packets were received from the input interface (to simulate a real network transit delay). Please refer to the "File (Packet Sending Minimum Cadences)" Law for more information. The values are expressed with an integer positive number. The unit is the millisecond. The separators used for decoding are: end of line (CR or CR-LF), semicolon, coma, and tab or space characters. One Delay & Jitter value is picked for each packet handled. When the end of the file is reached, the **NetDisturb** driver restarts with the first values of the file. If a line starts with a sharp (#) character, the rest of the line is ignored i.e. up to the End of Line (CR or CR-LF)

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



7.4.5.11 Constant Delay & File (Throughput & Duration)

This law is used to change the output throughput from time to time. It is a throughput simulation law where the throughput varies.

The throughput and the duration of the throughput are positive and integer values. The values are extracted from the user-defined file. This file must be a text file.
Separators used for decoding are End of Line (CR or CR-LF), semicolon, comma, tab or space characters.

If a line starts with a sharp (#) character, the rest of the line is ignored i.e. up to the End of Line (CR or CR-LF)

There are a couple of values to read:
- The first value is the throughput. The unit of the throughput is the Kbps.
- The second value read is the duration of the throughput. The duration unit is the millisecond.

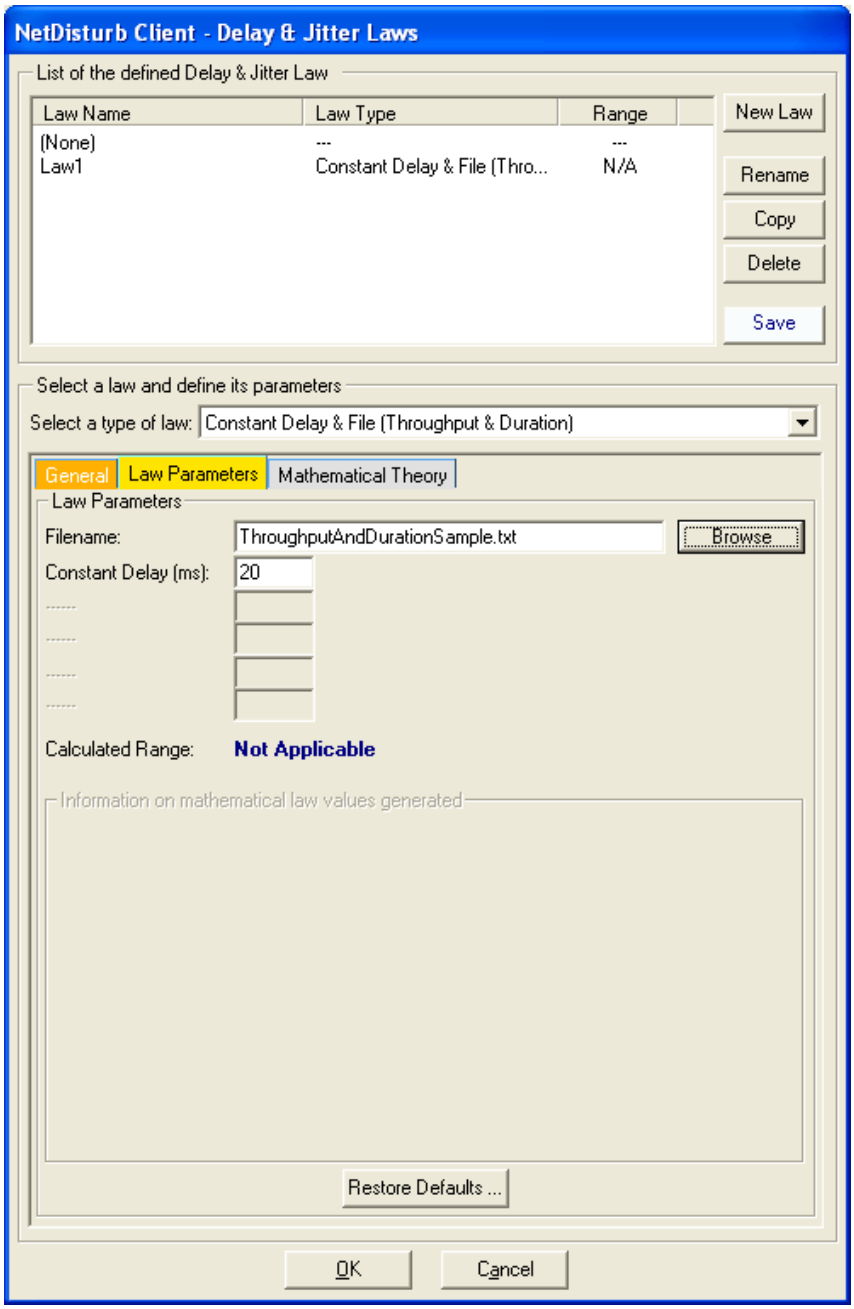
To assure performance, the file is read in one shot and stored in memory at law selection time. The values extracted from the file fill a table transmitted to the **NetDisturb** driver. In order to not overload the memory resources, the maximum read number of values is limited to 40,960 i.e. 20,480 couples.

If the file size exceeds the 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, the file is read again from the beginning to complete the table.

The **NetDisturb** driver extracts a couple of values from the table to get the throughput to apply and its duration. When the duration expires, the next couple of values is extracted from the table, and so on.

A constant delay can be added to each packet, to simulate the network delay, for example the satellite upload or download frame delay.



The constant delay of 20ms is the minimum delay applying to each packet of the flow. The values extracted from the file are added to the constant delay, helping to create a jitter.

If V is the set of values extracted from the file, k the constant delay, the delay D for the packet n is calculated as shown below:

$$D(n) = V(n) + k$$
$$D(n+1) = V(n+1) + k$$

The jitter or Inter Packet Delay Variation (IPDV) is calculated by the formula:

$$D(n+1) - D(n) => V(n+1) + k - V(n) - k = V(n+1) - V(n)$$

The jitter is generated by the values extracted from the file.

7.4.6 The Content Impairment Law Configuration

NetDisturb can change the packets content following a mathematical law configured by the user or using values extracted from an input file. These values apply to the packets matching to the selected Filter, if a loss law hasn't previously lost the packets.

Up to 100 Content Impairment Laws can be created.
By default the following laws are defined in the **Default.wsx** context file:

Combo-box (Law identifier)	Comment area	Description
(None)	(None)	With this option, no impairment is applied to the IP Flow.
1 out of 10	1 Packet out of N	Range (N): 10
Percentage	Percentage	Percentage: 5
Normal Law Impairment	Normal Law (Laplace-Gauss)	The domain of values is [0..100]. Parameters of the law are : ▪ Average:30 ▪ Standard deviation:10 ▪ threshold: 40
Uniform Law Impairment	Uniform Law	Domain values [1 to 100] Threshold = 20

For each law coming from the **Default.wsx** context file, the default packet content impairment parameters are used. See 7.4.6.7 Packet Content Impairment Type for more details.

7.4.6.1 Content Impairment Law and the Working Mode

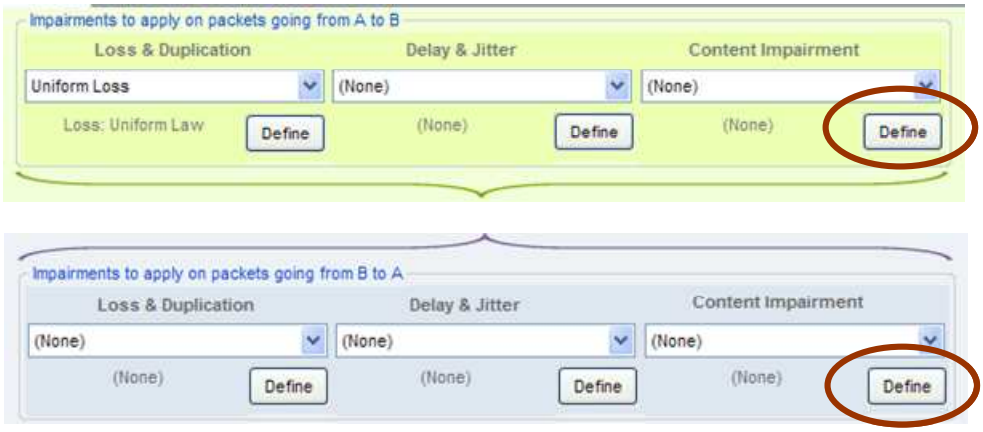
Contrary to the other types of disturbance, the Content Impairment laws are not concerned by the Working Mode. When a Content Impairment law is selected over a given Flow, the law applies to all packets matching the Filter.

For each new packet, a new value is extracted from the law or from the file, depending on the type of law selected. These values are stored in a global table by **NetDisturb**. When the table is empty, **NetDisturb** Server provides a new table to the **NetDisturb** driver with new values depending on the law.

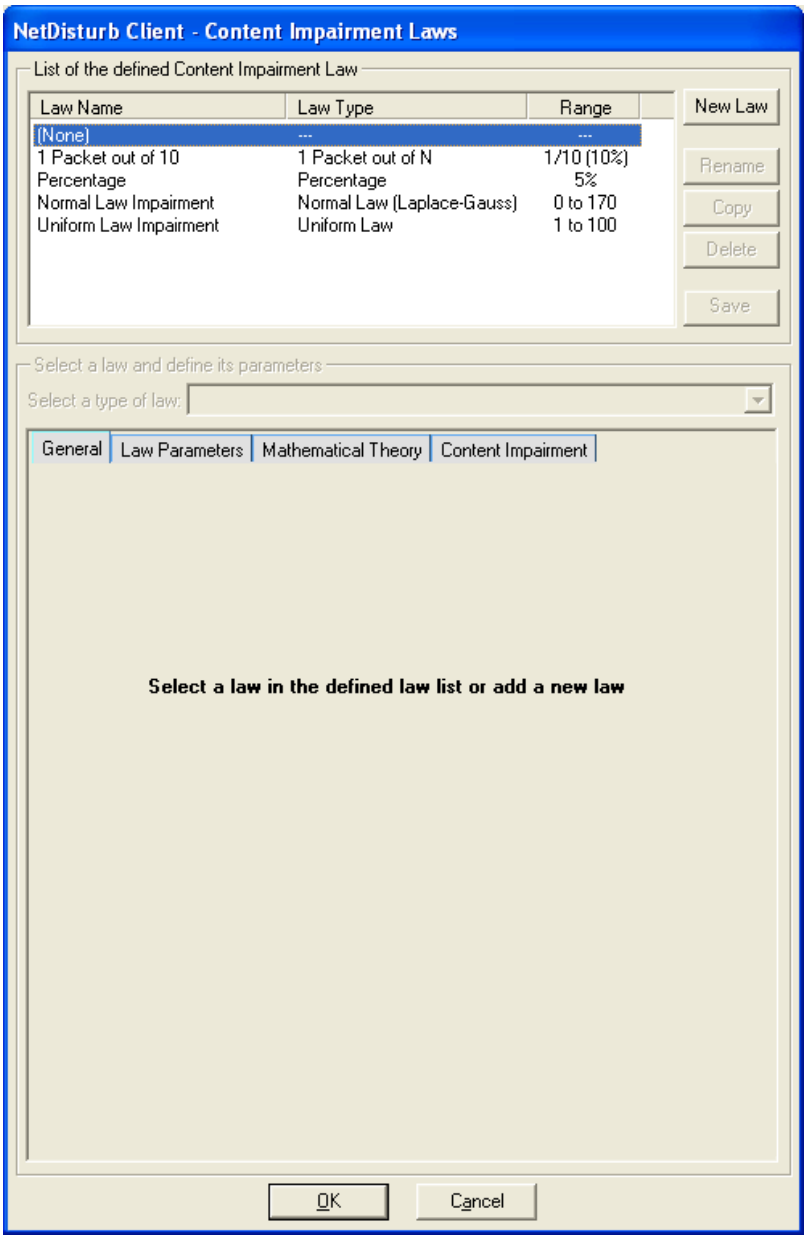
This value is compared to the Threshold: if the value is greater or equal than the Threshold, the packet content is impaired.

7.4.6.2 How to create or edit the Content Impairment Law

To create or configure a Packet Content Impairment Law click on the **Define** button at the top or bottom part of the main window.



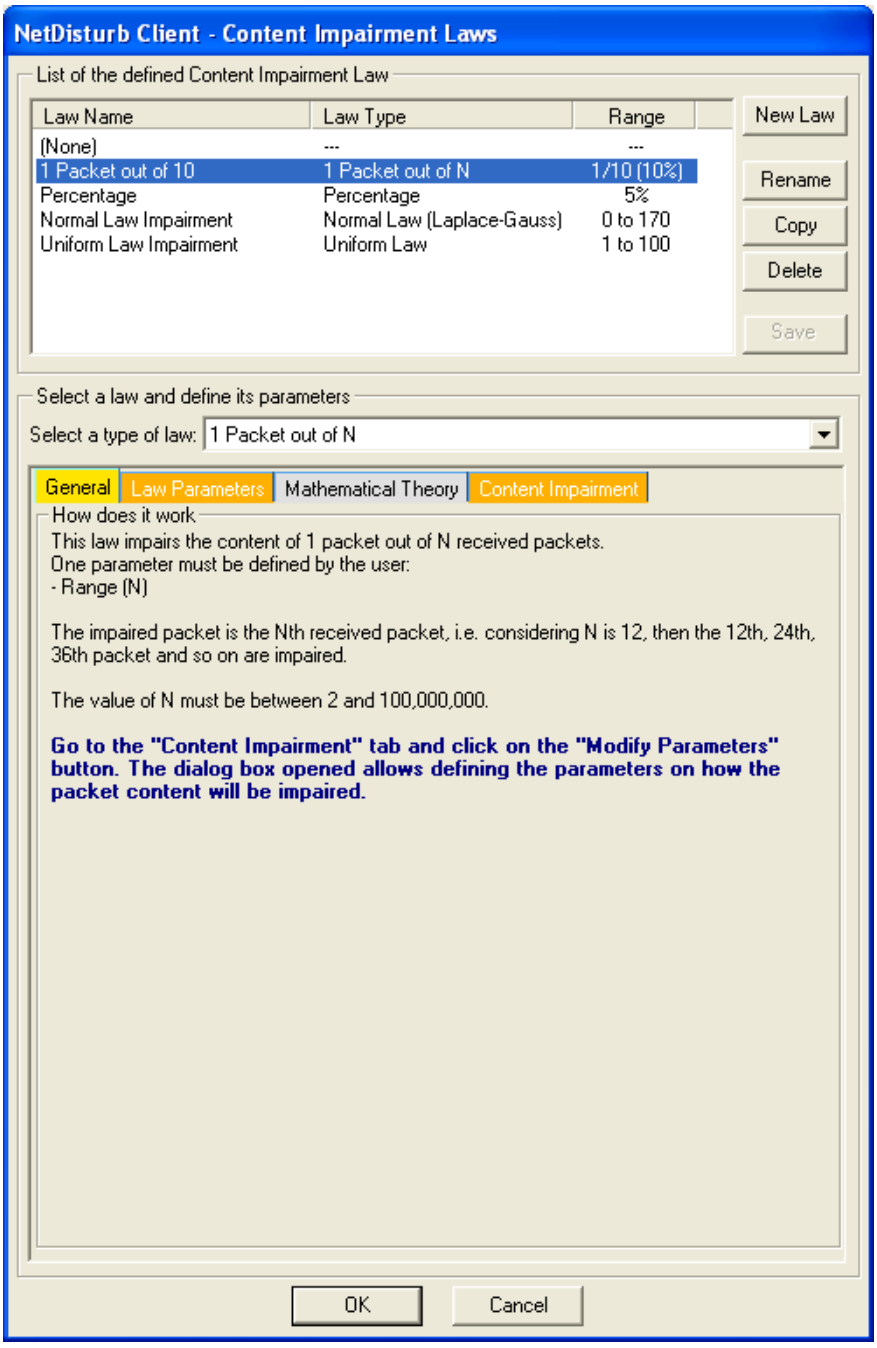
The following window is then displayed:



This window allows creating a new law or modifying an existing one.

If **(None)** is selected, only the **New Law** button is enabled and the tabs to define the parameters are disabled.

If you select a preexisting law in the current list-box, then the parameters and the details about this law can be viewed and the first "General" tab is enabled as in the example below:



This window is composed of two areas:

- **List of the defined Delay & Jitter Law**: a list-box displays the defined laws and five buttons allow managing the laws: **New Law**, **Rename**, **Copy**, **Delete** and **Save**.
- **Select a Law and define its parameters:** a list-box displays the loss and duplication laws authorized by the software. Then there are 4 tabs to define and to help the user to set up the parameters of the selected law.
  - (Tab 1) **General** (explaining how does the impairment law work)
  - (Tab 2) **Law Parameters**

- (Tab 3) **Mathematical Theory** (only available with Content Impairment Laws using a mathematical law)
- (Tab 4) **Content Impairment**

7.4.6.2.1 List of the Content Impairment Laws defined

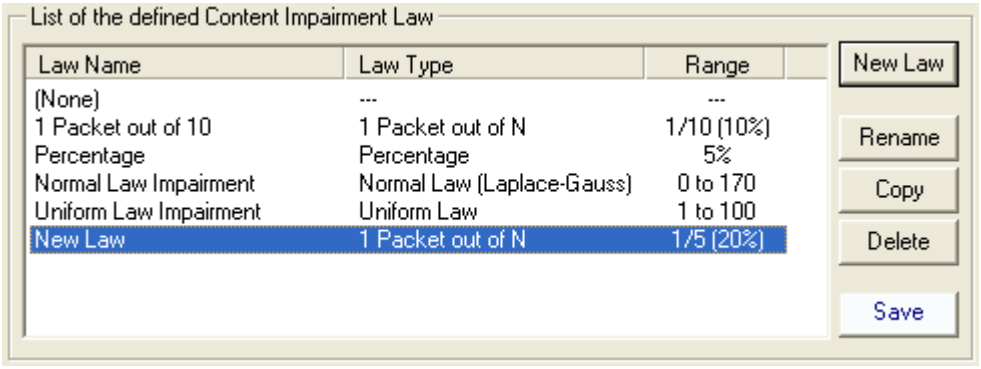
The list-box displays for each defined law the summary of the characteristics, except for (None) corresponding to 'No Content Impairment Law' selected:

- Law Name: Name of the law
- Law Type: The type of Content Impairment law chosen amongst the pre-defined list (more details available in 7.4.6.2.2 Select a law and define its parameters)
- Range: Range of values generated by the specified laws.

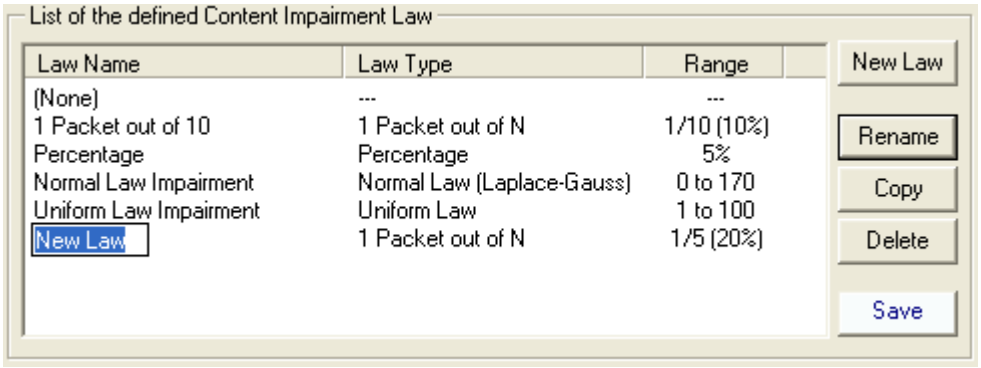
To manage the Law list, various buttons are available:

New Law: this button should be used to add a new Law in the defined Law list.

After pressing the New Law button, a new entry is added at the end of the list-box with 'New Law' as name of the law:

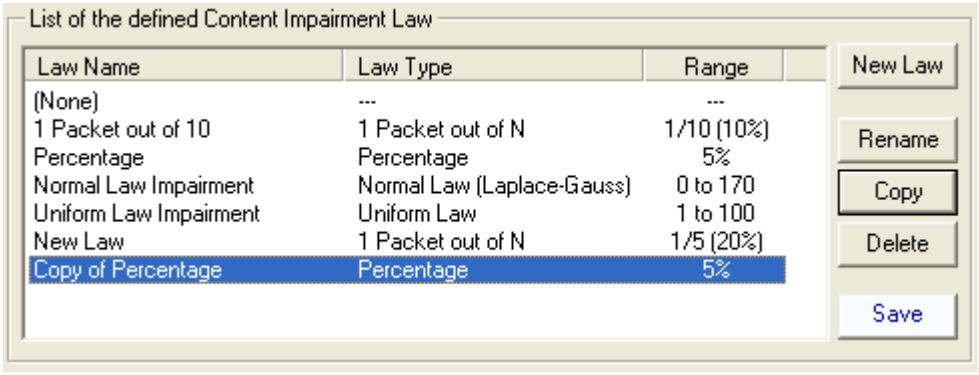


Then click on 'New Law' label to rename this entry or press the Rename button:

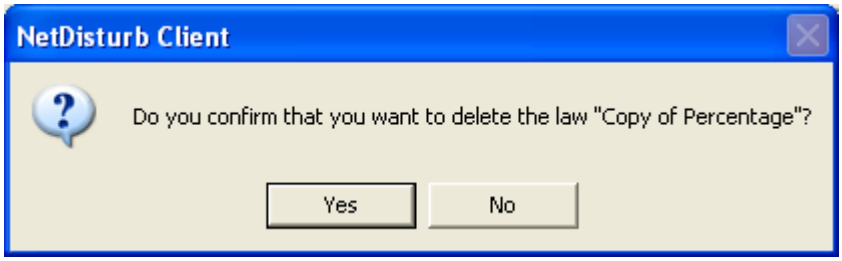


Rename: to rename the Law. This button should be used to change the Law name.

Copy: this button copies the current selected law at the end of the list with a new name. The following example shows the new list-box after copying the existing Percentage law:



Delete: this button should be used to remove a Law from the current list.
First select in the list-box the law to delete and then press the Delete button. A confirmation window is then displayed:



Save: to save all changes related to the laws.

7.4.6.2.2 Select a law and define its parameters

Once a law has been created, then you can define or modify the parameters of the law:

The first step is to choose the law type amongst the list of the pre-defined Content Impairment laws. Then there are 4 tabs to define and to help the user to set up the parameters of the selected law.

- (Tab 1) **General** (explaining how does the impairment law work)
- (Tab 2) **Law Parameters**
- (Tab 3) **Mathematical Theory** (only available with Content Impairment Laws using a mathematical law). This tab gives some details on the theory of the mathematical law used.
- (Tab 4) **Content Impairment**

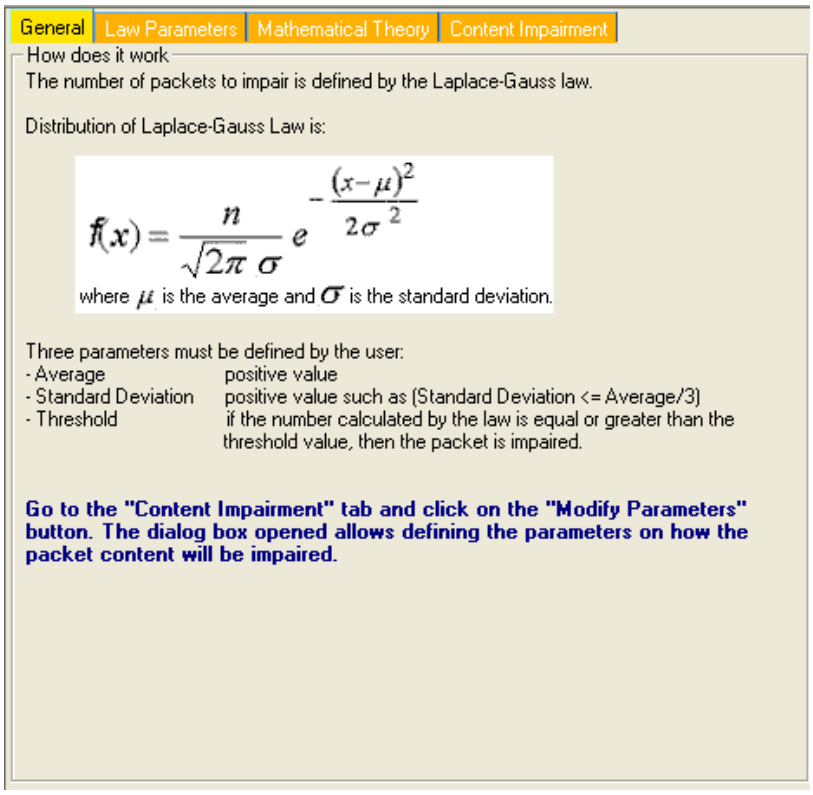
⇨ Select a type of law

A combo box allows selecting a law among the following pre-defined laws:

- 1 Packet out of N
  Parameter: range (N)
- Percentage
  Parameter: percentage
- Uniform law
  Parameters: alpha, beta, threshold
- Normal law (Laplace-Gauss)
  Parameters: average, standard deviation, threshold

⇨ The "General" tab (tab 1)

Details on the law type chosen and on the way to choose the parameters are provided on this tab as shown on the figure below:



⇨ The “Law Parameters” tab (tab 2)

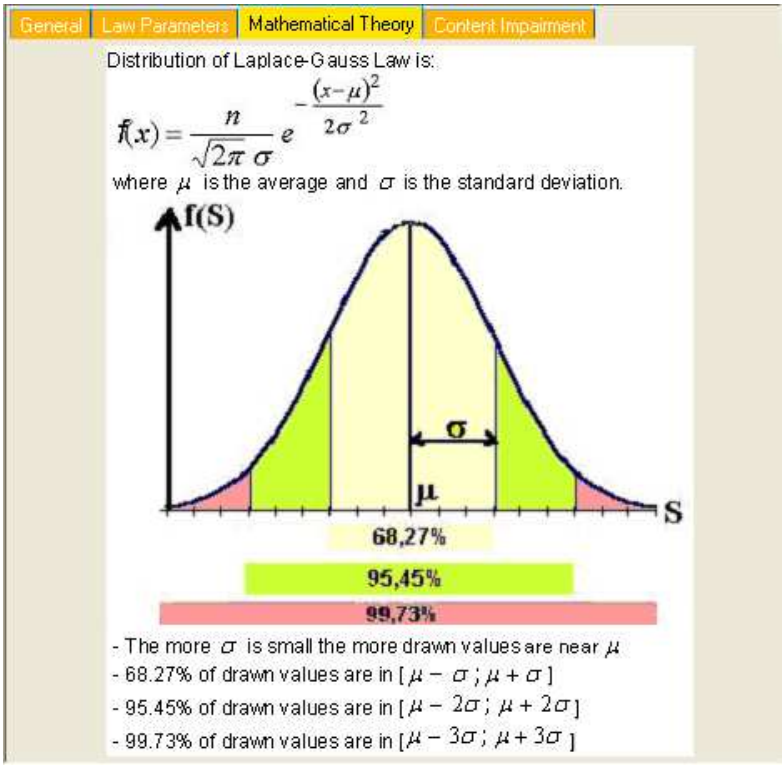
This tab is described for each law type here after.

⇨ The “Mathematical Theory” tab (tab 3)

This tab is available with the following laws only:

- Normal Law
- Uniform Law

This tab provides the main explanations of the mathematical theory of the law as shown on the figure below:



⇨ The “Content Impairment” tab (tab 4)

This tab is described in paragraph 7.4.6.7 Packet Content Impairment Type.

⇨ Action buttons

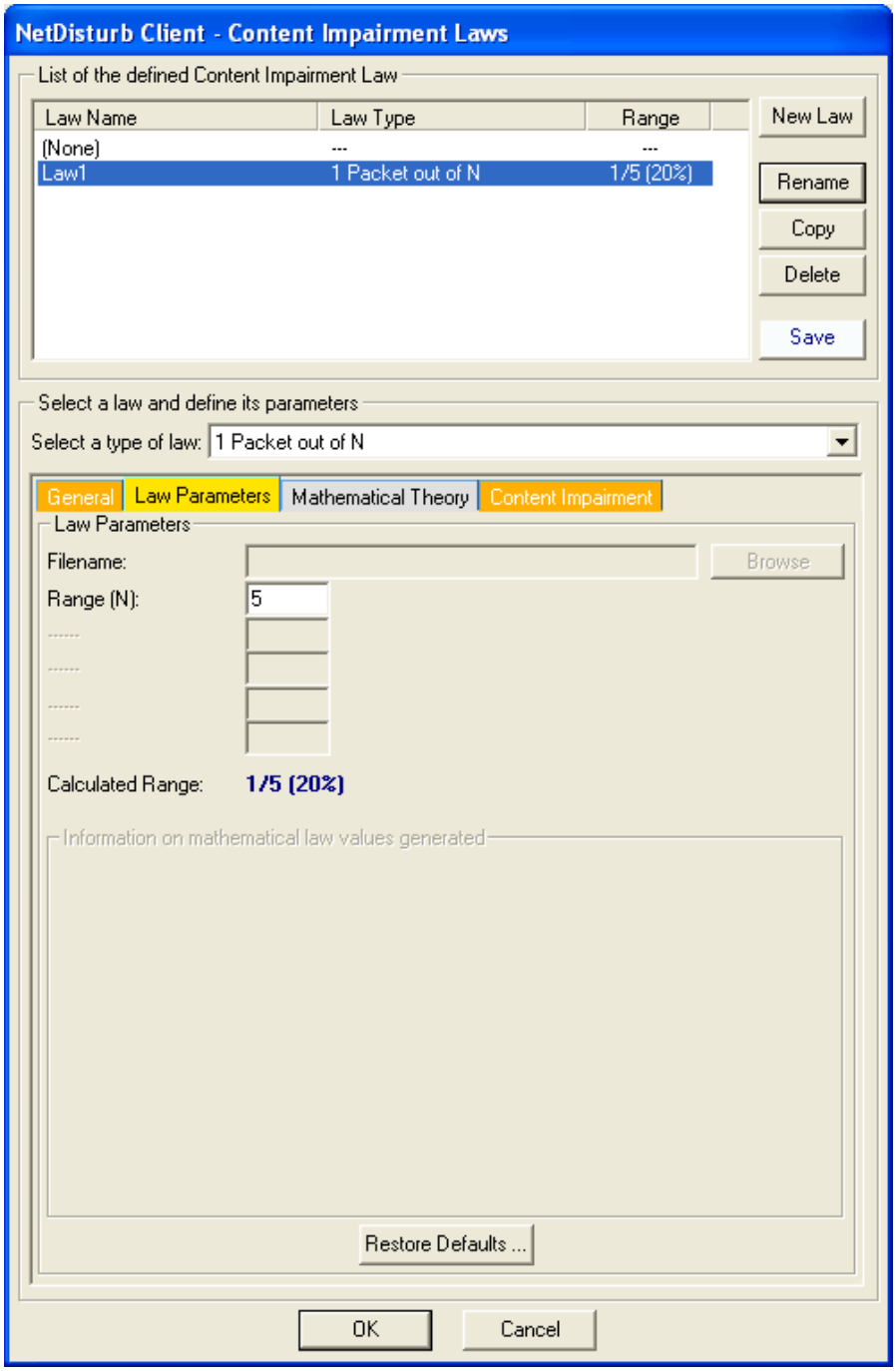
The "Content Impairment Laws" window handles a temporary list of laws until the **OK** or **Cancel** button is pressed.

Button	*Action*
Restore Defaults …	Reset all parameters of the current law.
OK	Save all modifications made if you didn't save them before. Moreover, the selected law in the list of the defined laws becomes the selected law in the combo-box of the Flow window.
Cancel	Ignore all modifications made if you didn't click on the Save button before. In that case, the last law selected in the combo-box of the Flow window is kept.

How to create a new Content Impairment Law:

1. Click on the "New Law" button,
2. Then click on the “Rename” button to modify the name of the law.
3. Choose one of the pre-defined law in the combo box
4. Select the "Law Parameters" tab,
5. Enter law parameter(s). The "General" tab and the "Mathematical Theory" tab contain information that can be useful to define the parameters.
6. Go to the "Content Impairment" tab and click on the "Modify Parameters" button to specify the parameters on the content impairment type.
7. Press the “Save“ button to save the changes and to continue to create or modify other laws.
8. Press “OK” to quit the “Content Impairment Laws” window and to select this new law as the law to be applied on the corresponding Flow.

7.4.6.3 1 Packet out of N

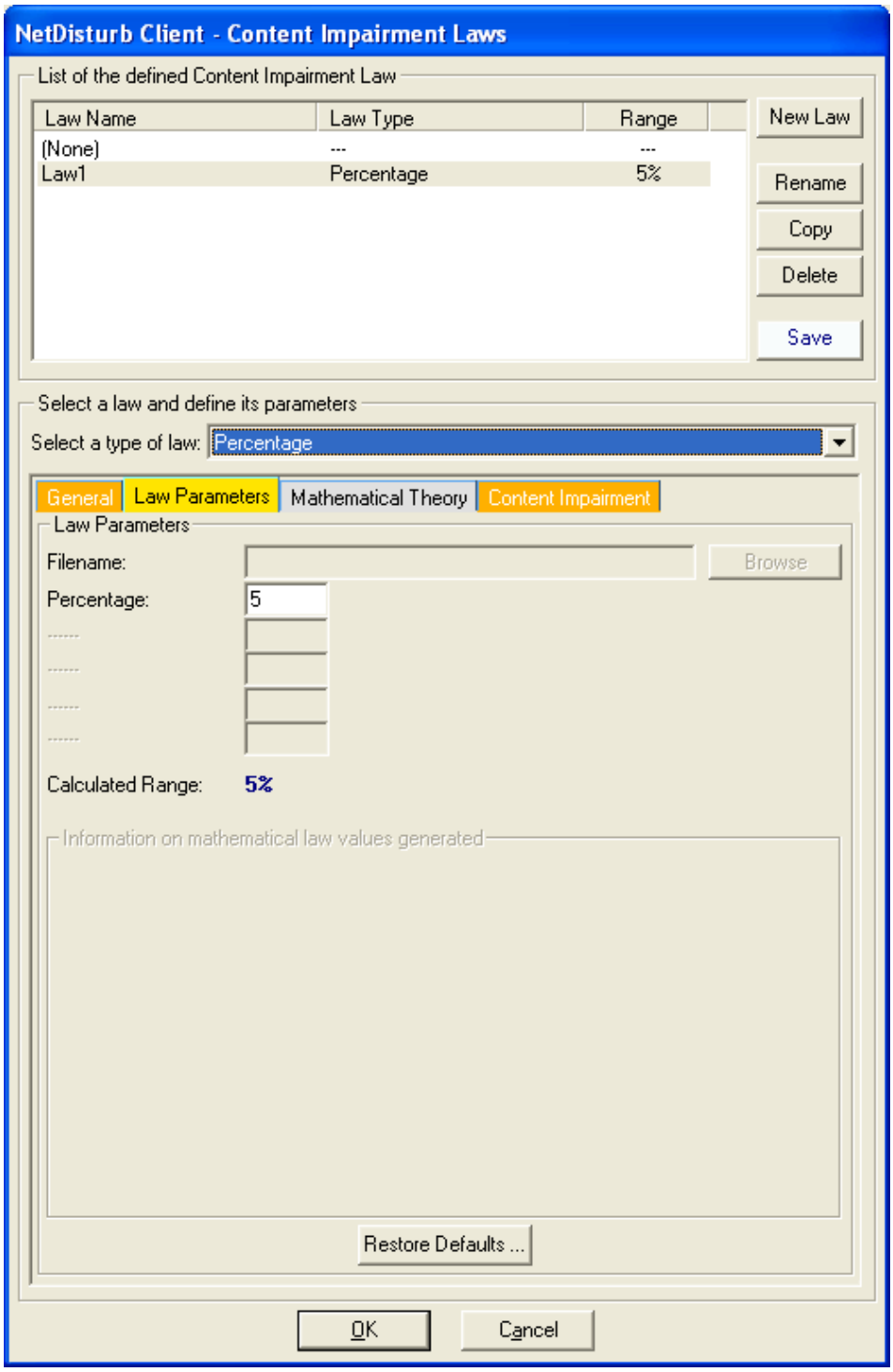


This law allows impairing the content of 1 packet out of N received packets. It affects a same packet based on its order.

The impaired packet is the Nth received packet, i.e. considering N is 12, then the 12th, 24th, 36th packet and so on are lost.

The value of N must be between 2 and 100,000,000.

7.4.6.4 Percentage



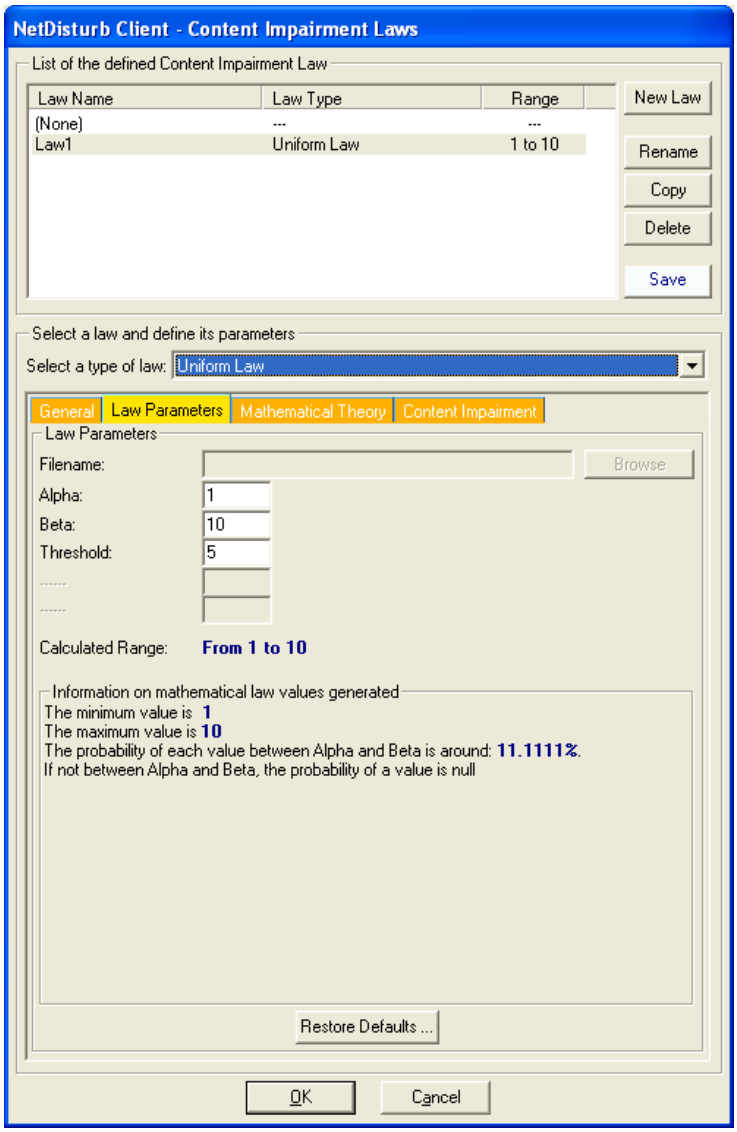
When this law is selected, a percentage of packets are impaired and the packets to impair are randomly selected.
The percentage of impaired packets is calculated on the basis of 100 received packets or a multiple of 100. For this reason, the percentage indicated has to be 1 or 2 consecutive digits, i.e. 12% and 0.00056% are allowed BUT NOT 10.2% or 0.00506%.

If the value of 100% is specified then all the packets are impaired.

The value of the percentage must be bounded between 0.00000001% and 100%, and the impaired packets are selected in a random way.

7.4.6.5 Uniform Law

When this law is selected, a uniform distribution of numbers contained between the **Alpha** and **Beta** values 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 7.4.4.1) for each selected packet. If this number is greater or equal than the threshold, then the packet is impaired.

The mathematical function used is (click on the “Mathematical Theory” tab or see the Uniform Law in Part 10 for more information):

Uniform law on (α, β) range

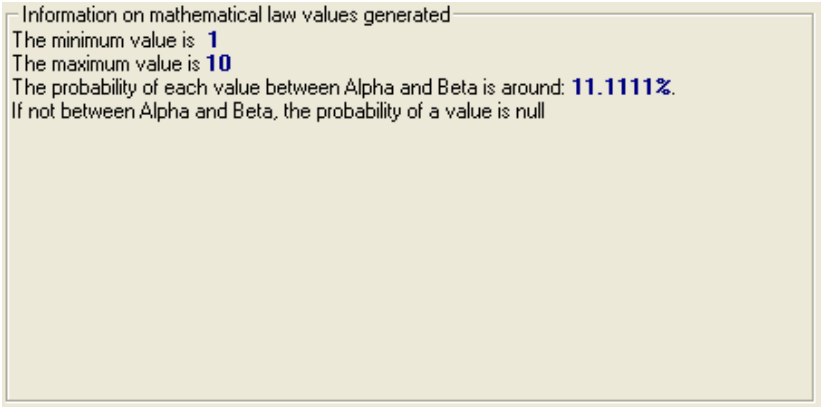
$f(x) = 1/(\beta - \alpha)$ if $\alpha < x < \beta$

$f(x) = 0$ else

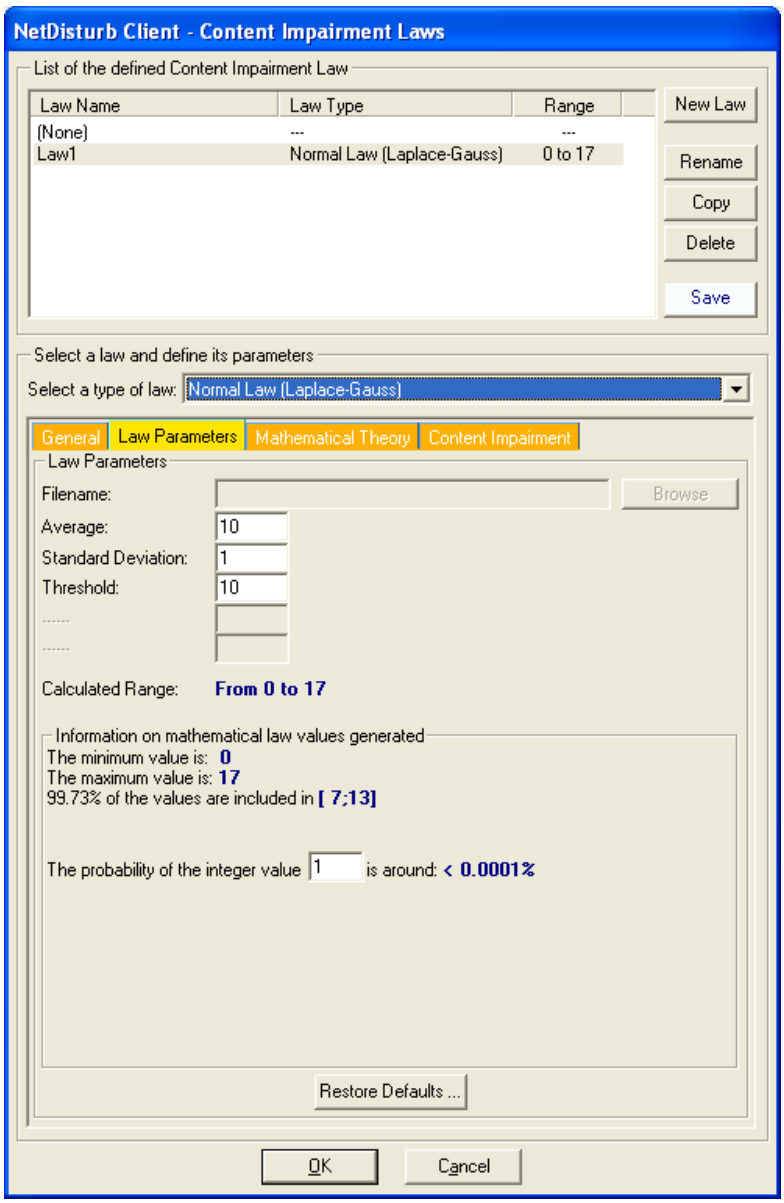
For this law, three parameters are defined:

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

An additional area, called “Information on mathematical law values generated” is available with this law. Here are provided some information about the minimum and maximum values. The mathematical law generates these values using the user-defined parameters. Moreover, the probability of each value that can be generated is also shown.



7.4.6.6 Normal (Laplace-Gauss) Law



The **NetDisturb** driver picks a number in the table (see also 7.4.4.1) for each selected packet. If this number is greater or equal than the threshold, then the packet is impaired.

The mathematical function used is (click on the “Mathematical Theory” tab or see the Normal Law in Part 10 for more information):

Normal law on (α, β) range

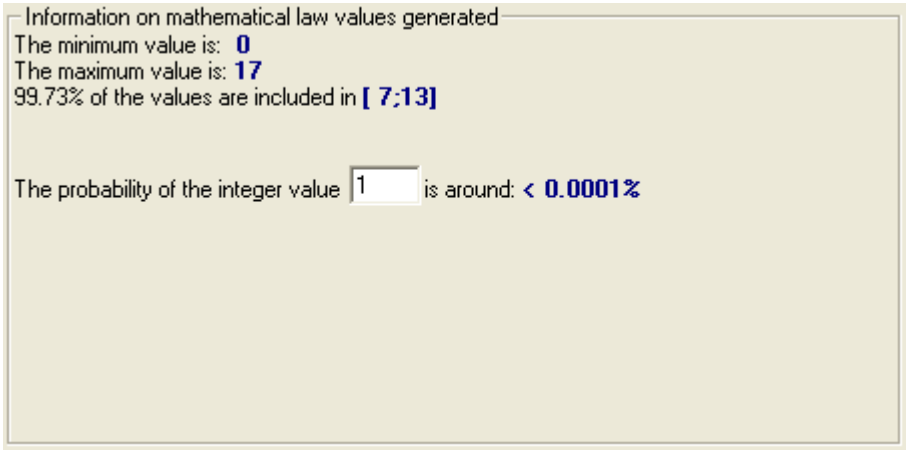
$f(x) = 1/(\beta - \alpha)$ **if** $\alpha < x < \beta$

$f(x) = 0$ **else**

For this law, three parameters are defined:

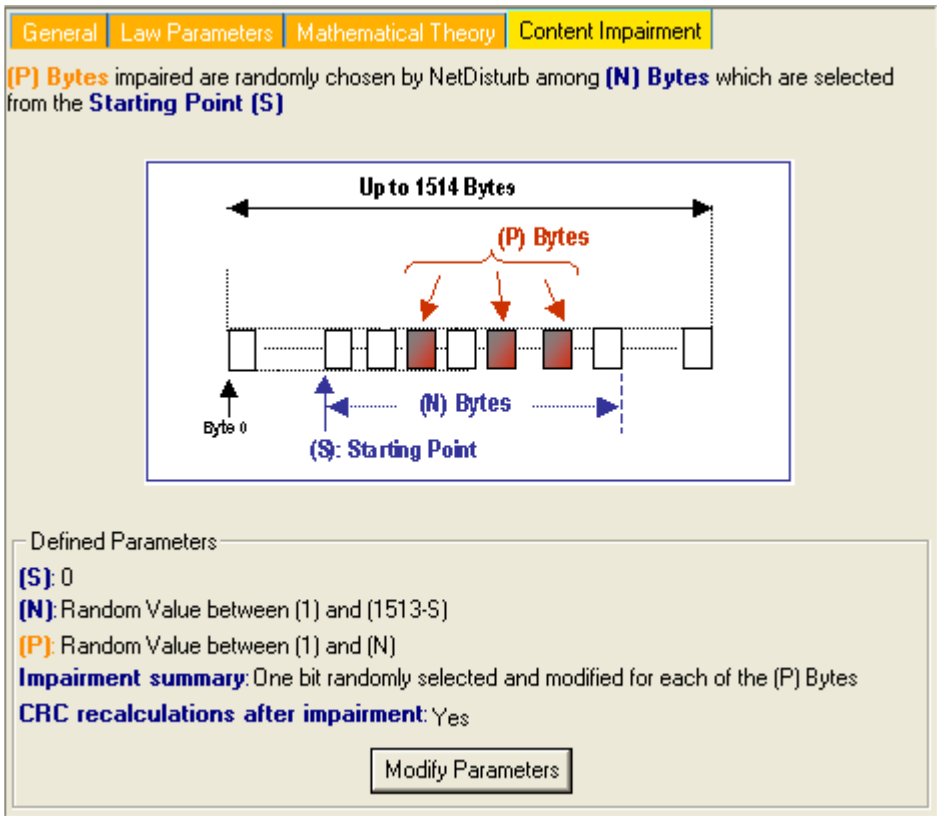
Average:	min value of the range
Standard Deviation:	max value of the range
Threshold:	if the number calculated by the law is greater or equal than the Threshold value, the packet is impaired.

An additional area, called “Information on mathematical law values generated” is available with this law. Here are provided some information about the minimum and maximum values. The mathematical law generates these values using the user-defined parameters. Moreover, the probability of each value that can be generated is also shown.

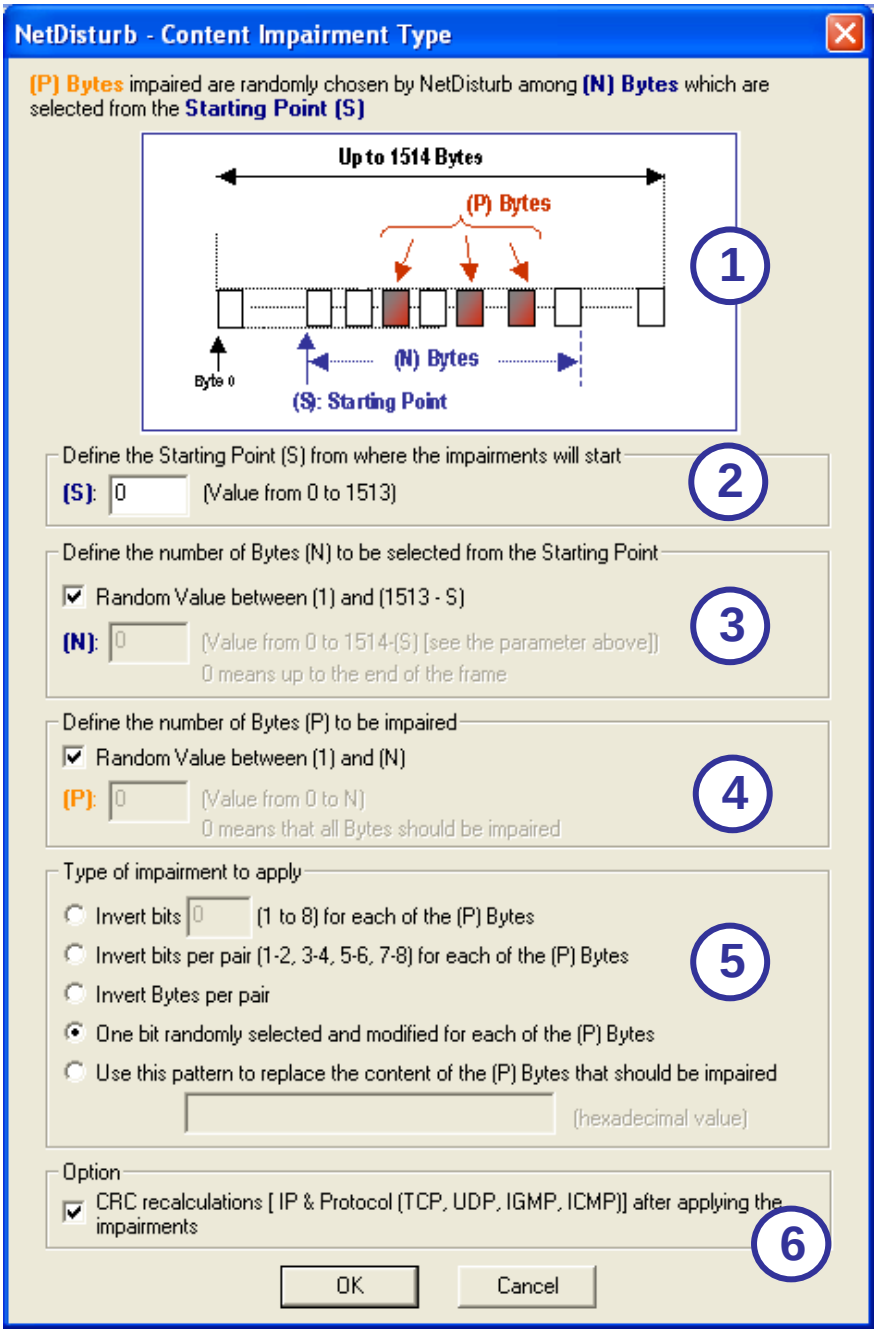


7.4.6.7 Packet Content Impairment Type

First, go to the "Content Impairment" tab. A figure shows the correspondence between the parameters to be specified and the Ethernet frame. This tab displays also a summary of the defined parameters for the content impairment type.
The button "Modify Parameters" allows modifying these parameters.



The following window is then displayed when you click on the "Modify Parameters" button:



This window is composed of 6 areas:

- **(1)** A figure showing the correspondence between the parameters (S), (N) and (P) and the Ethernet frame.

- **(2)** The first area allows defining the Starting Point (S) from where the impairment will start.

- **(3)** The second area offers two options to specify the number of Bytes (N) to be selected from the Starting Point.
  - either the number of Bytes (N) is randomly selected
  - or the number of Bytes (N) is fixed. If the value is 0, that means up to the end of the frame.

- **(4)** The third area allows setting the number of Bytes (P) to be impaired. Here two options are available:
  - either the number of Bytes (P) is randomly selected
  - or the number of Bytes (P) is fixed. If the value is 0, that means all bytes are impaired.

- **(5)** This area of this section defines the type of impairment to apply on the selected bytes.

  There are five type of impairment available:

  - **Invert a specified number of bits** for each of the (P) Bytes (sequential inversion from the least significant bit to the most significant bit)

    Example: inversion of 7 bits for each of the (P) Bytes
    The initial byte value is:

    EA (Hex)
    11101010 (Bin)

    7 bits should be inverted:

    10010101 (Bin)
    95 (Hex)

  - **Invert bits per pair** for each of the N bytes
    Example:
    The initial byte value is:

    39 (Hex)
    00111001 (Bin)

    Bits are inverted per pair:

    00110110 (Bin)
    36 (Hex)

  - **Invert Bytes per pair**
    Example:

    The initial bytes sequence is : A0 BF E4 C7

    After the inversion, the sequence is: BF A0 C7 E4

  - **One bit randomly selected and modified** for each of the (P) Bytes
    Example:
    The initial byte value is:

    AF (Hex)
    10101111 (Bin)

    A bit randomly selected is inverted (here the third bit):

    10101011 (Bin)
    AB (Hex)

  - **Use a V pattern** to replace the content of the (P) Bytes that should be impaired. If the V pattern is bigger than (P) Bytes to replace, only the (P) first Bytes of the V pattern are used. If the V pattern is smaller than (P) bytes, all or part of the V pattern is used several times to replace the (P) bytes.

- **(6)** Finally, the possibility to recalculate the CRC is offered. The CRC recalculation can be necessary for some protocols. NetDisturb recalculates the CRC for a restricted list of protocol (IP and protocols TCP, UDP, ICMP, IGMP)

How does it work?

a) The calculation of the CRC depends on the localization of the impairment and the type of the modified frame. This is done automatically.

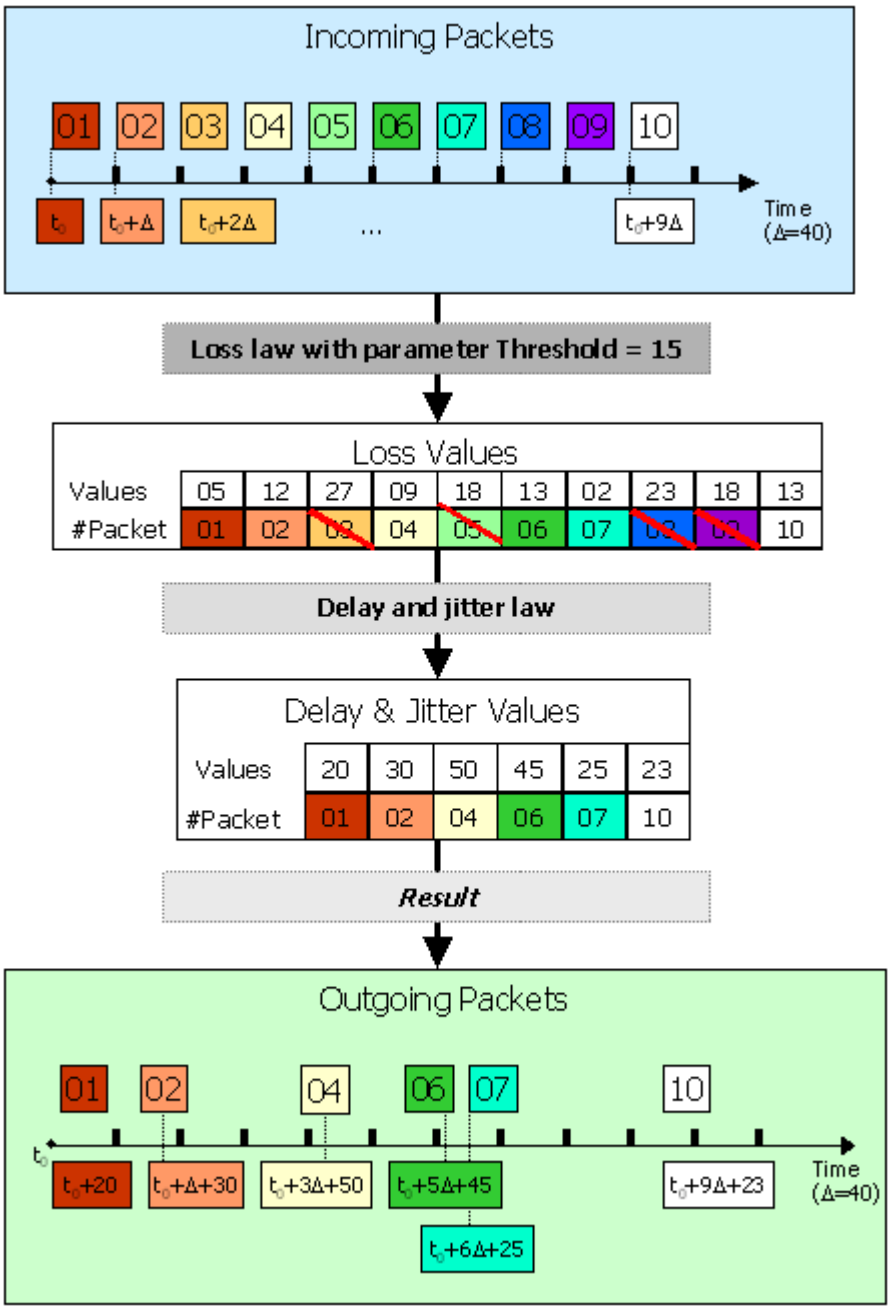
b) List of the headers generating a calculation of the CRC:
   i. **IP Header** (16 bits CRC)
   The checksum field is coded on 16 bits and allows checking the packet validity of the layer 3. Before doing the calculation, this field is set to 0 and only the IP header is considered.

   ii. **UDP Header** (16 bits CRC, if the CRC is different from 0) and TCP Header (16 bits CRC)
   The checksum field is coded on 16 bits and allows checking the TCP/UDP packet validity of the layer 4.
   The checksum field is the 16 bit one's complement of the one's complement sum of all 16-bit words in the header and text. If a segment contains an odd number of header and text bytes, the last octet is padded on the right with zeros to make a 16-bit word for checksum purposes. The pad is not transmitted as part of the segment. While computing the checksum, the checksum field itself is replaced with zeros.
   The checksum also covers a 96-bit pseudo header prefixed to the TCP header. This pseudo header contains the Source Address, the Destination Address, the Protocol, and the TCP length.

   iii. **ICMP Header** (16 bits CRC) and IGMP Header (16 bits CRC)
   The checksum field is coded on 16 bits and allows checking the ICMP or IGMP packet validity of the layer 3. Before doing the calculation, this field is set to 0

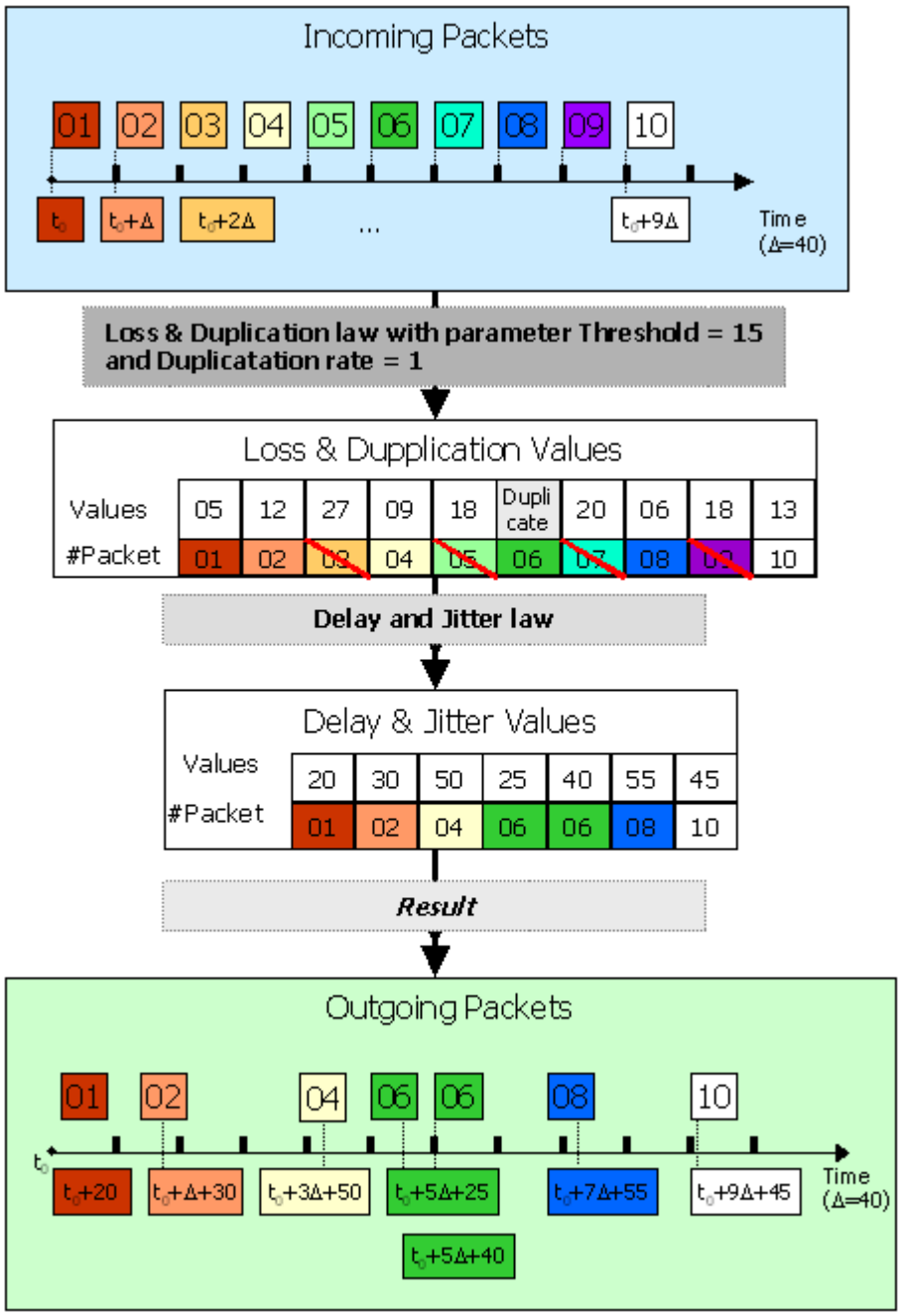
7.4.7 Loss/Duplication, Delay/Jitter Dynamics

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



7.4.8 Loss with Duplication and Delay/Jitter Dynamics

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



7.5 Use of the Aggregates

7.5.1 What is an aggregate?

An aggregate is an association of several IP Flows (at least 2) sharing the same Delay & Jitter Laws.
To be defined, the aggregate has to have a Delay & Jitter Law for at least one direction (A➔B and/or B➔A).
The IP Flow order in the aggregate defines the priority of packets to delay. While the top IP Flow get the highest priority, the other IP Flows are queuing until there are no higher priority packets.

All the IP Flows related to the aggregate must have their own Filter and possibly a Loss & Duplication Law, but they lose their own Delay & Jitter Law for the benefit of the law defined in the aggregate.
For a given IP Flow belonging to an aggregate, the non-lost packets are subjected to the Delay & Jitter Law of the aggregate.

A priority level applies to packets according to the IP Flow they belong to. The priority is decreasing according to the Flow number, i.e. the packets of the Flow # X get a higher priority than the packets of the Flow # X+1, etc.
All the packets of the Flow # X will be handled before the packets of the Flow # X+1 are taken into account. By waiting to be handled, the packets of the Flow # X+1 are put into a queue. When the queue of a Flow is full, the new packets of this Flow are lost.

All the IP Flows of an aggregate start and stop simultaneously. To start an aggregate, all the IP Flows defined for this aggregate must have a defined Filter.

7.5.2 When do we need to use an aggregate?

We use an aggregate when we wish to have different priorities for the various IP Flows to be impaired and when we wish to apply the same Delay & Jitter Law to these IP Flows.

Example of the simulation of a satellite access (IPv4 and IPv6) with a varying time bandwidth and a priority rule for the IP packets

In this example, we define an aggregate with three IP Flows with the following properties that defines the order of treatment for the received IP packets:

1) The first IP Flow is related to HTTP packets and we associate a Loss Law,
2) The second IP Flow is related to the TCP packets and we associate a Duplication Law,
3) The third IP Flow is related to the UDP packets without applying a Loss & Duplication Law.

So the HTTP packets are first processed with the IP Flow # 01, then the TCP packets are handled with the IP Flow # 02 and the UDP packets are finally processed with the IP Flow # 03.

To implement this example, the following steps must be considered:

- **Step 1:** define the Filter and the Loss & Duplication Law for the three IP Flows:
  - IP Flow #01:
    - Filter: Source Port List = 80
    - Loss & Duplication Law: select 1 predefined loss law
  - IP Flow #02:
    - Filter: Protocol = TCP
    - Loss & Duplication Law: select 1 predefined duplication law
  - IP Flow #03:
    - Filter: Protocol = UDP
    - No Loss & Duplication Law

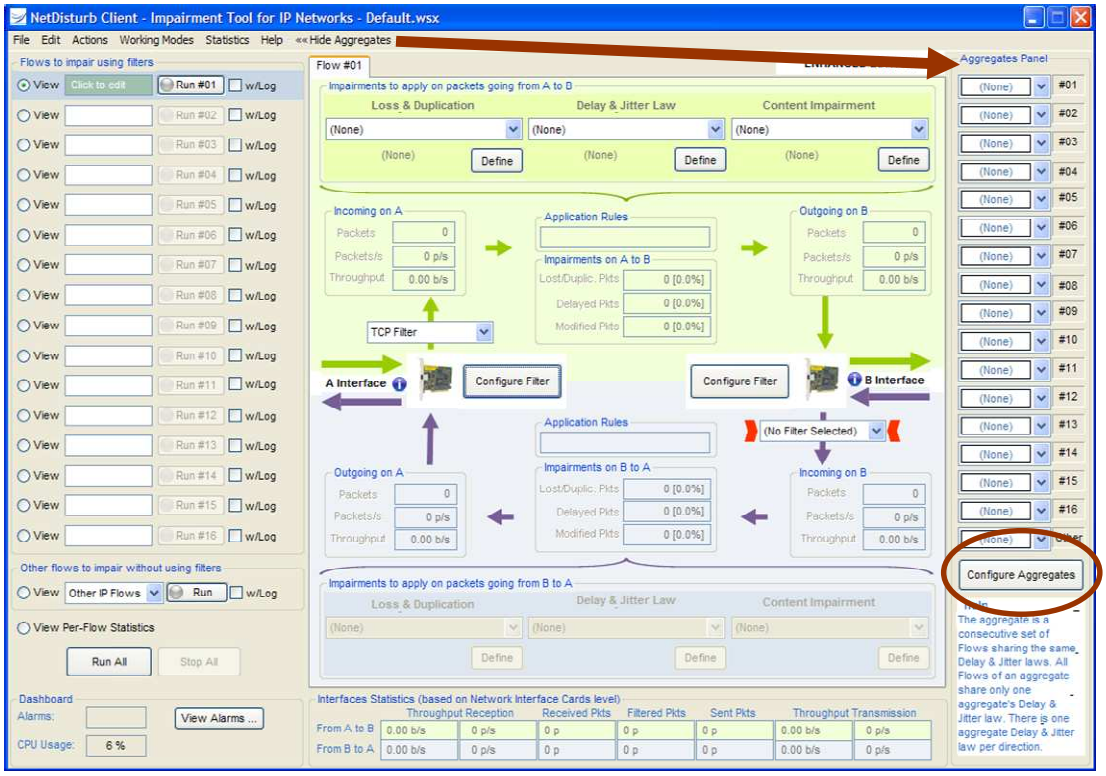
- **Step 2:** create now an aggregate (blue color for example) with the following Delay & Jitter Law: the 'Constant Delay &File (Packet Sending Minimum Cadences)' law allowing to simulate the bandwidth variation according to the time (a file containing a couple of integer and positive values <Throughput (in Kbps) | Duration (in ms)> must already exist).

- **Step 3:** apply now the blue aggregate to the three IP Flows.

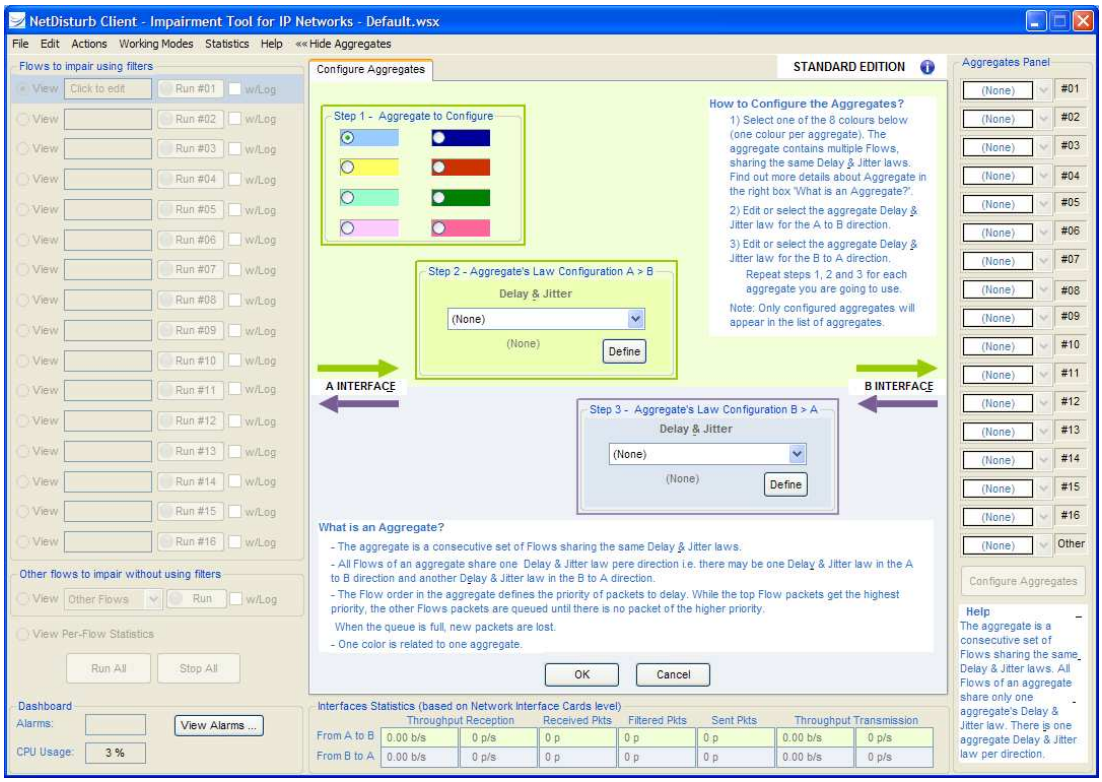
- **Step 4:** Run "IP Flow # 01" to start. When an IP packet is received, **NetDisturb** checks if this packet can be associated to one of the IP Flows of the aggregate. If yes, it will apply the Loss & Duplication Law before the Delay & Jitter Law of the aggregate.

7.5.3 How to configure the aggregates

Click the **Show Aggregates >>** menu to display the aggregates section on the right of the window.



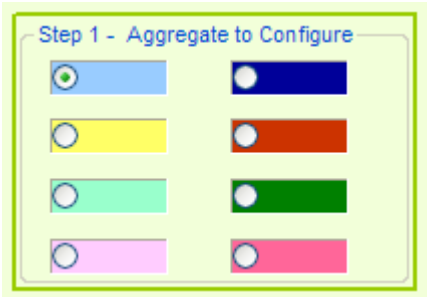
Then press the "Configure Aggregates" button, and the center part of the main window now displays the section to configure the aggregates as shown below:



You can define up to 8 aggregates and one aggregate is associated with one color.

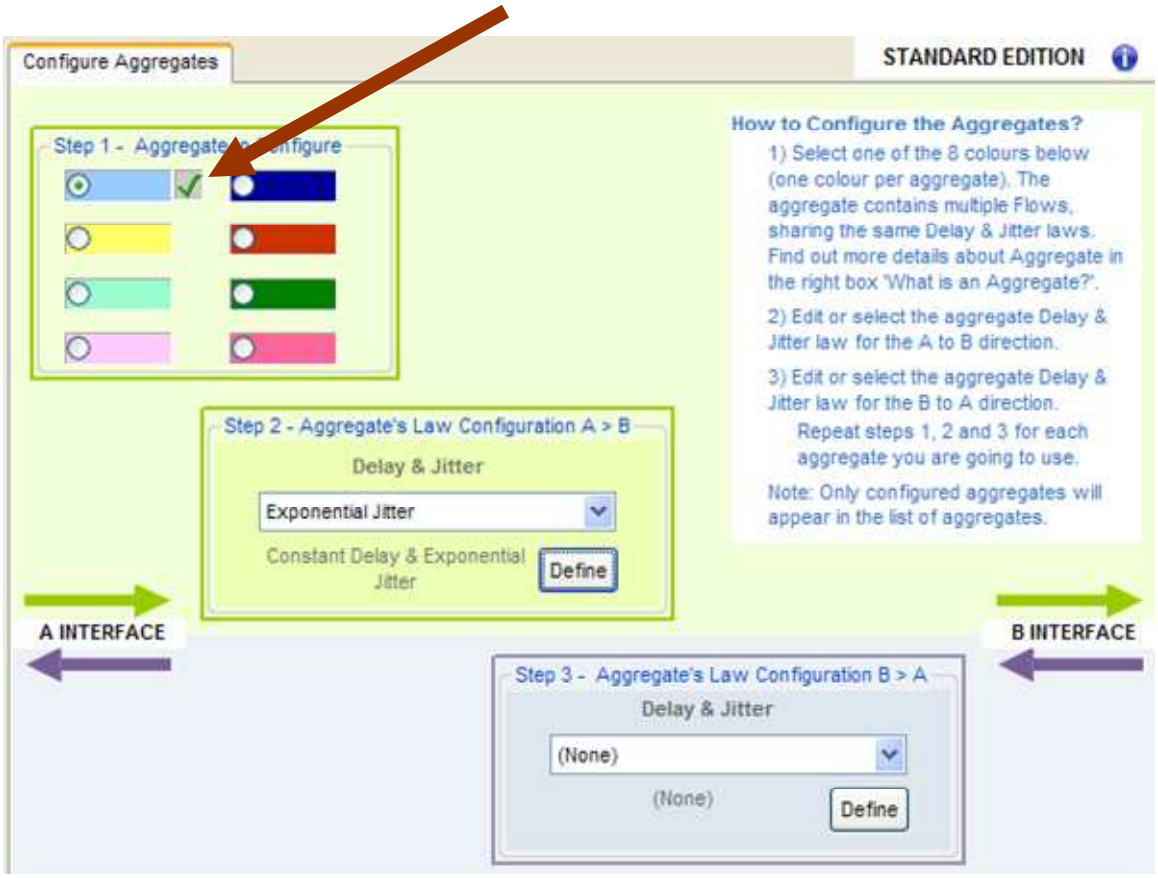
Four steps are necessary to parameter an aggregate.
The step 2 and the step 3 are optional, but **at least one Delay & Jitter Law should be defined**.

- Step 1: Select first a color among 8 for the aggregate



- Step 2 (optional): Select or define a Delay & Jitter Law in the A ➔ B direction

Once a law has been selected or defined, a tick mark is displayed on the right of the color box, as shown below:



- Step 3 (optional): Select or define a Delay & Jitter Law in the B ➔ A direction

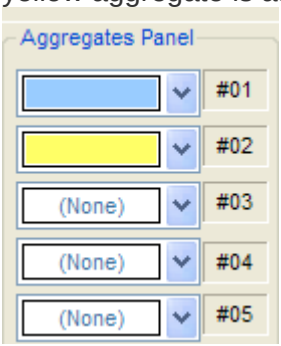
Once the law has been selected or defined, if the tick mark was not already present, it will be displayed on the right of the color box.

- Step 4: Click OK to save the aggregate

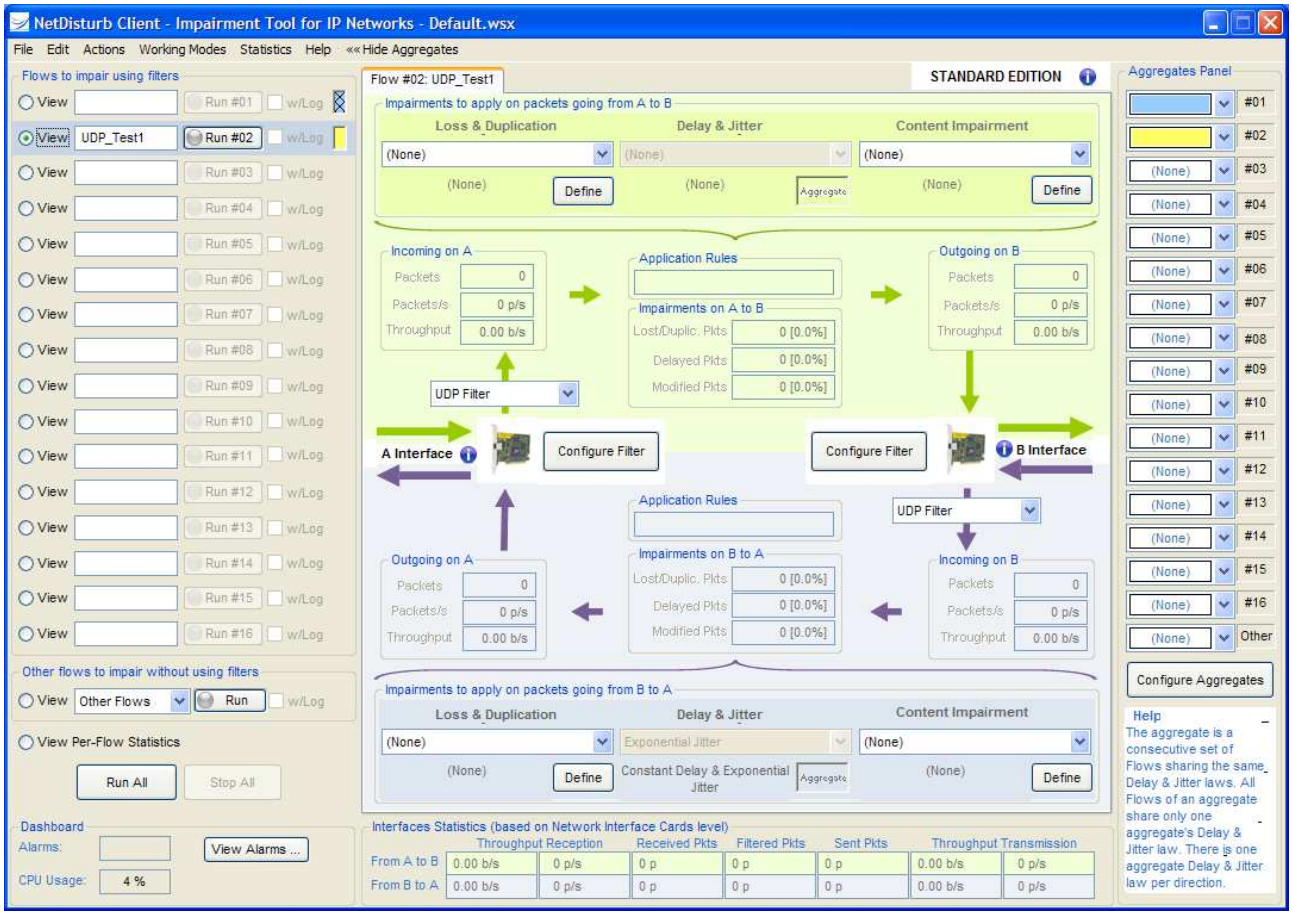
7.5.4 How to associate a colored aggregate to a Flow

Click the combo-box as shown below - in this example two aggregates have been defined: **Light Blue** and **Yellow**.
Then select the colored aggregate.

For the following example, the light blue aggregate is associated to the IP Flow # 01, and the yellow aggregate is associated to the IP Flow # 02.



Once the aggregate is selected, a colored mark is displayed on the right of the Flow.

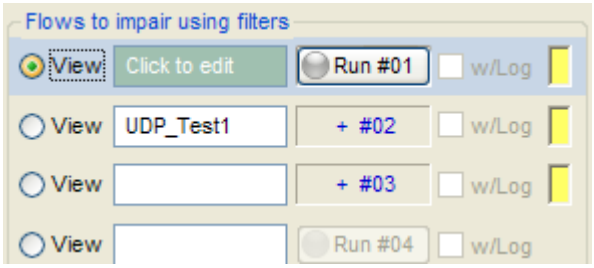


For the following example, the light blue aggregate is associated to the Flow # 01, and the yellow aggregate is related to the Flow # 02.

The colored mark located on the right may have two states:

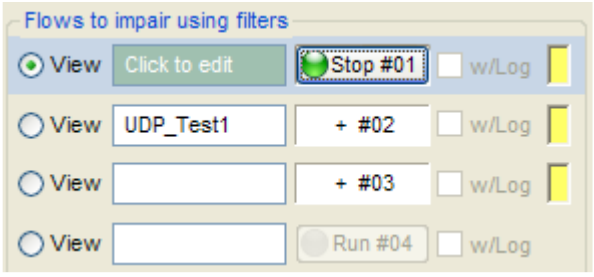
- full color, for example  meaning that a Filter is defined for this Flow
- or hatched color, for example  meaning that a Filter is not defined for this Flow and can't be started.

You can associate the same colored aggregate to several Flows as in the example below where three Flows are associated to the yellow aggregate:



Note that the label of the buttons change when an aggregate is associated to several Flows (except for the first one): the label of the "Run #02" and "Run #03" buttons change to "+ #02" and "+ #03".

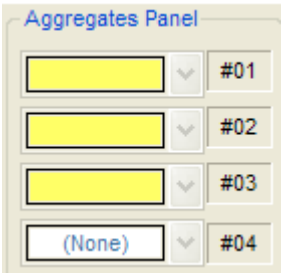
To start the aggregate, press the "Run #xx" button.



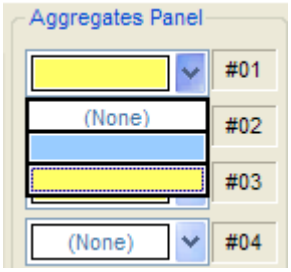
To stop the aggregate, press the "Stop #xx" button related to the first flow of the aggregate.

7.5.5 How to disassociate an IP Flow belonging to a colored aggregate

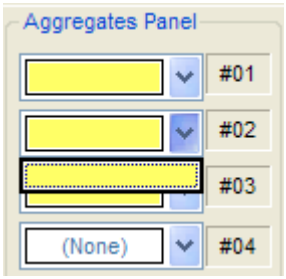
Example:
A yellow aggregate is associated with three Flows: #01, #02 et #03.



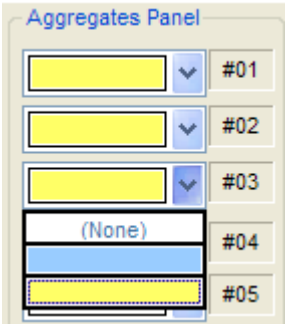
You can only dissociate a Flow belonging to an aggregate if this Flow is the first or the last of the aggregate. Click on the combo-box related to the Flow to select **(None)** in order to dissociate the Flow.



When you click on the combo-box for the Flow #01, the **(None)** choice is available to dissociate the Flow from this blue aggregate.



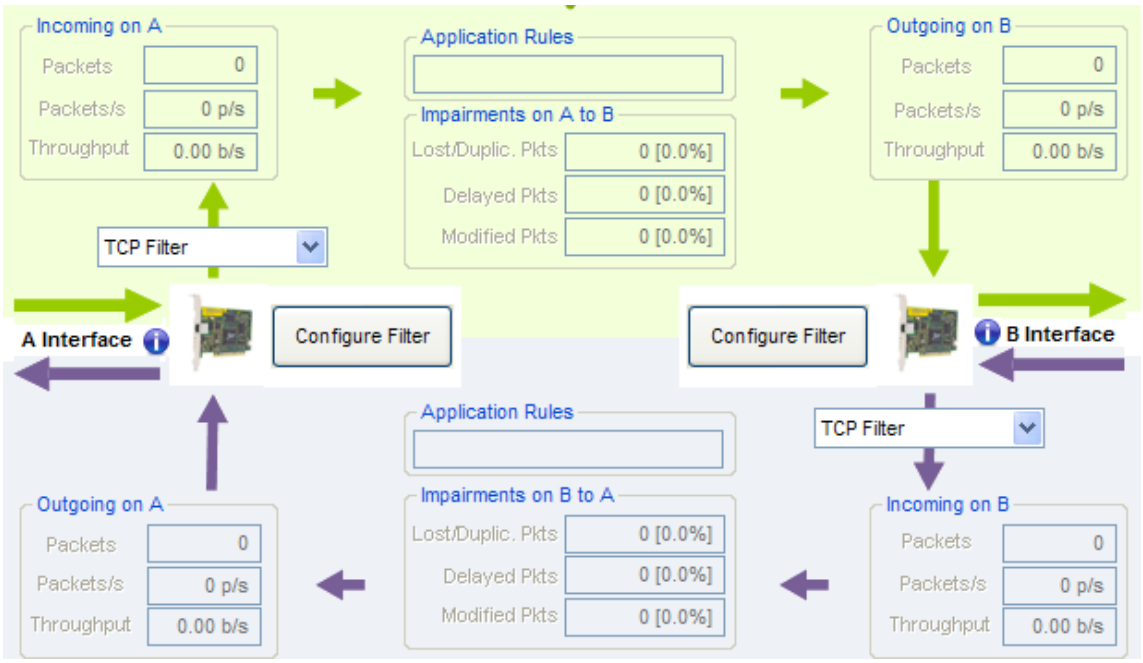
The Flow #02 can't be disassociated because the previous Flow (#01) and the next Flow (#03) are associated to the aggregate.
When you click on the combo-box for the Flow #02, the **(None)** choice is not available.



With this configuration, you can disassociate the Flow #03.

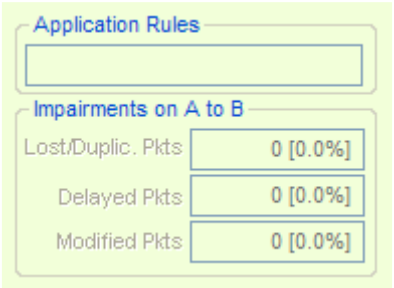
7.6 The NetDisturb Client Statistics

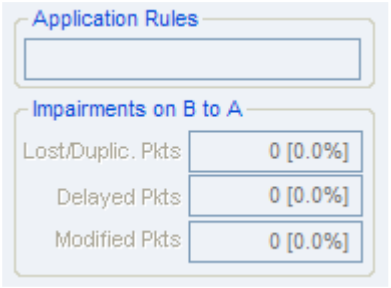
The traffic on the two interfaces is displayed in the central part of the window when a Flow is selected, with a section for each interface A and B.
Each section includes one receiving area (**incoming**) and one sending area (**outgoing**).
The GUI displays the following statistics:



# Packets	This field presents the instant number of packets received for the Flow.
# Packets/Second	This field presents the instant number of packets per second for the Flow.
Throughput	This field displays the instant throughput in bit/s, kb/s or Kib/s, Mb/s or Mib/s, according to the sampling period defined in the **NetDisturb** Client configuration.

For each direction (**A to B** or **B to A**), impairment statistics are given:

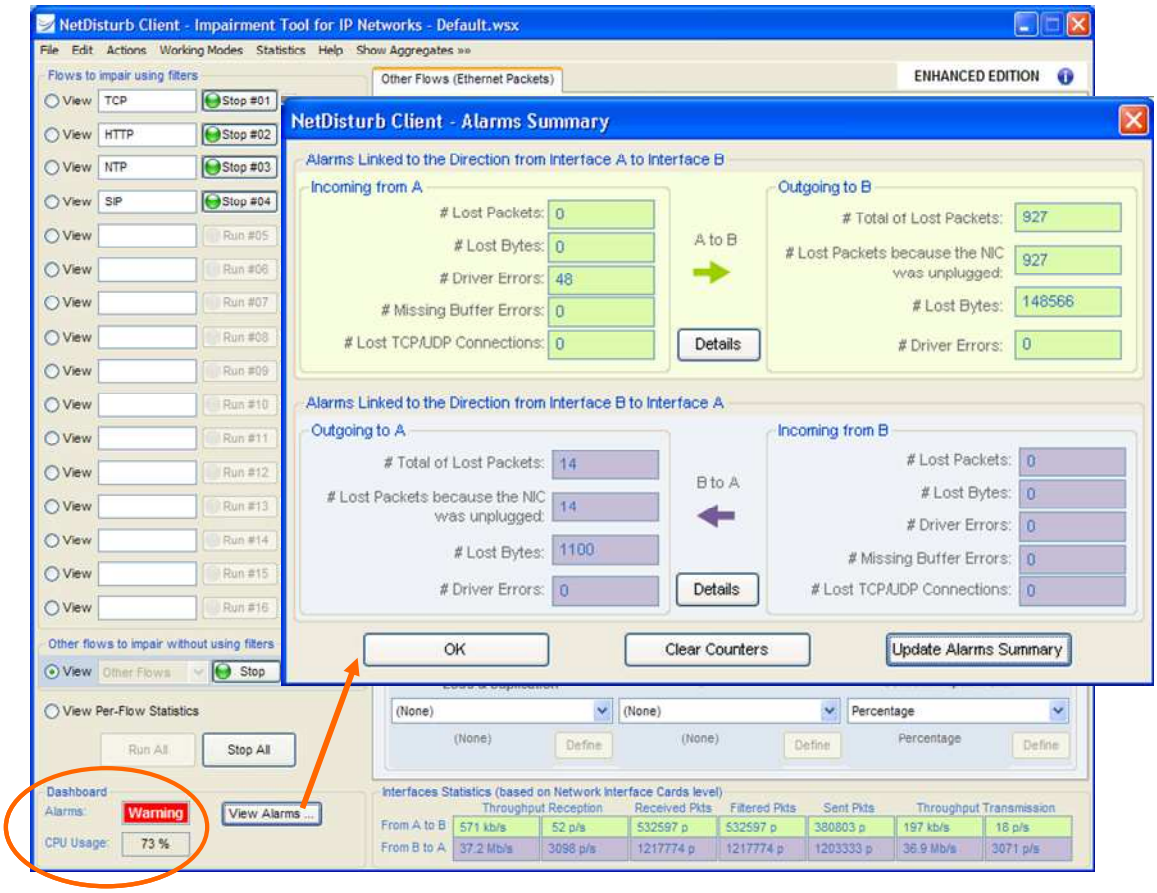




Application Rules	This field presents the state related to the application of impairments. List of five possible states: **- Applying Impairments** **- Waiting for the Trigger** **- Delay before Impairments** **- Delay before next cycle** **- No more impairments**
Lost/Duplic. Pkts	This field presents the instant number of lost or duplicated packets per second for the Flow.
Delayed Pkts	This field presents the instant number of delayed packets per second for the Flow.
Modified Pkts	This field presents the instant number of modified packets per second for the Flow.

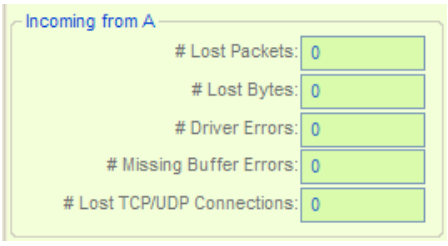
7.7 The Errors Detected by the NetDisturb Driver

If errors occur at the **NetDisturb** driver level, the 'Alarms' button located at the left bottom of the client window is red colored.



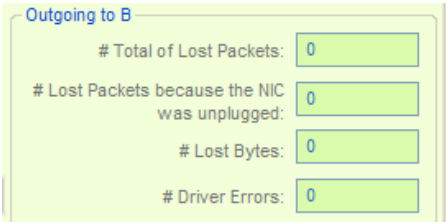
Click on the "View Alarms" button to get details about the errors and the following window is displayed:

The alarms are classified per direction: **A ➔ B** and **B ➔ A**.
The Information displayed is different depending of the direction (incoming or outgoing).



For the incoming direction:

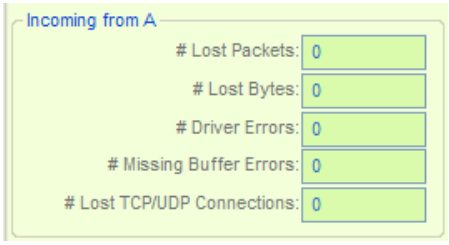
- Number of lost packets
- Number of lost bytes
- Number of errors returned by the driver of the Network Interface Card
- Number of buffers that were missing to keep all packets
- Number of lost or ignored TCP/UDP connections



For the outgoing direction:

- Total number of lost packets
- Number of lost packets due to a NIC unplugged
- Number of lost bytes
- Number of errors returned by the driver of the Network Interface Card

7.7.1 Details for the Incoming Errors



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

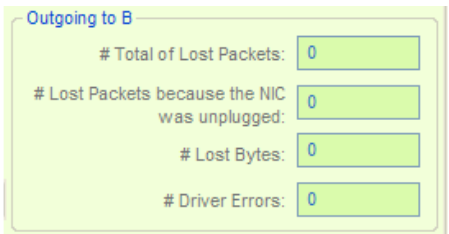
- **# Lost Bytes**
  Number of lost bytes (total packet size including the MAC header) due to memory allocation errors or interface access errors.

- **# 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

- **# Missing Buffer 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 10.2 to increase the number of buffers)

- **# Lost TCP/UDP Connections**
  This counter is handled only when the working mode "Laws apply to each IP Flow" is selected. When a packet is received for a new connection but that new connection cannot be added because the maximum number of connections configured has been reached or due to a memory allocation error, this counter is increased for each packet received (see paragraph 10.2 to increase the number of connections).

7.7.2 Details for the Outgoing Errors



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

- **# Lost Packets because the NIC was unplugged**
  Number of lost packets due to the unplugged Network Interface Card.

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

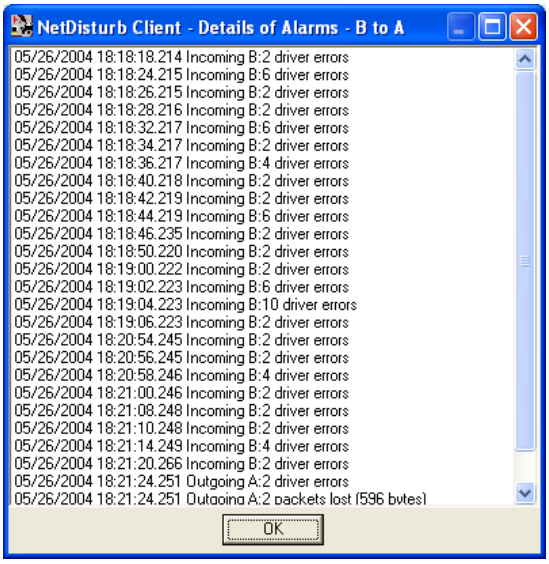
- **# Driver Errors**
  This error counter is the number of alarms returned by the NIC driver indicating that some errors have occurred from the started time of the NIC. Errors can be due to one of the following reasons:
  - CRC error
  - NIC or Driver Buffer overrun error

7.7.3 Alarm Management

Four buttons are used to manage these alarms.

- **Details button**

This button opens a window with details for the alarms:
- Timestamp
- Number of errors
- Error type



- **Clear Alarms button**

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

- **Update Alarms Summary button**

The ‘Update Alarms Summary’ button interrogates the **NetDisturb** driver to refresh the error list.

- **OK button**

The OK button closes the Alarms List window and reset the status of the "Alarms" button in the Client Window.

The Alarm Button changes from red color 

to gray 

until new errors occur.

7.8 Flow Logs and Events (Enhanced Edition only)

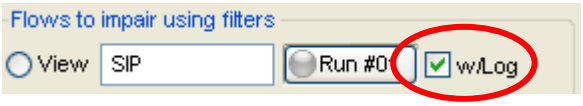
NetDisturb Enhanced Edition offers a way to get a detailed view about the activity of each individual flow when they are running. This activity is saved automatically into 2 files generated by **NetDisturb Enhanced Edition**:

1. One file contains the raw capture of the both directions traffic that matches the flow before the packets have been impaired, in an Ethereal compatible file format: the suffix for this file is pcap.
2. The other file contains the impairments applied to each packet in a text file, and the major events that have occurred to the flow e.g. law selection or dynamic connection identification for FTP or RTP.

The window displays summary of events; it allows launching the relevant viewer for these files and impairment details may be up-to-date in a list.

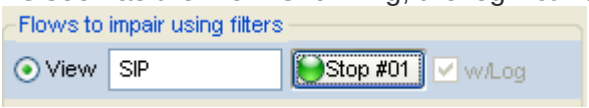
7.8.1 How to get the Flow Log

For each Flow, there is a button **w/Log**. When this button is checked, this selects the generation of the 2 files logs.

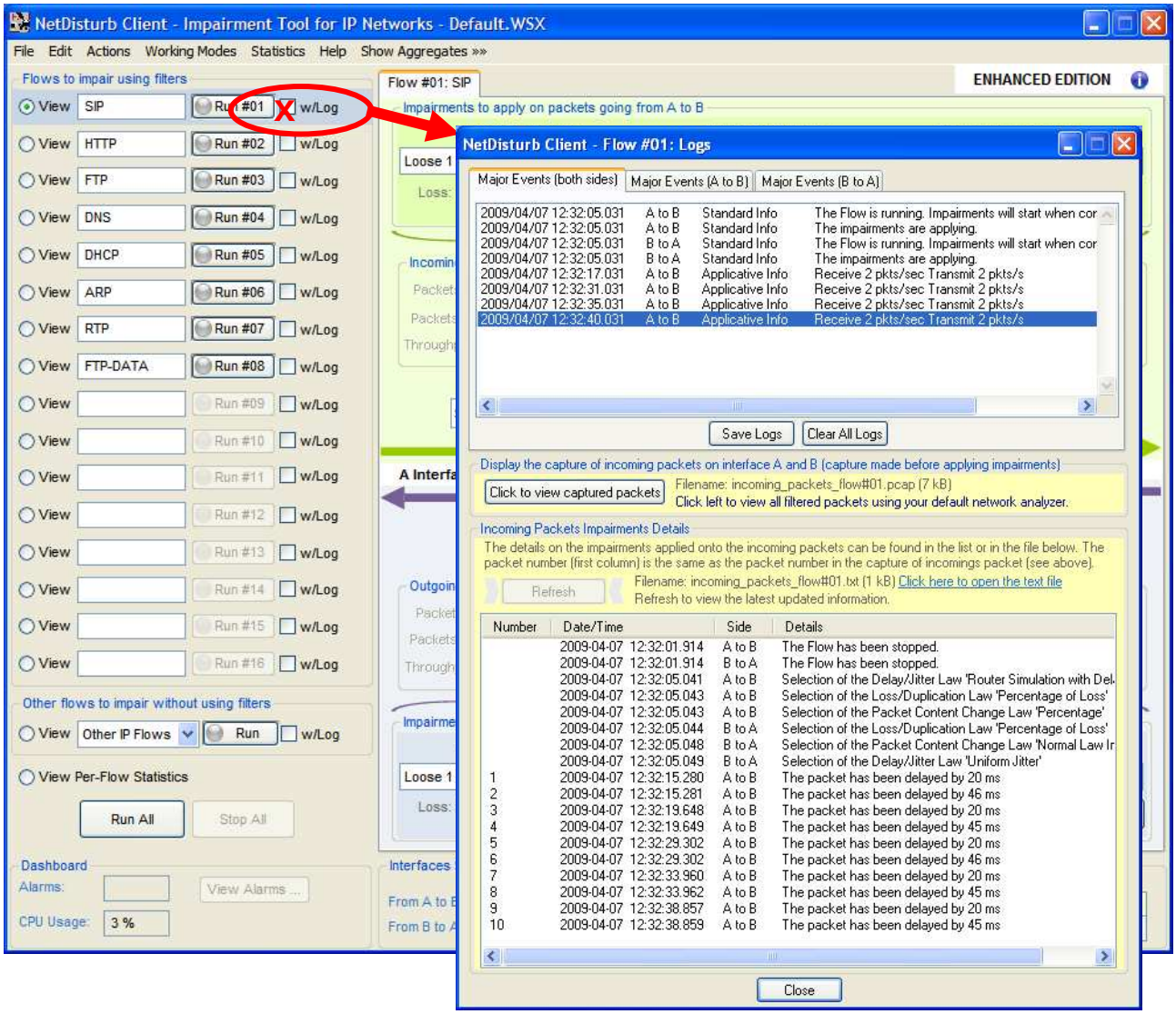


7.8.2 What is happening when the Flow runs

As soon as the Flow is running, the log Activity starts. The button **w/Log** becomes grayed.



A new window that details the current activity of the flow is displayed.



Details about the Flow log window can be found in paragraph 7.8.4.

7.8.3 When Does NetDisturb Enhanced Edition write into the individual flow log files

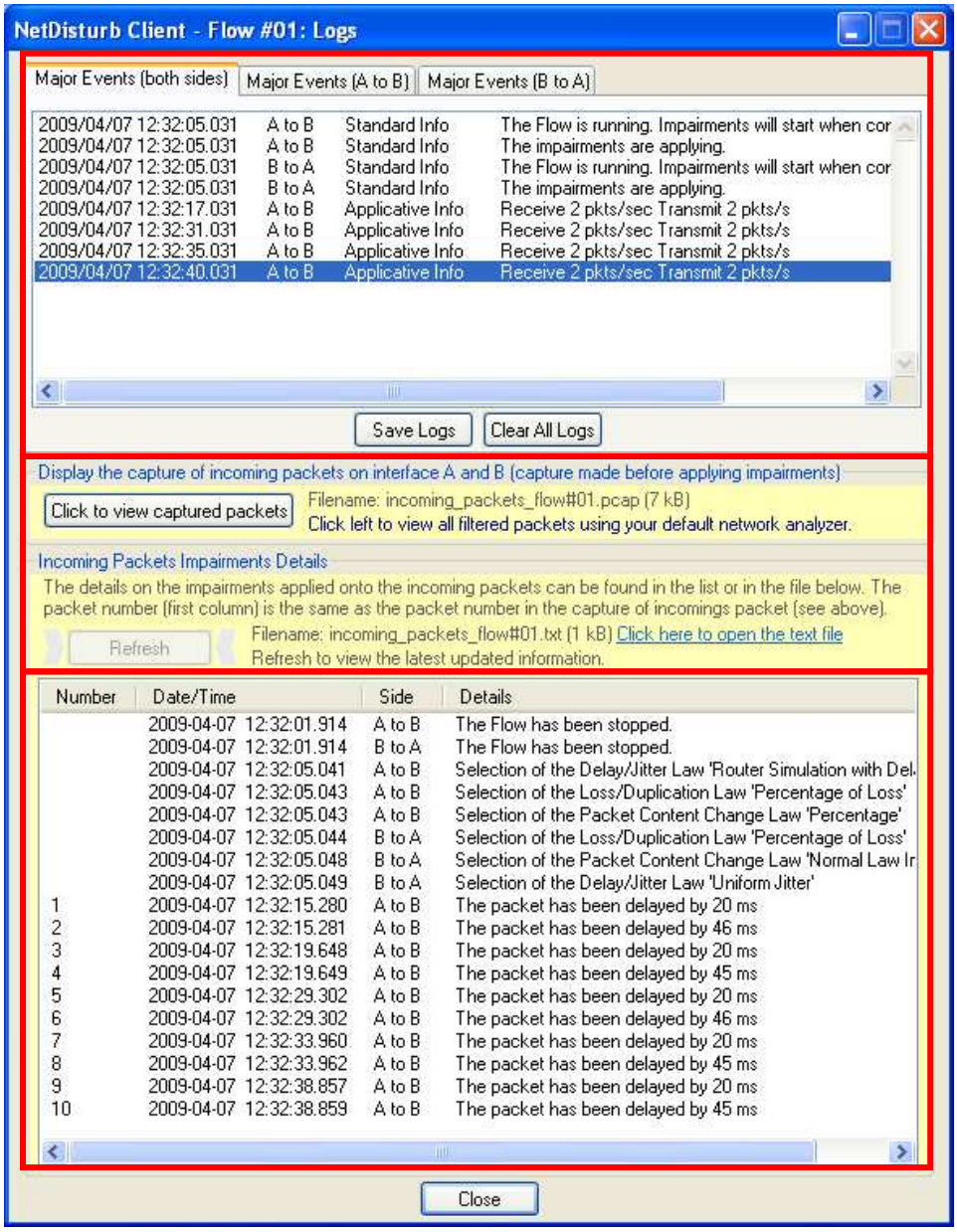
NetDisturb Enhanced Edition starts to generate flow logs into the 2 files as soon as the Flow is started. The files are located in the **Client** subdirectory where **NetDisturb** has been installed (e.g. C:\Program Files\NetDisturb\Client). Previous content of the files is lost.

As soon as you start the Flow where the content of the files that got the previous log activity for this flow is lost.
When you are intended to keep the content of a previous log activity, you should make a copy of those files before to run the flow.

The files are created in a way that you may open them for reading while **NetDisturb Enhanced Edition** continues to fill them.

7.8.4 The individual flow logs windows

The Flow log window is divided in 3 parts:

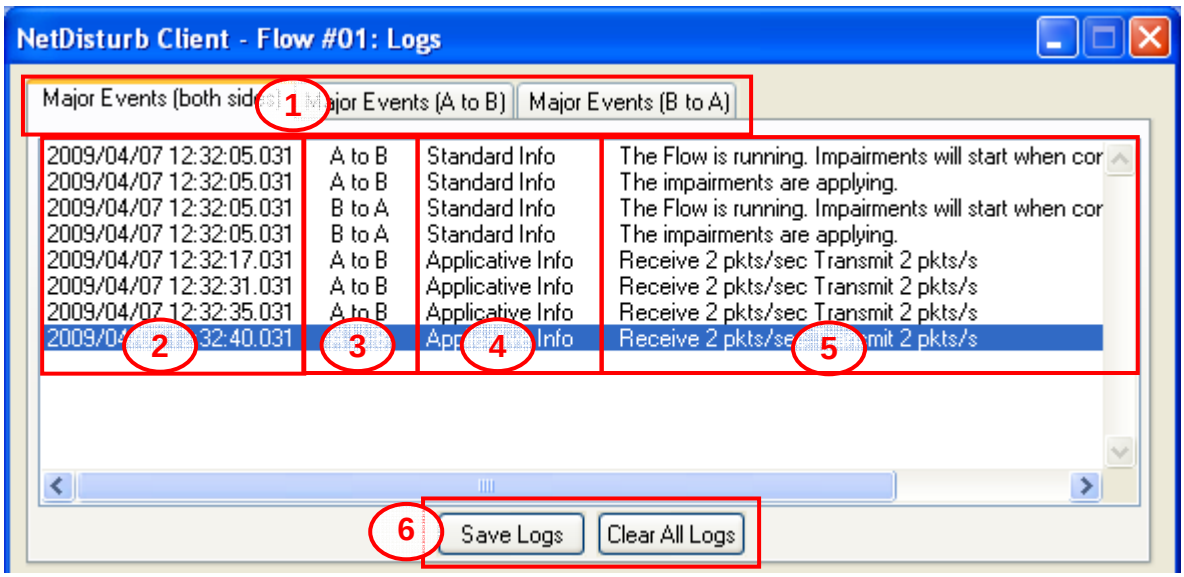


1. The part 1 keeps track of the major events that applied to the flow, either both directions mixed together or direction per direction. The tab allows selecting the direction.
2. The part 2 provides information about the capture activity. It shows the name of the files generated and their current size. A button helps to launch he associated software viewer of the Ethereal file formatted log. Another button refreshes the content of the part 3. An active area launches the text viewer.
3. The part 3 lists the detailed information related to the flow. Detailed information may be a NetDisturb management event such as a change in the law selection, or the impairment to a packet. Each detailed information get a UTC timestamp.
4. The Close button hides definitively the Flow Logs windows for the selected flow.

Once the Flow log window has been closed, there is no way to reopen it *without stopping then restarting the flow.*
However, the log files continue to be updated with the packets captured and the impairment details until the flow is stopped.

7.8.4.1 Major Events

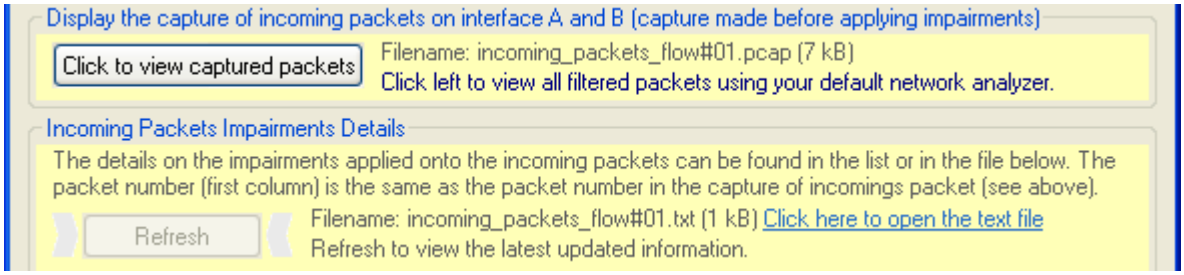
The Major Event area may be split into 6 sub-areas, as shown in the figure below.



1. The area 1 is the tab that helps selecting the direction of events (Both directions, A -> B or B-> A)
2. The first column indicates the date and the time of the event, where the time reference is UTC. The events are ordered using the time they occurred.
3. The second column is the direction where the event occurred.
4. The Third column contains the origin of the event.
   - Standard info means the message has been generated by the **NetDisturb Driver** component.
   - Applicative info means the message has been generated by the **NetDisturb Client** component.
5. The fourth column is the event description, where the list of events is:
   - Flow is running
   - Impairments are applying
   - Receive and Transmit statistics (in packets per second unit)
   - RTP or RTCP flow detection with and detailed information
   - FTP Data start and stop with and detailed information
6. The last sub-area contains 2 buttons, to :
   - Save the content of the Major event area in a text file
   - Clear the content of the Major event area

7.8.4.2 Capture activity

The capture activity area informs about the name and the size of the files where the logs are saved in, and give access to the files content using to the relevant default viewer.



The files are located in the Client subdirectory e.g. **C:\Program Files\NetDisturb\Client**.

The radix for the name of the files is **incoming_packets_flow#*XX*** where ***XX*** is the number of the flow i.e. 01 to 16 for the flow with filter, and 17 for the 'Other Flows' flow.

The suffix is **pcap** when the file contains the packets captured; it is an Ethereal format file.
The suffix is **txt** when the file contains impairment details (see paragraph 7.8.4.4 for more information about the structure of this file).

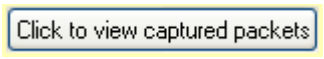
> Example: **incoming_packets_flow#04.pcap** contains the both directions packets captured that were matching the filters for the Flow #04.

The size of each file is indicated in kilobytes: you should take care to the file size when refreshing the details list (see paragraph 7.8.4.4) or when opening the Ethereal format file because a high length may be CPU consuming.

7.8.4.3 Capture activity buttons

There are 2 buttons and one active area in the capture activity that helps to get details about the current impairment.

Button related to the pcap file



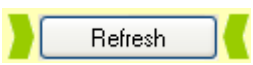
The **Click to view captured packets** button open the pcap file using your default network analyzer.

There should be a shell association between the pcap files and the viewer to display the content of such files. The association is generally done at software installation: Wireshark does it automatically for example.

*To check the association, open **Windows Explorer**, menu **Tools/Folder options…** and look for the pcap Extension in the **Files type** tab.*

Button related to the Impairment details file

The refresh button indicates that new information are available in the Impairment details file i.e. **incoming_packets_flow#*XX*.txt**.



The **Refresh** button is active and the arrows are green when the list of impairment details (see paragraph 7.8.4.4) needs an update to be in line with the latest impairments and events that occurred.

The **Refresh** button is grayed when the list of impairment details is up-to-date.

Notice that the update of the list of Impairment details may take time because all the list is refreshed. We don't recommend the refresh this list when the size of the file exceeds 1 Mbytes.

Active area to open the Impairment details file

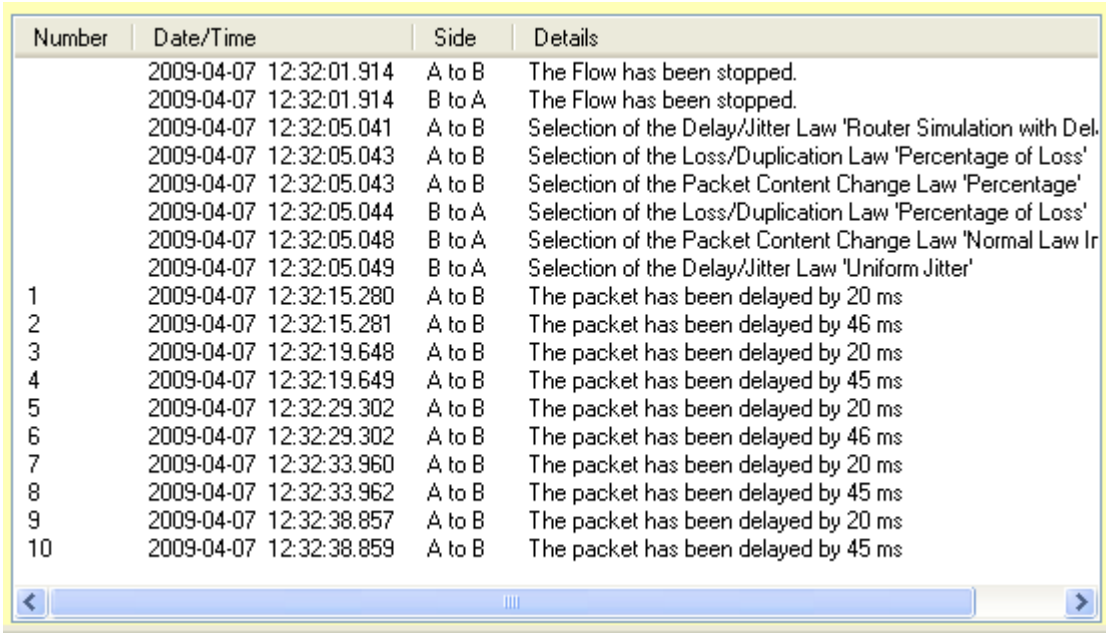
There is a way to open the Impairment details file using your default text editor software, by clicking the active area in blue, at the right side to the file name.

There should be a shell association between the txt files and the text editor software to display the content of this file. In general, the default association software is notepad.

*To check the association, open **Windows Explorer**, menu **Tools/Folder options…** and look for the **txt** Extension in the **Files type** tab.*

7.8.4.4 Impairment Details List

The impairment details list contains the events related to the flow and the impairments that have applied to each packet. Both directions are included in the list.



Number	Date/Time	Side	Details
	2009-04-07 12:32:01.914	A to B	The Flow has been stopped.
	2009-04-07 12:32:01.914	B to A	The Flow has been stopped.
	2009-04-07 12:32:05.041	A to B	Selection of the Delay/Jitter Law 'Router Simulation with Del
	2009-04-07 12:32:05.043	A to B	Selection of the Loss/Duplication Law 'Percentage of Loss'
	2009-04-07 12:32:05.043	A to B	Selection of the Packet Content Change Law 'Percentage'
	2009-04-07 12:32:05.044	B to A	Selection of the Loss/Duplication Law 'Percentage of Loss'
	2009-04-07 12:32:05.048	B to A	Selection of the Packet Content Change Law 'Normal Law Ir
	2009-04-07 12:32:05.049	B to A	Selection of the Delay/Jitter Law 'Uniform Jitter'
1	2009-04-07 12:32:15.280	A to B	The packet has been delayed by 20 ms
2	2009-04-07 12:32:15.281	A to B	The packet has been delayed by 46 ms
3	2009-04-07 12:32:19.648	A to B	The packet has been delayed by 20 ms
4	2009-04-07 12:32:19.649	A to B	The packet has been delayed by 45 ms
5	2009-04-07 12:32:29.302	A to B	The packet has been delayed by 20 ms
6	2009-04-07 12:32:29.302	A to B	The packet has been delayed by 46 ms
7	2009-04-07 12:32:33.960	A to B	The packet has been delayed by 20 ms
8	2009-04-07 12:32:33.962	A to B	The packet has been delayed by 45 ms
9	2009-04-07 12:32:38.857	A to B	The packet has been delayed by 20 ms
10	2009-04-07 12:32:38.859	A to B	The packet has been delayed by 45 ms

The details are ordered in time. There are 4 columns in the list of Impairment details:

Number: The Number column contains the packet number. The packet number is the same as the packet number in the associated pcap file. When the packet number is missing, the Details information doesn't refer to a packet but to an event related to this flow (such as change of a law or the dynamic connection start or stop).

Date/Time: The Date/Time column contains the timestamp when Details happens, including the millisecond (format is YYYY-MM-DD HH:MM:SS.ms). When the Date/Time is missing, the Details refer to the previous packet and the previous Date/Time should be assumed for this Details.

Side: The Side column contains the direction relevant to the Details (A -> B or B -> A). When the Side is missing, the Details refer to the previous packet and the previous Side should be assumed.

Details: The Details column contains the information. It couldn't be empty. The information may be one of the following:

- Flow Stopped
- Selection of the Loss/Duplication law followed with the law name
- Selection of the Delay/Jitter law followed with the law name
- Selection of the Packet content law followed with the law name
- Packet has been delayed followed with the delay value (in millisecond)
- Packet has been lost
- Packet has been delayed followed with the delay value (in millisecond)
- Packet content has been changed followed with the change details
- Found RTP/RTCP Flow followed with the IP address and port
- Found FTP Data Flow followed with the IP address and port
- Release FTP Data Flow followed with the IP address and port

The Impairment details file format

The file **incoming_packets_flow#*XX*.txt** contains all the information presented in the list of Impairment details. The format for each line of this text file is the following:

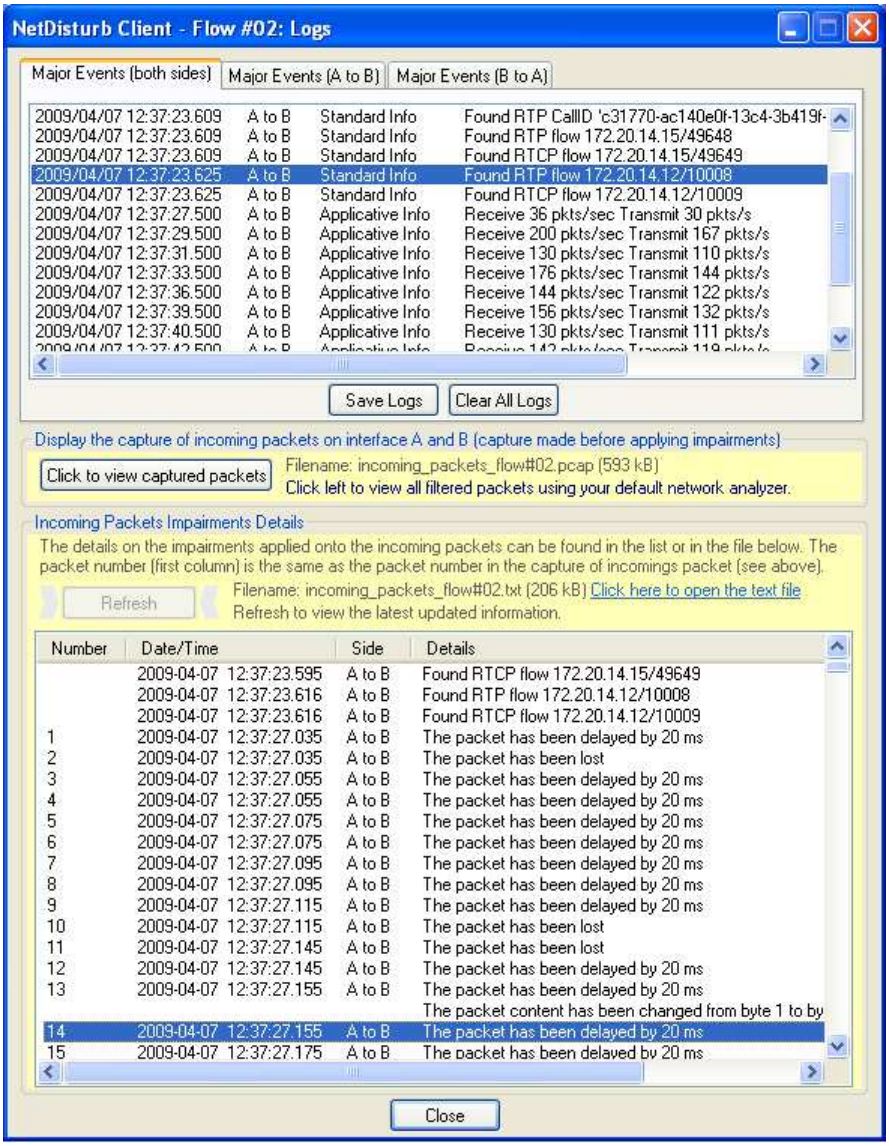
<Packet number> or empty <tab> <Date-time> or empty <tab> <direction> or empty <tab> <Detailed information> CR LF

Notes:

- *The packet number is empty when the line refers to an event that occurs for this flow. This is the only case when the packet number is only missing information i.e. the date-time is there.*
- *The packet number, the Date-time and the Direction are empty when the detailed information refers to the previous packet. This information should be taken from the previous line.*

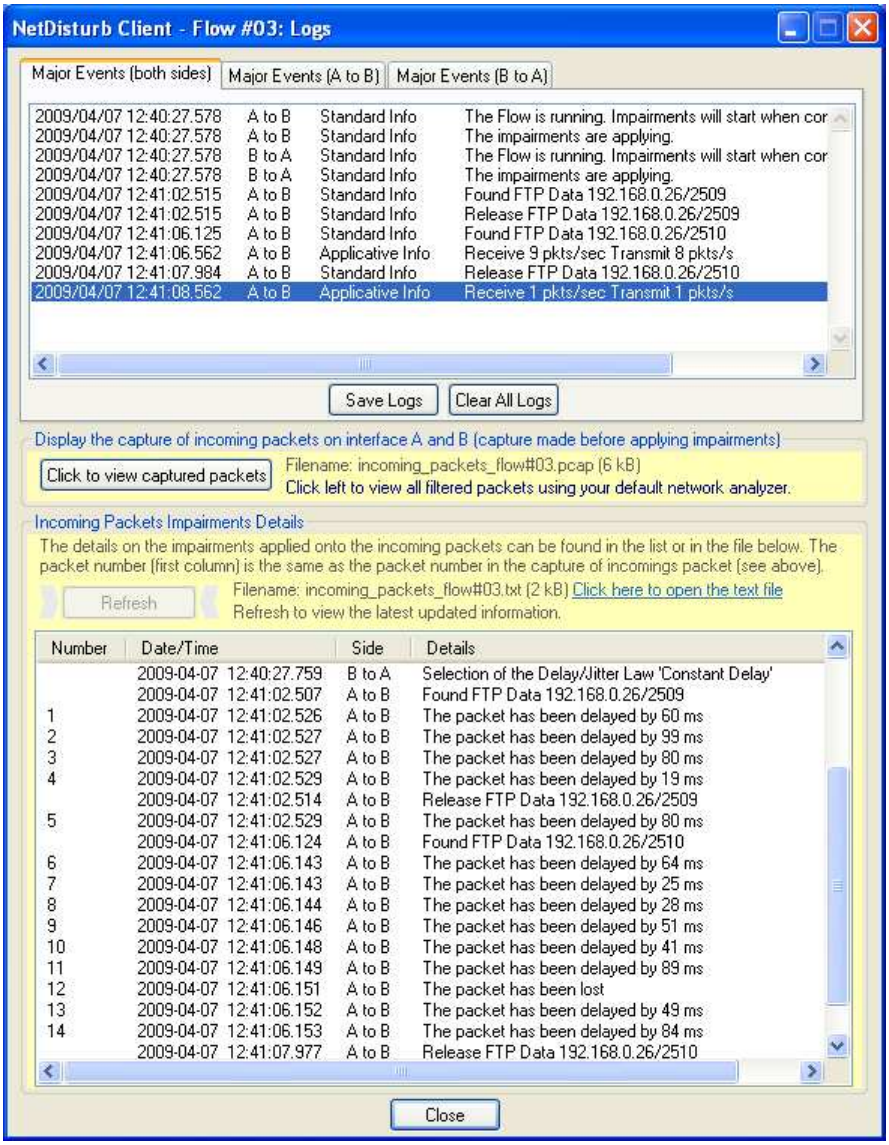
Flow log details with RTP flows

The next figure presents the Flow log windows when a RTP filter has been defined.



Flow log details with FTP Data flows

The next figure presents the Flow log windows when a FTP Data filter has been defined.



Part 8 Using the NetDisturb Command Line Interface

NetDisturb is offering a Command Line Interface (CLI) allowing the integration of **NetDisturb** in test beds which are controlled through batch processes. **NetDisturbCLI.exe** software, located in the **NetDisturb** Client directory, provides the Command Line Interface feature.

With the Command Line Interface, you can load a context, start and/or stop the Flows, manage the statistics and shutdown NetDisturb.

8.1 General rules

8.1.1 Command Line Interface's Execution

The Command Line Interface can be run from any location, from ***Command Prompt*** or from a batch file.

8.1.2 How to use the Command Line Interface

Each command line is made as follows: NetDisturbCLI /(Action) [Parameters]

Each command is prefixed using a '/'.

Both **–** or ***/*** can be used as prefix.

One or more commands can be sent at a time as shown hereafter:

NetDisturbCLI /Start 10 /Stop 9

(see paragraph 8.3 for more details about the priority between commands)

8.1.3 Options

Some commands may require a parameter. For example **NetDisturbCLI /Start 10** will ***start*** the Flow ***#10,*** where ***10*** is the mandatory parameter of the command ***Start***.

When the parameter is a file, the file name path may be absolute or relative. You should take into account that the relative path must refer to the NetDisturb Client directory.

If the file name or the path is including spaces, don't forget to use quotes i.e. **"C:\Program Files\NetDisturb\Client\Default.wsx"**

8.2 Commands and parameters

The commands with their parameters are displayed in priority order.
The result of the command is a text including a prefix word. It indicates the command execution result and is followed by an additional text. The 3 prefixes are the following:

OK: means the command was executed successfully
Warning: means the command was executed but was not necessary
Error: means the command was not executed successfully

The prefixes are subjected to change and could be extended in the next versions. These prefixes are referring to the version 1.0 of NetDisturbCLI.

8.2.1 Display the usage (/?)

Command: `NetDisturb /?`
Display the command list which describes each command and its parameters.

Result:

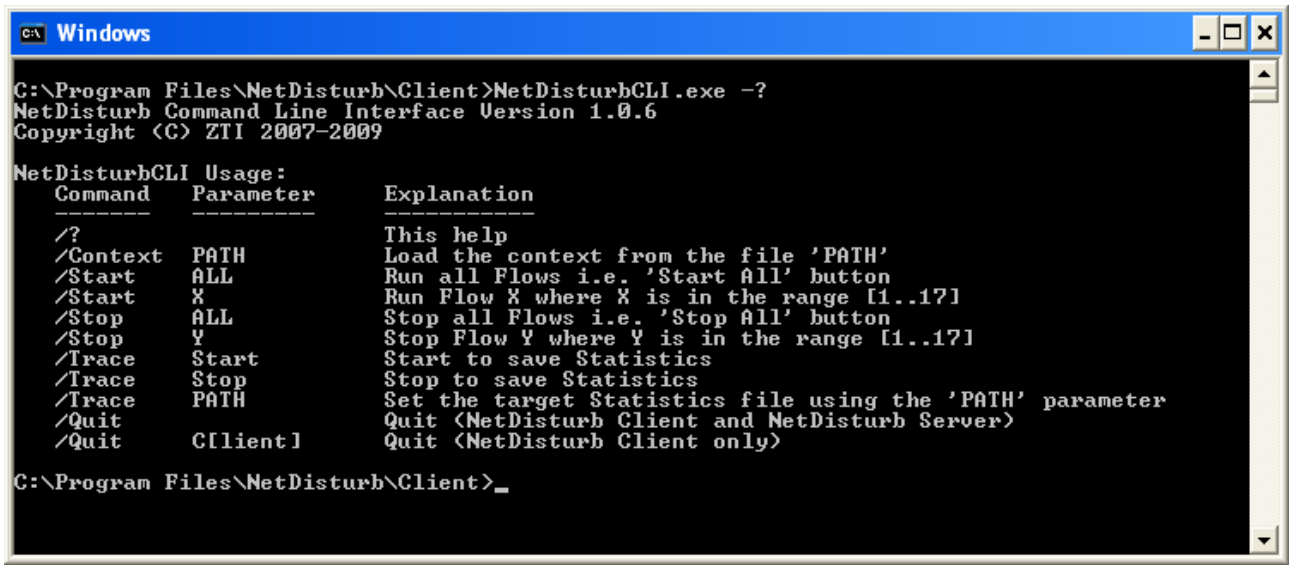


Figure 6 - Command Line Interface Help

Neither error message nor warning message can be displayed with this command.

8.2.2 Stop and shutdown NetDisturb Client and NetDisturb Server (/Quit)

Command: `NetDisturb /Quit`
Stop **NetDisturb Server** and **NetDisturb Client** then shutdown both applications.

Result:

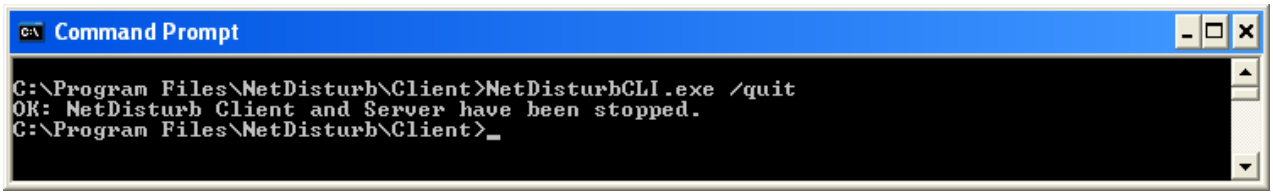


Figure 7 – Stop NetDisturb Server and NetDisturb Client, then shutdown both applications

Error message: None

Warning message: None

8.2.3 Stop and shutdown NetDisturb Client only (/Quit Client)

Command: `NetDisturb /Quit Client`
Stop and shutdown **NetDisturb Client**.

Result:

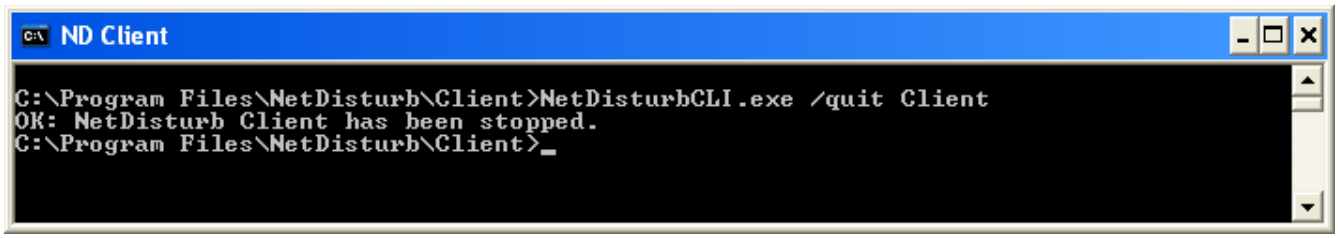


Figure 8 – Stop and shutdown NetDisturb Client

Error message: None

Warning message: None

8.2.4 Open and Start NetDisturb Server (/Run)

Command: `NetDisturb /run`
Open and start **NetDisturb Server**.

Result:

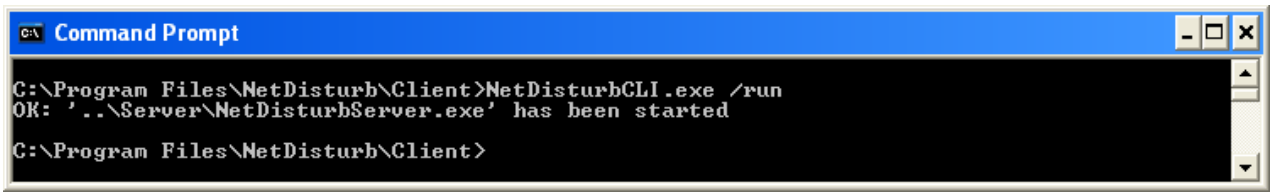


Figure 9 – Open and start NetDisturb Server

Error message:

- Error: Can't create '..\Server\NetDisturbServer.exe': **Windows error message**
  The <**Windows error message**> gives the reason why **NetDisturb Server** did not start.

Warning message: None

8.2.5 Load the context file (/Context filename)

Command: `NetDisturb /context` *`filename`*
Load a **NetDisturb** context like in the menu File/Open of the **NetDisturb Client** GUI.

Result:

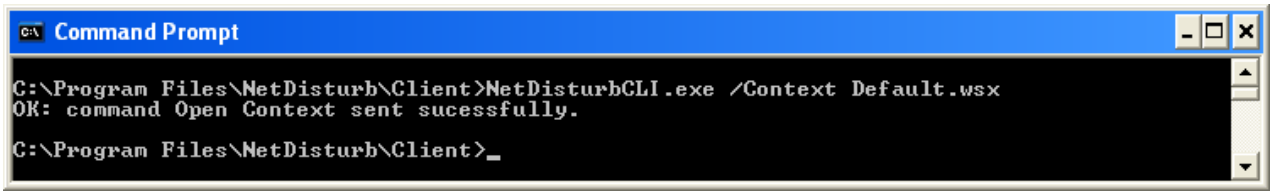


Figure 10 – Define the context file and load it

Note that any changes in the previous context will be lost.

Error messages:

- Error: No NetDisturb Client loaded. The command can't be sent.
  This message indicates that NetDisturb Client has not been started yet.
- Error: NetDisturb Client was unable to handle the context file 'filename'.
  This message indicates that NetDisturb Client was not able to handle the file. It may be due to an error in the file name or in the path.
- Error: At least one IP Flow is still running. Please stop all running Flows to be able to change the context.

Warning message: None

8.2.6 Set the file name where to store the statistics (/Trace filename)

Command: `NetDisturb /trace filename`
Define the file that will store the statistics generated by **NetDisturb Client** To start or stop the statistics saving process, please refer to paragraphs 8.2.7 and 8.2.8.

Result:

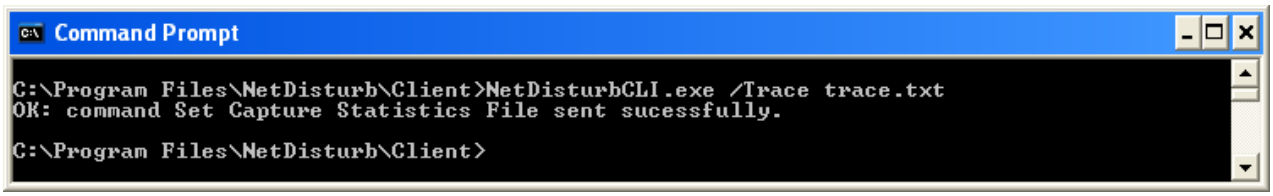


Figure 11 – Define the statistics file name

Error messages:

- Error: No NetDisturb Client loaded. The command can't be sent.
  This message indicates that NetDisturb Client has not been started yet.
- Error: NetDisturb Client is saving the statistics. The statistics file name can not be changed.
  This message indicates that NetDisturb Client was not able to set the statistics file name because the statistics saving process is still running. The saving process should be stopped before changing the file name.

Warning message: None

8.2.7 Start saving the statistics (/Trace start)

Command: `NetDisturb /trace start`
Send a request to **NetDisturb Client** to start saving statistics into a file.

Result:

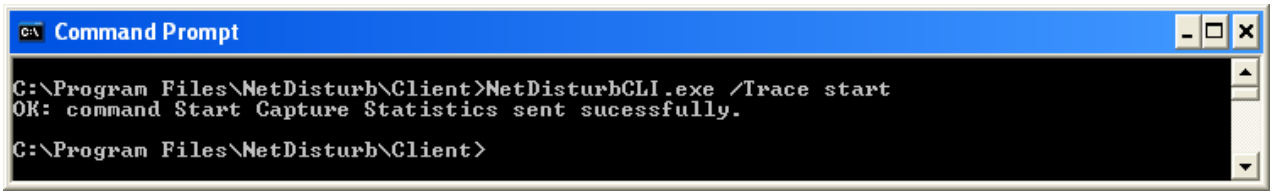


Figure 12 – Start saving the statistics into a file

Error messages:

- Error: No NetDisturb Client loaded. The command can't be sent.
  This message indicates that NetDisturb Client has not been started yet.

- Error: NetDisturb Client was not able to open the target statistics file.
  This message indicates that an error was encountered when opening the file that should store the statistics. The two main causes are: a wrong path was specified or the file is write-protected.

Warning message:

- Warning: NetDisturb Client is already saving the statistics.

8.2.8 Stop saving the statistics (/Trace stop)

Command: `NetDisturb /trace stop`
Send a request to **NetDisturb Client** to stop saving statistics into a file.

Result:

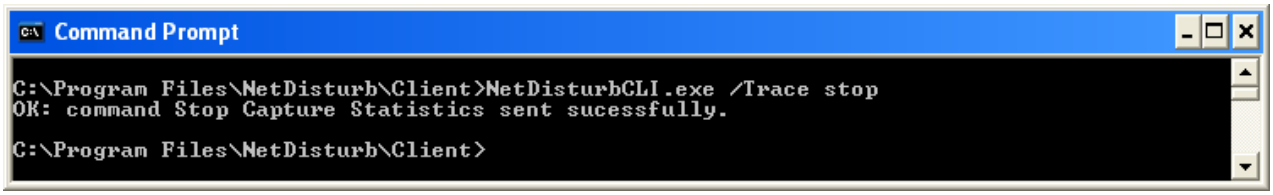


Figure 13 – Stop saving the statistics into a file

Error messages:

- Error: No NetDisturb Client loaded. The command can't be sent.
  This message indicates that NetDisturb Client has not been started yet.

Warning message:

- Warning: NetDisturb Client is not saving the statistics.

8.2.9 Stop a Flow (/Stop X)

Command: `NetDisturb /stop X`
Send a request to **NetDisturb Client** to stop the Flow X, where X should be a number in the range [1..17] (the value 17 corresponds to 'Other IP Flows'/'Other Frames' flow).

Result:

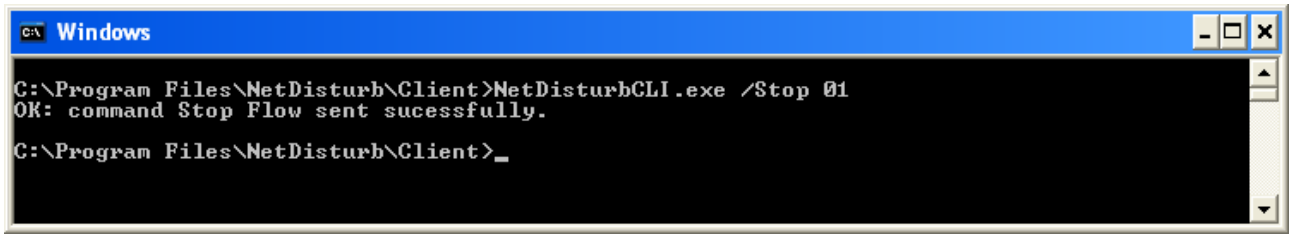


Figure 14 – Stop the Flow #01

Error messages:

- Error: No NetDisturb Client loaded. The command can't be sent.
  This message indicates that NetDisturb Client has not been started yet.
- Error: No Interface selected. The command can't be executed.
  The interfaces used by NetDisturb should be selected before stopping a Flow.
- Error: The Flow X is out of range. Allowed range: from 1 to 17 included.
  The Flow number must be in the range from 1 to 17.
- Error: NetDisturb Client was unable to stop the Flow X.
  More details should be available into the internal log file about the reason why NetDisturb Client couldn't stop the Flow.

Warning message:

- Warning: The Flow X is already stopped.
  The command doesn't change the status of the Flow because it was stopped.

8.2.10 Stop all Flows (/Stop all)

Command: `NetDisturb /stop all`
Send a request to **NetDisturb Client** to stop all Flows.

Result:

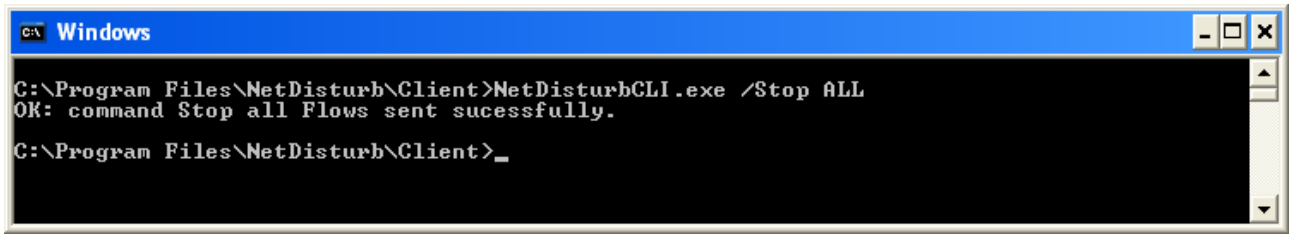


Figure 15 – Stop all IP Flows

Error messages:

- Error: No NetDisturb Client loaded. The command can't be sent.
  This message indicates that NetDisturb Client has not been started yet.
- Error: No Interface selected. The command can't be executed.
  The interfaces used by NetDisturb should be selected before stopping a Flow.

Warning message: None

8.2.11 Start a Flow (/Start X)

Command: `NetDisturb /start X`

Send a request to **NetDisturb Client** to run the Flow X, where X should be a number in the range [1..17] (the value 17 corresponds to 'Other IP Flows'/'Other Frames' flow).

Result:

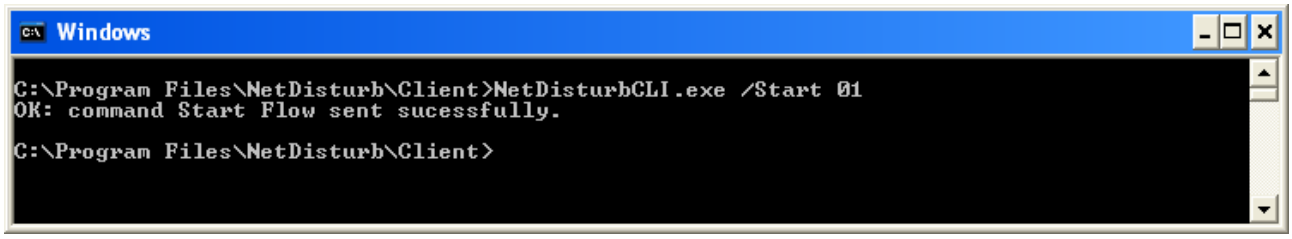


Figure 16 – Run the Flow #01

Error messages:

- Error: No NetDisturb Client loaded. The command can't be sent.
  This message indicates that NetDisturb Client has not been started yet.

- Error: No Interface selected. The command can't be executed.
  The interfaces used by NetDisturb should be selected before starting a Flow.

- Error: The Flow X has no filter defined.
  A filter should be selected before starting a Flow.

Warning message:

- Warning: The Flow X is already started.
  The command doesn't change the status of the Flow because it is running already.

8.2.12 Start all Flows (/Start all)

Command: `NetDisturb /start all`
Send a request to **NetDisturb Client** to start all Flows.

Result:

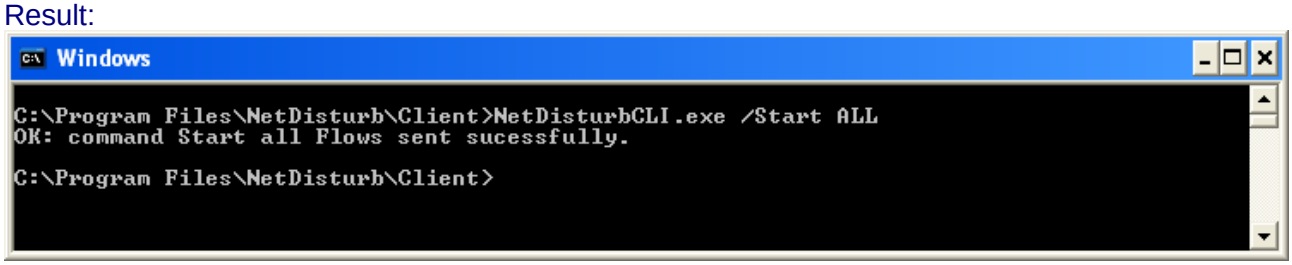


Figure 17 – Start all Flows

Error messages:

- Error: No NetDisturb Client loaded. The command can't be sent.
  This message indicates that NetDisturb Client has not been started yet.
- Error: No Interface selected. The command can't be executed.
  The interfaces used by NetDisturb should be selected before starting Flows.
- Error: The Flow X has no filter defined.
  A filter should be selected before starting a Flow.

Warning message: None

8.3 Commands execution order

When using multiple commands in the Command Line Interface, some high priority commands ignore the other commands sent (see Table 1 below).
Moreover priorities exist between each command: the Table 1 below is showing the execution order when multiple commands are sent.

Priority *(highest->lowest)*	Command	Ignore other commands
Highest ↓ Lowest	/?	**Yes**
	/Quit	**Yes**
	/Run	No
	/Context	No
	/Trace	No
	/Stop # or All	No
	/Start # or All	No

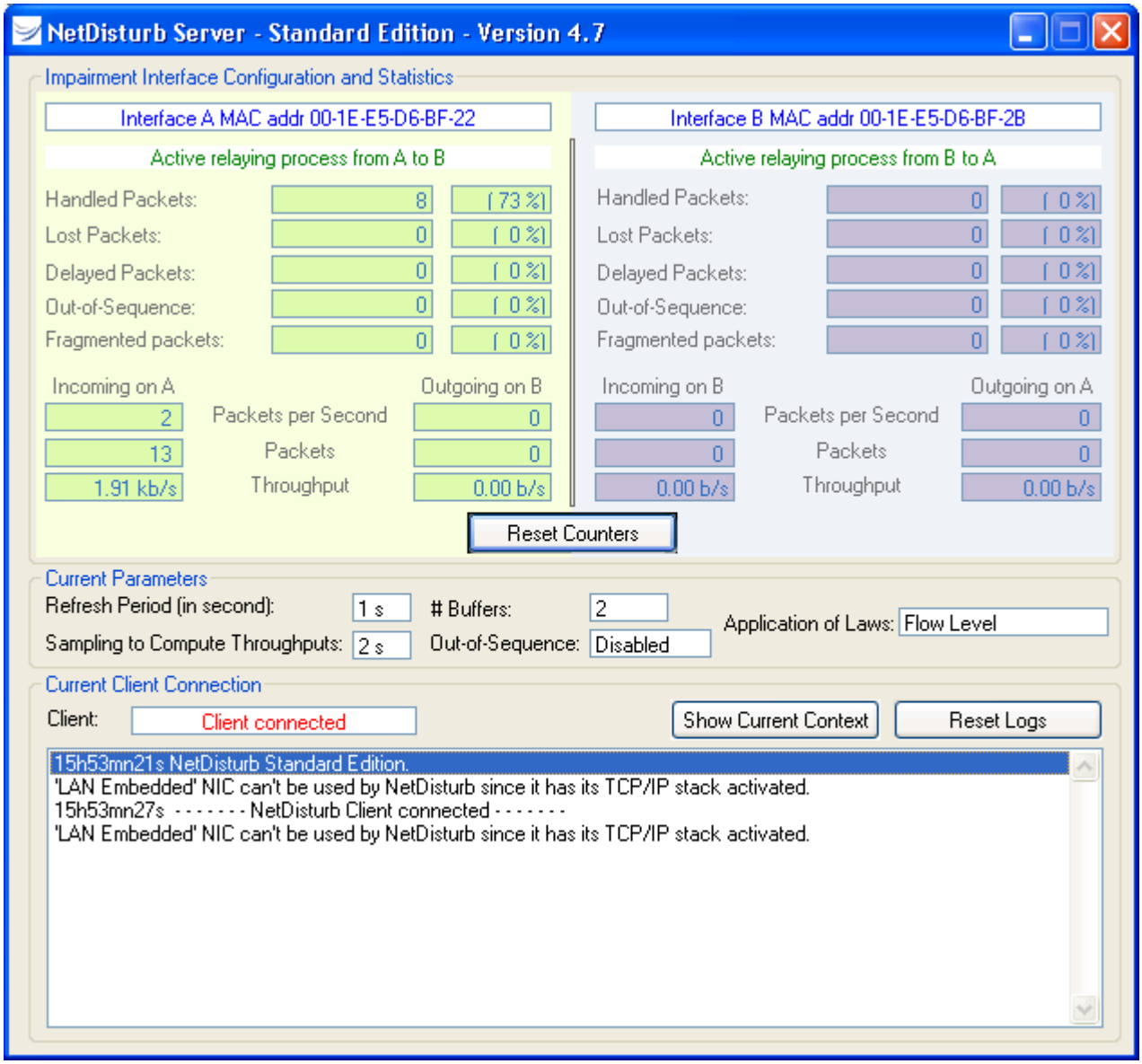
Table 1 - Commands execution order

Part 9 Using the NetDisturb Server

The **NetDisturb** Server links the **NetDisturb** driver and the **NetDisturb** Client. In addition, it performs the following tasks:

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

The **NetDisturb** Server window is composed of three sections:



⇨ Impairment Interface Configuration and Statistics

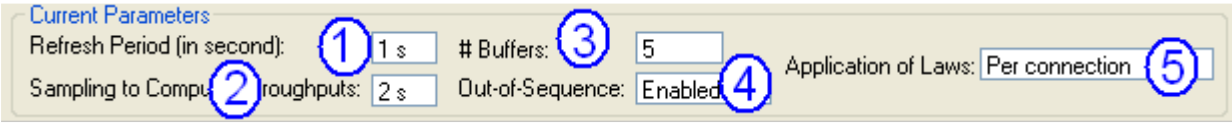
This section displays the used NICs. Statistics (percentages or absolute values) are associated to each impairment parameter: number of handled, lost, delayed, Out-of-Sequence and fragmented packets.
The # Fragmented Packets statistics shows the number of packets rejected by the **NetDisturb** driver because it can't handle IP packet with the fragment flag set.

This section displays also the numbers of incoming and outgoing packets, the number of packets per second and the throughput. The indication on the relaying process is presented as follows:

No packets handled (red color)	The **NetDisturb** driver doesn't handle any packet (physical cut off of the Ethernet link).
Active relaying process (green color)	The **NetDisturb** driver is running, the relayed packets are processed following the selected Filters and the defined impairment laws.

The **Reset Counters** button allows the reset of the **NetDisturb** Server Interface counters. This action has no incident for the **NetDisturb** Client. This button is available only when the driver is running.

⇨ Current Parameters



This section reminds the current configuration and includes:

(1) The refresh period to display statistics for the **NetDisturb** Server.
(2) The sampling period used to calculate the throughput displayed by the **NetDisturb** Server.
(3) The number of buffers for laws values related to TCP/UDP connections.
(4) The Out-of-Sequence i.e. out-of-order mode: Enabled or Disabled
(5) The method to apply the laws:
- 'Flow level' means Laws apply to the IP Flow
- or 'Per connections' means Laws apply to each TCP/UDP connection of the IP Flow

⇨ Current Client Connection

This section shows whether a client is currently connected, the opened context and the trace list.

In this section the following buttons can be pressed:

- **Show Context:** displays the content of the current context.
- **Reset Trace:** allows clearing the traces displayed in the window bottom part.

Part 10 Appendices

10.1 The New Context Values

• Refreshing time for statistics display	1s
• Sampling period for throughput computing	2s
• Relaying process	Relaying packets without operations on both interfaces
• Working Mode	Enable Out-of-Sequence Packets Laws apply to the IP Flow
• Traces	Active
• Driver relaying status	Not active
• Buffer number	2
• Flow mode	Mono-flow
• For the 16 definable flows	
Filter	*Not defined*
Loss & Duplication law	*Not defined*
Delay & Jitter law	*Not defined*
Content Impairment law	*Not defined*
• Other IP Flows	
Loss & Duplication law	*Not defined*
Delay & Jitter law	*Not defined*
Content Impairment law	*Not defined*

10.2 The NetDisturb Registry Values

*This paragraph describes the Registry parameters for the **NetDisturb** Client, **NetDisturb** Server and **NetDisturb** driver.*
*You should be careful when changing in one of these values because inappropriate value may render **NetDisturb** unusable. We recommend to backup the Registry before or at least to save the key's values before any change.*

You need administrator rights access to change the Registry database. The system 'regedit.exe' program can be used to check and modify the Registry. A name, a type and a value identify each parameter in the Registry. The parameters are located in 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.

10.2.1 The Registry parameters related to the NetDisturb Client

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

10.2.1.1 Parameters Configuration

Key = HKEY_LOCAL_MACHINE\SOFTWARE\ZTI\NetDisturbClient

Name	Type	Value
AcroReadInfo	REG_SZ	Date of the help file (**the user should not change it)**
AcroReadTimer	REG_DWORD	Internal timeout related to the Adobe Reader®
ExchangeTimeout	REG_DWORD	Internal timeout related to the **NetDisturb** Client to **NetDisturb** Server dialog (default is 5000 ms)
Help_Menu	REG_DWORD	Index in the help file (**the user should not change it)**
IPAddress	REG_SZ	**NetDisturb** Server IP Address (default: 127.0.0.1)
PortNumber	REG_SZ	HTTP port number used to dialog with the **NetDisturb** Server part (default: 8080)
ServerPath	REG_SZ	Location of the **NetDisturb** Server software (default: C:\Program Files\NetDisturb\Server)
TraceLevel	REG_DWORD	Trace level generated by the Client (see note) (default: 0)
TraceFileName	REG_SZ	File name where traces are saved in when the TraceLevel flag is saved. (default: empty)

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 [using the WIN32 API *OutputDebugString()*].
- Flag values are shown in **hexadecimal**:
  - `0001` Errors level
  - `0002` Information level
  - `0008` Verbose level
  - `0010` Time: add timestamp information
  - `0100` File: traces are saved in a file too (the TraceFileName entry is used)
  - `1000` SOAP: add the SOAP trace information

  Example: If TraceLevel = 113 means Error and Information level of traces are saved also in a file and including the timestamp for each trace.

10.2.1.2 The Most Recent File list

This list is for information only.

It is handled by the system and you must 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

10.2.2 The Registry parameters related to the NetDisturb Server

Key = HKEY_LOCAL_MACHINE\SOFTWARE\ZTI\NetDisturbServer

Name	Type	Value
ApplicationName	REG_SZ	Trace viewer (Default: notepad.exe)
IHMRefresh	REG_DWORD	Period of refresh, in second. (default is 1)
Interface A	REG_SZ	MAC address of the latest selected Interface A
Interface B	REG_SZ	MAC address of the latest selected Interface B
Sampling	REG_DWORD	Sampling period to compute throughput (default: 2)
PortNumber	REG_SZ	HTTP port number used to dialog with the Client part (default: 8080)
TraceLevel	REG_DWORD	Trace level generated by **NetDisturb** Server (see note) (default: 0)
TraceFileName	REG_SZ	File name where traces are saved in when the TraceLevel flag is saved. (default: empty)
Note: See the note of the Registry parameters related to the NetDisturb Client here above.		

10.2.3 The Registry parameters related to the NetDisturb driver

Key = HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetDisturb

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

10.2.4 The NetDisturb Driver Traces

There is another key related to the level of traces generated by the **NetDisturb** driver. These traces can be captured via a tool such as ***DebugMon*** from OSR Inc. (www.osronline.com -> go to the *Download* section) or ***DebugView*** from Microsoft (http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx).

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

Key = HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetDisturb\Parameters

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

10.3 The Mathematical Laws used by NetDisturb

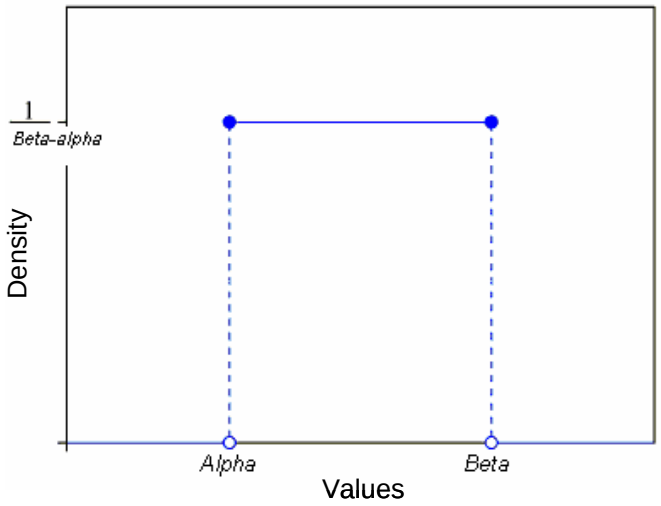
10.3.1 Uniform law

Distribution of Uniform Law is:

$$f(x) = \frac{1}{Beta - Alpha} \qquad for \quad Alpha < x < Beta$$

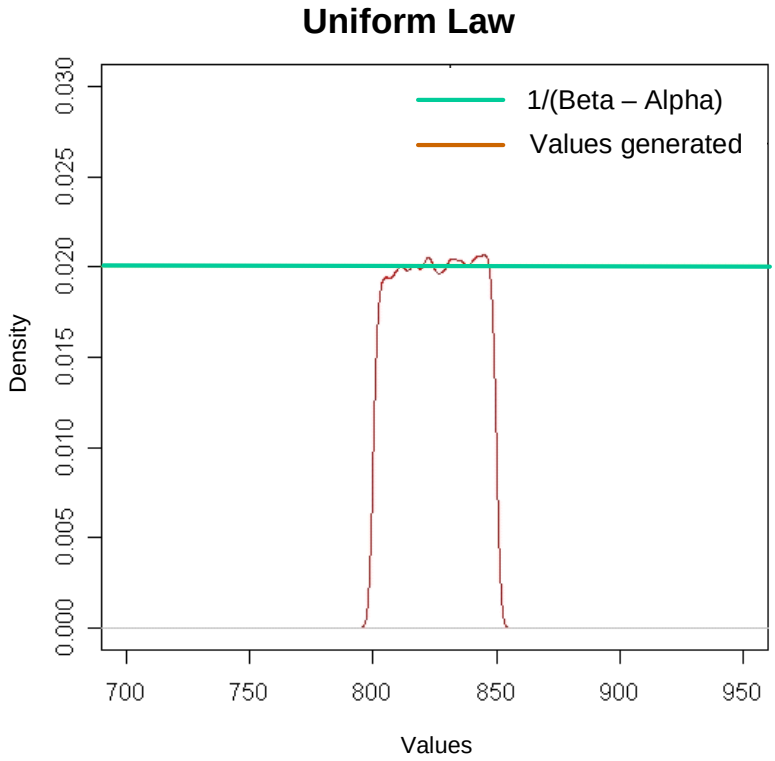
$$f(x) = 0 \qquad for \quad x < Alpha \quad or \quad x > Beta$$

where *Alpha* is the inferior parameter and *Beta* the superior one.



Values between *Alpha* and *Beta* have the same probability to be drawn = 1 / (*Beta* – *Alpha*). When this law is used, the unit is the millisecond for the starting time of a connection or byte for the data volume to send.

Example of values generated by NetDisturb in the interval [800, 850]



*Density of probability for the values generated by **NetDisturb***

10.3.2 The 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).

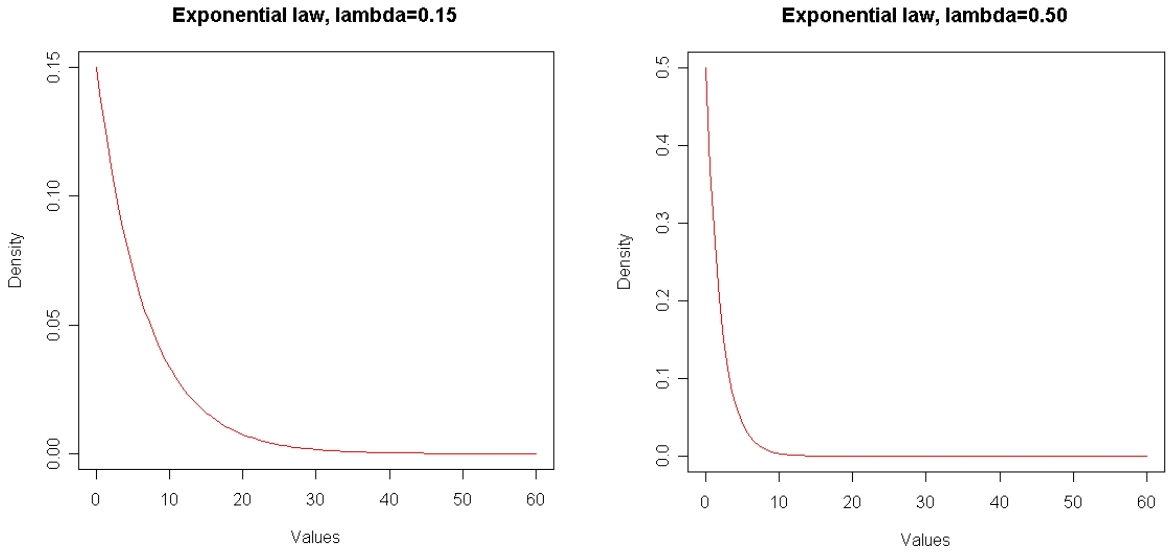
10.3.3 Exponential law

10.3.3.1 Theory

The probability density function of the exponential law is:

$$f(x;\lambda) = \begin{cases} \lambda e^{-\lambda x} & , x \geq 0, \\ 0 & , x < 0. \end{cases}$$

where $\lambda > 0$ is the parameter of the distribution (*the rate parameter*).



The graphs above represent the theoretical density of the exponential distribution with λ=0.15 and λ=0.50.

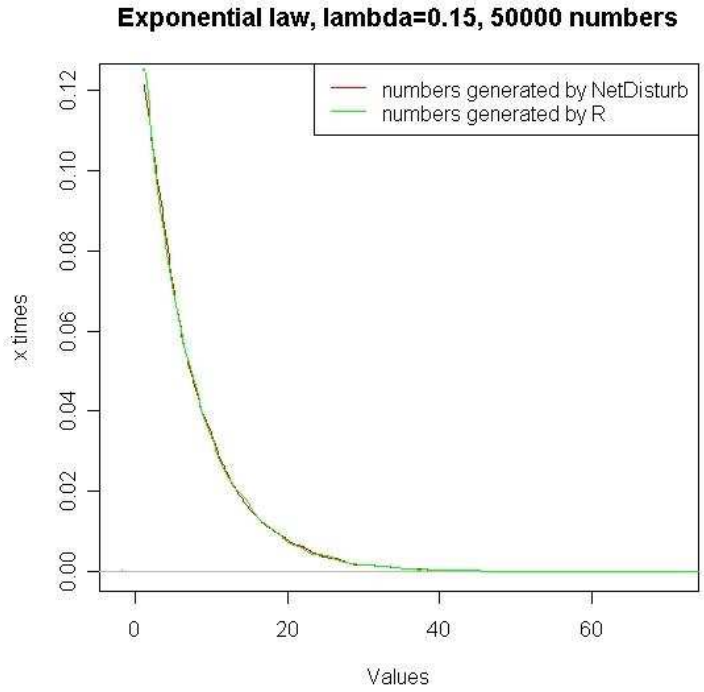
When we use the exponential distribution to draw random numbers, most the drawn values are theoretically small and the probability to draw big numbers is smaller.

As a result of the increase of λ, the incline of the distributions curve increases. Therefore the probability to draw small numbers is bigger than the one to draw big numbers.

10.3.3.2 Practice

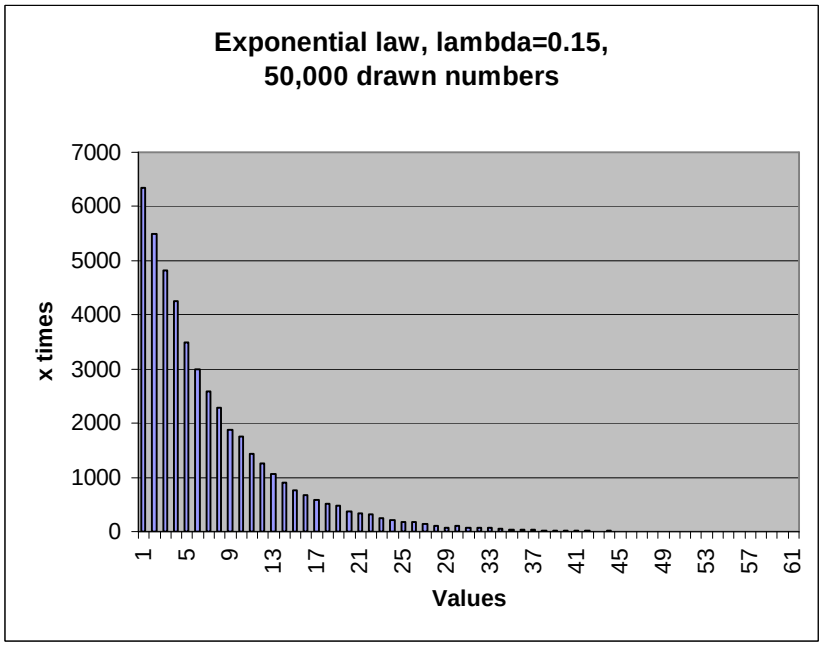
The exponential function is implemented in ***NetDisturb*** to generate numbers following an exponential distribution.
When this law is used, the unit is the millisecond for the starting time of a connection or byte for the data volume to send.

Using this function with λ=0.15 as a parameter, we drew such numbers and then we plotted, by using a mathematical tool (*R* software), the distribution of those. Then we got the following graph.

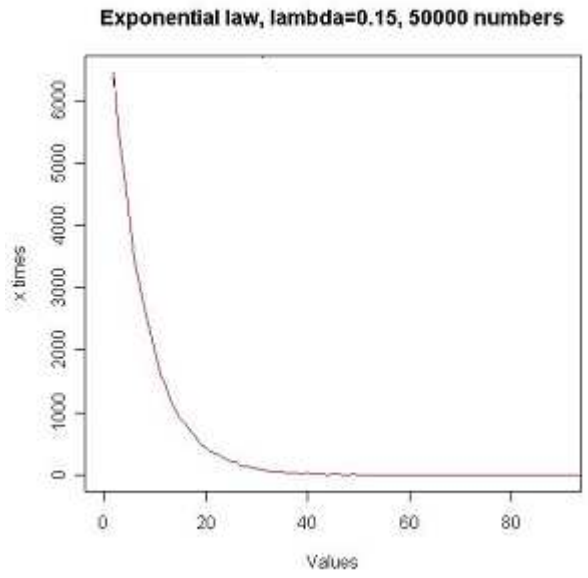


The green curve represents the distribution of random numbers generated by R and the red one represents the distribution of those generated by ***NetDisturb***. They are very similar.
As shown in the theoretical part, the probability to have small numbers is much bigger than the probability to have big ones.

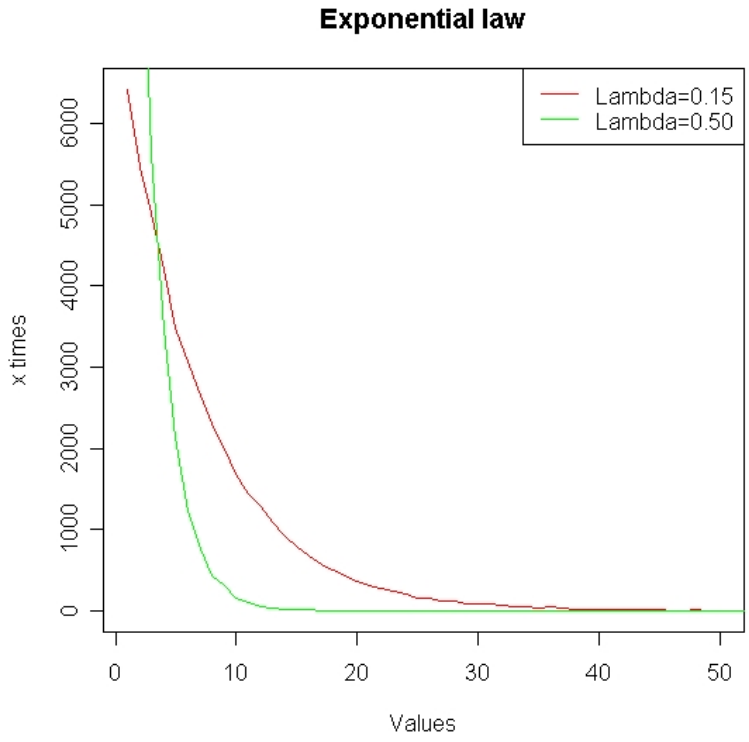
For example, we generate 50000 numbers following the exponential law with λ=0.15. As the numbers generated by the exponential function are of type “double”, we round them up to the nearest integer (e.g. 10.3 rounded up to 10 and 12.8 to 13). The histogram below summarizes the results.



The generated values are on the abscissa axis, and how many times each value is generated on the ordinate axis.
The same results may be displayed by a curve as shown in the next figure below:



In order to see the effect of the parameter λ we repeat the same operation as before with λ=0.15 and λ=0.50 and we plot both curves:



As the legend shows, the red curve represents the result of using the exponential law with λ=0.15 as parameter, and the green one the result of using the same law with λ=0.50. We observe that the more the parameter λ is big, the more the maximum number generated is small and the other numbers generated are smaller too.

The table below summarizes the probability (in percent) to draw a value using the exponential function of ***NetDisturb*** with different values for λ in {0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1}.

~ Actually generated values	λ									
	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
0	4.946	9.358	14.126	18.294	22.334	25.850	29.722	33.220	36.050	36.050
1	8.956	16.044	22.426	26.874	30.432	33.538	35.274	36.732	37.956	37.956
2	8.200	13.368	16.178	17.974	18.654	18.488	17.546	16.548	15.364	15.364
3	7.394	10.904	12.478	12.324	11.476	9.908	8.934	7.468	6.308	6.308
4	6.524	9.148	9.048	8.176	6.790	5.580	4.280	3.334	2.574	2.574
5	6.198	7.432	6.468	5.314	4.078	3.028	2.134	1.498	1.056	1.056
6	5.556	6.136	4.848	3.680	2.496	1.642	1.070	0.636	0.408	0.408
7	5.034	4.998	3.718	2.466	1.554	0.868	0.504	0.306	0.166	0.166
8	4.512	4.130	2.766	1.622	0.838	0.502	0.252	0.148	0.058	0.058
9	4.084	3.312	2.074	1.050	0.470	0.272	0.142	0.052	0.042	0.042
10	3.698	2.778	1.484	0.810	0.322	0.174	0.068	0.032	0.008	0.008
11	3.306	2.266	1.146	0.418	0.208	0.054	0.040	0.010	0.004	0.004
12	2.964	1.812	0.822	0.346	0.144	0.034	0.022	0.010	0.006	0.006
13	2.832	1.542	0.600	0.236	0.078	0.036	0.008	0.006	0	0
14	2.584	1.252	0.484	0.124	0.056	0.012	0	0	0	0
15	2.078	0.976	0.330	0.098	0.030	0.004	0.004	0	0	0
16	1.900	0.836	0.242	0.072	0.012	0.004	0	0	0	0
17	1.810	0.658	0.210	0.032	0.014	0.006	0	0	0	0
18	1.646	0.558	0.144	0.030	0.004	0	0	0	0	0
19	1.484	0.420	0.108	0.018	0.008	0	0	0	0	0
20	1.360	0.352	0.112	0.014	0	0	0	0	0	0
21	1.220	0.344	0.048	0.004	0.002	0	0	0	0	0
22	1.088	0.288	0.034	0.008	0	0	0	0	0	0
23	1.004	0.184	0.022	0.004	0	0	0	0	0	0
24	0.976	0.184	0.018	0.010	0	0	0	0	0	0
25	0.780	0.130	0.020	0	0	0	0	0	0	0
26	0.750	0.100	0.018	0.002	0	0	0	0	0	0
27	0.692	0.080	0.008	0	0	0	0	0	0	0
28	0.568	0.064	0.004	0	0	0	0	0	0	0
29	0.552	0.074	0.010	0	0	0	0	0	0	0
30	0.540	0.044	0.002	0	0	0	0	0	0	0
31	0.442	0.032	0	0	0	0	0	0	0	0
32	0.446	0.038	0.004	0	0	0	0	0	0	0
33	0.376	0.026	0	0	0	0	0	0	0	0
34	0.386	0.036	0	0	0	0	0	0	0	0
35	0.280	0.016	0	0	0	0	0	0	0	0
36	0.274	0.012	0	0	0	0	0	0	0	0
37	0.280	0.016	0	0	0	0	0	0	0	0
38	0.212	0.014	0	0	0	0	0	0	0	0
39	0.184	0.006	0	0	0	0	0	0	0	0
40	0.182	0.012	0	0	0	0	0	0	0	0
41	0.166	0	0	0	0	0	0	0	0	0
42	0.142	0.004	0	0	0	0	0	0	0	0
43	0.152	0.004	0	0	0	0	0	0	0	0
44	0.110	0.004	0	0	0	0	0	0	0	0
45	0.110	0.002	0	0	0	0	0	0	0	0
46	0.110	0.004	0	0	0	0	0	0	0	0
47	0.096	0	0	0	0	0	0	0	0	0
48	0.078	0	0	0	0	0	0	0	0	0
49	0.088	0.002	0	0	0	0	0	0	0	0

(continue)

50	0.072	0	0	0	0	0	0	0	0	0
51	0.060	0	0	0	0	0	0	0	0	0
52	0.060	0	0	0	0	0	0	0	0	0
53	0.048	0	0	0	0	0	0	0	0	0
54	0.034	0	0	0	0	0	0	0	0	0
55	0.036	0	0	0	0	0	0	0	0	0
56	0.022	0	0	0	0	0	0	0	0	0
57	0.044	0	0	0	0	0	0	0	0	0
58	0.018	0	0	0	0	0	0	0	0	0
59	0.018	0	0	0	0	0	0	0	0	0
60	0.030	0	0	0	0	0	0	0	0	0
61	0.016	0	0	0	0	0	0	0	0	0
62	0.008	0	0	0	0	0	0	0	0	0
63	0.016	0	0	0	0	0	0	0	0	0
64	0.018	0	0	0	0	0	0	0	0	0
65	0.010	0	0	0	0	0	0	0	0	0
66	0.014	0	0	0	0	0	0	0	0	0
67	0.014	0	0	0	0	0	0	0	0	0
68	0.014	0	0	0	0	0	0	0	0	0
69	0.018	0	0	0	0	0	0	0	0	0
70	0.014	0	0	0	0	0	0	0	0	0
71	0.010	0	0	0	0	0	0	0	0	0
72	0	0	0	0	0	0	0	0	0	0
73	0.004	0	0	0	0	0	0	0	0	0
74	0.006	0	0	0	0	0	0	0	0	0
75	0.002	0	0	0	0	0	0	0	0	0
76	0.004	0	0	0	0	0	0	0	0	0
77	0	0	0	0	0	0	0	0	0	0
78	0.008	0	0	0	0	0	0	0	0	0
79	0.008	0	0	0	0	0	0	0	0	0
80	0.006	0	0	0	0	0	0	0	0	0
81	0	0	0	0	0	0	0	0	0	0
82	0.002	0	0	0	0	0	0	0	0	0
83	0.004	0	0	0	0	0	0	0	0	0
84	0	0	0	0	0	0	0	0	0	0
85	0.002	0	0	0	0	0	0	0	0	0
86	0	0	0	0	0	0	0	0	0	0
87	0	0	0	0	0	0	0	0	0	0
88	0.002	0	0	0	0	0	0	0	0	0
89	0	0	0	0	0	0	0	0	0	0
90	0.004	0	0	0	0	0	0	0	0	0
91	0	0	0	0	0	0	0	0	0	0
92	0	0	0	0	0	0	0	0	0	0
93	0	0	0	0	0	0	0	0	0	0
94	0	0	0	0	0	0	0	0	0	0
95	0	0	0	0	0	0	0	0	0	0
96	0	0	0	0	0	0	0	0	0	0
97	0.002	0	0	0	0	0	0	0	0	0
98	0	0	0	0	0	0	0	0	0	0
99	0	0	0	0	0	0	0	0	0	0

(continue)

100	0	0	0	0	0	0	0	0	0	0
101	0	0	0	0	0	0	0	0	0	0
102	0	0	0	0	0	0	0	0	0	0
103	0	0	0	0	0	0	0	0	0	0
104	0.002	0	0	0	0	0	0	0	0	0
105	0	0	0	0	0	0	0	0	0	0

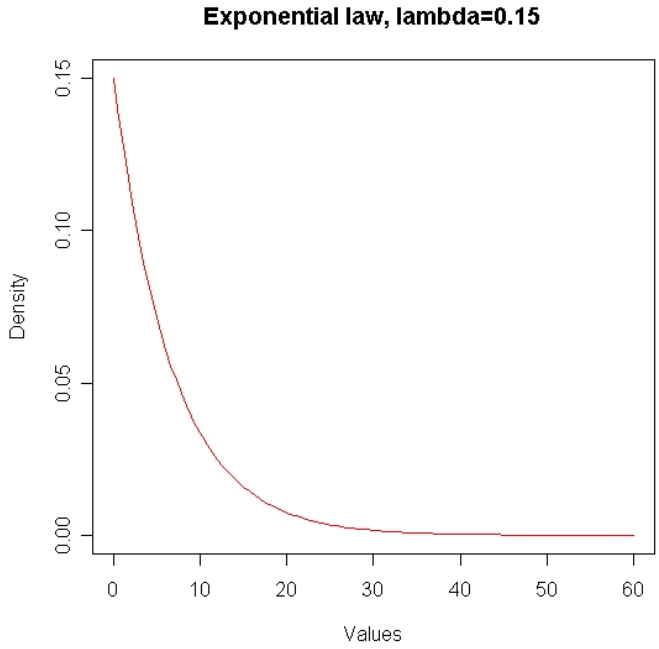
In fact, the generated values are of type double. Here is example of values generated by the exponential law of ***NetDisturb*** with λ =0.1:

0.227489
1.961810
1.217468
13.854097
0.474025
5.870118
2.353334
0.766254
4.868133
0.802894

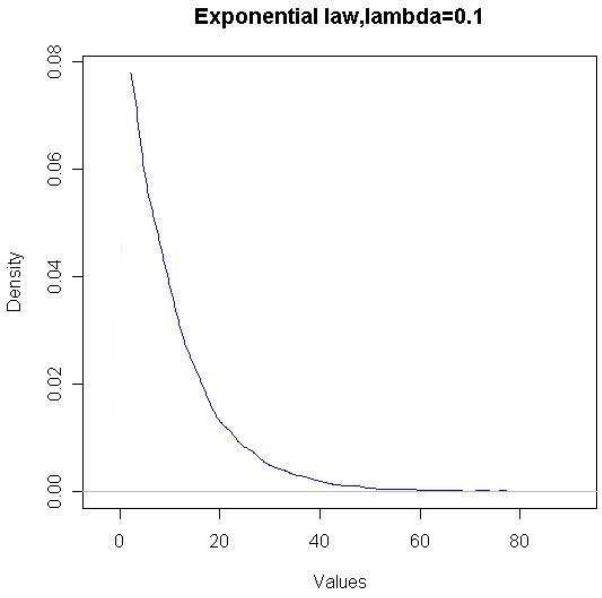
To represent those values in a simple way we round up double to the nearest integer, for example:

real values	represented values
0.227489	0
1.961810	2
1.217468	1
13.854097	14
0.474025	0
5.870118	6
2.353334	2
0.766254	1
4.868133	9
0.802894	1

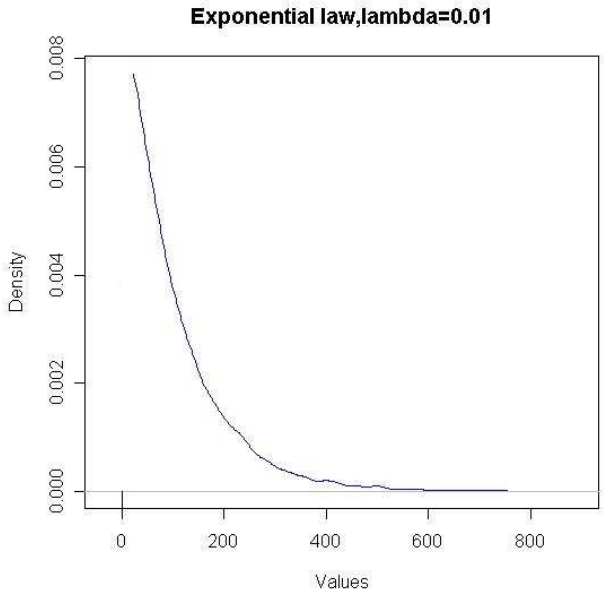
As a result, the values of the first column **approximately** correspond to the “x” in the theoretical representation of the exponential law.
The effect of this approximation is more important when we draw values near “0”. Thus the probability in the table to generate “0” is smaller than “1”.



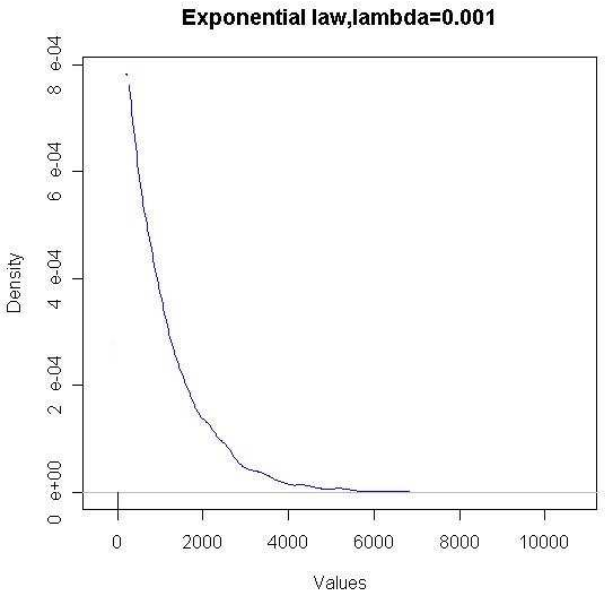
This graph is plotted with real values generated by **NetDisturb**. We observe that the probability for x="0" (=λ) is bigger than for x="1". Here are below graphs plotted with small values for λ.



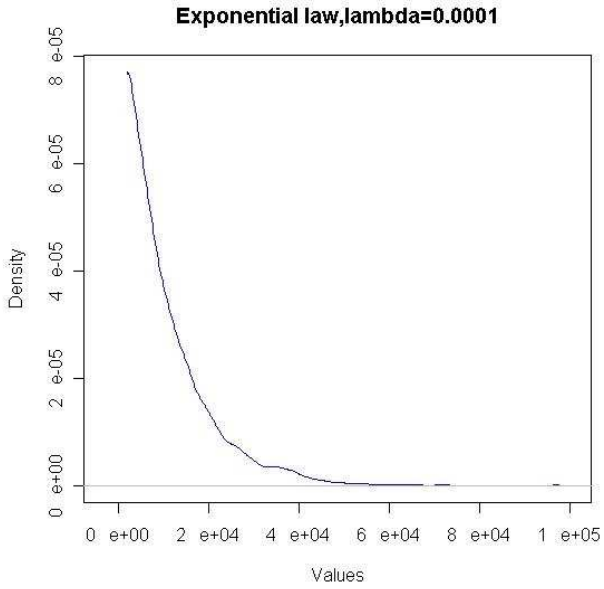
Maximum* drawn value = 221



Maximum* drawn value = 2218



Maximum* drawn value = 22180



Maximum* drawn value = 221807

**Maximum drawn value by the software, theoretically there is no maximum for the exponential law!*

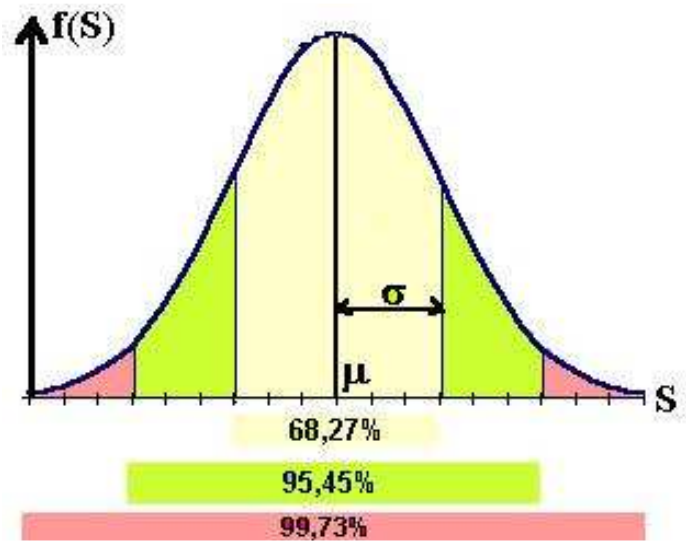
10.3.4 Laplace-Gauss law

When this law is used, the unit is the millisecond for the starting time of a connection or byte for the data volume to send.

The probability density function of the Laplace-Gauss Law is:

$$f(x) = \frac{n}{\sqrt{2\pi}\,\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

where μ is the average and σ is the standard deviation..



- The more σ is small the more drawn values are near μ
- 68.27% of drawn values are in $[\mu - \sigma ; \mu + \sigma]$
- 95.45% of drawn values are in $[\mu - 2\sigma ; \mu + 2\sigma]$
- 99.73% of drawn values are in $[\mu - 3\sigma ; \mu + 3\sigma]$

μ and σ must be defined such as: $\mu > 0$ and $\mu \geq 3\sigma$ with $\sigma > 0$