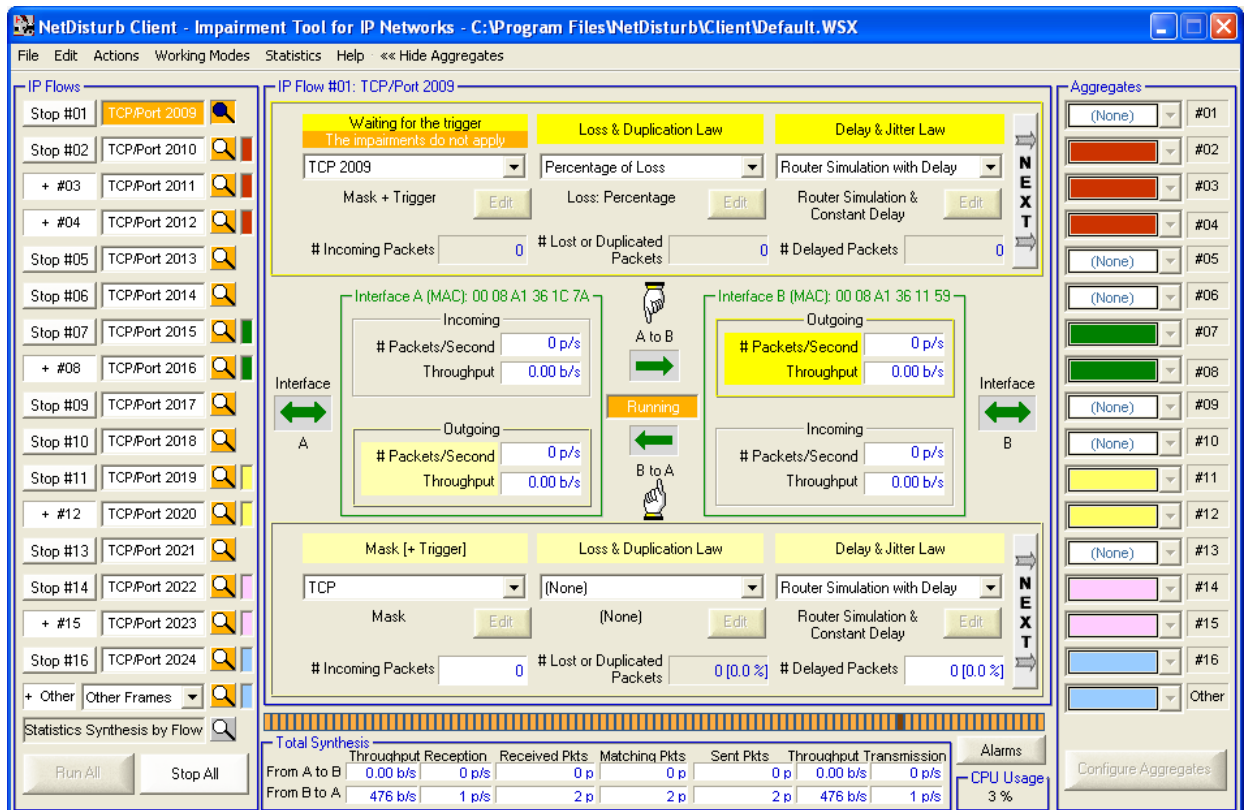




Version 4.6

Impairment Emulator Software for IP Networks (IPv4 & IPv6)



User Guide

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

Copyright ZTI 1998-2008. All rights reserved.
France Telecom licensed product.

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

No part of this manual may be copied, reproduced, translated or recorded by any mean without prior written consent from ZTI.

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

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:

- a unique Site Code that requires the corresponding unique Site Key to be entered
- 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 GUINGAMP-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	7
0.1	ORGANIZATION OF THIS MANUAL	7
0.2	MINIMUM SYSTEM REQUIREMENTS	8
0.3	TECHNICAL SUPPORT	8
PART 1	NETDISTURB OVERVIEW	9
1.1	PRODUCT REQUIREMENTS	10
1.2	CONFIGURATIONS.....	10
1.3	PRODUCTS FEATURES.....	11
1.3.1	Key features	11
1.3.2	How does it work?	14
1.3.3	Introduction of a Trigger for the Mask.....	15
1.3.4	Packet impairments	16
1.3.5	Working modes	17
1.3.6	IP Flows and Aggregates.....	18
1.3.7	Statistics & Alarms.....	19
1.4	PERFORMANCES	22
1.5	CUSTOMER REFERENCES	25
1.6	CONDITIONS OF USE	25
1.7	DELIVERY	25
PART 2	WHAT'S NEW IN NETDISTURB VERSION 4.6?.....	26
PART 3	INSTALL NETDISTURB	27
3.1	FOREWORDS BEFORE UPGRADING FROM VERSIONS 4.2, 4.3, 4.4 AND 4.5.....	27
3.2	FOREWORDS BEFORE UPGRADING FROM VERSIONS 4.1 AND UNDER.....	27
3.3	HOW TO INSTALL THE SOFTWARE DOWNLOADED FROM THE INTERNET	27
3.4	HOW TO INSTALL THE SOFTWARE FROM THE CD-ROM	27
3.5	HOW TO INSTALL THE NETDISTURB CLIENT ONLY (FROM THE CD-ROM)	27
3.6	DURING THE INSTALLATION	28
3.6.1	NetDisturb packages in a few words	28
3.6.2	Which package should I install?	29
3.7	WHAT HAS BEEN INSTALLED ON MY COMPUTER?.....	30
3.7.1	IMPORTANT STEP: I must configure the driver before running NetDisturb	30
3.7.2	Start Menu Shortcuts Created	30
3.8	HOW TO REINSTALL ANOTHER PACKAGE?	31
3.9	HOW TO TRANSFER THE SOFTWARE TO ANOTHER COMPUTER?	31
PART 4	HOW TO HANDLE YOUR LICENSE?	32
4.1	NETDISTURB TRIAL.....	32
4.1.1	NetDisturb Server License Information window	32
4.1.2	End of the fifteen-day trial period.....	32
4.2	NETDISTURB & SOFTWARE PROTECTION KEY	33
4.2.1	Installation of the Software Protection Key	33
4.2.2	Software Protection Key Transfers.....	35
4.3	NETDISTURB & <i>USB SOFTWARE PROTECTION KEY</i>	40
PART 5	UNINSTALL NETDISTURB	40

PART 6	RUN NETDISTURB	41
6.1	FIRST RUN	41
6.2	DETAILED DESCRIPTION OF THE SERVER AND CLIENT STARTUP	48
6.2.1	The NetDisturb Server Startup Modes	48
6.2.2	The NetDisturb Client Startup Options	48
PART 7	USING THE NETDISTURB CLIENT	49
7.1	THE NETDISTURB CLIENT MAIN WINDOW	49
7.2	MENU DESCRIPTION	51
7.2.1	File Menu	51
7.2.2	Edit Menu	52
7.2.3	Actions Menu	54
7.2.4	Working Modes Menu	56
7.2.5	Statistics Menu	57
7.2.6	Help Menu	59
7.2.7	Hide or Show Aggregates Menu	59
7.3	THE IP FLOWS	61
7.3.1	General Description	61
7.3.2	Status of the IP Flows	62
7.3.3	The "Other Frames"/"Other IP Flows"	62
7.3.4	The Statistics Synthesis View	63
7.4	THE IMPAIRMENT PARAMETERS AND ASSOCIATED COMMANDS	66
7.4.1	Selection of a Filter Mask or an Impairment Law	67
7.4.2	The Mask [+ Trigger] Configuration	67
7.4.3	The Loss & Duplication Law Configuration	91
7.4.4	The Delay & Jitter Law Configuration	118
7.4.5	The Content Impairment Law Configuration	139
7.4.6	Loss/Duplication, Delay/Jitter Dynamics	157
7.4.7	Loss with Duplication and Delay/Jitter Dynamics	158
7.5	USE OF THE AGGREGATES	159
7.5.1	What is an aggregate?	159
7.5.2	When do we need to use an aggregate?	159
7.5.3	How to configure the aggregates	161
7.5.4	How to associate a colored aggregate to an IP Flow	164
7.5.5	How to disassociate an IP Flow belonging to a colored aggregate	166
7.6	THE NETDISTURB CLIENT STATISTICS	167
7.7	THE ERRORS DETECTED BY THE NETDISTURB DRIVER	167
7.7.1	Details for the Incoming Errors	169
7.7.2	Details for the Outgoing Errors	169
7.7.3	Alarm Management	170
PART 8	USING THE NETDISTURB COMMAND LINE INTERFACE	171
8.1	GENERAL RULES	171
8.1.1	Command Line Interface's Execution	171
8.1.2	How to use the Command Line Interface	171
8.1.3	Options	171
8.2	COMMANDS AND PARAMETERS	172
8.2.1	Display the usage (/?)	172
8.2.2	Stop and shutdown NetDisturb Client and NetDisturb Server (/Quit)	173
8.2.3	Stop and shutdown NetDisturb Client only (/Quit Client)	173
8.2.4	Open and Start NetDisturb Server (/Run)	174
8.2.5	Load the context file (/Context filename)	174
8.2.6	Set the file name where to store the statistics (/Trace filename)	175
8.2.7	Start saving the statistics (/Trace start)	175
8.2.8	Stop saving the statistics (/Trace stop)	176

8.2.9	Stop an IP Flow (/Stop X)	176
8.2.10	Stop all IP Flows (/Stop all).....	177
8.2.11	Start an IP Flow (/Start X)	177
8.2.12	Start all IP Flows (/Start all).....	178
8.3	COMMANDS EXECUTION ORDER	178
PART 9	USING THE NETDISTURB SERVER	179
PART 10	APPENDICES	181
10.1	THE NEW CONTEXT VALUES	181
10.2	THE NETDISTURB REGISTRY VALUES	181
10.2.1	The Registry parameters related to the NetDisturb Client	182
10.2.2	The Registry parameters related to the NetDisturb Server	183
10.2.3	The Registry parameters related to the NetDisturb driver	183
10.2.4	The NetDisturb Driver Traces	183
10.3	THE MATHEMATICAL LAWS USED BY NETDISTURB	184
10.3.1	Uniform law	184
10.3.2	The Uniform Correlated Law	185
10.3.3	Exponential law	186
10.3.4	Laplace-Gauss law	194

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 4.6**

Is a general overview of new features, main improvements provided with **NetDisturb** version 4.6.

- **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 256 MB memory at least
- Two identical Ethernet NICs: 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 **NetDisturb** is available but without the help file.*



PC multiprocessors and processor with hyper-threading are also supported.

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.

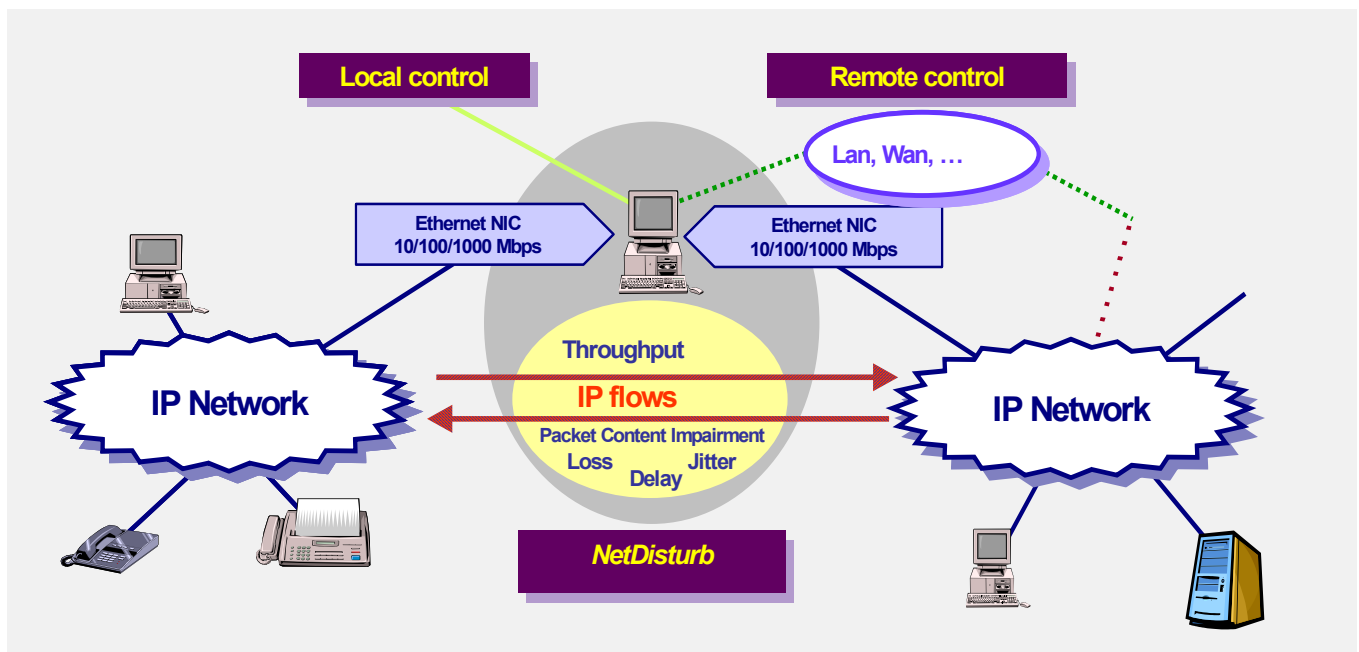
You can contact Technical Support by:

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 06:00 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 like: latency, delay, jitter, bandwidth limitation, lost, duplicate packets and impaired the content over the IP networks (IPv4 and IPv6). **NetDisturb** allows the user to disturb flows on an IP network and so to study the behavior of applications, devices or services in a disturbed network environment.

NetDisturb is inserted between two Ethernet segments (on the same IP network or two different IP networks) and operates bi-directional packet transfer on Ethernet, Fast Ethernet and Gigabit network interface cards.



1.1 Product Requirements

- * Platform: Pentium PC running Windows 2000, XP or Server 2003 with Microsoft TCP/IP installed and at least 256 MB Ram.
- * Hyper-threading and PC multiprocessors are also supported.
- * Two Identical Network Interfaces Cards (NIC): Ethernet, Fast Ethernet, or Gigabit Ethernet network interface card.
- * 1024 x 768 display, DPI setting = Normal size (96 DPI) and Font size = Normal.

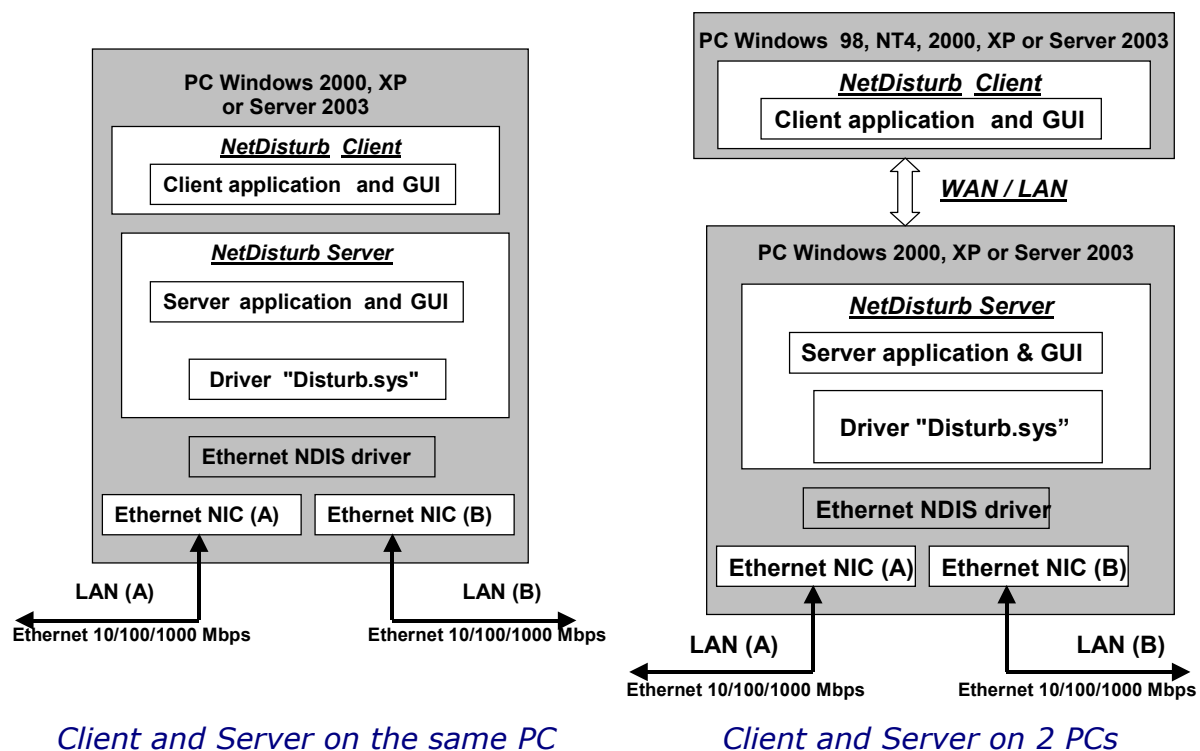


1.2 Configurations

Based on Client Server architecture, the **NetDisturb** software is made of two parts: a Server and a Client. The 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 host (local control), or the Server part is located on one PC and the Client part 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.

Both configurations require two identical Ethernet Cards for the Server.



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.

1.3 Products features

What are the major features of **NetDisturb** V4.6?

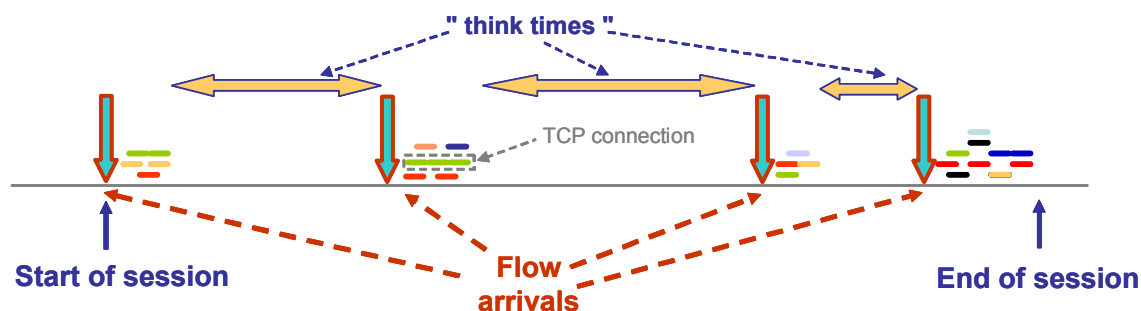
1.3.1 Key features

- 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.
- Impairments: Latency, Loss, Duplication, bandwidth limitation, Delay and Jitter, Content Impairment (mathematical laws and user-defined files)
- 16 configurable IP flows per direction with optional trigger condition
- Aggregates of IP flows can be defined (set of IP flows sharing the same Delay & Jitter Law)
- Unidirectional or bi-directional packet impairments
- Change the Law and the mask on-the-fly
- Connections per IP flow: impairments are applied to the IP flow or to each connection of the IP flow
- Ethernet / Internet modes (packets out of sequence)
- Easy to use and intuitive Graphical User Interface
- Statistics display and export detailed statistics in a file
- Command Line Interface (CLI) to use NetDisturb in test beds
- Ability to handle Ethernet Jumbo frames (payload up to 17976 bytes)
- Ability to impair the remaining network traffic that could be either only the IP packets or all the Ethernet frames.

NetDisturb is based on the notion of IP 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 a n-tuple.

In the typical case, the following 5-tuple is used: IP addresses, protocol and port numbers.

An IP flow is composed of connections (such as TCP connections to make FTP transfer by example).

To define the n-tuple for an IP flow, **NetDisturb** uses the notion of mask. A mask is the combination of the following optional parameters:

Frame Type (ARP Frame or IP Frame:IPv4, IPv6 or IPv4 & IPv6)

Ethernet header

- MAC destination address
- MAC source address

List of VLAN-ID (Ethernet frames 802.1Q)

IP Header

- Destination IP address
- Source IP address
- Protocol (ICMP, TCP, UDP, SIP, RTP...)
- Differentiated services (TOS)

List of Ports (for TCP or UDP packets)

- Destination port list
- Source port list



A trigger can be associated optionally with the mask.

With **NetDisturb** you can define up to 16 masks, i.e. 16 IP flows. An additional item named "Other IP Flows" is in charge to handle all IP flows that have not been user defined. For this item no mask 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 IP flows by **NetDisturb**.

NetDisturb Client - Impairment Tool for IP Networks - C:\Program Files\NetDisturb\Client\Default.WSX

File Edit Actions Working Modes Statistics Help Show Aggregates >>

IP Flows

- Run #01 VLAN
- + #02 ICMP
- Run #03 SIP
- Run #04 RSVP
- + #05 UDP
- + #06 TCP
- Run #07
- Run #08
- Run #09
- Run #10
- Run #11
- Run #12
- Run #13
- Run #14
- Run #15
- Run #16
- Run Other Frames
- Statistics Synthesis by Flow
- Run All Stop All

IP Flow #04: RSVP

Mask [+ Trigger]: RSVP

Loss & Duplication Law: % of Loss & Time

Delay & Jitter Law: Delay & F.(Throughput, Time)

Mask Edit Loss: Percentage & Duration Edit Constant Delay & File (Throughput, Duration) Aggregate

Incoming Packets 0 # Lost or Duplicated Packets 0 [0.0 %] # Delayed Packets 0 [0.0 %]

Interface A (MAC: 00 08 A1 36 1C 7A)

Incoming: # Packets/Second 0 p/s Throughput 0.00 b/s

Outgoing: # Packets/Second 0 p/s Throughput 0.00 b/s

Interface B (MAC: 00 08 A1 36 11 59)

Outgoing: # Packets/Second 0 p/s Throughput 0.00 b/s

Incoming: # Packets/Second 0 p/s Throughput 0.00 b/s

Mask [+ Trigger]: RSVP

Loss & Duplication Law: Burst Uniform Loss

Delay & Jitter Law: Delay & F.(Throughput, Time)

Mask Edit Loss: Burst Uniform Law Edit Constant Delay & File (Throughput, Duration) Aggregate

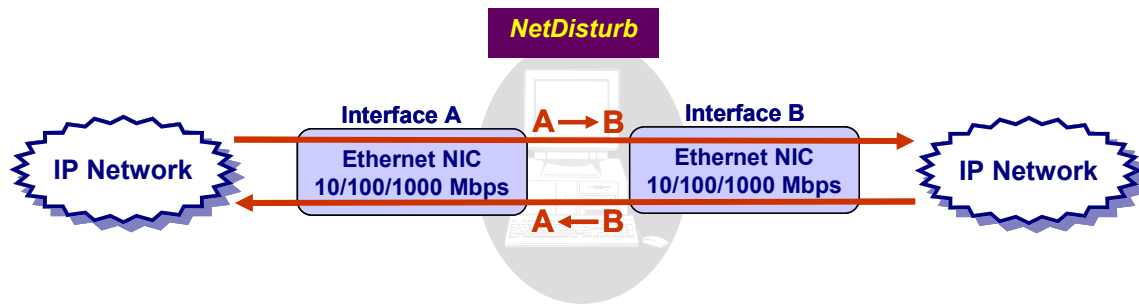
Incoming Packets 0 # Lost or Duplicated Packets 0 [0.0 %] # Delayed Packets 0 [0.0 %]

Total Synthesis

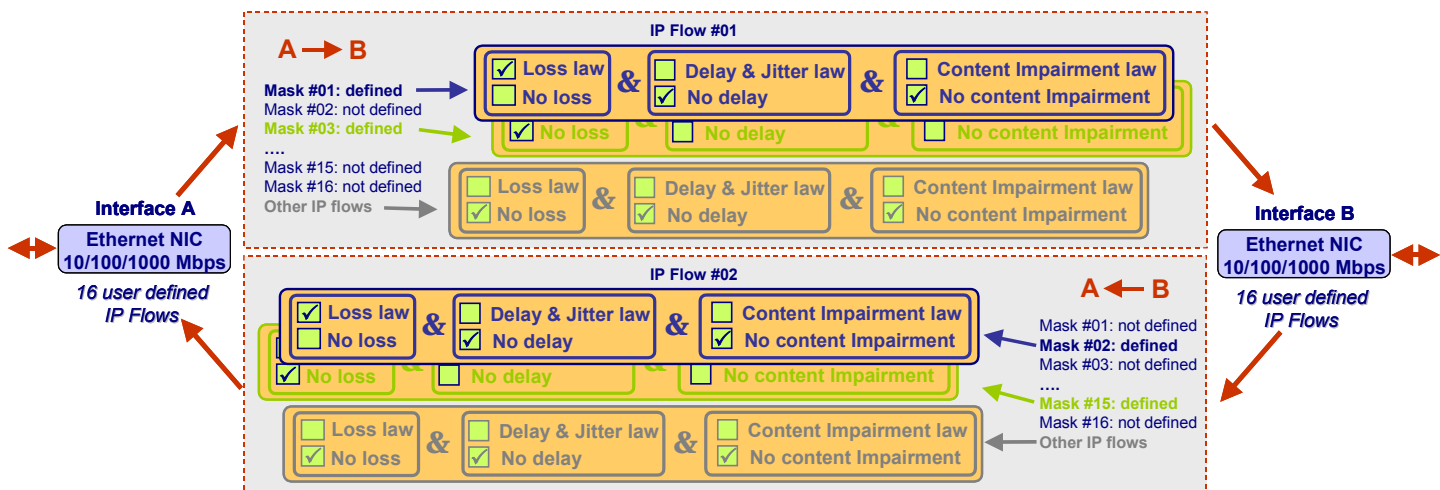
	Throughput Reception	Received Pkts	Matching Pkts	Sent Pkts	Throughput Transmission	
From A to B	0.00 b/s	0 p/s	0 p	0 p	0.00 b/s	0 p/s
From B to A	0.00 b/s	0 p/s	0 p	0 p	0.00 b/s	0 p/s

Alarms: CPU Usage 2 %

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



For each direction $A \rightarrow B$ or $B \rightarrow A$, 16 flows can be defined by the user. And for each IP flow, loss & duplication and / or delay and / or 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 $A \rightarrow B$

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

Direction $B \rightarrow A$

- The Mask #02 defines the "IP Flow #02", and a loss law is applied to the packets of this flow,
- The Mask #15 defines the "IP Flow #15", a delay law and a content impairment law are applied to the packets of this flow,
- As no loss and delay law is applied to the 'Other IP flows', all non-matching packets with the masks #02 and #15 are relayed directly from B to A.

1.3.2 How does it work?

The Figure 1 illustrates how **NetDisturb** handles incoming packets from the A interface to the B interface.

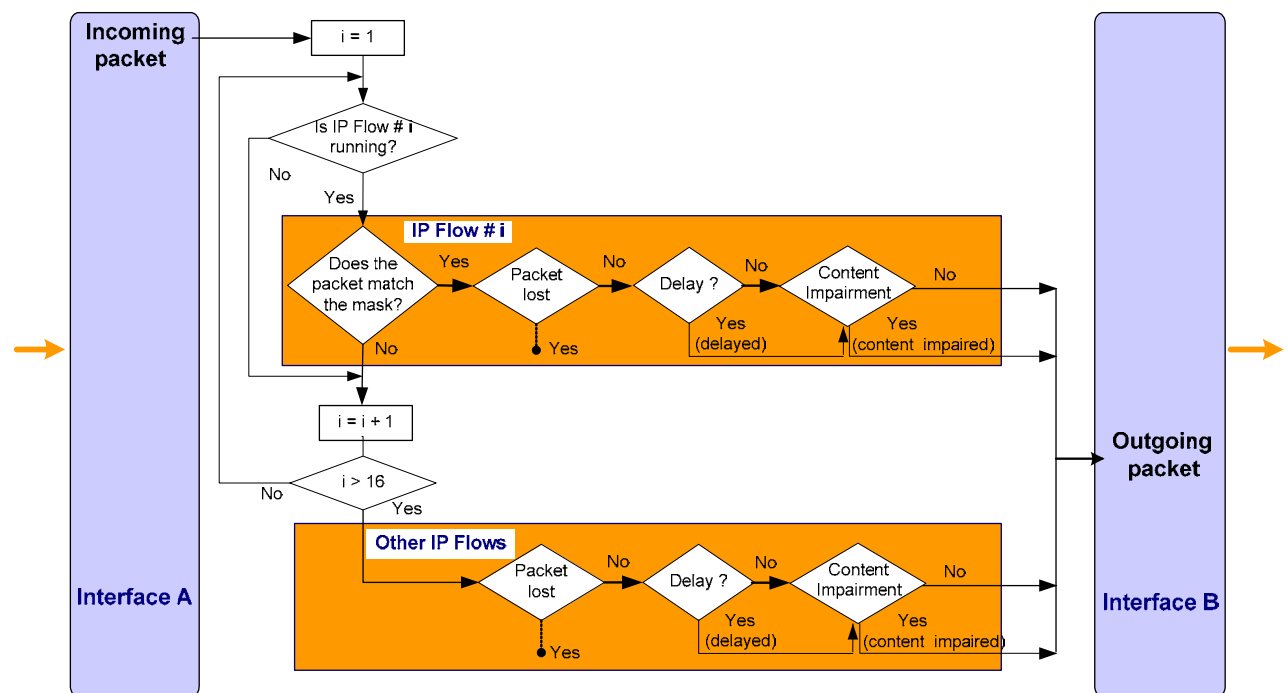


Figure 1 - NetDisturb Incoming Packets Management

Depending on the active user-defined IP flows, **NetDisturb** identifies if the incoming packet belongs to an IP flow before applying loss, delay or content impairment treatments.

If this packet matches with the mask of an IP Flow (IP Flow #i for example), then **NetDisturb** identifies if this packet must be lost/duplicated and/or delayed and/or if its content must be impaired.

If this packet does not match any mask (a mask defines an IP flow), then **NetDisturb** applies the treatments for the 'Other IP Flows' and identifies if this packet must be lost/duplicated and/or delayed and/or if its content must be impaired. For each packet received on an interface, **NetDisturb** analyzes in order the masks from 1 to 16 before considering this packet to belong to the "Other IP Flows".

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

1.3.3 Introduction of a Trigger for the Mask

One of the features of **NetDisturb** is the use of a trigger to link the launch of the impairments with an event.

The Trigger is an intermediate step after the frame has been classified in an IP Flow and before the frame is impaired.

The Trigger includes various parameters:

- The **activation condition** based on the Ethernet frame content.
- The **delay before applying the impairments**
- The **impairment duration** (0 = no limit).
- The **number of cycles** for the trigger (0=unlimited) if the impairment duration is not null.

Thus two main categories of triggers are defined:

- The Trigger time-limited to be applied on the impairments
- The Trigger time-unlimited to be applied on the impairments (a loop counter can be used)

As soon as the activation condition is performed, the impairment on the IP flow can be immediate or delayed with a duration expressed in milliseconds (delay of impairment).

If the impairment is immediate, the frame that has triggered can be included or not (if the delay before impairment is null).

The impairment can be time limited according to a duration expressed in milliseconds.

When **NetDisturb** is running an IP flow with a defined trigger, four states are possible:

- ⇒ **Waiting for the Trigger**: the impairments do not apply. This state is the initial state of the Trigger.
- ⇒ **The Trigger was found**: the impairments still do not apply because a delay is defined before the impairments. This state changes to the next state when the activation condition is reached.
- ⇒ **The Trigger is active**: the impairments are applied.
- ⇒ **The Trigger is finished**: the impairments do not apply any more. This is the final state of the Trigger.



A Trigger can remain active permanently if no duration limit was defined.

1.3.4 Packet 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, $\text{Min} \leq n \leq \text{Max}$
- Duplication: 1 Packet out of M (duplicate 1 packet n times every M received packets). Parameters: range(M), $\text{Min} \leq n \leq \text{Max}$
- 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

1.3.5 Working modes

NetDisturb offers two working modes by applying impairments:

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

.

Enable/Disable Desequencing 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 can simulate the Internet network (enable desequencing packets) or can react as Ethernet does (disable desequencing packets).

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

NetDisturb can analyze IP packets to dispatch them into the TCP or UDP connection they belong to. This mode makes possible to apply the same impairment values to each packet of each connection. For instance if the impairment has been defined with a loss law: lose the third packet for 10 packets received.

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

When this option is selected, every received packet matching the mask 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**.

1.3.6 IP Flows and Aggregates

Up to 8 aggregates of IP flows can be defined. An aggregate is a consecutive set of IP flows sharing the same Delay & Jitter Laws. All IP flows of an aggregate share only one aggregate's Delay & Jitter law (with one law per direction).

The IP flow order in the aggregate defines the priority of packets to delay. While the top IP flow packets get the highest priority, the other IP flow packets are queuing until there are no higher priority packets.

In the Figure 2 below, two aggregates have been defined:

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

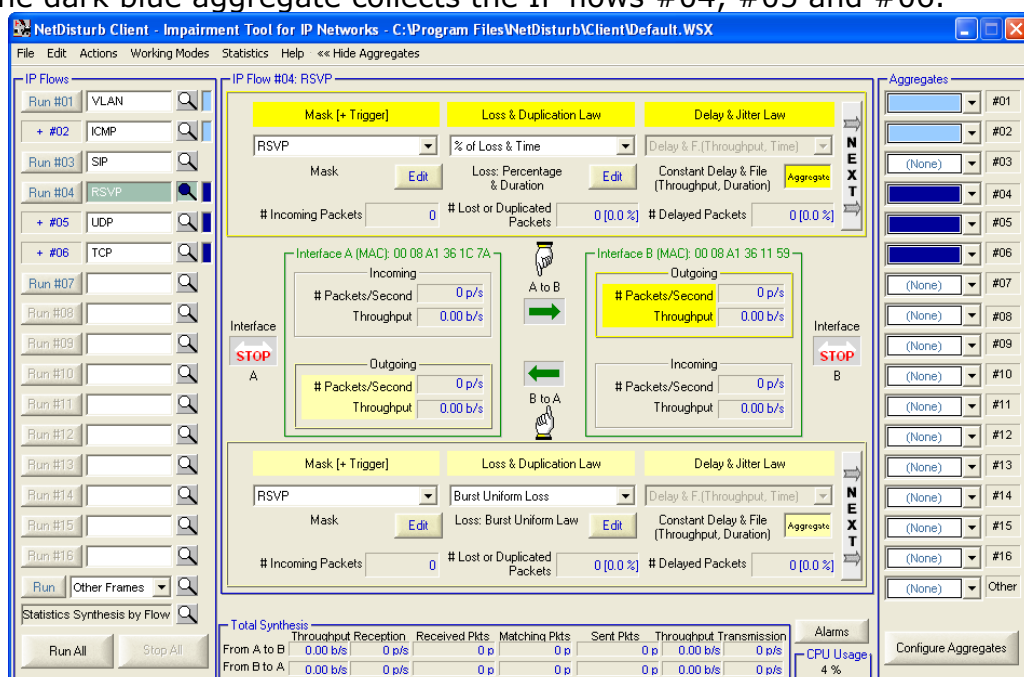


Figure 2 - Two aggregates defined

1.3.7 Statistics & Alarms

Different statistics are calculated and displayed by **NetDisturb**:

- For each IP Flow (and for both directions)
- Statistics synthesis by Flow
- Total synthesis & Alarms

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

Statistics for each IP Flow

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

- The number of packets matching the mask
- The number and the percentage of lost or duplicated packets
- The number and the percentage of delayed packets
- The number and the percentage of the packets where the content has been impaired

Mask [+ Trigger]	Loss & Duplication Law	Delay & Jitter Law
UDP	Percentage of Loss	Router Simulation with Delay
Mask	Loss: Percentage	Router Simulation & Constant Delay
# Incoming Packets: 184942	# Lost or Duplicated Packets: 173137 [94 %]	# Delayed Packets: 11805 [6.4 %]

Loss & Duplication Law	Delay & Jitter Law	Content Impairment Law
F.(Percentage & Time)	Router Simulation with Delay	Normal Law Impairment
Loss: File (Percentage & Duration)	Router Simulation & Constant Delay	Normal Law (Laplace-Gauss)
# Lost or Duplicated Packets: 2443 [70 %]	# Delayed Packets: 1050 [30 %]	# Modified Packets: 1050 [30 %]

- And a complete view of traffic statistics (number of packets and throughput) over the A and B interfaces as shown in Figure 3 below:

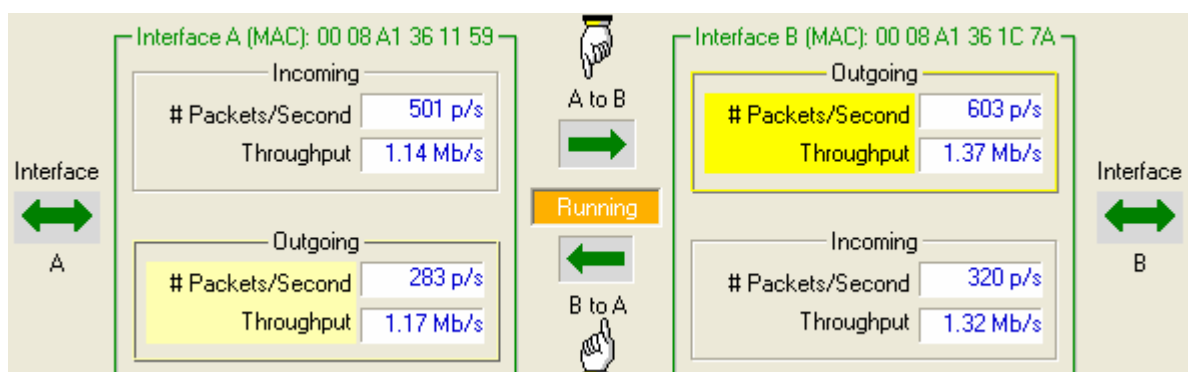


Figure 3 – Complete view of Traffic Statistics between interface A and B

Statistics Synthesis by Flow

The synthesis for all IP Flows displays for each flow and for each direction:

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

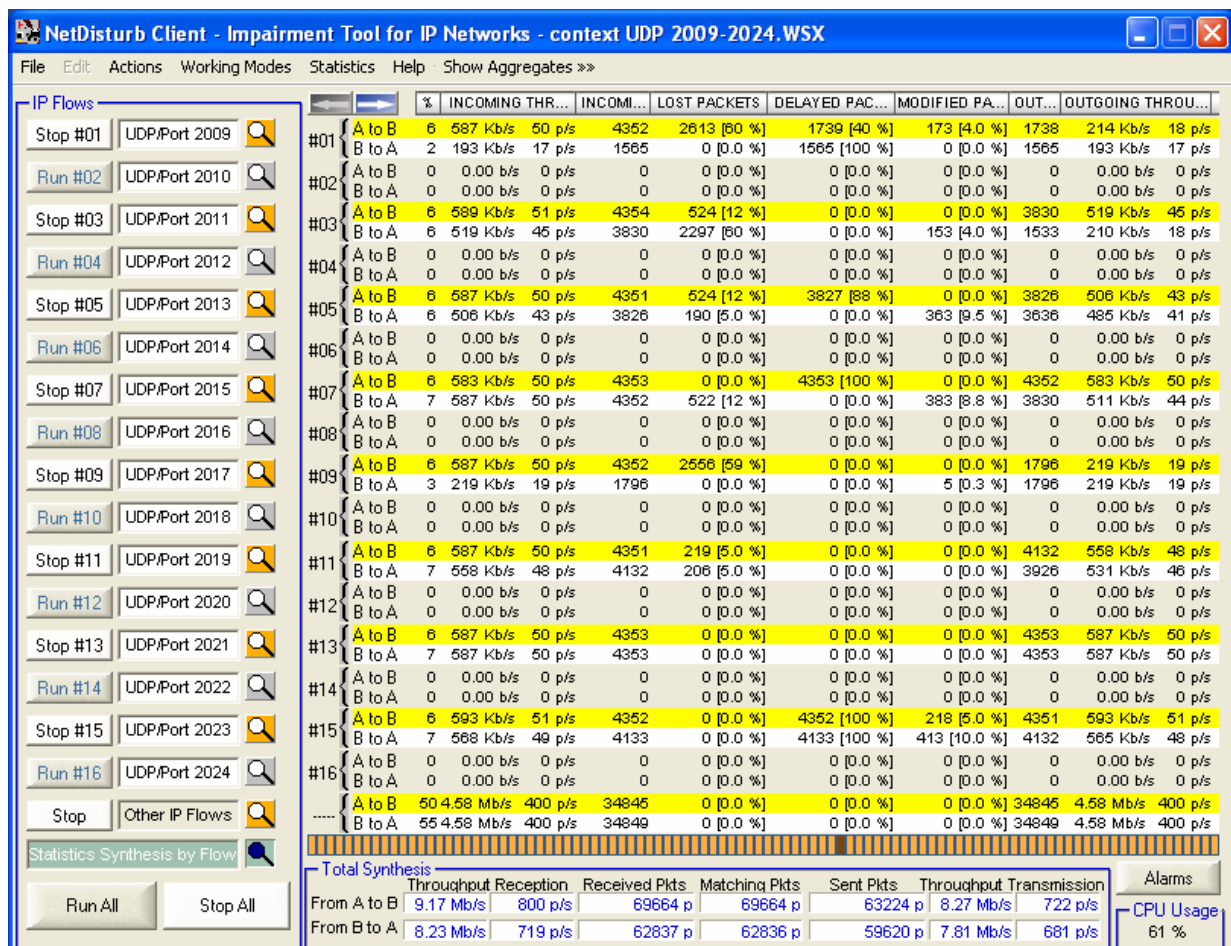


Figure 4 – Statistics Synthesis by Flow example

Total synthesis

At the bottom of the Client window, the total synthesis displays the following parameters for both directions (A → B or B → A):

- Throughput and number of packets per second received
- Number of packets received
- Number of matching packets
- Number of packets sent
- Throughput and number of packets per second transmitted

Total Synthesis							Alarms
	Throughput Reception	Received Pkts	Matching Pkts	Sent Pkts	Throughput Transmission		
From A to B	1.16 Mb/s	491 p/s	28675 p	28381 p	1.12 Mb/s	487 p/s	CPU Usage 18 %
From B to A	4.16 Mb/s	745 p/s	81630 p	81630 p	4.16 Mb/s	745 p/s	

Alarms

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

<i>Incoming direction</i>	<i>Outgoing direction</i>
<ul style="list-style-type: none"> • Number of lost packets • Number of lost bytes • Number of errors returned by the Driver at the Interface • Number of missing buffers to keep packets • Number of ignored flows (when the multi-flows option is active). 	<ul style="list-style-type: none"> • Number of lost packets • Number of lost bytes • Number of errors returned by the Driver at the interface

NetDisturb Client - Alarms Summary

Alarms Linked to the Direction from Interface A to Interface B

Incoming from A

- # Lost Packets: 0
- # Lost Bytes: 0
- # Driver Errors: 0
- # Missing Buffer Errors: 0
- # Lost TCP/UDP Connections: 0

A to B

Outgoing to B

- # Lost Packets: 0
- # Lost Bytes: 0
- # Driver Errors: 0

Details

Alarms Linked to the Direction from Interface B to Interface A

Outgoing to A

- # Lost Packets: 0
- # Lost Bytes: 0
- # Driver Errors: 0

B to A

Incoming from B

- # Lost Packets: 0
- # Lost Bytes: 0
- # Driver Errors: 0
- # Missing Buffer Errors: 0
- # Lost TCP/UDP Connections: 0

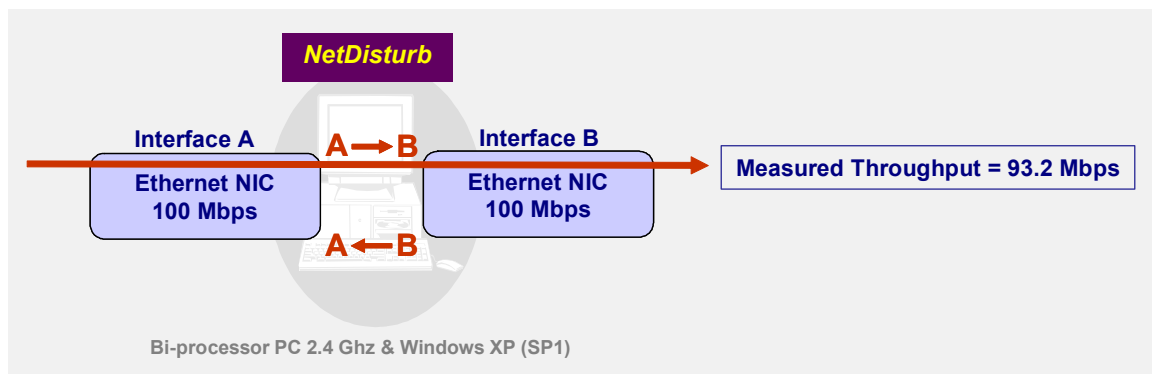
Details

OK Clear Alarms Update Alarms Summary

1.4 Performances

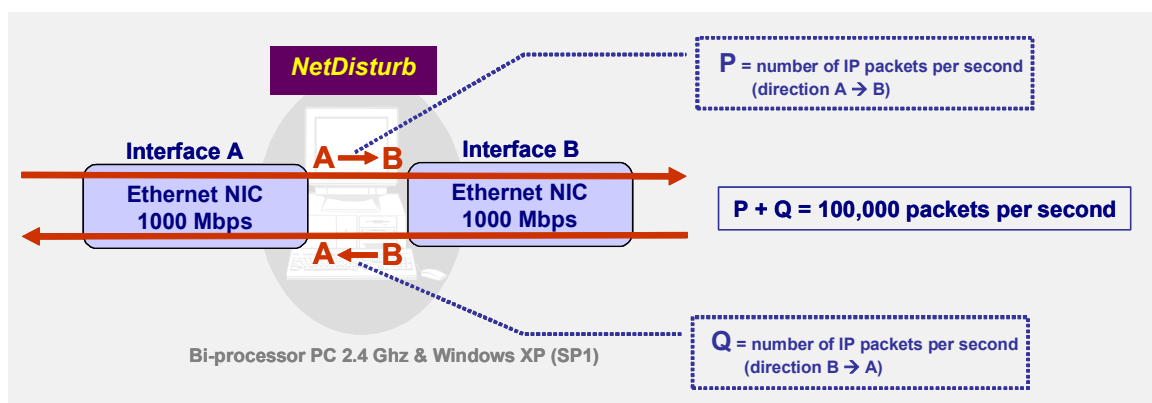
To illustrate the key performances of **NetDisturb**, 2 examples are presented hereafter (by using an Intel Xeon 5140 2.33 GHz with Windows XP SP2).

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 97Mbps in one direction.

Example 2: use of 2 Gigabit Ethernet NICs



By using 2 Gigabit NICs, **NetDisturb** can handle up to 150,000 packets per second with 16 IP flows defined (for both directions).

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

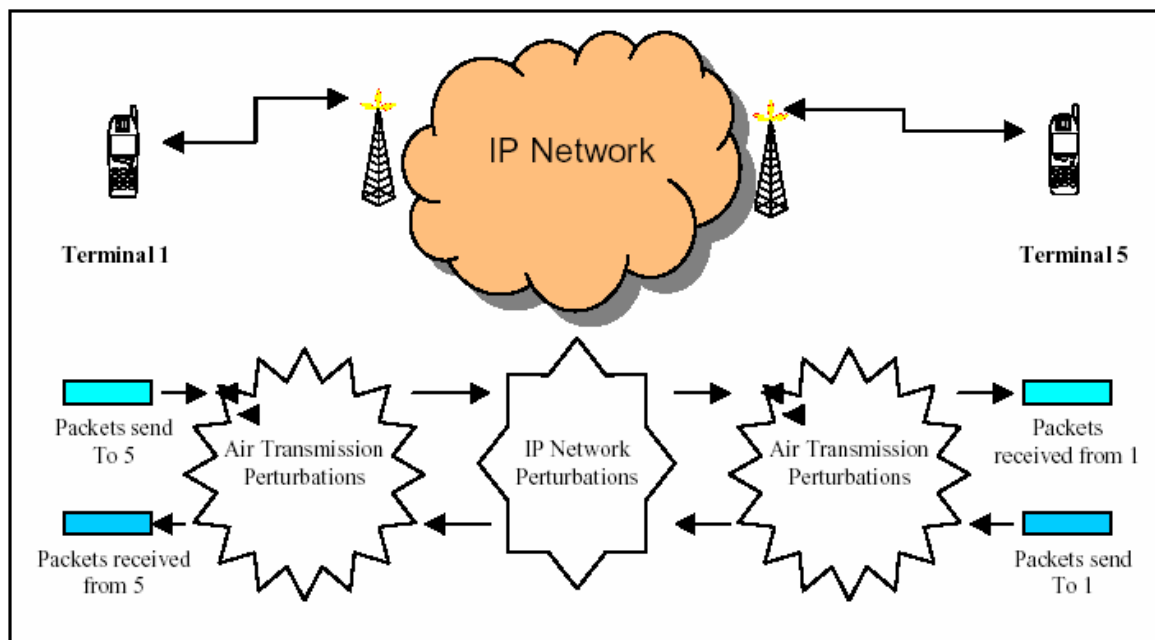
Applications

- *Performance & Acceptance Tests:* Qualify and evaluate the behavior of IP equipments (phone, fax, gateway, etc.) and applications (audio and video streaming, etc.) 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, streaming audio and video, and other distributed applications.
- *Emulation of symmetric or asymmetric network conditions (LAN, MAN, WAN):* latency, jitter, packet loss, bandwidth limitations, etc. to test IP applications (VoIP, streaming audio & video, etc.), services and products sensitive to various real conditions.

*Some publications mentioning the use of **NetDisturb***

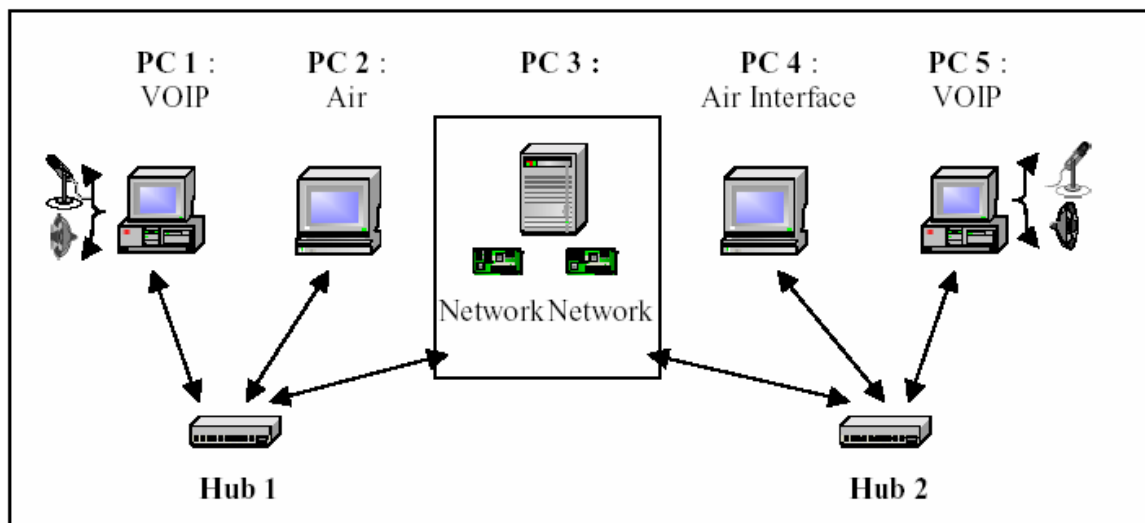
- The Communications and Information network Association of Japan (CIAJ) which represents manufacturers supplying network devices and terminals has published a report in 2002: Report on speech quality investigation of VoIP Terminals (gateways and IP phones): http://www.ciaj.or.jp/tusin/pressrelease/voip_1e.html "We adopted **NetDisturb**, ... as a network simulator because of its ease of installation and operation in Windows".
- 3GPP Technical Specification Group Services and System Aspects TSG-S4
- Test Plan for the Adaptive Multi-Rate Wide-Band (AMR-WB) and Narrow-Band (AMR-NB) in packet switched networks.
- Test Plan for 3G packet switched conversation tests (comparison of quality offered by different speech coders over packet switched networks)
NetDisturb is used as the simulated network.

The following illustrations describe the system that is simulated for these tests.



Packet switch audio communication simulator

This is simulated by using 5 PCs as shown below, with PC# 3 using **NetDisturb** as network simulator.



Simulation platform

1.5 Customer references

Present on the market since 1998, **NetDisturb** is used in more than 40 countries.

See some worldwide references of satisfied customers:

Alcatel, ANZ Bank, AT&T, Bell Canada, Cisco, Commtech Wireless, Department of Defense, Equant, France Telecom, Gensight, Global Crossing, Iwatsu, Juniper, Motorola, Nortel Networks, NEC, NTT, Panasonic, Philips, PIKA Technologies, Polycom, Psytechnics, Raytheon, Schlumberger, Scopus, Tekelec, TF1, Toshiba, UTStarcom, WL Gore, Xerox, etc. as well as many universities and telecom institutes.

1.6 Conditions of use

NetDisturb is licensed on a per workstation basis. You will need to purchase a separate license for each machine that you run it on.

Each licensed copy of the software gets one corresponding USB Software Protection Key that should be inserted on the target PC before starting the **NetDisturb** server.

1.7 Delivery

Includes CD with documentation, printed installation guide, one USB Software Protection Key, technical support and software maintenance (including major and minor software upgrades) for a period of twelve months from the date of purchase.

To download the trial version of **NetDisturb**, please visit us at:
<http://www.zti-telecom.com/pages/main-ip.htm>

Part 2 What's new in NetDisturb version 4.6?

This part is a general overview of new features and improvements provided with **NetDisturb** version 4.6 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 4.6 are listed below:

- ⇒ The licensed version of the software uses a USB Software Protection Key. The USB Software Protection Key is the most flexible way to transfer your license to any other PC.
- ⇒ The Command Line Interface has been added to the NetDisturb Client part. It enables the integration of **NetDisturb** in Command Line tests beds.
- ⇒ The exchanges between NetDisturb Client and NetDisturb Server's parts are based on the SOAP interface. It allows going through Firewall in an easier way.
- ⇒ The previous versions of **NetDisturb** were allowing handling only the remaining IP packets. From version 4.6, **NetDisturb** is also able to impair the complete **remaining Ethernet frames** such as IP Frames, MPLS, Appletalk, IPX frames, and so on.
- ⇒ **NetDisturb** manages the jumbo Ethernet Frame up a size of 17976 bytes.
- ⇒ The context files and the User data files are now located on the NetDisturb Client PC and the user is allowed to change the file location i.e. not only the default directory (C:\Program Files\NetDisturb\Client) can be used but any.
- ⇒ The laws could be changed 'on-the-fly'.
- ⇒ Multiple corrections have been included in the laws management.

To get more details about how to switch from the old software license mechanism to the new **USB Software Protection Key**, please refer to the paragraph 4.3.



The contexts created with version 4.2, version 4.3 RC3, and version 4.4 and version 4.5 are reused automatically. When saved, they get the new NetDisturb v4.6 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, 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 your administrators rights.*

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

NetDisturb version 4.6 has introduced a new Software Protection using a USB key but previous users of **NetDisturb** can continue to use their Software License Key. **When upgrading from a previous version of NetDisturb, 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 4.6** 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 4.6**, 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 number when upgrading to version 4.6 with the new site code.

3.3 How to install the software downloaded from the Internet

The installation procedure is a standard installation program.

- If you have downloaded the file **NetDisturb.zip** from our 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.

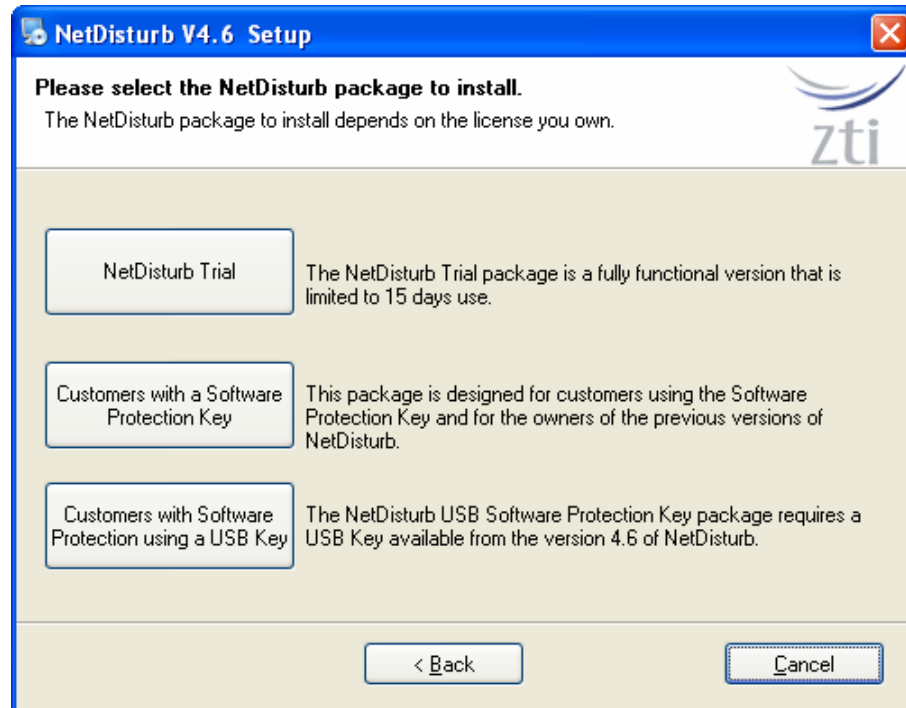
3.5 How to install the NetDisturb Client only (from the CD-ROM)

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

To install the **NetDisturb** Client on a machine (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.



3.6.1 NetDisturb packages in a few words

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

- The **NetDisturb Trial package** allows you to use **NetDisturb** during 15 days after the first run. When the trial period has expired, the license should be purchased.
- The **NetDisturb Software Protection Key package** has been designed 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.
- For new users, the **NetDisturb USB Software Protection Key package** requires a USB key with 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 Software Protection key plugged in.



As previous users, 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 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 (for previous users) or the USB Software Protection key. Each new licensed copy of the software gets a USB Software Protection key that can be moved from one installation to the other.



The USB Software Protection key contains only the license information. The 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 V4.6**

In that case, choose the “*NetDisturb Trial*” package. 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 “*Customers with a Software Protection Key*” package. 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 “*Customers with Software Protection using a USB Key*”. Plug the USB Software Protection Key before launching **NetDisturb**.

3.6.2.3 I just bought **NetDisturb** ...



This paragraph is related to the users purchasing **NetDisturb V4.6**.

... and I chose the **Electronic Software Delivery (ESD)**

In that case, choose the package “*Customers 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 mail 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 Software Protection Key. More details about the way to proceed are available in paragraph “**4.2.1 Installation of the Software Protection Key**”.

... and I received the **CDROM & USB Software Protection Key**

In that case, choose the package “*Customers with Software Protection using a USB Key*”. Plug the USB Software Protection Key before running **NetDisturb**.

... and I will receive **CDROM & USB Software Protection Key** in a few days

In that case, choose the package “*Customers 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** in the following directory:
C:\Program Files\NetDisturb with the following subdirectories:

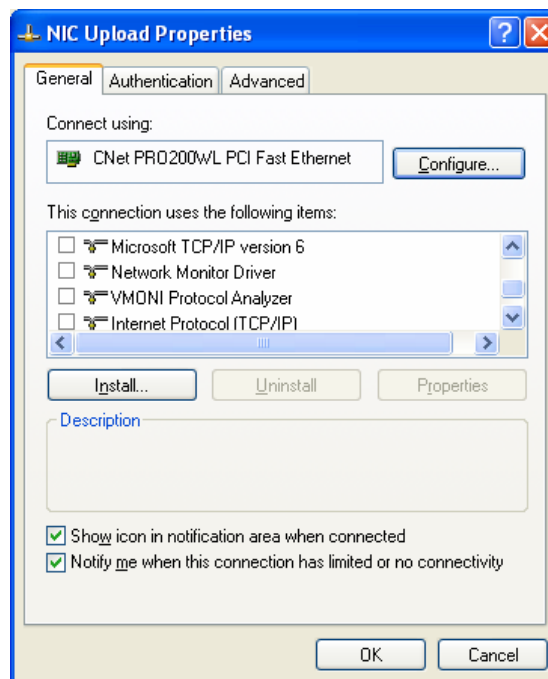
C:\Program Files\NetDisturb\Client
C:\Program Files\NetDisturb\Driver
C:\Program Files\NetDisturb\Server

3.7.1 IMPORTANT STEP: I must configure the driver 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

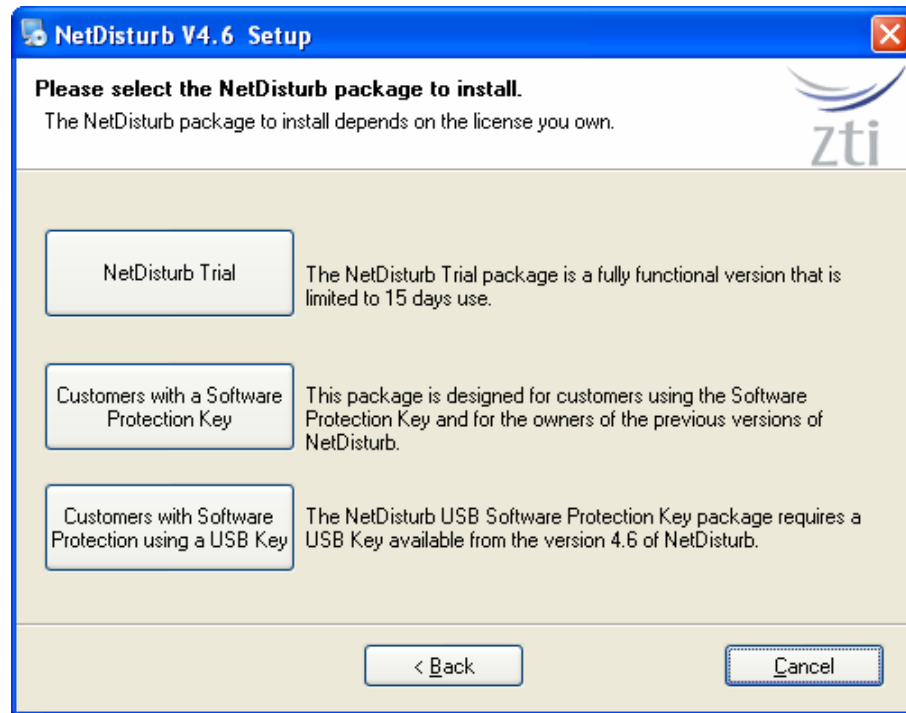
3.7.2 Start Menu Shortcuts Created

Start > All Programs > **NetDisturb**

- ⇒ **NetDisturb (start both Server and Client)**
- ⇒ **1) NetDisturb Server Only**
- ⇒ **2) NetDisturb Client Only**
- ⇒ **USB Key Viewer (USB Software Protection Key version only)**
- ⇒ **Uninstall NetDisturb**
- ⇒ **Read Me First**
- ⇒ **User Guide**

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?

Install the software on the target computer. You don't need to do any particular operation with the *"Customers with Software Protection using a USB Key"* and *"NetDisturb Trial"* packages.

With **NetDisturb** & USB Software Protection Key, you do need to plug the USB key before running the software on the target computer.

With the package *"Customers with a Software Protection Key"*, install the software on the target computer and refer to the 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

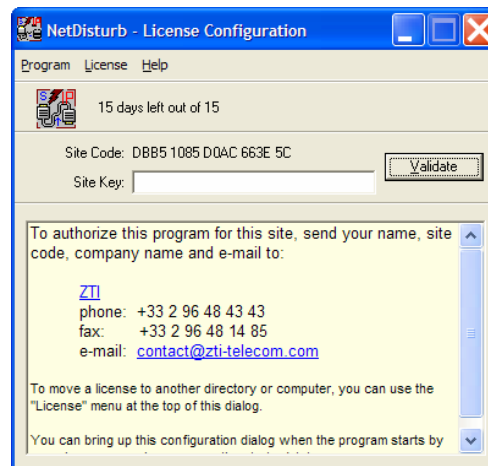


This software is licensed on a per workstation basis. This means that you will need to get a separate license for each machine you will install it on. Each licensed copy of the software installed on a system has a unique **Site Code** that requires a corresponding unique **Site Key** to work. A period 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:



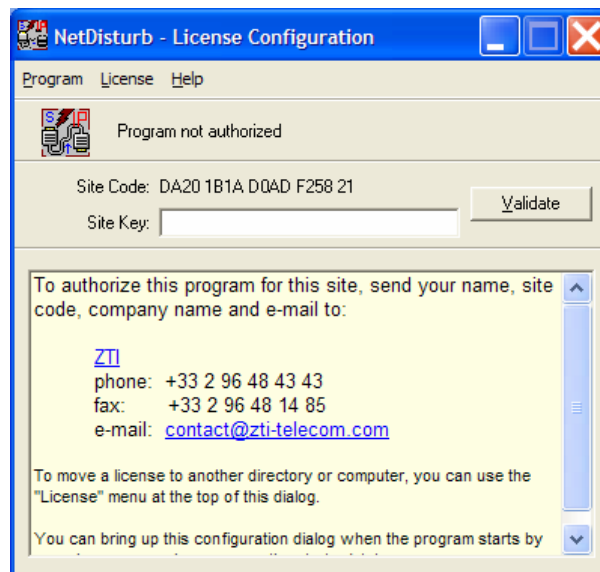
Then, you will see the following Software Protection Key configuration window:



*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.*

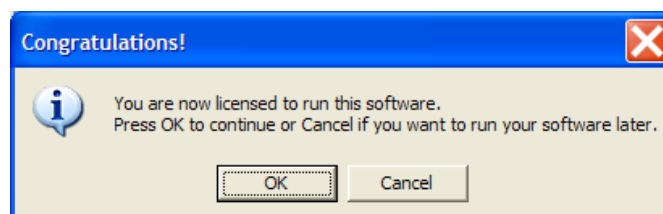
To get the **Site Key** and obtain a permanent license, please send an email to contact@zti-telecom.com or contact@zti.fr with the following information:

- 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.

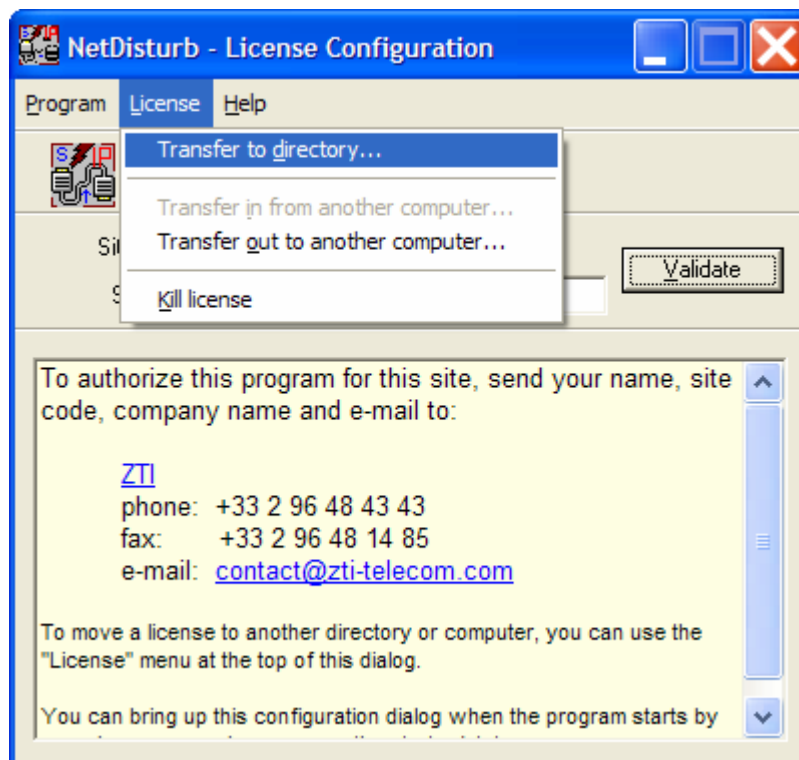
Software Protection Keys can be transferred using one of the following methods:

- ⇒ **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.

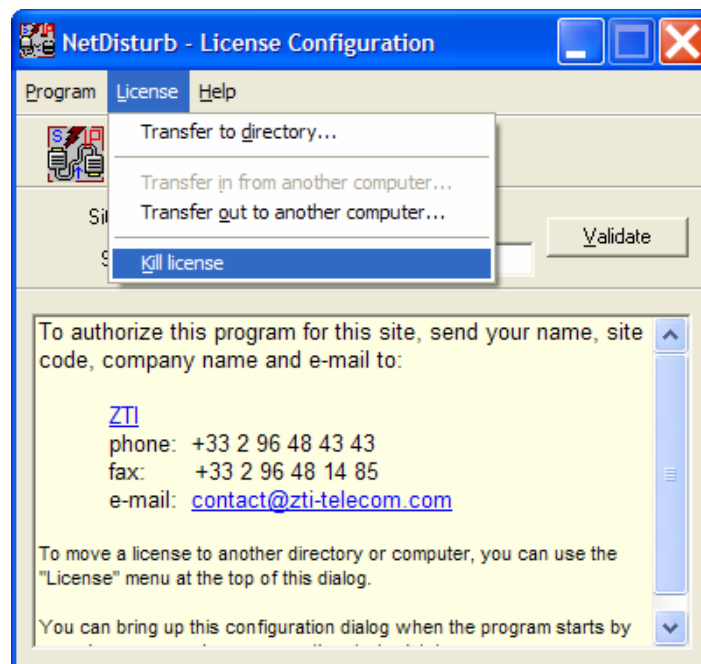
To transfer the Software Protection Key from the source PC (PC #1) to the target PC (PC #2), proceed as described in the following order:

- 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.

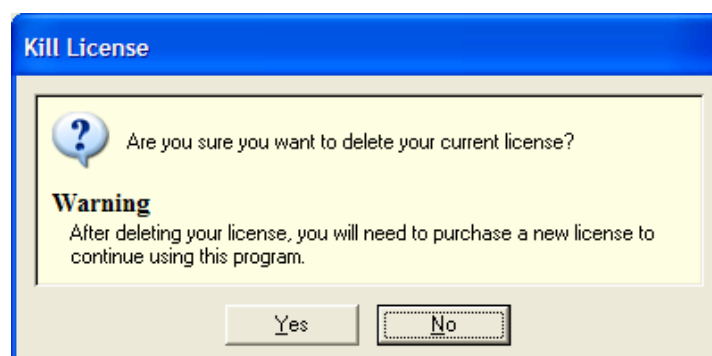
If the "Transfer in from another computer ..." item of the license menu is disabled, you must kill the Software Protection Key.

How to kill the Software Protection Key?

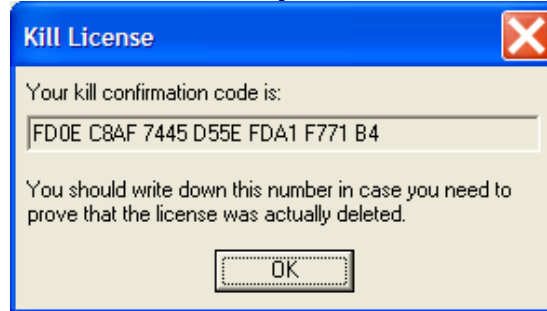
When the Software Protection Key configuration window appears, press **Enter** and select "License > Kill license" in the license menu.



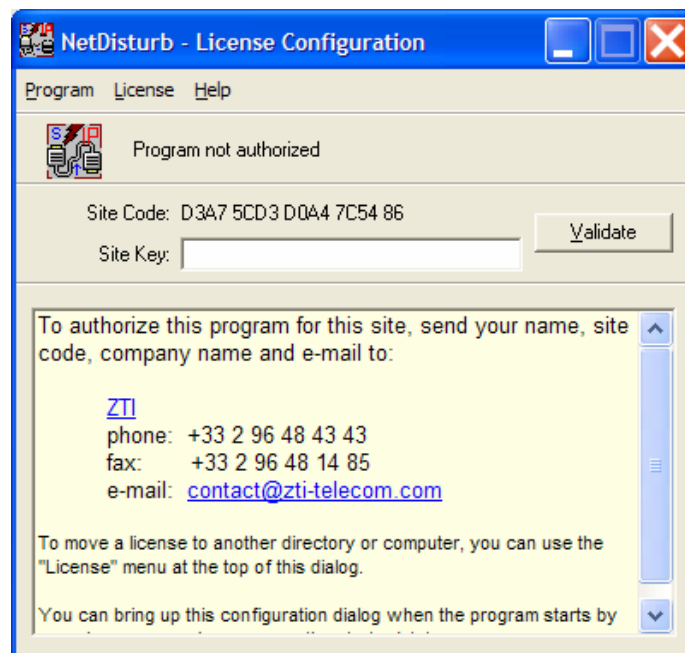
A message box will appear:



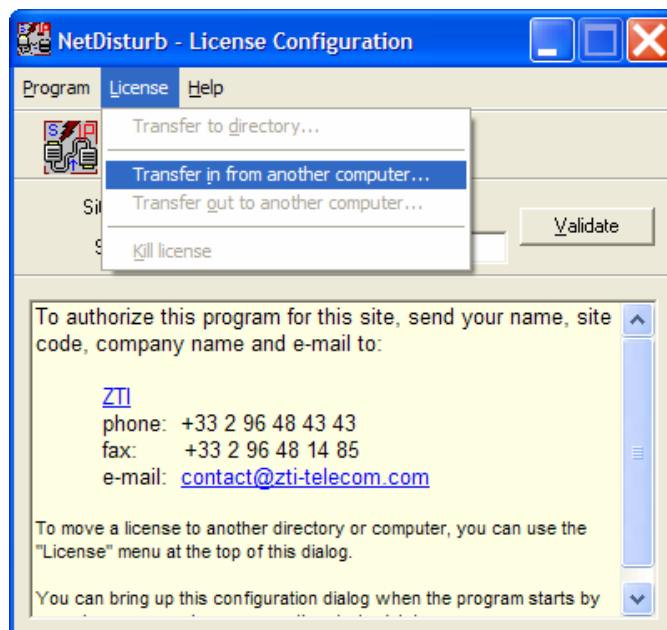
Press 'Yes' to kill the Software Protection Key and a confirmation code is displayed:



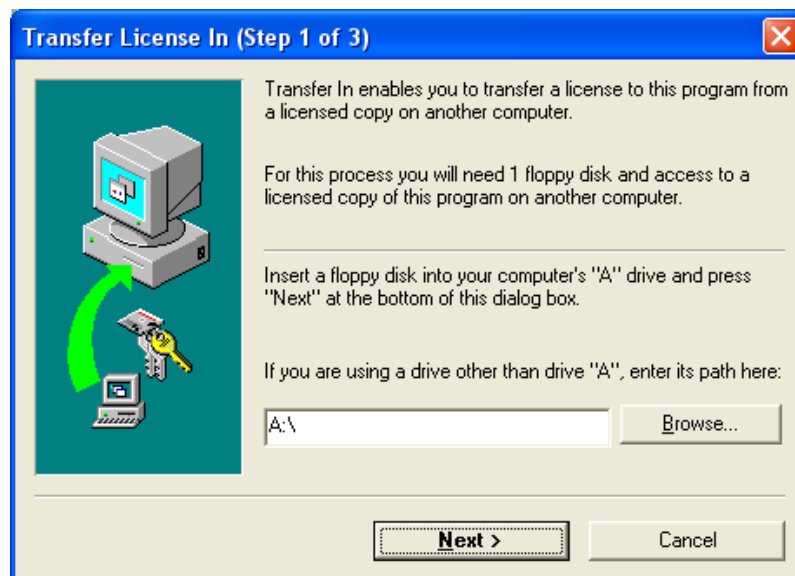
Click 'OK' and the Software Protection Key window displays now "Program not authorized":



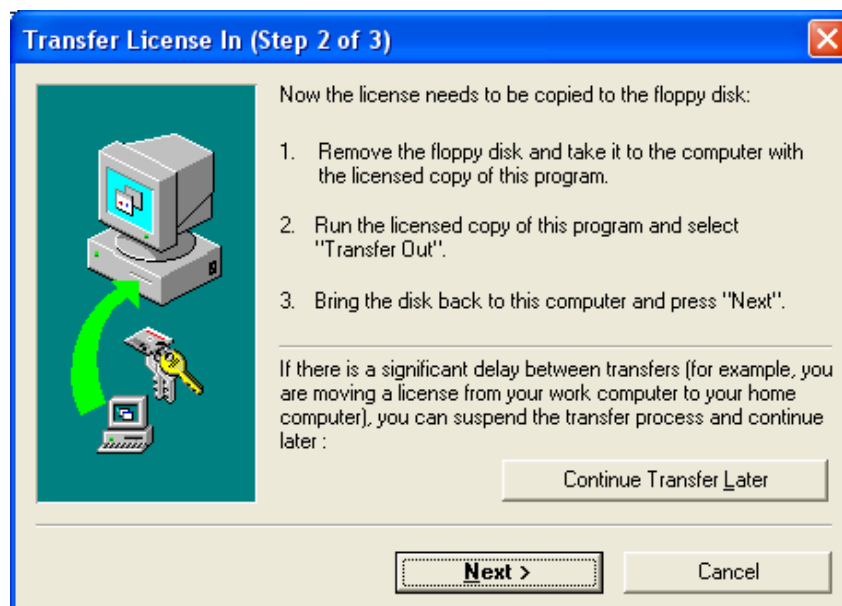
3) Select "License > Transfer in from another computer ..." from in the Software Protection Key License menu:



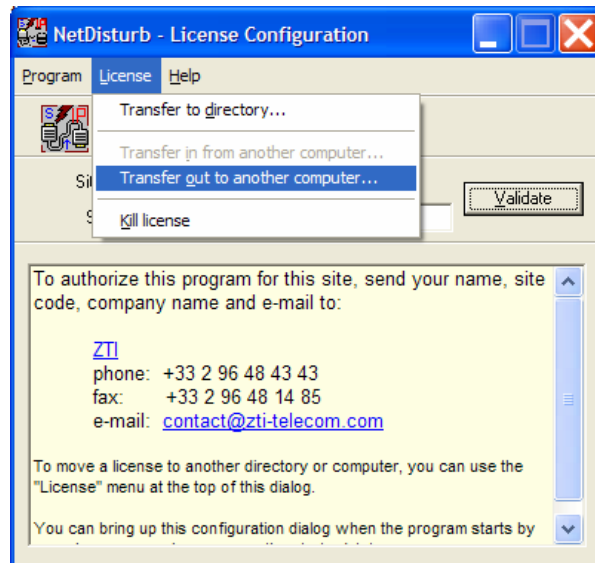
The "Transfer License In (Step 1 of 3)" window is displayed:



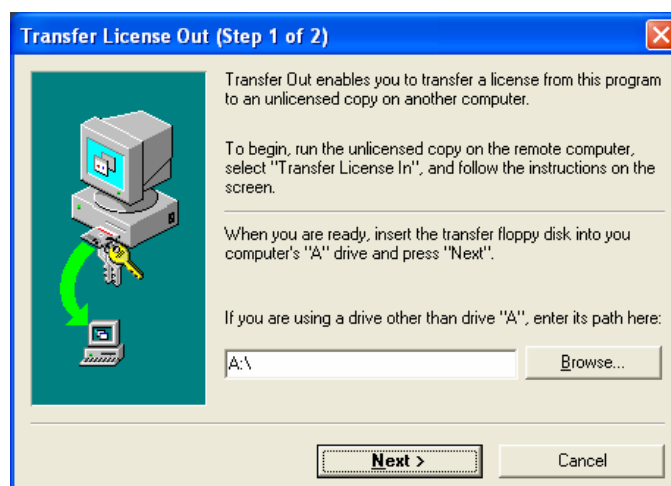
4) Insert a floppy disk or use a USB key as requested in step 1 of 3 and specify the path. Then press "Next >": the "Transfer License In (Step 2 of 3)" window is displayed:



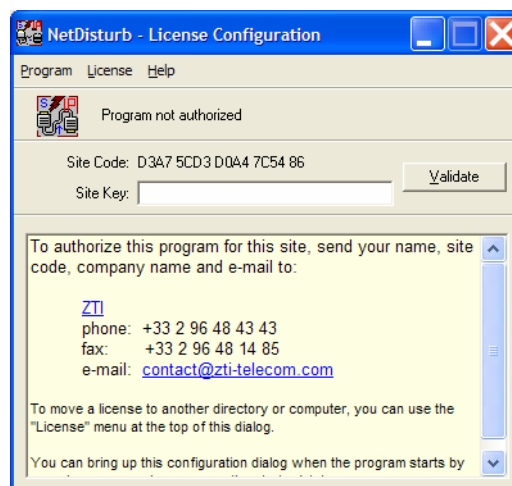
5) Go to the source PC (PC #1) and insert the media (USB key or floppy disk). Then start the program on PC #1. When the license configuration window appears, press **Enter** and select "License > Transfer out to another computer ..." as shown below:



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 on 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 the USB Software Protection key interests you, please contact the Sales Offices (sales@zti-telecom.com) to get some information about how to exchange your Site Key to a **USB Software Protection key**.

Part 5 Uninstall NetDisturb

To uninstall **NetDisturb**, please select “Uninstall NetDisturb” in the “Start > Programs > NetDisturb” menu.

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

Part 6 Run 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 this software in this order, click on:

Start ► All Programs ► NetDisturb ► NetDisturb (start both Server and Client)

6.1 First Run

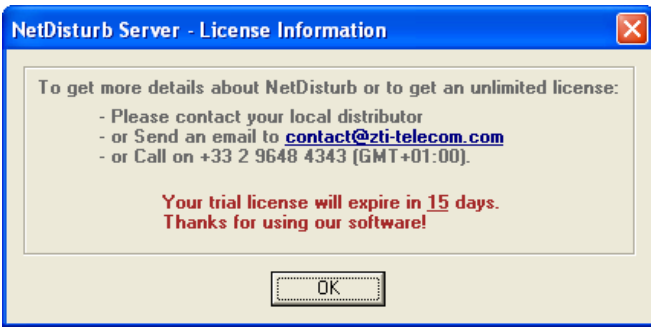

1) The NetDisturb Server startup

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



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 ► 1) NetDisturb Server Only**

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

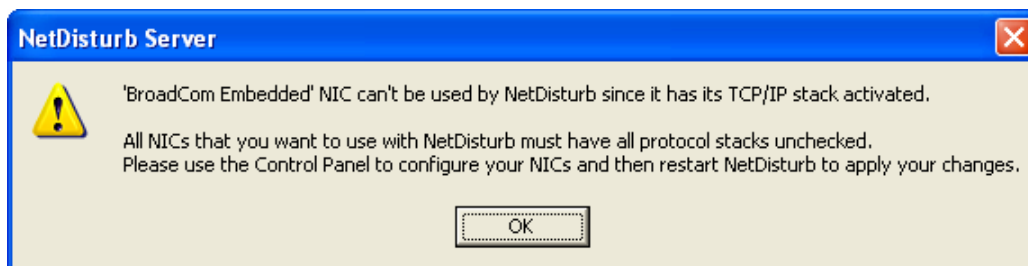
<i>fifteen-day trial version license</i>	<i>Software License version</i>
	
USB Software Protection key	
When you use a USB Software Protection key, there is no window!	

The next window displayed is **NetDisturb Server**

The screenshot shows the 'NetDisturb Server - Version 4.6' window. It is divided into several sections:

- Impairment Interface Configuration and Statistics:** This section is split into two columns for 'Interface A : not selected' and 'Interface B : not selected'. Each column contains input fields for '# Handled Packets:', '# Lost Packets:', '# Delayed Packets:', 'Desequenced:', and '# Fragmented packets:'. Below these are sections for 'Incoming on A/B' and 'Outgoing on A/B', each with fields for '# Packets per Second', '# Packets', and 'Throughput'. At the bottom of each column is a red bar with the text 'No transmission'. A 'Reset Counters' button is centered below the interface sections.
- Current Parameters:** This section contains input fields for 'Refresh Period (in second):', '# Buffers:', 'Sampling to Compute Throughputs:', 'Desequencing:', and 'Application of Laws:'.
- Current Client Connection:** This section shows 'Client: (No client connected)' and two buttons: 'Show Current Context' and 'Reset Logs'.
- A large text area at the bottom for logs or messages.

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




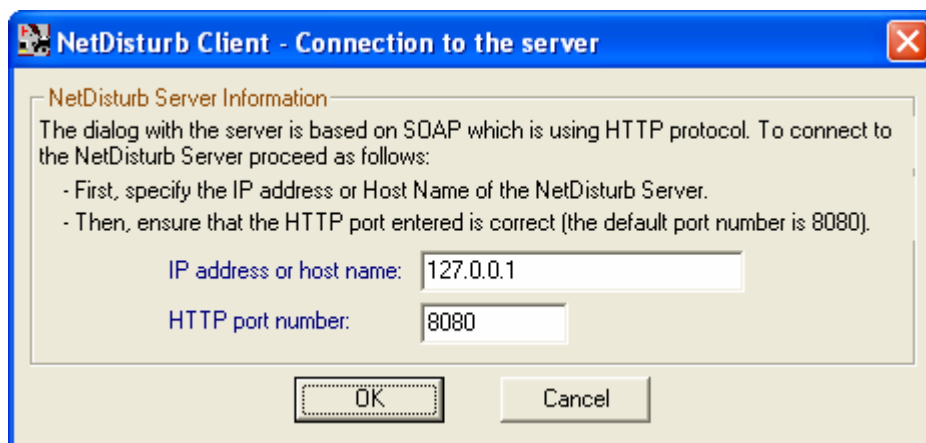
Use **NetDisturb** Client to select the network interfaces (or NICs).

2) NetDisturb Client startup

NetDisturb Client is started automatically when using the **NetDisturb (start both Server and Client)** 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** ► 2) **NetDisturb Client Only**. When **NetDisturb Client** starts, it will ask you to enter the parameters to connect to the **NetDisturb Server** machine:

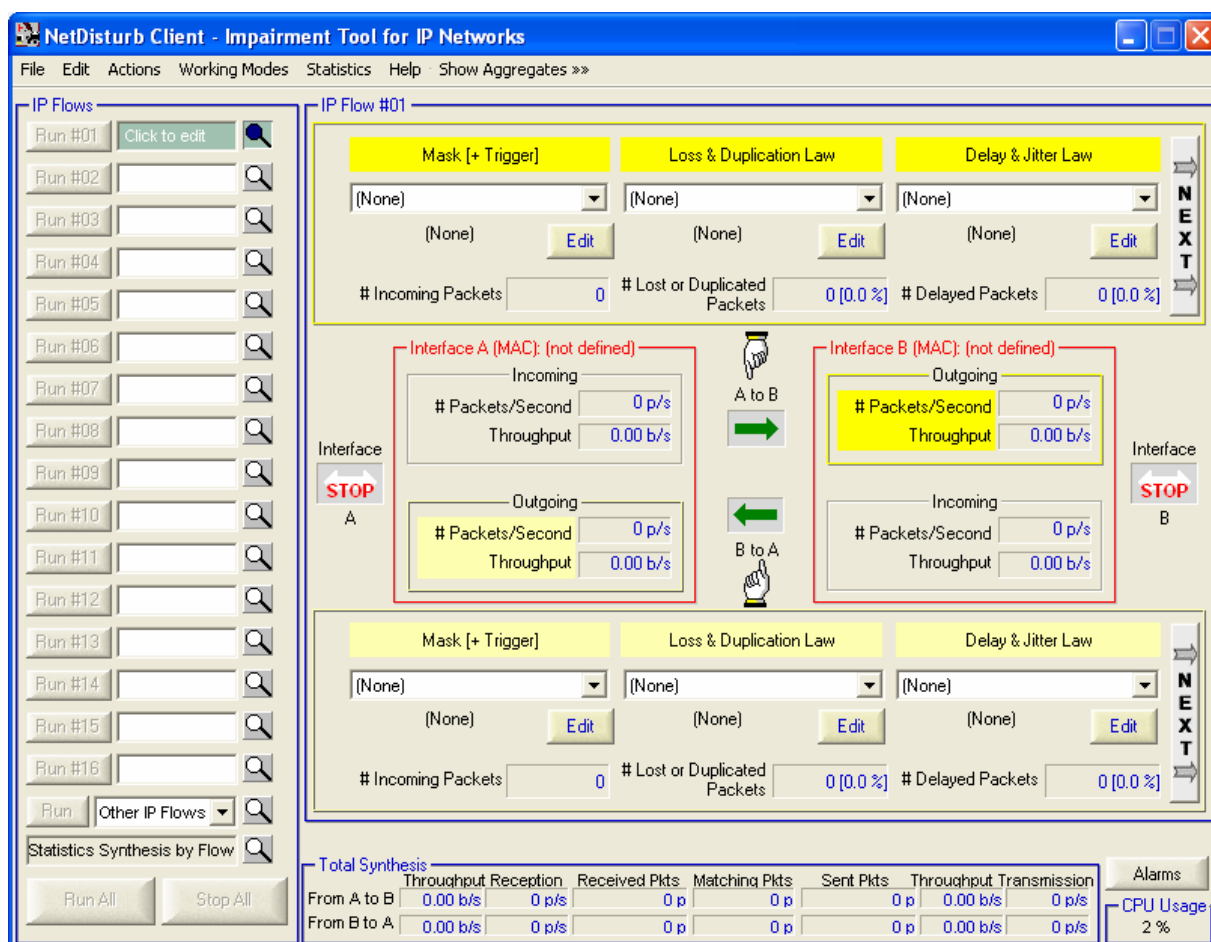




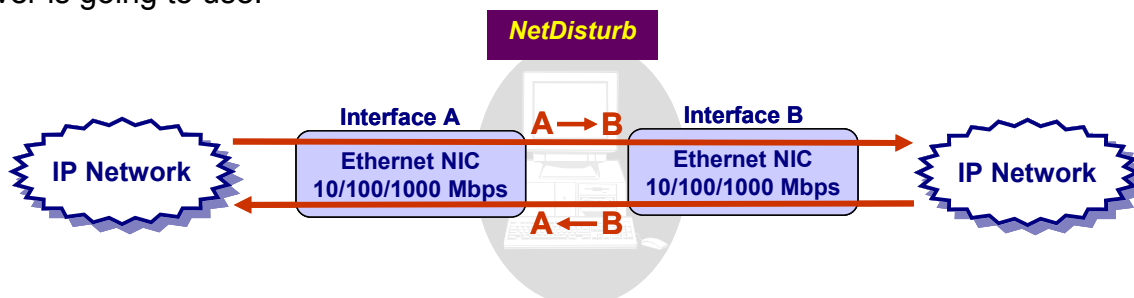
On the first run, there is no Interface defined. **NetDisturb Client** will tell you how to configure those 2 interfaces.



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. The Parameters configuration window is displayed:

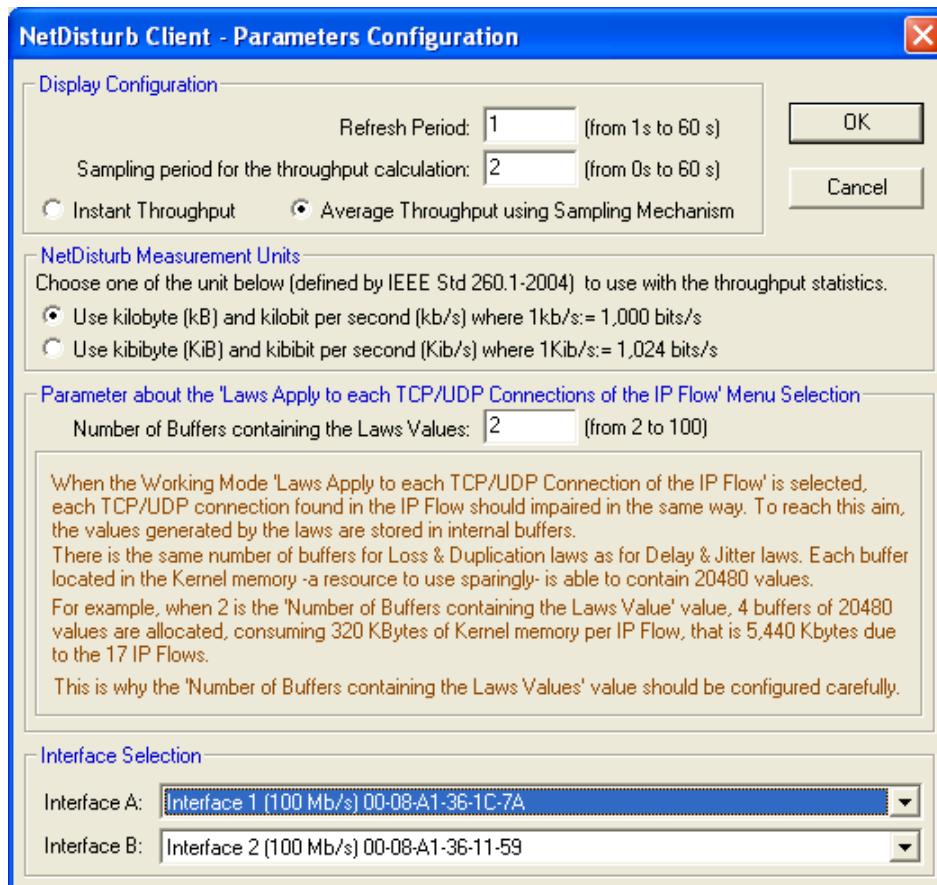
At the bottom of this window in the "Interface Selection" part, select one NIC for Interface A and another NIC for Interface B, and then confirm with “OK”.

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):

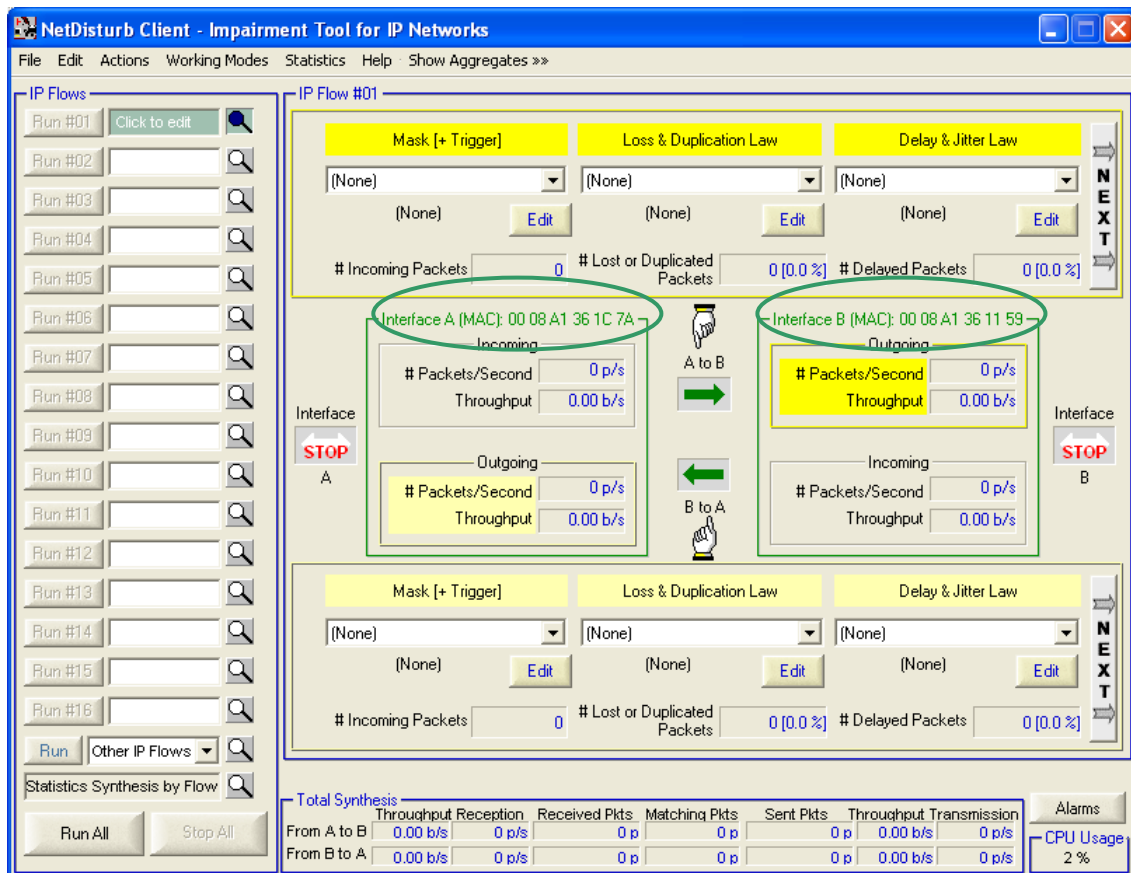


The image shows the 'NetDisturb Client - Parameters Configuration' dialog box. It has a blue title bar with a close button. The dialog is divided into several sections:

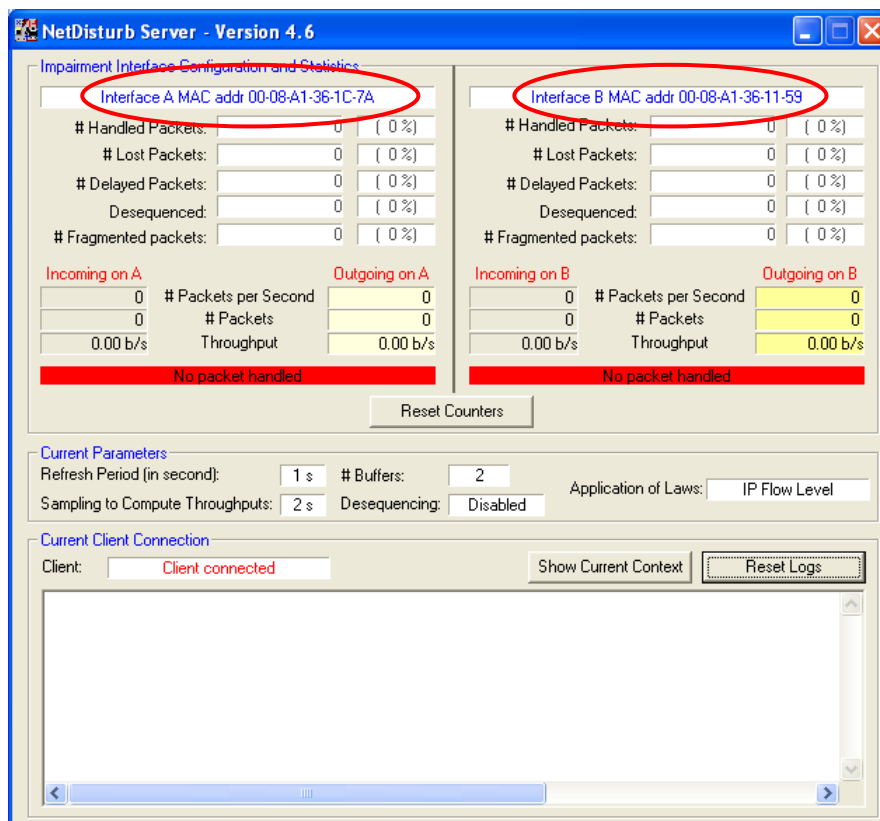
- Display Configuration:** Contains 'Refresh Period' (set to 1, range from 1s to 60s) and 'Sampling period for the throughput calculation' (set to 2, range from 0s to 60s). There are 'OK' and 'Cancel' buttons. Two radio buttons are present: 'Instant Throughput' (unselected) and 'Average Throughput using Sampling Mechanism' (selected).
- NetDisturb Measurement Units:** A section with a blue header. It says 'Choose one of the unit below (defined by IEEE Std 260.1-2004) to use with the throughput statistics.' There are two radio buttons: 'Use kilobyte (kB) and kilobit per second (kb/s) where 1kb/s:= 1,000 bits/s' (selected) and 'Use kibibyte (KiB) and kibibit per second (Kib/s) where 1Kib/s:= 1,024 bits/s' (unselected).
- Parameter about the 'Laws Apply to each TCP/UDP Connections of the IP Flow' Menu Selection:** Contains 'Number of Buffers containing the Laws Values' (set to 2, range from 2 to 100). Below this is a text box with orange text explaining the buffer mechanism and memory usage.
- Interface Selection:** Contains two dropdown menus. 'Interface A' is set to 'Interface 1 (100 Mb/s) 00-08-A1-36-1C-7A'. 'Interface B' is set to 'Interface 2 (100 Mb/s) 00-08-A1-36-11-59'.

As soon as the configuration is done, the **NetDisturb** Server recognizes “Interface A” and “Interface B”.

The MAC Addresses of the selected interfaces are displayed in the **NetDisturb** Client and **NetDisturb** Server windows:



Graphical user interface for the **NetDisturb** Client with two Ethernet NICs configured



Graphical user interface for the **NetDisturb** Server with two Ethernet NICs configured

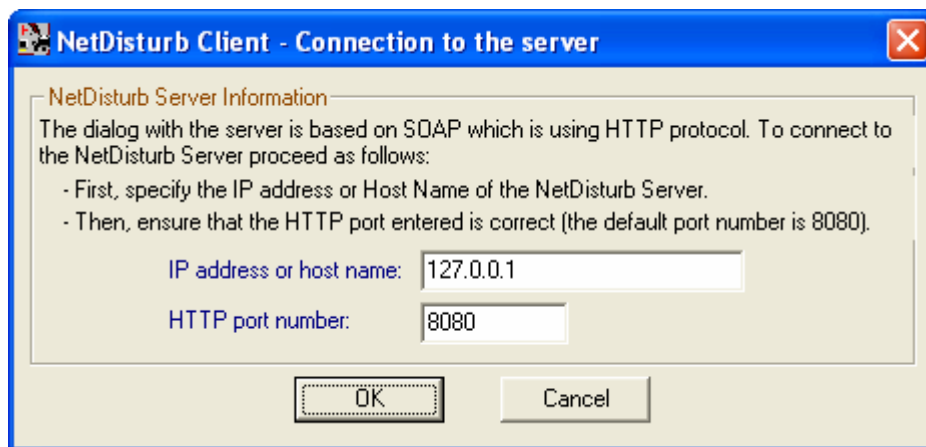
6.2 Detailed Description of the Server and Client Startup

6.2.1 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.

6.2.2 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:

1. The **NetDisturb** Server IP address
2. 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.

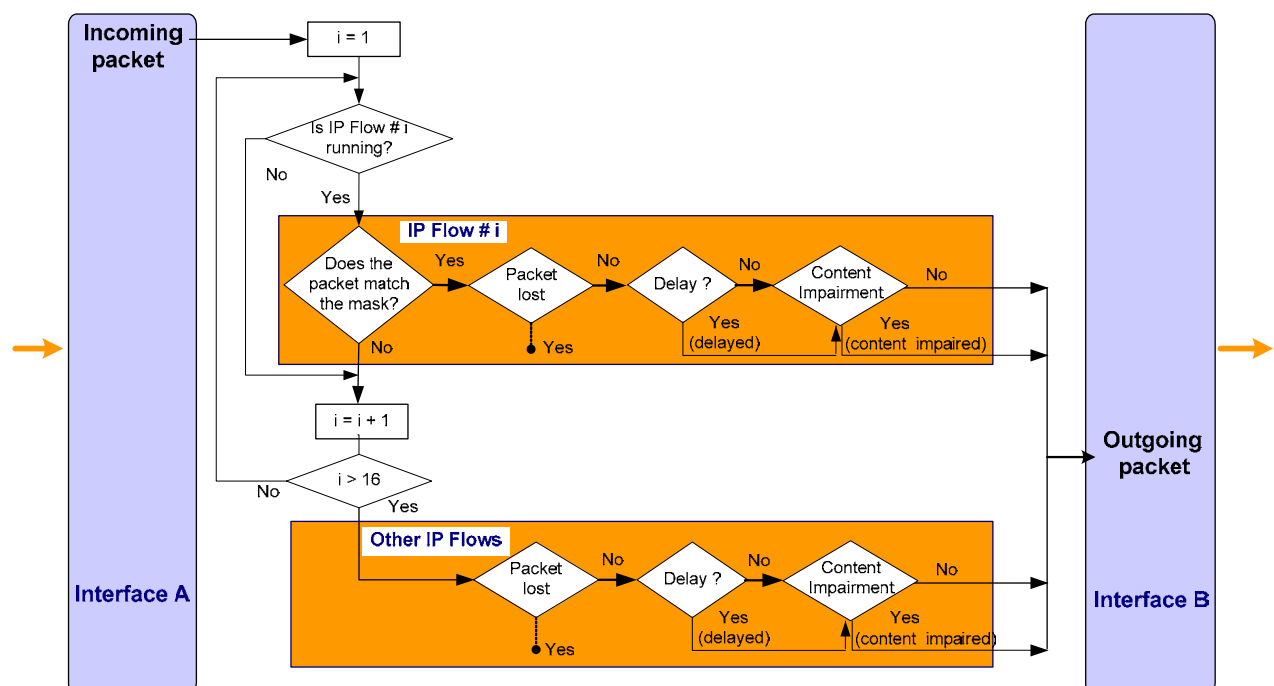


To use **NetDisturb**:

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

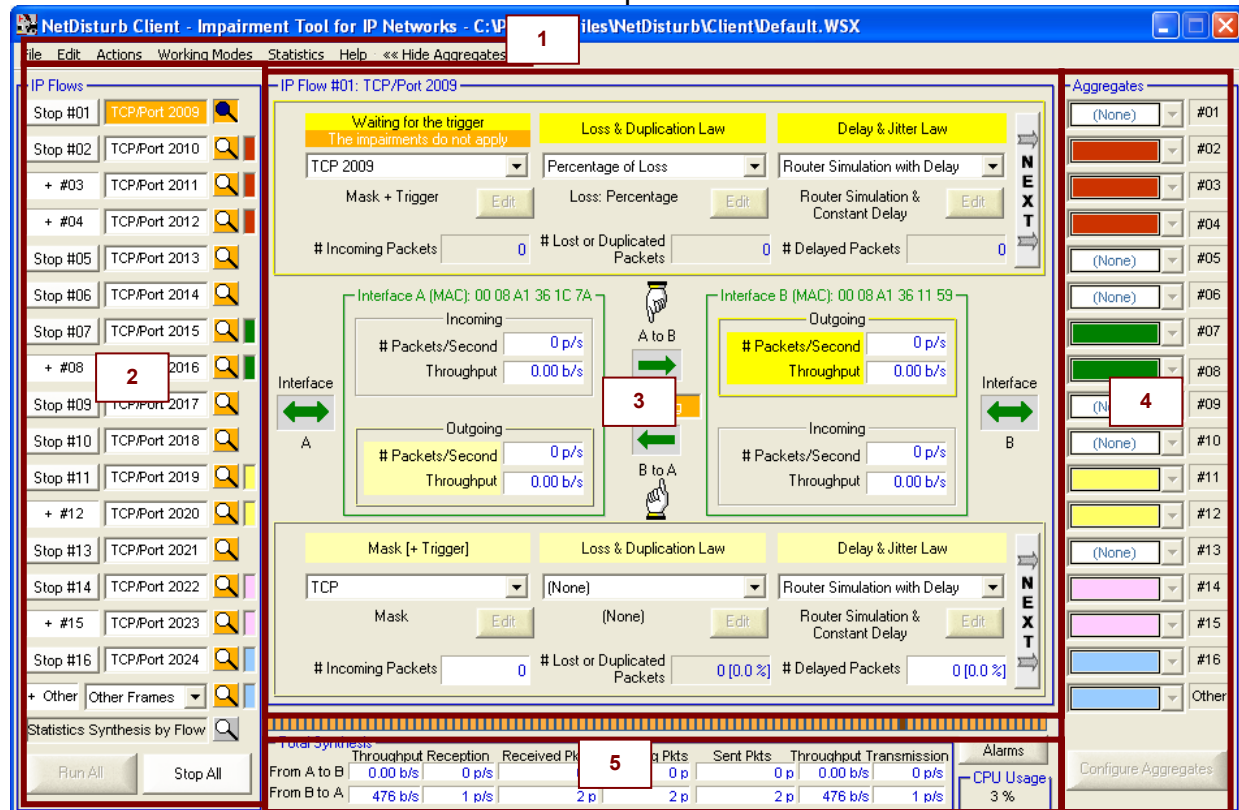
7.1 The NetDisturb Client Main Window

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)

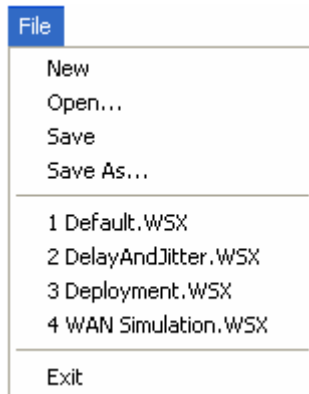
The **NetDisturb** Client main window is composed of five areas:



- **(1)** The menu is a standard application menu. The items of the menu are detailed in paragraph 7.2 Menu Description.
- **(2)** The 'IP Flows' area lists mnemonic-names of flows. This area is used to either start and to stop each IP Flow or to start and stop all flows at the same time. The magnify button is used to selected flow individually. The last two flows have a predefined behavior:
 - The "Other IP Flows"/"Other Frames" object allows applying specific loss, delay laws and content impairment laws to non-previously filtered IP packets.
 - The "Statistics Synthesis by Flow" magnify summarizes the flows #01 to #16. These areas are explained in paragraph 7.3.
- **(3)** This central-part shows traffic statistics on each IP 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 masks. The content impairment laws are available by clicking on the white and blue arrows located on the right side of this central-part.
- **(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 global statistics information is presented. 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.

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 Script folder of the **NetDisturb** Server directory.

A context file contains:

- The impairment parameters (selected mask & 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 version 4.4 contexts 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 version 4.4 contexts can't be used by an older version of **NetDisturb**.

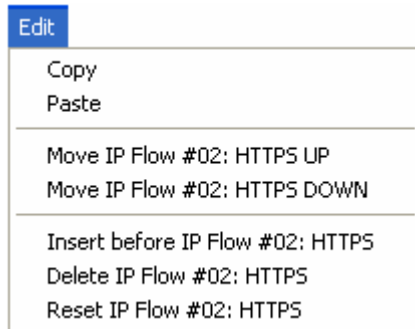
7.2.1.5 File/Recent Files

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 were 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 IP Flow into memory for further use. Copy includes the current selected Mask, Loss & Duplication Law, Delay & Jitter Law and Content Impairment Law for the both directions. The IP Flow mnemonic is also concerned.

7.2.2.2 Edit/Paste

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

7.2.2.3 Edit/Move xxx Up

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

7.2.2.4 Edit/Move xxx Down

The Move Down item moves the IP flow location to one position down. The Move Down item includes the item's mnemonic on which the operation applies. For example 'Move IP Flow #04 Down' switches IP Flow #04 with IP Flow #05, where the content of IP Flow #04 is moved into the fifth position, while the content of IP Flow #05 is moved into the fourth position. The IP 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 the IP Flow is not changed by an action from the Edit menu.

7.2.3 Actions Menu

Actions

Configuration
Reset Counters
Reset Server

7.2.3.1 Actions/Configuration

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

NetDisturb Client - Parameters Configuration

Display Configuration

Refresh Period: (from 1 s to 60 s)

Sampling period for the throughput calculation: (from 0 s to 60 s)

☐ Instant Throughput ☒ Average Throughput using Sampling Mechanism

NetDisturb Measurement Units

Choose one of the unit below (defined by IEEE Std 260.1-2004) to use with the throughput statistics.

☒ Use kilobyte (kB) and kilobit per second (kb/s) where 1kb/s:= 1,000 bits/s

☐ Use kibibyte (KiB) and kibibit per second (Kib/s) where 1Kib/s:= 1,024 bits/s

Parameter about the 'Laws Apply to each TCP/UDP Connections of the IP Flow' Menu Selection

Number of Buffers containing the Laws Values: (from 2 to 100)

When the Working Mode 'Laws Apply to each TCP/UDP Connection of the IP Flow' is selected, each TCP/UDP connection found in the IP Flow should impaired in the same way. To reach this aim, the values generated by the laws are stored in internal buffers. There is the same number of buffers for Loss & Duplication laws as for Delay & Jitter laws. Each buffer located in the Kernel memory -a resource to use sparingly- is able to contain 20480 values. For example, when 2 is the 'Number of Buffers containing the Laws Value' value, 4 buffers of 20480 values are allocated, consuming 320 KBytes of Kernel memory per IP Flow, that is 5,440 Kbytes due to the 17 IP Flows. This is why the 'Number of Buffers containing the Laws Values' value should be configured carefully.

Interface Selection

Interface A:

Interface B:

This window is divided in five parts: **Display configuration**, **Measurement Units**, **Parameter about the 'Working Mode / Laws apply to each TCP/UDP connection of the IP 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 1024 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 'Working Modes / Laws apply to each TCP/UDP connection of the IP 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 IP Flow" (see paragraph 7.2.4.2), i.e. each TCP/UDP connection found in the IP 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.



Data compression is useful when the **NetDisturb** Client and **NetDisturb** Server exchange. For example when 2 is the number of buffers, 8 buffers (2 per direction) of 20,480 values are allocated, consuming 640 Kbytes of kernel memory per IP Flow, that is 10,880 Kbytes due to the 17 IP Flows handled by NetDisturb. *That is why the 'Number of Buffers containing the Laws values' should be configured carefully.*



Content Impairment Laws are not concerned by the working modes.

⇒ Interface selection

This section allows selecting the Ethernet NIC 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 IP Flow, pending packets remain in the output queue.

7.2.4 Working Modes Menu

Working Modes	
<input type="checkbox"/>	Enable Desequencing Packets (Internet-like)
<input checked="" type="checkbox"/>	Disable Desequencing Packets (Ethernet-like)
<hr/>	
<input checked="" type="checkbox"/>	Laws to be applied to the IP Flow
<input type="checkbox"/>	Laws to be applied to each TCP/UDP Connection of the IP Flow

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 TCP or UDP connection they belong to. This mode makes possible to apply the same impairment values to each packet of each connection, e.g. to loose the third packet of each connection for example.

7.2.4.1 Working Modes/ Enable & Disable Desequencing Packets

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

The **NetDisturb** Driver can simulate an Internet network or can react as Ethernet does.

How **NetDisturb** creates an out-of-order 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 Desequencing Packets is selected?

When a packet should be sent before previous ones and the Desequencing 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 IP Flow or to each TCP/UDP Connection of the IP Flow

- Laws to be applied to the IP Flow

When the 'Laws Apply to the IP Flow' option is selected, every packet matching the masks 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 IP 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.

⇒ Buffers

The number of buffers defines the number of values (delay or loss) kept by the **NetDisturb** driver and used for each **Connection of an IP 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.

7.2.5 Statistics Menu



The **NetDisturb** Client statistics can be saved in a text file. The values saved are shown in the 'Statistics Synthesis' view (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 IP Flow in the statistics file.

7.2.5.1 Statistics/Start

Start to save statistics in the file. An abstract of each selected connection (Mask 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.

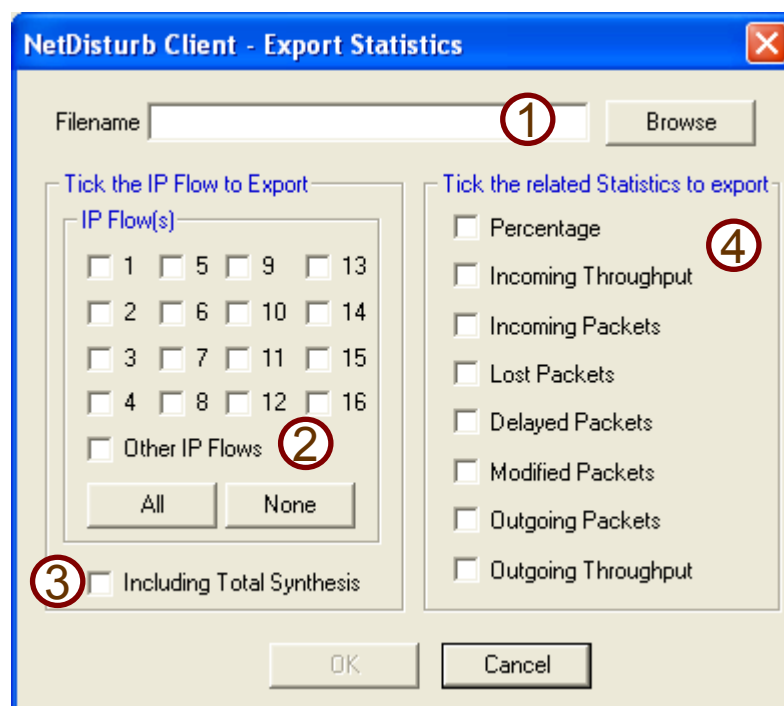
The throughput values are expressed in Kbps or Kibibit per second (More information are available in paragraph 7.2.3.1 Actions/Configuration)

7.2.5.2 Statistics/Stop

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

7.2.5.3 Statistics/Configuration

This option allows defining various configuration parameters.

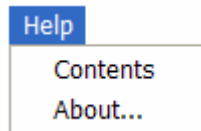


Statistics can start if at least the filename, one flow and one Statistics item are selected.

- **(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 IP Flow(s) to Export:** This section is used to select IP Flows to include in the statistics file. IP Flow #01 to IP Flow #16, plus the "Other IP Flows" can be selected. The Total Synthesis **(3)** refers to the bottom part of the Client Windows (Part 7 in the detailed description 7.1).
- **(3) Include the Total Synthesis:** This option is used 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:
 - Rx (Receive) and Tx (Transmit) Throughput
These statistics include the volume throughput (in kb/s or Kib/s) and the packet throughput (packet per second).
 - Packets Filtered, Lost, Delayed or Modified
These statistics include the number of packets and the percentage.
 - Packet Sent
This statistic includes the number of packets.

7.2.6 Help Menu



7.2.6.1 Help/Contents

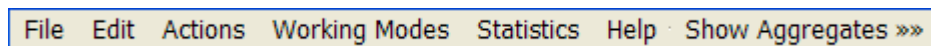
This command opens the **NetDisturb** User Guide as a PDF file. So you need a PDF reader to view the contents.

7.2.6.2 Help/About

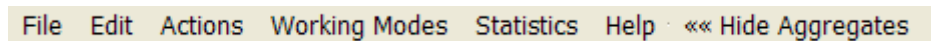
This command displays the version number and copyright of the software.

7.2.7 Hide or Show Aggregates Menu

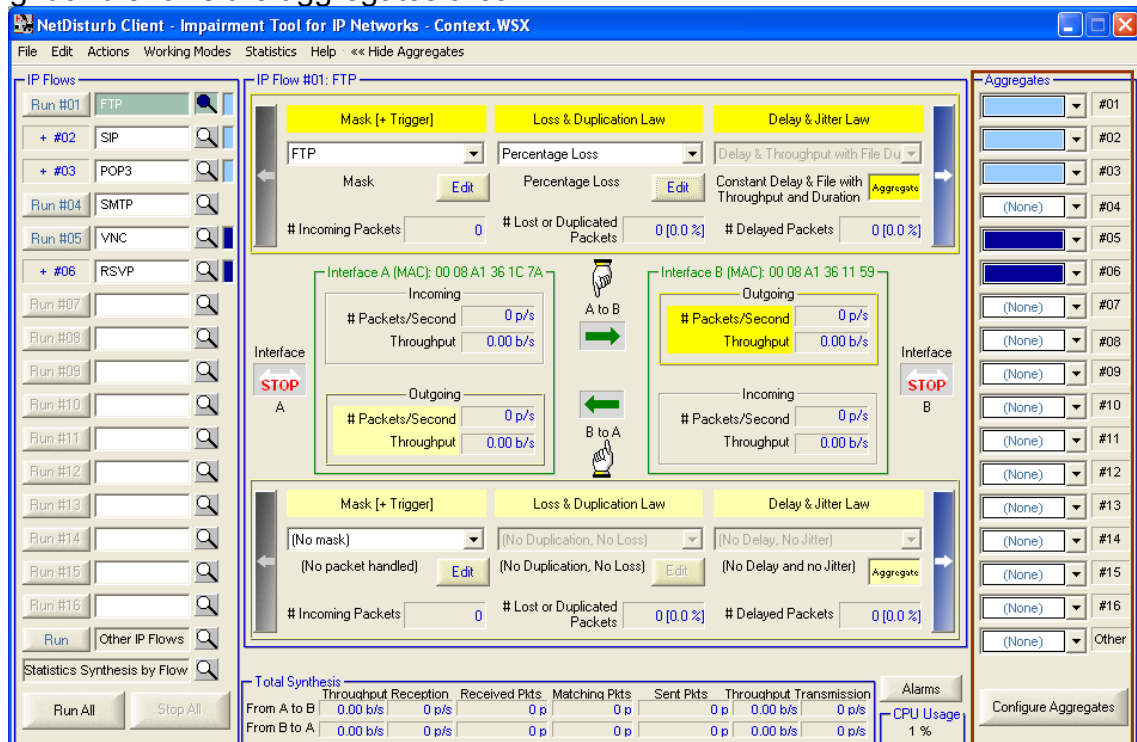
This menu has two states:



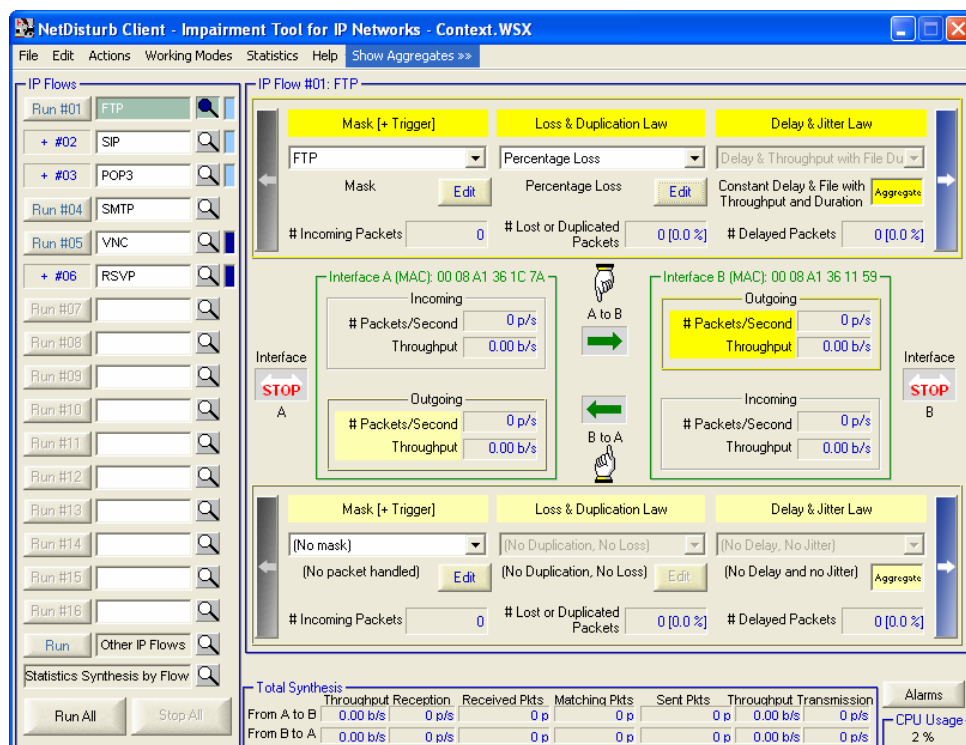
Or



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



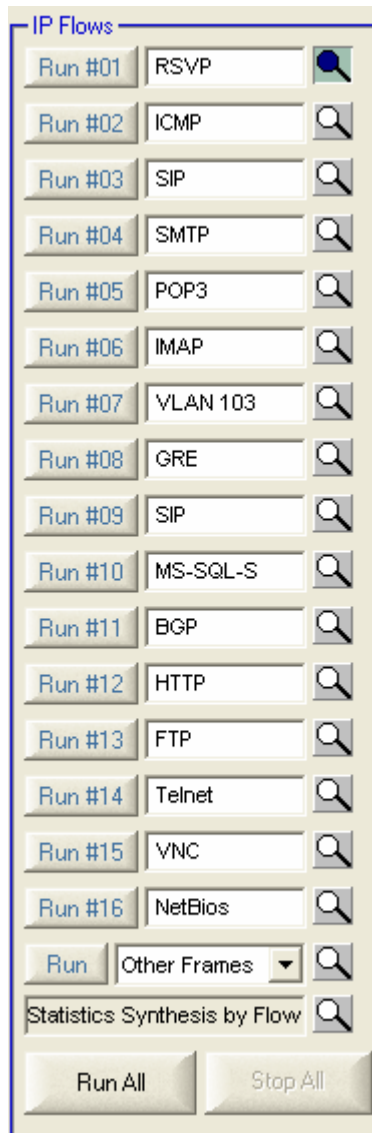
By clicking on the 'Hide Aggregates' menu, the **NetDisturb** Client window is reduced by hiding the aggregates area:



7.3 The IP Flows

This section describes the IP Flow Client part area.

7.3.1 General Description



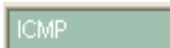
Left buttons (Run #xx/Stop #xx)



Each IP Flow can be started or stopped individually.

The button 'Run/Stop #xx' indicates the status of the IP Flow will get if the button is pressed. This button is grayed when Interface A and B aren't defined.

Edit area



IP Flow #01 to IP Flow #16 can be named with a mnemonic that helps to remember impairment parameters or filter mask used.

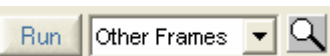
Magnify buttons



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

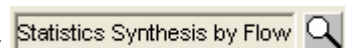
The color changes to show the current status of the flow.

Ethernet/IP Frames



The "Other IP Flows"/"Other Frames" Flow is in charge to handle the remaining traffic that wasn't filtered by the previous IP Flows. It can't be renamed: its specific characteristics are described in paragraph 7.3.3.

Statistics Synthesis flow



When selecting this view by pressing the magnify button, the user can get an abstract of the activity of all flows. Details can be found in paragraph 7.3.4

Bottom buttons



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

The 'Stop All' button stops all running IP Flows.

7.3.2 Status of the IP Flows

Idle status

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



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



Active Status

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



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



7.3.3 The “Other Frames”/“Other IP Flows”

This object is in charge to handle the remaining traffic. This is why the filter mask isn't available for this Flow.

The traffic filtered by this flow could be one of the following:

	<p>The traffic 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.</p>
	<p>The traffic 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.</p>



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

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

The colored rules described in paragraph 7.3.2 are relevant to this object.

7.3.4 The Statistics Synthesis View

To get this view you have to press the magnify button of the 'Statistics Synthesis by Flow' item.

NetDisturb Client - Impairment Tool for IP Networks - C:\Program Files\NetDisturb\Client\Default.WSX

File Edit Actions Working Modes Statistics Help Show Aggregates >>

IP Flows

Run #01 RSVP

Run #02 ICMP

Run #03 SIP

Run #04 SMTP

Run #05 POP3

Run #06 IMAP

Run #07 VLAN 103

Run #08 GRE

Run #09 SIP

Run #10 MS-SQL-S

Run #11 BGP

Run #12 HTTP

Run #13 FTP

Run #14 Telnet

Run #15 VNC

Run #16 NetBios

Run Other IP Flows

Statistics Synthesis by Flow

Run All Stop All

	%	INCOMING THROUGHPUT	INCOMING P...	LOST PACKETS	DELAYED PACKETS	MODIFIED PACKETS
#01 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#01 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#02 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#02 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#03 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#03 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#04 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#04 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#05 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#05 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#06 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#06 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#07 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#07 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#08 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#08 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#09 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#09 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#10 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#10 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#11 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#11 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#12 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#12 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#13 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#13 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#14 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#14 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#15 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#15 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#16 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#16 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]

Total Synthesis

	Throughput	Reception	Received Pkts	Matching Pkts	Sent Pkts	Throughput	Transmission
From A to B	0.00 b/s	0 p/s	0 p	0 p	0 p	0.00 b/s	0 p/s
From B to A	0.00 b/s	0 p/s	0 p	0 p	0 p	0.00 b/s	0 p/s

Alarms

CPU Usage 2 %

On this screenshot no IP Flow is running.

Detailed Description:

	%	INCOMING THROUGHPUT	INCOMING P...	LOST PACKETS	DELAYED PACKETS	MODIFIED PACKETS
#01 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]
#01 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]

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 Interface A to Interface B 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).

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 mask (or 'Interface B' for the second line respectively).

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

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

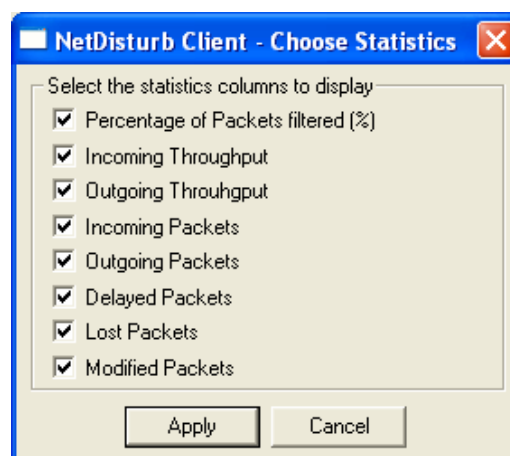
Delayed Packets: This column presents the number of packet delay, and the percentage of those packets regarding the global number of packets filtered (**Incoming Packets** column), for the relevant direction.

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.

Outgoing Packets: This column presents the number of packet 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.

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 IP Flows are active, corresponding lines are colored as shown below:

- The yellow color is related to the A→B direction
- The white color is related to the B→A direction

NetDisturb Client - Impairment Tool for IP Networks - context UDP 2009-2024.WSX

File Edit Actions Working Modes Statistics Help Show Aggregates >>

IP Flows

- Stop #01 UDP/Port 2009
- Run #02 UDP/Port 2010
- Stop #03 UDP/Port 2011
- Run #04 UDP/Port 2012
- Stop #05 UDP/Port 2013
- Run #06 UDP/Port 2014
- Stop #07 UDP/Port 2015
- Run #08 UDP/Port 2016
- Stop #09 UDP/Port 2017
- Run #10 UDP/Port 2018
- Stop #11 UDP/Port 2019
- Run #12 UDP/Port 2020
- Stop #13 UDP/Port 2021
- Run #14 UDP/Port 2022
- Stop #15 UDP/Port 2023
- Run #16 UDP/Port 2024
- Stop Other IP Flows

Statistics Synthesis by Flow

Run All Stop All

	%	INCOMING THR...	INCOMI...	LOST PACKETS	DELAYED PAC...	MODIFIED PA...	OUT...	OUTGOING THROU...
#01 A to B	6	587 Kb/s	50 p/s	4352	2613 [60 %]	1739 [40 %]	1738	214 Kb/s 18 p/s
#01 B to A	2	193 Kb/s	17 p/s	1565	0 [0.0 %]	1565 [100 %]	1565	193 Kb/s 17 p/s
#02 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#02 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#03 A to B	6	589 Kb/s	51 p/s	4354	524 [12 %]	0 [0.0 %]	3830	519 Kb/s 45 p/s
#03 B to A	6	519 Kb/s	45 p/s	3830	2297 [60 %]	0 [0.0 %]	1533	210 Kb/s 18 p/s
#04 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#04 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#05 A to B	6	587 Kb/s	50 p/s	4351	524 [12 %]	3827 [88 %]	3826	506 Kb/s 43 p/s
#05 B to A	6	506 Kb/s	43 p/s	3826	190 [5.0 %]	0 [0.0 %]	3636	485 Kb/s 41 p/s
#06 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#06 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#07 A to B	6	583 Kb/s	50 p/s	4353	0 [0.0 %]	4353 [100 %]	4352	583 Kb/s 50 p/s
#07 B to A	7	587 Kb/s	50 p/s	4352	522 [12 %]	0 [0.0 %]	3830	511 Kb/s 44 p/s
#08 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#08 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#09 A to B	6	587 Kb/s	50 p/s	4352	2556 [59 %]	0 [0.0 %]	1796	219 Kb/s 19 p/s
#09 B to A	3	219 Kb/s	19 p/s	1796	0 [0.0 %]	5 [0.3 %]	1796	219 Kb/s 19 p/s
#10 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#10 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#11 A to B	6	587 Kb/s	50 p/s	4351	219 [5.0 %]	0 [0.0 %]	4132	558 Kb/s 48 p/s
#11 B to A	7	558 Kb/s	48 p/s	4132	206 [5.0 %]	0 [0.0 %]	3926	531 Kb/s 46 p/s
#12 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#12 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#13 A to B	6	587 Kb/s	50 p/s	4353	0 [0.0 %]	0 [0.0 %]	4353	587 Kb/s 50 p/s
#13 B to A	7	587 Kb/s	50 p/s	4353	0 [0.0 %]	0 [0.0 %]	4353	587 Kb/s 50 p/s
#14 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#14 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#15 A to B	6	593 Kb/s	51 p/s	4352	0 [0.0 %]	4352 [100 %]	4351	593 Kb/s 51 p/s
#15 B to A	7	568 Kb/s	49 p/s	4133	0 [0.0 %]	4133 [100 %]	4132	565 Kb/s 48 p/s
#16 A to B	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
#16 B to A	0	0.00 b/s	0 p/s	0	0 [0.0 %]	0 [0.0 %]	0	0.00 b/s 0 p/s
..... A to B	50	4.58 Mb/s	400 p/s	34845	0 [0.0 %]	0 [0.0 %]	34845	4.58 Mb/s 400 p/s
..... B to A	55	4.58 Mb/s	400 p/s	34849	0 [0.0 %]	0 [0.0 %]	34849	4.58 Mb/s 400 p/s

Total Synthesis

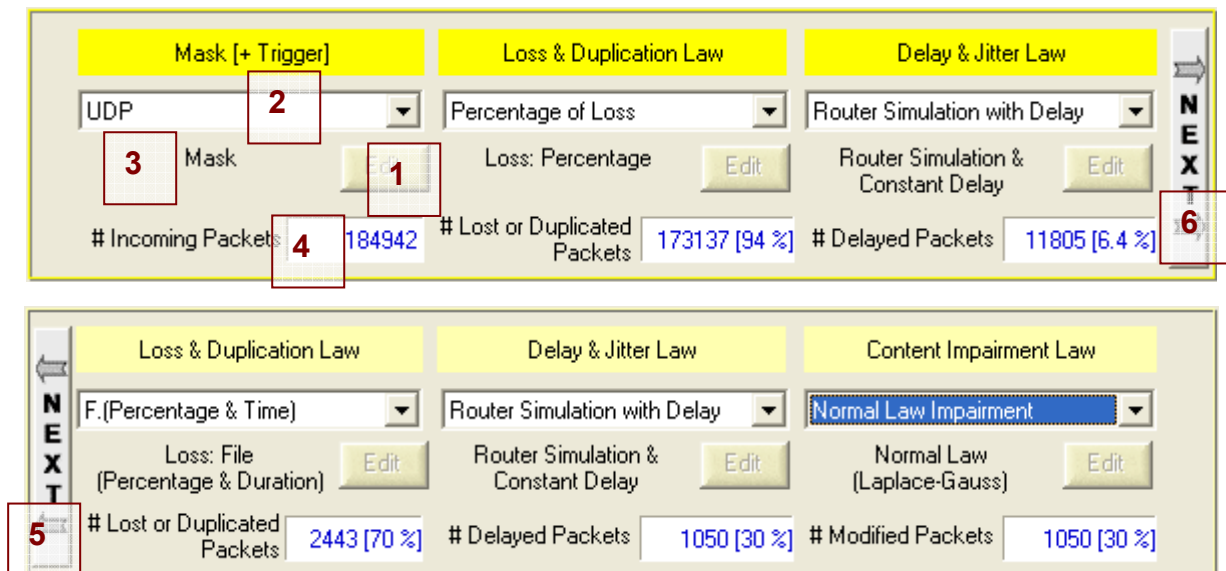
	Throughput Reception	Received Pkts	Matching Pkts	Sent Pkts	Throughput Transmission
From A to B	9.17 Mb/s	800 p/s	69664 p	63224 p	8.27 Mb/s
From B to A	8.23 Mb/s	719 p/s	62837 p	59620 p	7.81 Mb/s

Alarms

CPU Usage 61 %

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 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.



Top area of the main Client window

This area is separated in four sections:

- ⇒ Mask [+ Trigger]
- ⇒ Loss & Duplication Law
- ⇒ Delay & Jitter Law
- ⇒ Content Impairment Law

Each section is composed of 6 objects:

- (1) The Edit button allows defining and modifying the mask or the impairment law.
- (2) The combo-box allows selecting the defined mask or law
- (3) The resume of the mask or law selected in the combo-box
- (4) A label and a counter showing the number of packets processed
- (5) The left arrow allows showing the Mask area
- (6) The right arrow allows hiding the mask area and displaying the Content Impairment area

• Mask [+ Trigger]

On the left part, the IP Filter mask is presented. This parameter allows selecting packets to process and eventually a trigger to apply. The number of packets that match the mask is displayed (# Incoming Packets) below the list box.

• Loss & Duplication Law

This central part presents the loss and/or duplication law applied to the selected packets. With a loss law, it displays the number of lost packets and the ratio of packets lost on the number of filtered packets for the current IP Flow. With a duplication law, it 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 IP 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.

- **Delay & Jitter Law**

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

- **Content Impairment Law**

By clicking on the left white and blue arrow button, NetDisturb presents the content impairment law applied to the filtered packets that were not lost. The number of modified packets and the percentage of modified packets on number of filtered & no lost packets are displayed.



Once created a new mask 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 Mask or an Impairment Law

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

7.4.2 The Mask [+ Trigger] Configuration

A mask is a set of parameters to select the packets that would be impaired.

A mask is composed of a combination of several items where each one of them is optional (except the Frame Type):

- Frame Type (ARP Frame or IP Frame: IPv4 or IPv6 or IPv4 & IPv6): mandatory
- MAC header:
 - MAC Destination address (with the operators 'Equal' and 'Different')
 - MAC Source Address (with the operators 'Equal' and 'Different')
 - VLAN-ID list (802.1Q) (with the operators 'Equal' and 'Different')
- IP header:
 - IP Destination address (with the operators 'Equal' and 'Different')
 - IP Source Address (with the operators 'Equal' and 'Different')
 - Protocol (with the operators 'Equal' and 'Different')
 - Differentiated Services or ToS (with the operators 'Equal' and 'Different')
- Ports (only available with the UDP or TCP protocol):
 - Destination Port List (with the operators 'Equal' and 'Different')
 - Source Port List (with the operators 'Equal' and 'Different')
- Optional Trigger condition (only available if the IP Flow doesn't belong to an aggregate) with 3 parameters:
 - **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** to set the trigger condition.

When the Trigger condition occurs the following parameters are considered before applying the impairments.

- Trigger parameters:
 - **Delay** before applying the impairments
 - **Impair or not the frame** that has triggered
 - **Duration** of the impairments
 - **Number of cycles** for the trigger

The format for the parameters with a **list** (i.e. VLAN list or Port list) is detailed in the paragraph 7.4.2.5.

By default, the following IPv4 masks are included with the default context called 'Default.wsx':

Combo-box	Comment area	Description
(None)	<i>No parameter</i>	This mask disables the IP Flow because no packet can match a Mask without selection criteria.
TCP	Mask	This filter considers only IP packets with a protocol set to TCP.
UDP	Mask	This filter considers only IP packets with the UDP protocol.
HTTP	Mask	This filter considers IP packets with the TCP protocol and the destination ports 80 or 8080.
HTTPS	Mask	This filter considers IP packets with the TCP protocol and the destination port 443.
ICMP	Mask	This filter considers only IP packets with ICMP (01) protocol.
SMTP	Mask	This filter considers IP packets with the TCP protocol and the destination port 25.
NETBIOS	Mask	This filter considers IP packets with the TCP protocol and destination ports 137, 138 or 139.
VoIP	Mask	This filter considers IP packets with the UDP protocol and the destination port 1250.
TFTP	Mask	This filter considers IP packets with the UDP protocol and the destination port 69.
VNC	Mask	This filter considers IP packets with the TCP protocol and destination port 5900.
Printer/Port	Mask	This filter considers IP packets with the TCP protocol and destination port 9100.
TELNET	Mask	This filter considers IP packets with the TCP protocol and the destination port 23.
GRE	Mask	This filter considers IP packets with the GRE (x2F) protocol.
SIP	Mask	This filter considers IP packets with the SIP (x29) protocol

(continue)

FTP	Mask	This filter considers IP packets with the TCP protocol and the destination ports 20 or 21.
BGP	Mask	This filter considers IP packets with the TCP protocol and destination port 179.
MS-SQL-S	Mask	This filter considers IP packets with the destination port 1433.
VLAN	Mask	This filter considers IP packets when the VLAN ID is included between 1 and 5.
POP3	Mask	This filter considers IP packets with the TCP protocol and the destination port 110.
NTP	Mask	This filter considers IP packets with the TCP protocol and the destination port 123.
RSVP	Mask	This filter considers IP packets with the RSVP (x2E) protocol.
SCTP	Mask	This filter considers IP packets with the SCTP (x84) protocol.

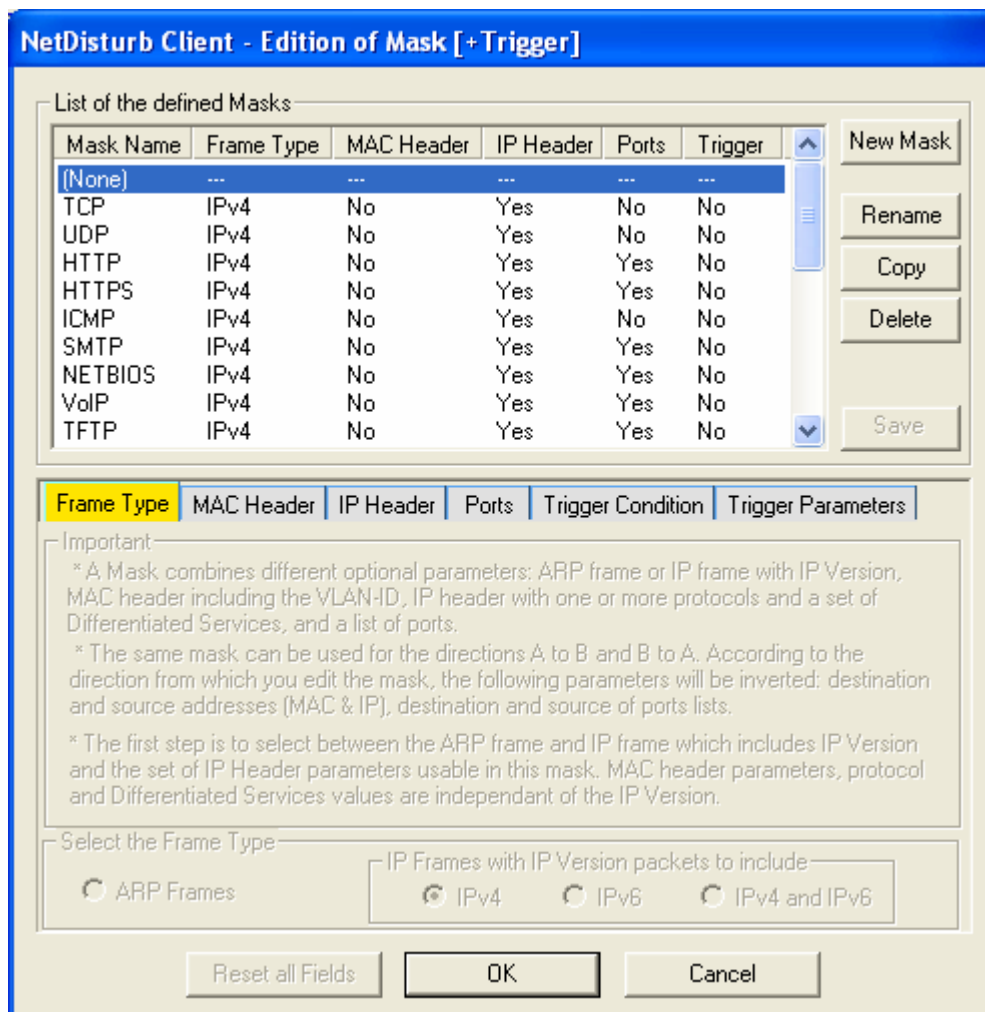


Supplementary masks may be added depending of the product release.

To define or edit an existing mask, press the Edit button as indicated below:

The screenshot shows the NetDisturb Client interface with three main sections: Mask [+ Trigger], Loss & Duplication Law, and Delay & Jitter Law. Each section has a dropdown menu set to '(None)' and an 'Edit' button. The 'Edit' button for the Mask section is circled in blue with an arrow pointing to it. Below the dropdowns, the status is shown: '# Incoming Packets' is 0, '# Lost or Duplicated Packets' is 0 [0.0 %], and '# Delayed Packets' is 0 [0.0 %].

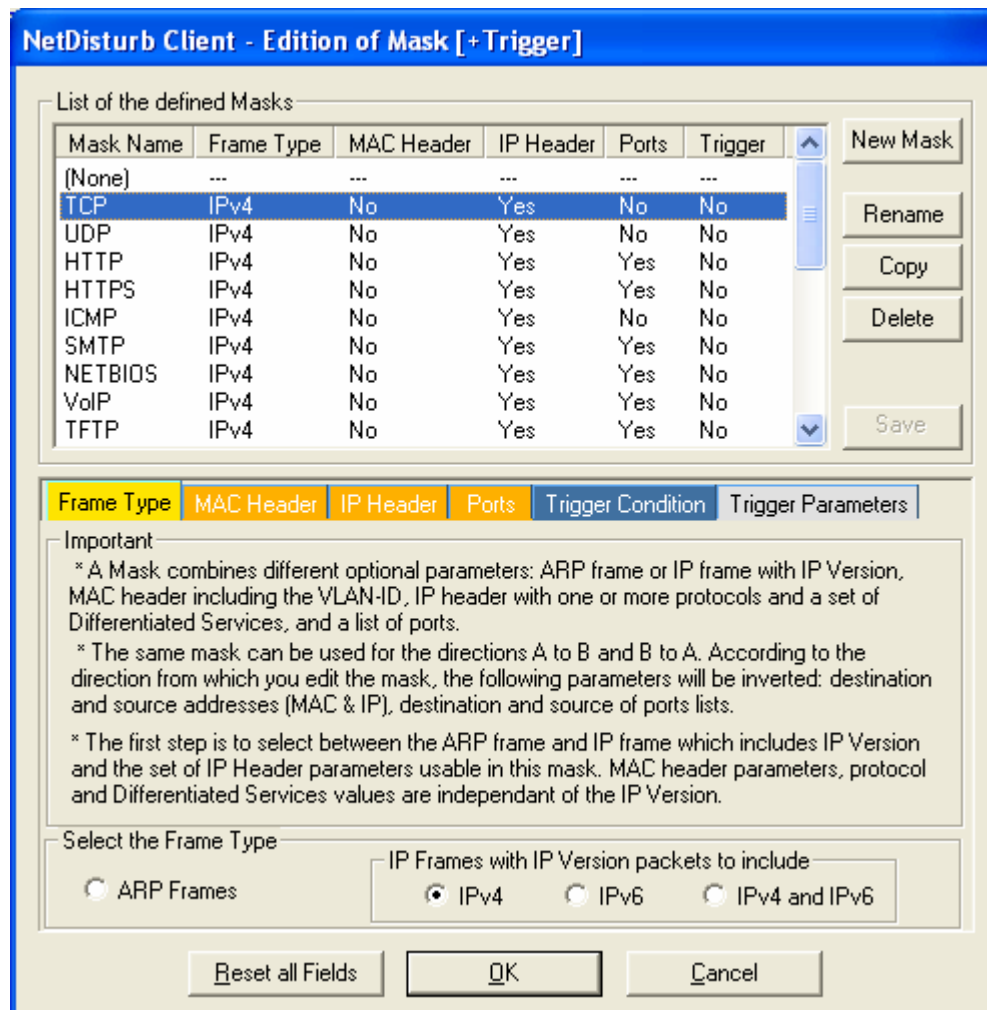
Then the following window will appear:



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

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

If you select a preexisting mask in the current list-box, then the parameters of this mask can be viewed and the first "Frame Type" tab is enabled as in the example below:



This window is composed of two areas:

- List of the defined Masks: a list-box displays the defined masks and five buttons allow managing the masks: New Mask, Rename, Copy, Delete and Save.
- 6 tabs to define the parameters of the selected mask and optional trigger parameters: The first 4 tabs concern the mask and the two last tabs are related to the trigger:
 - (tab 1: mask) Frame Type
 - (tab 2: mask) MAC Header
 - (tab 3: mask) IP Header
 - (tab 4: mask) Ports
 - (tab 5: trigger) Trigger Condition
 - (tab 6: trigger) *Trigger Parameters (enabled if a Trigger Condition has been defined)*

7.4.2.1 List of the defined Masks

The list-box displays for each defined mask the summary of the characteristics, except for (None) corresponding to 'No Mask' selected:

- Mask Name: name of the mask
- Frame Type: ARP | IPv4 | IPv6 | IPv4 & IPv6
- MAC Header: Yes | No
- IP Header: Yes | No
- Ports: Yes | No
- Trigger: Yes | No

To manage the Mask list, various buttons are available:

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

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

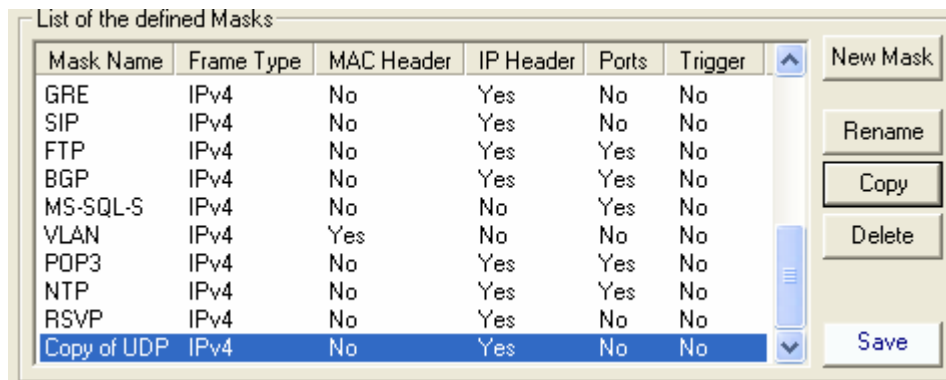
Mask Name	Frame Type	MAC Header	IP Header	Ports	Trigger		New Mask
GRE	IPv4	No	Yes	No	No		
SIP	IPv4	No	Yes	No	No		
FTP	IPv4	No	Yes	Yes	No		
BGP	IPv4	No	Yes	Yes	No		
MS-SQL-S	IPv4	No	No	Yes	No		
VLAN	IPv4	Yes	No	No	No		
POP3	IPv4	No	Yes	Yes	No		
NTP	IPv4	No	Yes	Yes	No		
RSVP	IPv4	No	Yes	No	No		
New Mask	IPv4	No	No	No	No		Save

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

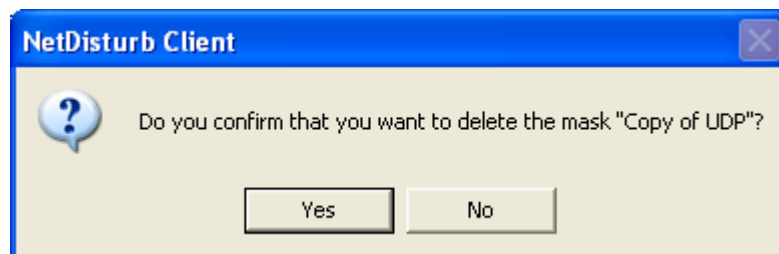
Mask Name	Frame Type	MAC Header	IP Header	Ports	Trigger		New Mask
GRE	IPv4	No	Yes	No	No		
SIP	IPv4	No	Yes	No	No		
FTP	IPv4	No	Yes	Yes	No		
BGP	IPv4	No	Yes	Yes	No		
MS-SQL-S	IPv4	No	No	Yes	No		
VLAN	IPv4	Yes	No	No	No		
POP3	IPv4	No	Yes	Yes	No		
NTP	IPv4	No	Yes	Yes	No		
RSVP	IPv4	No	Yes	No	No		
New Mask	IPv4	No	No	No	No		Save

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

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



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



Save: to save all changes related to the masks.

7.4.2.2 Six tabs to define the parameters of the Mask and the Trigger

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

- (tab 1: mask) Frame Type
- (tab 2: mask) MAC Header
- (tab 3: mask) IP Header
- (tab 4: mask) Ports
- (tab 5: trigger) Trigger Condition
- (tab 6: trigger) *Trigger Parameters (enabled if a Trigger Condition has been defined)*

A mask is defined by the combination of four types of parameters: Frame Type, MAC header, IP header and Ports.

Each parameter of a mask is optional except the frame type. When a parameter is set then the parameter **have to** be present in the IP Frame to match the mask.

Each mask 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 Mask: the "Frame Type" tab

NetDisturb Client - Edition of Mask [+ Trigger]

List of the defined Masks

Mask Name	Frame Type	MAC Header	IP Header	Ports	Trigger
GRE	IPv4	No	Yes	No	No
SIP	IPv4	No	Yes	No	No
FTP	IPv4	No	Yes	Yes	No
BGP	IPv4	No	Yes	Yes	No
MS-SQL-S	IPv4	No	No	Yes	No
VLAN	IPv4	Yes	No	No	No
POP3	IPv4	No	Yes	Yes	No
NTP	IPv4	No	Yes	Yes	No
RSVP	IPv4	No	Yes	No	No
Mask 1	IPv4	No	No	No	No

New Mask
Rename
Copy
Delete
Save

Frame Type | MAC Header | IP Header | Ports | Trigger Condition | Trigger Parameters

Important:

- * A Mask combines different optional parameters: ARP frame or IP frame with IP Version, MAC header including the VLAN-ID, IP header with one or more protocols and a set of Differentiated Services, and a list of ports.
- * The same mask can be used for the directions A to B and B to A. According to the direction from which you edit the mask, the following parameters will be inverted: destination and source addresses (MAC & IP), destination and source of ports lists.
- * The first step is to select between the ARP frame and IP frame which includes IP Version and the set of IP Header parameters usable in this mask. MAC header parameters, protocol and Differentiated Services values are independant of the IP Version.

Select the Frame Type

☐ ARP Frames ☒ IP Frames with IP Version packets to include

☐ IPv4 ☐ IPv6 ☐ IPv4 and IPv6

Reset all Fields OK Cancel

The first step is to select the frame type: ARP Frames or IP Frames with the related IP version (**IPv4** or **IPv6** or **IPv4 and IPv6**).

The choice of the IP version will affect the parameters handled by **NetDisturb** in the "IP Header" tab.

NetDisturb Client - Edition of Mask [+ Trigger]

List of the defined Masks

Mask Name	Frame Type	MAC Header	IP Header	Ports	Trigger
GRE	IPv4	No	Yes	No	No
SIP	IPv4	No	Yes	No	No
FTP	IPv4	No	Yes	Yes	No
BGP	IPv4	No	Yes	Yes	No
MS-SQL-S	IPv4	No	No	Yes	No
VLAN	IPv4	Yes	No	No	No
POP3	IPv4	No	Yes	Yes	No
NTP	IPv4	No	Yes	Yes	No
RSVP	IPv4	No	Yes	No	No
Mask 1	ARP	No	No	No	No

New Mask
Rename
Copy
Delete
Save

Frame Type | MAC Header | IP Header | Ports | Trigger Condition | Trigger Parameters

Important:

- * A Mask combines different optional parameters: ARP frame or IP frame with IP Version, MAC header including the VLAN-ID, IP header with one or more protocols and a set of Differentiated Services, and a list of ports.
- * The same mask can be used for the directions A to B and B to A. According to the direction from which you edit the mask, the following parameters will be inverted: destination and source addresses (MAC & IP), destination and source of ports lists.
- * The first step is to select between the ARP frame and IP frame which includes IP Version and the set of IP Header parameters usable in this mask. MAC header parameters, protocol and Differentiated Services values are independant of the IP Version.

Select the Frame Type

☒ ARP Frames ☐ IP Frames with IP Version packets to include

☐ IPv4 ☐ IPv6 ☐ IPv4 and IPv6

Reset all Fields OK Cancel

If the frame type selected is ARP, the other tabs are disabled i.e. ARP filtering is not concerned by the other parameters offered by the NetDisturb mask.

7.4.2.2.2 Mask: the "MAC Header" tab

NetDisturb Client - Edition of Mask [+Trigger]

List of the defined Masks

Mask Name	Frame Type	MAC Header	IP Header	Ports	Trigger
GRE	IPv4	No	Yes	No	No
SIP	IPv4	No	Yes	No	No
FTP	IPv4	No	Yes	Yes	No
BGP	IPv4	No	Yes	Yes	No
MS-SQL-S	IPv4	No	No	Yes	No
VLAN	IPv4	Yes	No	No	No
POP3	IPv4	No	Yes	Yes	No
NTP	IPv4	No	Yes	Yes	No
RSVP	IPv4	No	Yes	No	No
Mask 1	IPv4	No	No	No	No

New Mask
Rename
Copy
Delete
Save

Frame Type | **MAC Header** | IP Header | Ports | Trigger Condition | Trigger Parameters

MAC Addresses

Destination: Equal []

Source: Equal []

e.g. 01:23:45:67:89:AB

VLAN (802.1Q)

VLAN-ID List: Equal []

As VLAN-ID List, you can enter:
 1) A range of values (i.e. 120-250 means from 120 to 250).
 2) Individual values separated by semicolon (i.e. 500;600).
 3) Both (i.e. 500;550-560;599).

Reset all Fields OK Cancel

MAC Addresses

- Destination with the Equal or Different operator
- Source with the Equal or Different operator

A destination or source MAC address has the following format (12 hexadecimal digits grouped by 2 and separated by the colon character):

XX:XX:XX:XX:XX:XX

Here is an example:

Destination Equal (to) **00:0B:DB:95:3D:BF**

and

Source Different (of) **00:80:C8:81:37:66**

The IP packets having a MAC destination address equal to **00:0B:DB:95:3D:BF** or a MAC source address different of **00:80:C8:81:37:66** will belong to this IP flow.

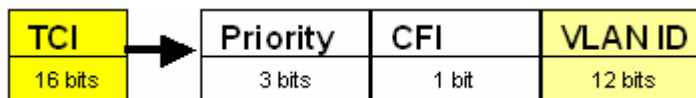
VLAN-ID list

- **VLAN-ID List with the Equal or Different operator** (enter a decimal value or a list – see 7.4.2.5 for more details).
The VLAN-ID can be used only with Ethernet type 8100 frames. In that case, the IEEE 802.1Q format is assumed.

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

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

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



You can input individual values separated by a semicolon or a range of values or a mix of both.



When the VLAN ID is 0, any VLAN value matches: the value 0 is used to select the VLAN property of the flow not a particular VLAN flow.

7.4.2.2.3 Mask: the "IP Header" tab

Depending of the IP version (**IPv4**, **IPv6** or **IPv4 and IPv6**) previously selected in the Frame Type tab, the format of some fields of this tab will be different.

- If IP version = **IPv4** then the IP Header tab is as follows:

Frame Type	MAC Header	IP Header	Ports	Trigger Condition	Trigger Parameters
IP Addresses					
Destination:	Equal				
Source:	Equal				
			address e.g. xxx.xxx.xxx.xxx	mask e.g. xxx.xxx.xxx.xxx	
Other IP fields					
Protocol:	Equal	6	<input type="radio"/> Predefined Protocols <input checked="" type="radio"/> User Protocols		
			Individual values in a User List are separated by a semicolon i.e. 6;11;18		
Differentiated Services (DS):	Equal		<input checked="" type="radio"/> Predefined DS <input type="radio"/> User DS		

⇒ IP Addresses

Three objects are defined for the Destination or Source address:

- Operator: Equal or Different
- IP address (enter a decimal value: ex. 192.168.0.17)
- Mask for the IP address (enter a decimal value: ex. 255.255.255.0)



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

⇒ Other IP fields

Protocol with three objects defined:

- Operator: Equal or Different
- The combo-box allows selecting one or several predefined protocols, or input a list of values separated by a semicolon you want to use
- The option to choose "Predefined Protocols" or "User Protocol List"

Other IP fields

Protocol: Equal 01 ICMP, 06 TCP

To enter special User List option

Differentiated Services (DS): Equal

01 ICMP
02 IGMP
04 IPinIP
06 TCP

Predefined Protocols
User Protocols
Predefined DS
User DS

Example by selecting the "Predefined Protocols" option

Other IP fields

Protocol: Equal 01;06;12;17

Individual values in a User List are separated by a semicolon i.e. 6;11;18

Differentiated Services (DS): Equal

Predefined Protocols
User Protocols
Predefined DS
User DS

Example by selecting the "User Protocol List" option

Differentiated Services (DS) (TOS byte) with three objects defined:

- Operator: Equal or Different
- The combo-box allows selecting one or several predefined values, or input a list of values separated by a semicolon you want to use
- The option to choose "Predefined DS" or "User DS List"

Other IP fields

Protocol: Equal 01;06;12;17

Individual values in a User List are separated by a semicolon i.e. 6;11;18

Differentiated Services (DS): Equal

10 Class 1 Gold (AF11)
00 Default PHB (Per-hop ...
08 Class 1
12 Class 1 Silver (AF12)

Predefined Protocols
User Protocols
Predefined DS
User DS

Save Changes Reset Cancel

Example by selecting the "Predefined DS" option

Example by selecting the "User DS List" option

- If IP version = **IPv6** then the IP Header tab is as follows:

The main difference with the previous case concerns the format of the IPv6 address and the IPv6 mask.

Refer above for details on the other fields.

- If IP version = **IPv4 and IPv6** then the IP Header tab is as follows:

In this case, the IP address fields are disabled because no sense..

Refer above for details on the other fields.

7.4.2.2.4 Mask: the "Ports" tab

Ports (available with UDP and TCP)

Destination Port List: Equal

Source Port List: Equal

Syntax for the Destination or Source Ports List

A Port List may be:

- 1) A range of values (i.e. 20-25 means from port 20 to port 25).
- 2) Individual values separated by a semicolon (i.e. 7;9;80).
- 3) Denied individual values if the symbol != is before (i.e. !=21).
- 4) A range of values and individual values (i.e. 7;9;20-25;80;435).
- 5) A range of values with denied individual values (i.e. 10-50;!=20;!=21 which means from 10 to 50 without 20 or 21)

Ports (to be applied only on the TCP or UDP protocol)

- [Destination Port List](#) (enter a decimal value or a list – see 7.4.2.5 for more details)
- [Source Port List](#) (enter a decimal value or a list – see 7.4.2.5 for more details)



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

7.4.2.2.5 Trigger: the "Trigger Condition" tab

☒ Use the Trigger to Apply Impairments (only available if the IP Flow is not in an aggregate)

About Trigger

- * The trigger is based on the Ethernet frame content. The analysis starts at the Offset position of the frame, where the content ANDed with the Pattern - up to the Pattern length - should be equal to the Result to set the Trigger condition.
- * When the Trigger condition occurs, the impairment(s) will apply for this frame (or not) and following, in BOTH directions.

Trigger Definition

Offset: (Decimal) (0 = first byte of the Ethernet frame)

Pattern: (Hexadecimal)

Result: (Hexadecimal)

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

The Trigger is activated when the content of an 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 a given 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 given 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 mask of each direction, the Trigger activated starts impairment(s) on both directions. Additional parameters of the Trigger apply also to both directions.



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

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 bytes of the Ethernet frame. The port number is located at the 37th bytes of the frame. The bytes between the protocol and the port number are not significant.

The definition of this trigger is:

Offset = 23

Pattern = FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF

Result = 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 15

The Pattern parameter and the Result parameter 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 three common Ethernet frames.

The analysis of the Ethernet frames made by NetDisturb is described below. In this example, the first frame is an ARP Request frame, the second frame is the ARP Reply and the third frame is the TCP SYN. 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 00 FF 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 08

Result expected: 06 00 00 00 00 00 00 00 00 00 00 00 15 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 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 00 FF 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 00 15 00 00 00 00 00 00 00 01

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

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

7.4.2.2.6 Trigger: the "Trigger Parameters" tab

This tab is accessible only if the Trigger Definition has been made in the "Trigger Condition" tab.

Frame Type | MAC Header | IP Header | Ports | Trigger Condition | **Trigger Parameters**

Trigger Parameters

Delay before applying the Impairment(s): (ms) (0 = no Delay)

☐ Impair the Frame that has triggered (available only if Delay before Impairment is 0)

Duration of the Impairment(s): (ms) (0 = Unlimited)

Number of Cycles for the Trigger: (ms) (0 = Unlimited)

* The Trigger Parameters applies at the same time in both directions of the IP Flows (i.e. A to B and B to A).
 * When the Number of Cycle is reached, the IP Flow should be stopped and restarted to allow the impairments activation.

The Trigger can be configured:

- To add an initial delay before the impairment.
- To include the Ethernet frame that matches the Result in the list of frames to impair or to leave this frame without impairment.
- To limit the impairment in time.
- To limit the number of loops of the impairment based on the Trigger analysis.

These configuration parameters are detailed below.

Delay before applying the Impairment

When a frame has activated the Trigger, an additional delay can be added before **NetDisturb** starts the impairment.

This delay is expressed in milliseconds. 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.

When this delay is zero, the parameter 'Impair the Frame that has triggered' can be set up.

A delay greater than zero is needed with some application protocols (i.e. video) when there is some information to exchange before starting the exchange of the most important frames.

Impair the Frame that has triggered

When the 'Impair the Frame that has triggered' 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.

Duration of the Impairment

The **Duration of the Impairment** parameter limits the impairment in the time. By default, this duration is zero so the impairment continues until the IP Flow is stopped.

When this duration is greater than zero the beginning of the Impairment(s) starts when the first frame is impaired. The **Delay before applying the Impairment** isn't included in this duration. When the impairment duration reach the **Duration of the Impairment** value, the impairment stops except if the **Number of Cycles for the Trigger** parameter is not zero.

When the impairment stops, the next frames matching the mask are transferred from the incoming Interface to the outgoing Interface immediately.

Number of Cycles for the Trigger

The **Number of Cycles for the Trigger** parameter is available when the **Duration of the Impairment** is not zero.

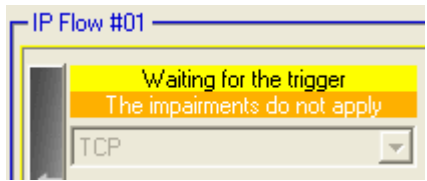
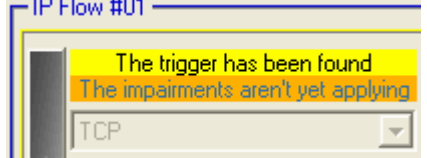
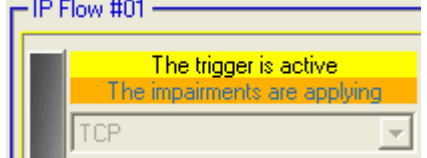
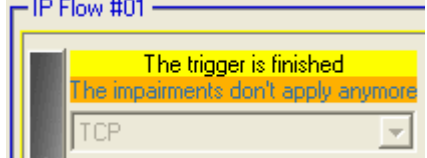
By default, the number of cycles is 0 i.e. the Trigger cycle is unlimited.

When a **Number of Cycles for the Trigger** is specified, the Trigger cycle restarts at the beginning of the frame analysis process until the number of cycles is reached.

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

7.4.2.2.7 The Trigger Dynamics

This paragraph gives some examples for the use of Trigger parameters to explain the 4 states of a Trigger:

<p>1. Waiting for the trigger. The Trigger gets this state before it has been found. There are 2 cases when a Trigger gets this state: either the IP Flow has just been started or the Duration of Impairment has been reached and the Number of Cycles hasn't been reached. Ethernet frames are relayed without impairment.</p>	
<p>2. The trigger has been found. The Trigger gets this state when the Ethernet frame has been found and a Delay before Impairment has not yet expired. Ethernet frames are relayed without impairment.</p>	
<p>3. The trigger is active. A Trigger gets this state when the Impairment applies, either after the Ethernet frame has been found without Delay before Impairment or when the Delay before Impairment has expired. Ethernet frames are impaired.</p>	
<p>4. The trigger is finished. A Trigger gets this state when the Number of Cycles has been reached. This state is a permanent state until the IP Flow is stopped. Ethernet frames are relayed without impairment.</p>	

The Figure 5 illustrates the configuration of a Trigger without Duration. When the Trigger has been reached, the Impairment remains active until the IP Flow is stopped.

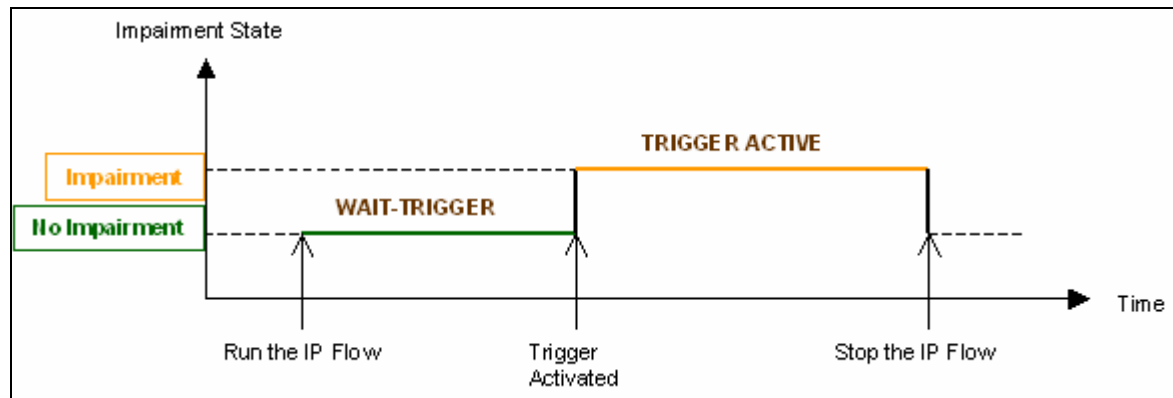


Figure 5 - Trigger without Duration

The Figure 6 illustrates the configuration of a Trigger with a Delay and no Impairment Duration. When the Trigger has been reached, the Impairment(s) starts after the Delay and remains active until the IP Flow is stopped.

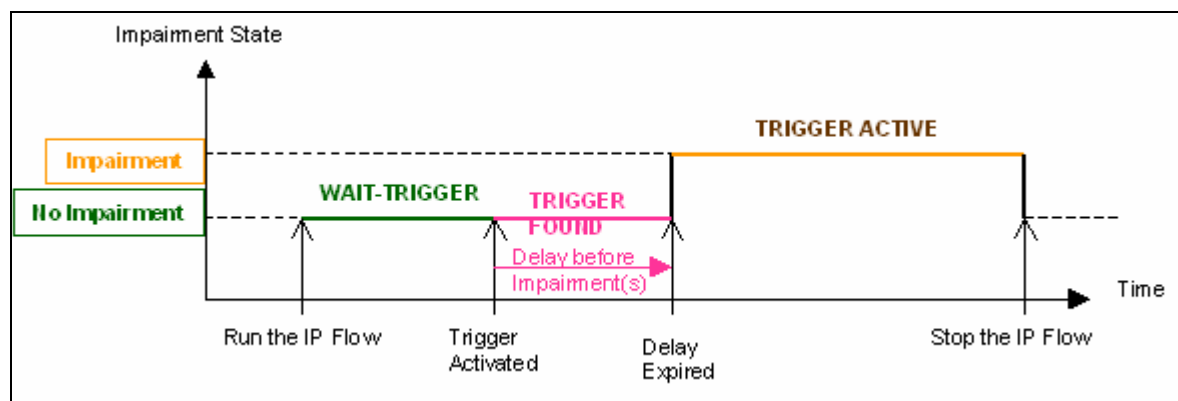


Figure 6 - Trigger with Delay and no Impairment Duration

The Figure 7 illustrates the configuration of a Trigger with the Duration of the Impairment not zero and an unlimited Number of Cycles.

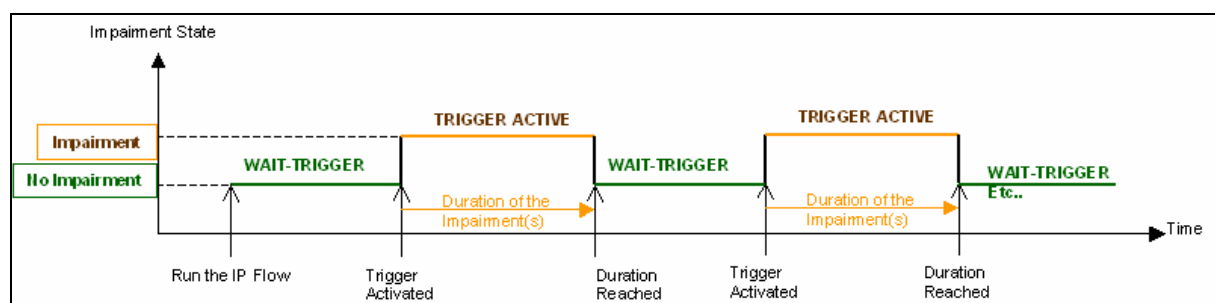


Figure 7 - Trigger with Impairment Duration

The Figure 8 - Trigger with the Impairment Duration and 1 Cycle illustrates the configuration of a Trigger with the Duration of the Impairment not zero and a Number of Cycles limited to 1.

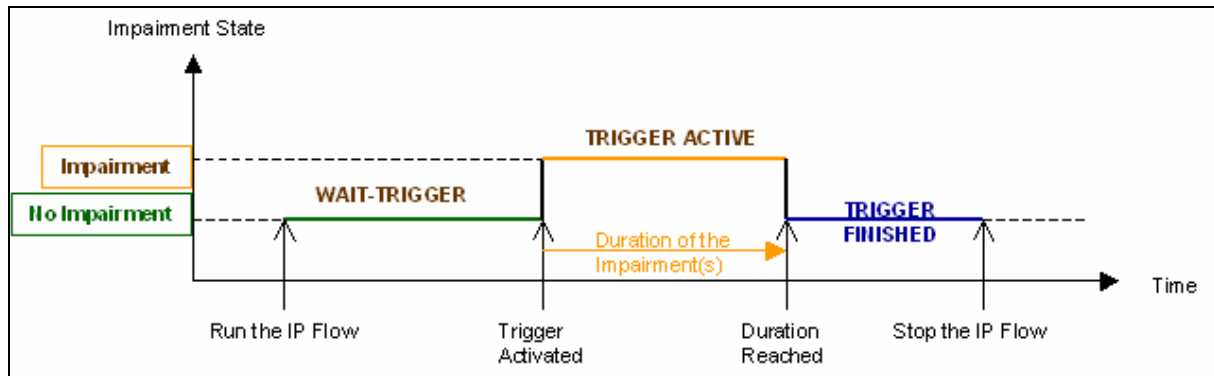


Figure 8 - Trigger with the Impairment Duration and 1 Cycle

The Figure 9 illustrates the configuration of a Trigger with a Delay Applying before the Impairment not zero, the Duration of the Impairment not zero and a Number of Cycles set to 2.

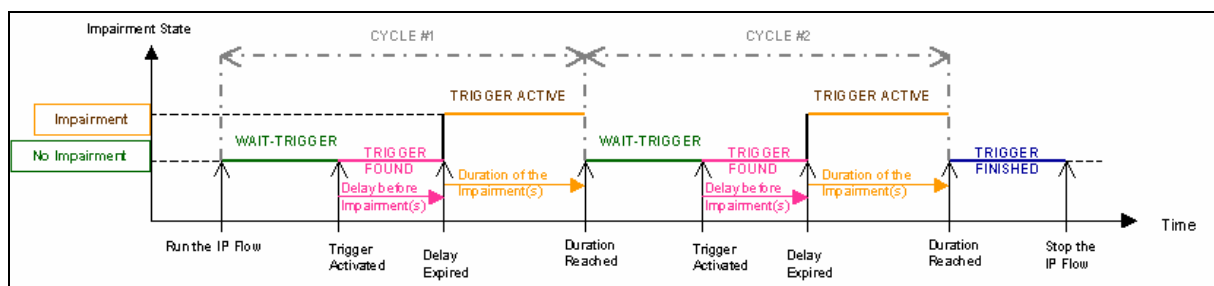
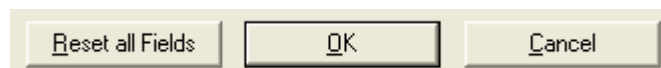


Figure 9 - Trigger with a Delay, Impairment Duration and a limited number of Cycles

7.4.2.3 The Action Buttons

To handle the Mask and Trigger parameters different buttons are available at the bottom of the window:



Reset all Fields: to reset all the values previously entered.

OK: saves all modifications made if you didn't save them before. Moreover, the mask selected in the list of the defined mask becomes the selected mask in the combo-box of the IP Flow window.

Cancel: to ignore all modifications made if you didn't click on the Save button before. In that case, the last mask selected in the combo-box of the IP Flow window is kept.

7.4.2.4 To Create a New Mask with its parameters in a few steps

1) Click on the "Edit" button as shown below:

The screenshot shows the main configuration window of the NetDisturb Client. It has three main sections: 'Mask [+ Trigger]', 'Loss & Duplication Law', and 'Delay & Jitter Law'. Each section has a dropdown menu set to '(None)' and an 'Edit' button. The 'Edit' button under the 'Mask [+ Trigger' section is circled with a blue '1'. Below these sections are three input fields: '# Incoming Packets' with value '0', '# Lost or Duplicated Packets' with value '0 [0.0 %]', and '# Delayed Packets' with value '0 [0.0 %]'. A 'NEXT' button is on the right side.

2) The "Edition of Mask [+ Trigger]" window is displayed.

The screenshot shows the 'Edition of Mask [+ Trigger]' window. It has a title bar 'NetDisturb Client - Edition of Mask [+ Trigger]'. Inside, there's a 'List of the defined Masks' table with columns: Mask Name, Frame Type, MAC Header, IP Header, Ports, and Trigger. The table contains several rows, including '(None)', TCP, UDP, HTTP, HTTPS, ICMP, SMTP, NETBIOS, VoIP, and TFTP. The 'IP Header' column for the 'NETBIOS' row is circled with a blue '2'. To the right of the table are buttons: 'New Mask', 'Rename', 'Copy', 'Delete', and 'Save'. Below the table are tabs: 'Frame Type', 'MAC Header', 'IP Header', 'Ports', 'Trigger Condition', and 'Trigger Parameters'. The 'Frame Type' tab is selected. Below the tabs is an 'Important' section with three bullet points explaining mask parameters. At the bottom, there's a 'Select the Frame Type' section with radio buttons for 'ARP Frames' and 'IP Frames with IP Version packets to include'. The 'IP Frames' section has three sub-radio buttons: 'IPv4' (selected), 'IPv6', and 'IPv4 and IPv6'. At the very bottom are 'Reset all Fields', 'OK', and 'Cancel' buttons.

Then press the New Mask button and a new entry (New Mask) is added at the end of the list.

NetDisturb Client - Edition of Mask [+Trigger]

List of the defined Masks

Mask Name	Frame Type	MAC Header	IP Header	Ports	Trigger
GRE	IPv4	No	Yes	No	No
SIP	IPv4	No	Yes	No	No
FTP	IPv4	No	Yes	Yes	No
BGP	IPv4	No	Yes	Yes	No
MS-SQL-S	IPv4	No	No	Yes	No
VLAN	IPv4	Yes	No	No	No
POP3	IPv4	No	Yes	Yes	No
NTP	IPv4	No	Yes	Yes	No
RSVP	IPv4	No	Yes	No	No
New Mask	IPv4	No	No	No	No

Buttons: New Mask, Rename, Copy, Delete, Save

Frame Type | **MAC Header** | **IP Header** | **Ports** | **Trigger Condition** | **Trigger Parameters**

Important

- * A Mask combines different optional parameters: ARP frame or IP frame with IP Version, MAC header including the VLAN-ID, IP header with one or more protocols and a set of Differentiated Services, and a list of ports.
- * The same mask can be used for the directions A to B and B to A. According to the direction from which you edit the mask, the following parameters will be inverted: destination and source addresses (MAC & IP), destination and source of ports lists.
- * The first step is to select between the ARP frame and IP frame which includes IP Version and the set of IP Header parameters usable in this mask. MAC header parameters, protocol and Differentiated Services values are independant of the IP Version.

Select the Frame Type

☐ ARP Frames

IP Frames with IP Version packets to include

☒ IPv4 ☐ IPv6 ☐ IPv4 and IPv6

Buttons: Reset all Fields, OK, Cancel

3) Press the Rename button and enter a new identifier.

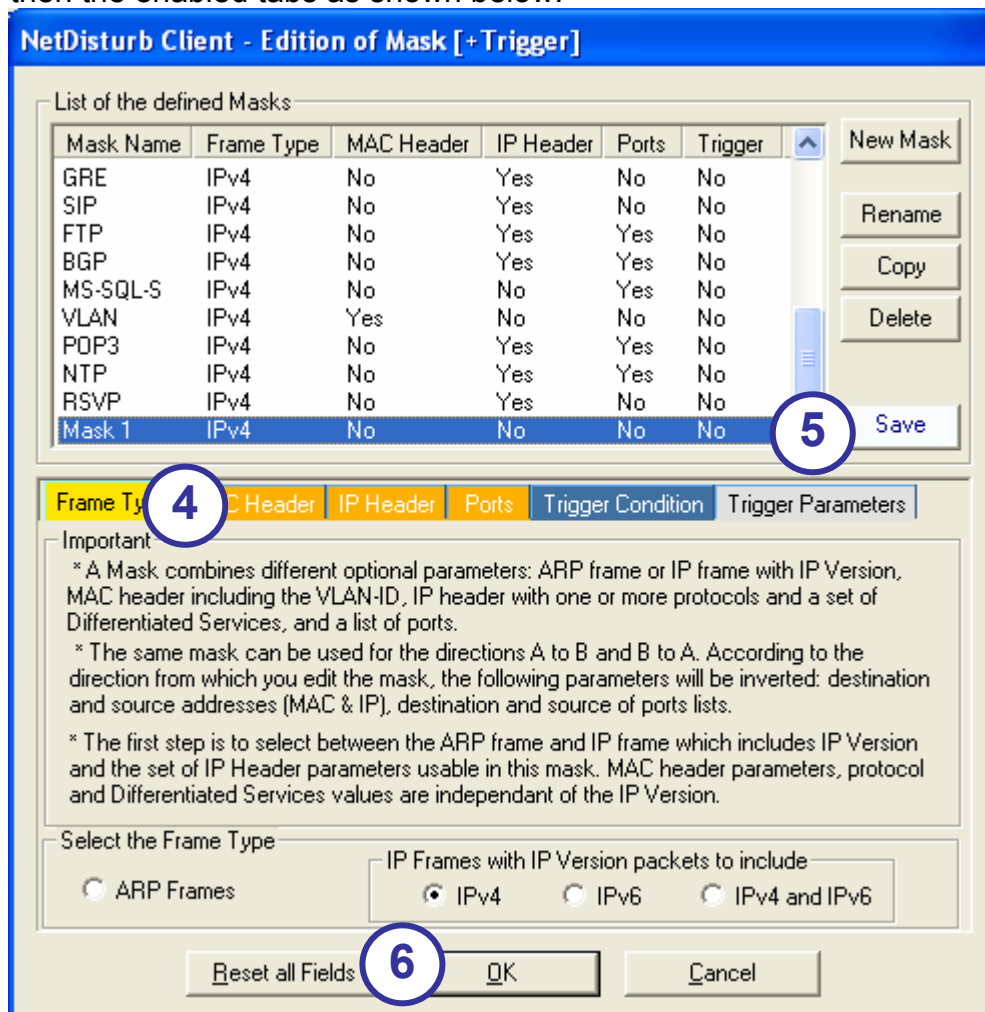
List of the defined Masks

Mask Name	Frame Type	MAC Header	IP Header	Ports	Trigger
GRE	IPv4	No	Yes	No	No
SIP	IPv4	No	Yes	No	No
FTP	IPv4	No	Yes	Yes	No
BGP	IPv4	No	Yes	Yes	No
MS-SQL-S	IPv4	No	No	Yes	No
VLAN	IPv4	Yes	No	No	No
POP3	IPv4	No	Yes	Yes	No
NTP	IPv4	No	Yes	Yes	No
RSVP	IPv4	No	Yes	No	No
New Mask	IPv4	No	No	No	No

Buttons: New Mask, Rename, Copy, Delete, Save

3

For example input Test as new identifier of the mask and then click on the line to validate. You have then the enabled tabs as shown below:



- 4) Now the tabs are enabled and you can define the parameters for this mask (Frame Type, MAC Header, IP Header and Ports) and if needed the Trigger Condition and Trigger Parameters.
- 5) Press the "Save" button to save the parameters and return at step 2 if you want continue to edit or create a new mask.
- 6) Press "OK" or "Cancel" to quit the "Edition of Mask" window.

7.4.2.5 List of Values

Some parameters in the Mask can be a list of values. To match the mask, the IP packet should include one value from the list. The syntax of 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.

7.4.2.5.1 Individual Value

An individual value is one and only one value.

Example: 135

7.4.2.5.2 List of Individual Values

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

Example: 25;80;110;435

7.4.2.5.3 Range of Values

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

Example: 2009-2020;3000-3100

7.4.2.5.4 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

7.4.3 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:

Combo-box (law identifier)	Comment area	Description
(None)	(None)	With this option, no duplication and no loss law apply to the IP Flow.

<i>Loss Law</i>		
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
F.(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.
F. (Percentage & Time)	Loss: File (Percentage & Duration)	Sample file: PercentageLossAndDurationSample.txt Loss up to 50 % with steps of 5% each 10 seconds.

<i>Duplication Law</i>		
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

7.4.3.1 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 mask. 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 mask.

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.

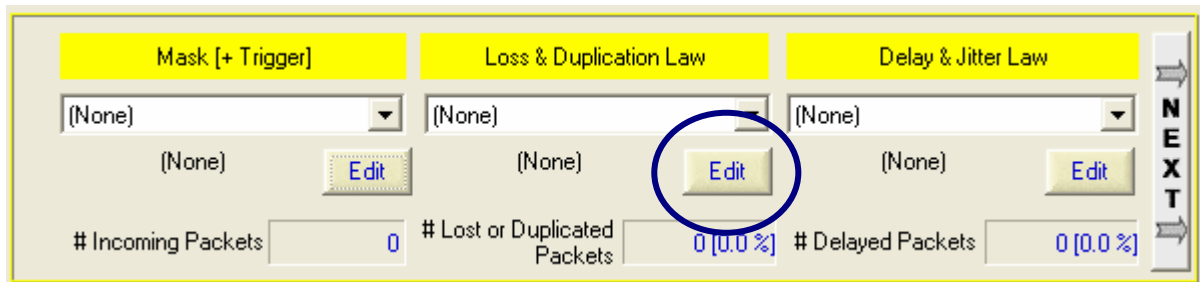
If the packet is TCP or UDP, the 5-tuple IP addresses, protocol and ports is used to classify the packet. Else the IP addresses and protocol are only used.

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.

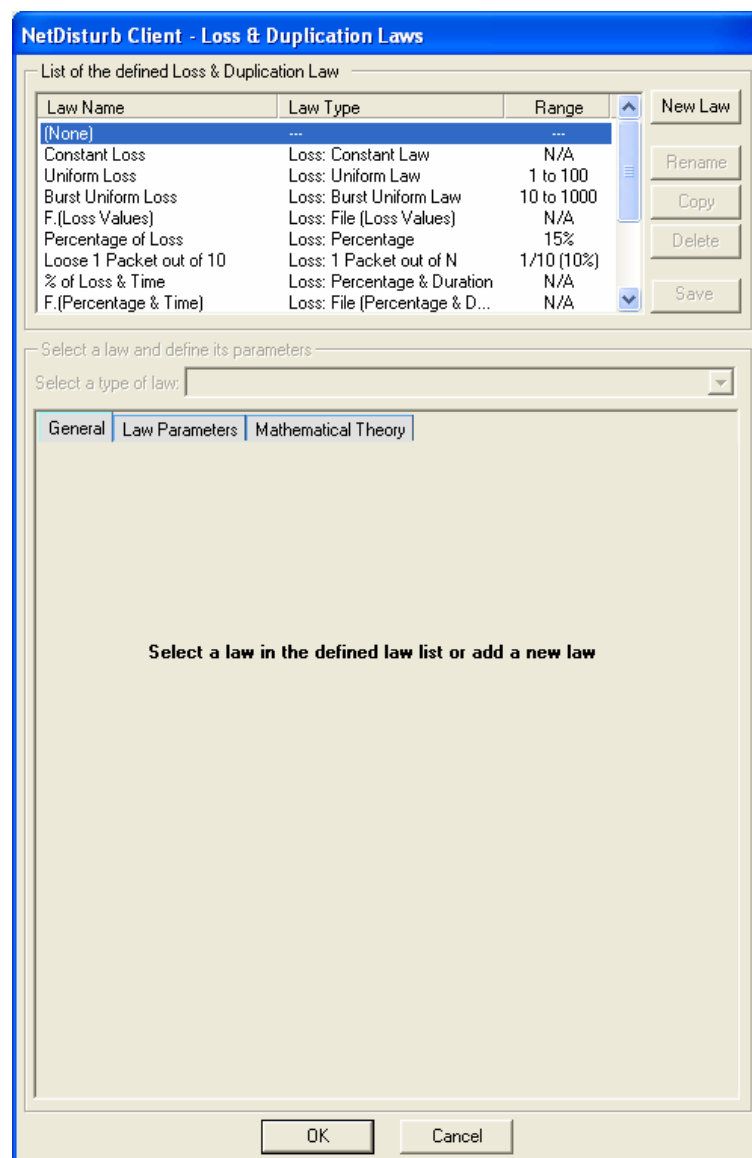
This value is compared to the Threshold: if the value is greater or equal than the Threshold, the packet is lost. Otherwise, the packet continue to be handled and may be delayed.

7.4.3.2 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.



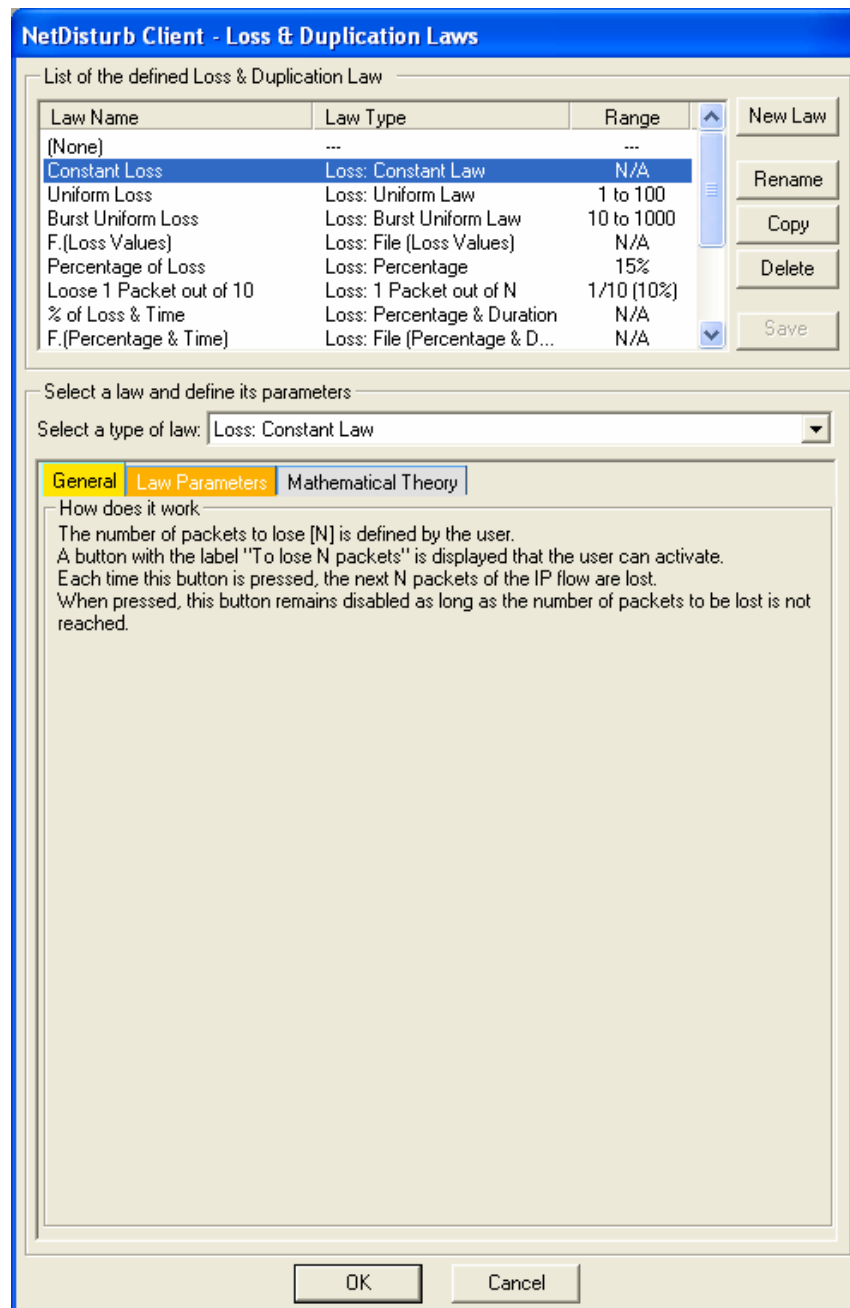
The following window is then displayed:



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 as in the example below:



This window is composed of two areas:

List of the defined Loss & Duplication Law: a list-box displays the defined laws and five buttons allow managing the laws: New Law, Rename, Copy, Delete and Save.

- The first step is to choose the law type amongst the list of the pre-defined Content Impairment 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)

7.4.3.2.1 List of the Loss & Duplication Laws defined

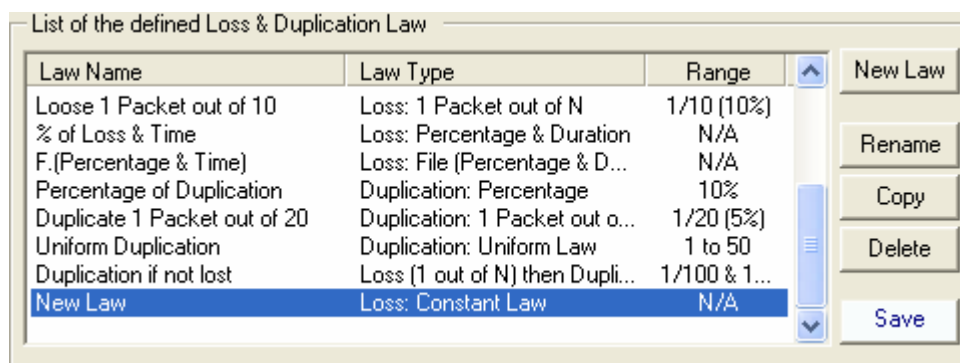
The list-box displays for each defined law the summary of the characteristics, except for (None) corresponding to 'No Loss & Duplication Law' selected:

- 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 7.4.3.2.2 Select a law and define its parameters)
- Range: range of values generated by the specified laws.

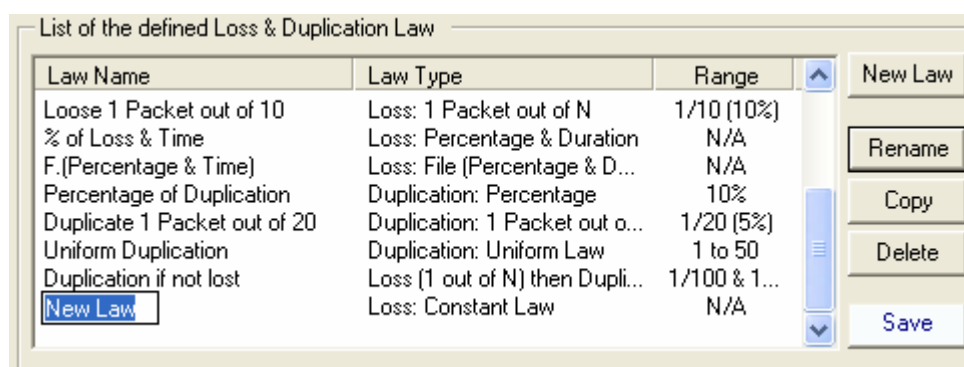
To manage the Law list, various buttons are available:

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:

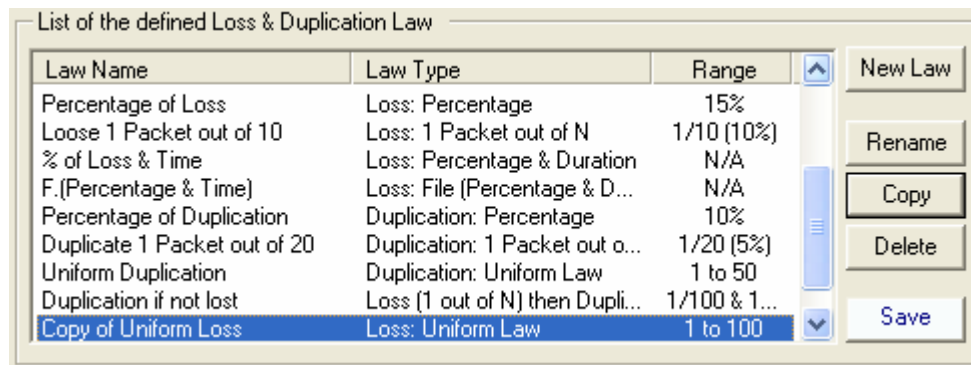


Then click on 'New Law' label to rename this entry or press the Rename button:

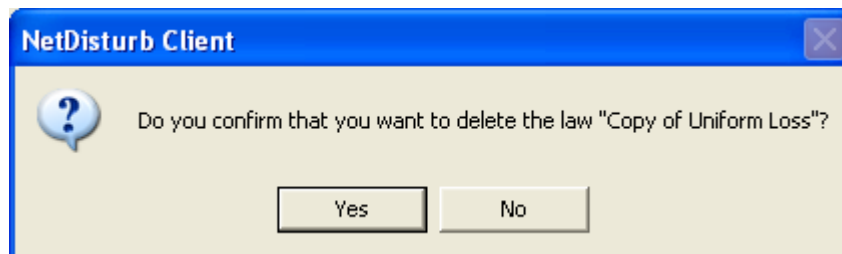


Rename: to rename the Law. This button should be used to change the Law name.

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 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.

7.4.3.2.2 *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 Loss & Duplication Laws using a mathematical law). This tab gives some details on the theory of the mathematical law used.

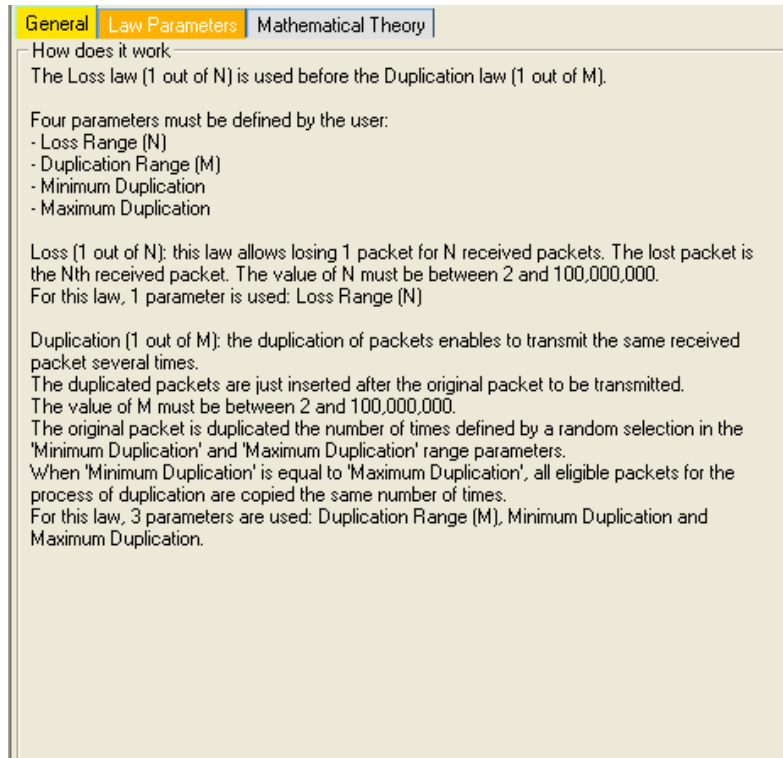
⇒ **Select a type of law**

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, $\text{Min} \leq n \leq \text{Max}$
- Duplication: 1 Packet out of M
Parameters: range(M), $\text{Min} \leq n \leq \text{Max}$
- 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)

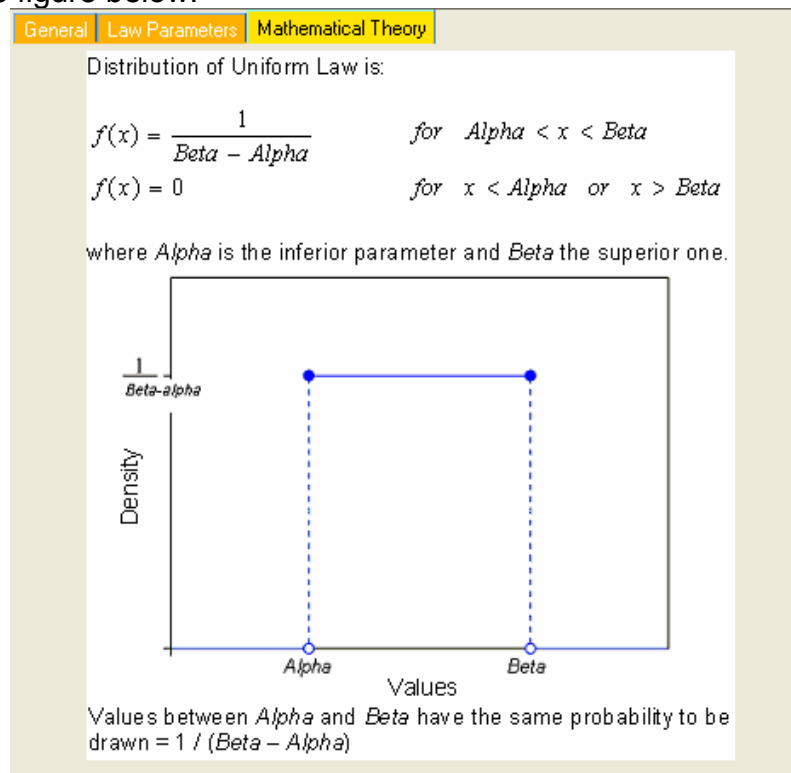
This tab is described for each law type here after.

⇒ 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.

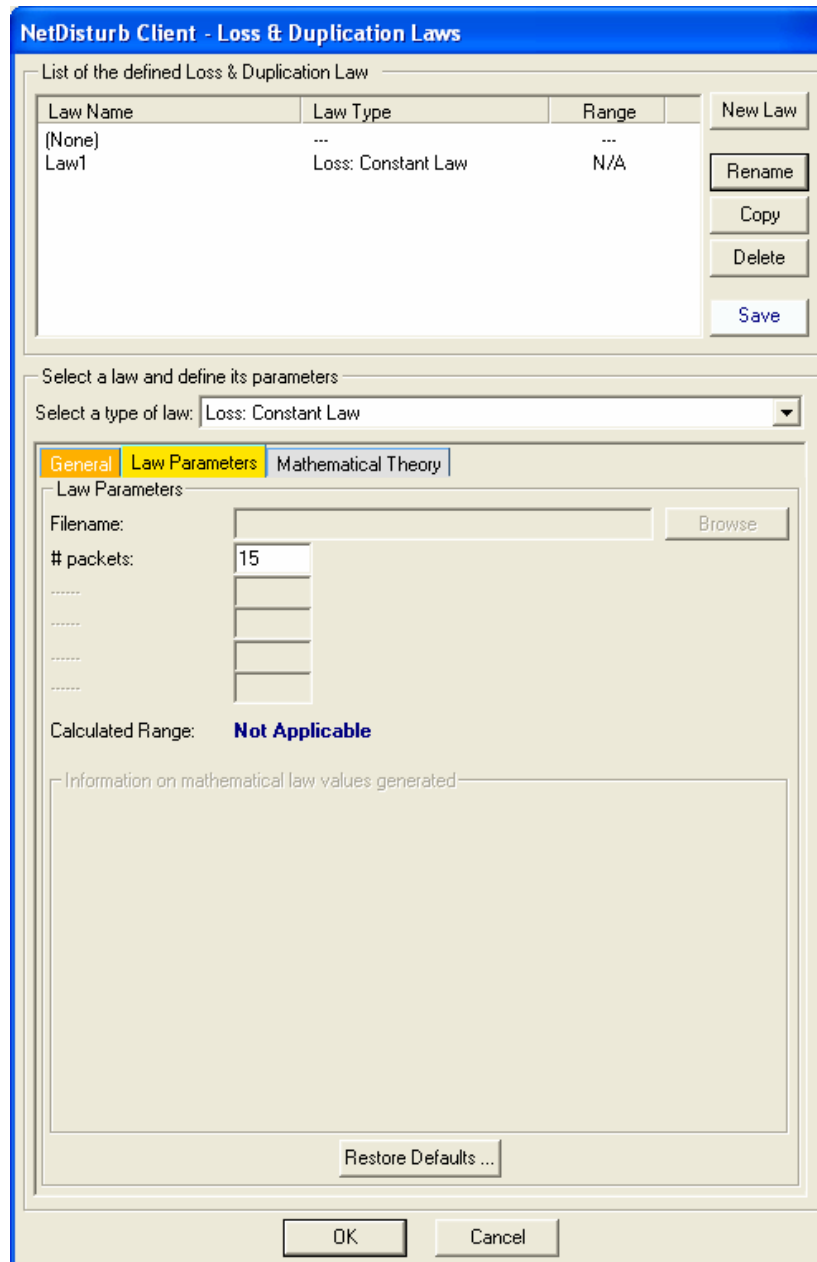
Button	Action
Restore Defaults ...	Reset all parameters of the current law.
OK	Save all modifications made if you didn't save them before. Moreover, the selected law in the list of the defined laws becomes the selected law in the combo-box of the IP Flow window.
Cancel	Ignore all modifications made if 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 IP Flow.

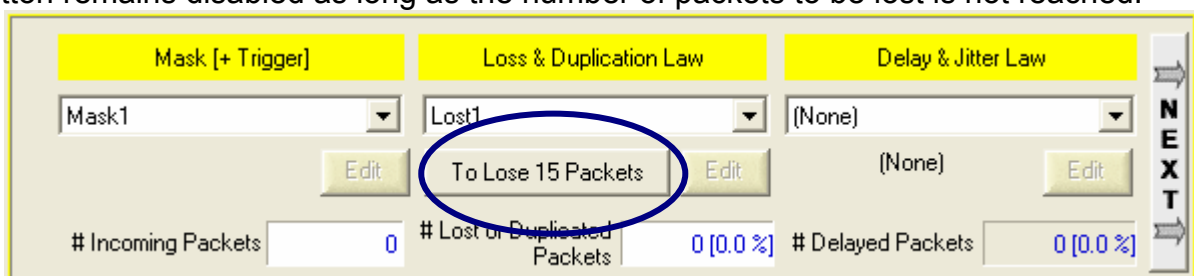
7.4.3.3 Loss: Constant Law

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



For this law, only one parameter must be defined: **# 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 IP flow are lost. When pressed, this button remains disabled as long as the number of packets to be lost is not reached.



7.4.3.4 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.

NetDisturb Client - Loss & Duplication Laws

List of the defined Loss & Duplication Law

Law Name	Law Type	Range
(None)	---	---
Law1	Loss: Uniform Law	1 to 10

Buttons: New Law, Rename, Copy, Delete, Save

Select a law and define its parameters

Select a type of law: Loss: Uniform Law

General | **Law Parameters** | Mathematical Theory

Law Parameters

Filename: Browse

Alpha:

Beta: must be > Alpha

Threshold:

Calculated Range: **From 1 to 10**

Information on mathematical law values generated

The minimum value is **1**

The maximum value is **10**

The probability of each value between Alpha and Beta is around: **11.1111%**

If not between Alpha and Beta, the probability of a value is null

Restore Defaults ...

OK Cancel

The **NetDisturb** driver picks a number in the table (see also 7.4.3.1) 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

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

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

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.

Information on mathematical law values generated

The minimum value is **1**

The maximum value is **10**

The probability of each value between Alpha and Beta is around: **11.1111%**.

If not between Alpha and Beta, the probability of a value is null

7.4.3.5 Loss: Burst Uniform Law

NetDisturb Client - Loss & Duplication Laws

List of the defined Loss & Duplication Law

Law Name	Law Type	Range
(None)	---	---
Law1	Loss: Burst Uniform Law	1 to 10

New Law
Rename
Copy
Delete
Save

Select a law and define its parameters

Select a type of law: **Loss: Burst Uniform Law**

General | **Law Parameters** | Mathematical Theory

Law Parameters

Filename: Browse

Alpha:

Beta: must be > Alpha

Threshold (n):

Threshold (n+x):

Depth:

Calculated Range: **From 1 to 10**

Information on mathematical law values generated

The minimum value is **1**

The maximum value is **10**

The probability of each value between Alpha and Beta is around: **11.1111%**.

If not between Alpha and Beta, the probability of a value is null

Restore Defaults ...

OK Cancel

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 7.4.3.1)
- ⇒ 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

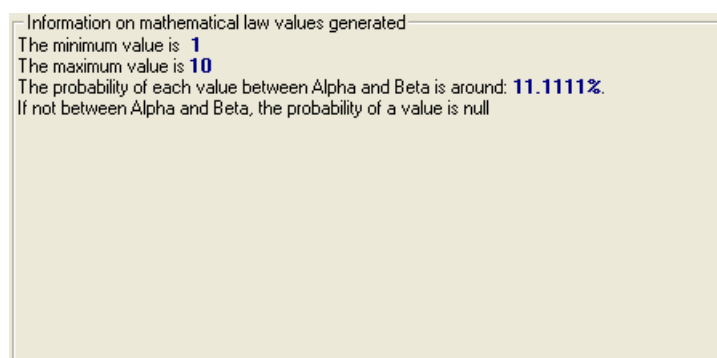
$$f(x) = 1/(\beta - \alpha) \quad \text{if } \alpha < x < \beta$$

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

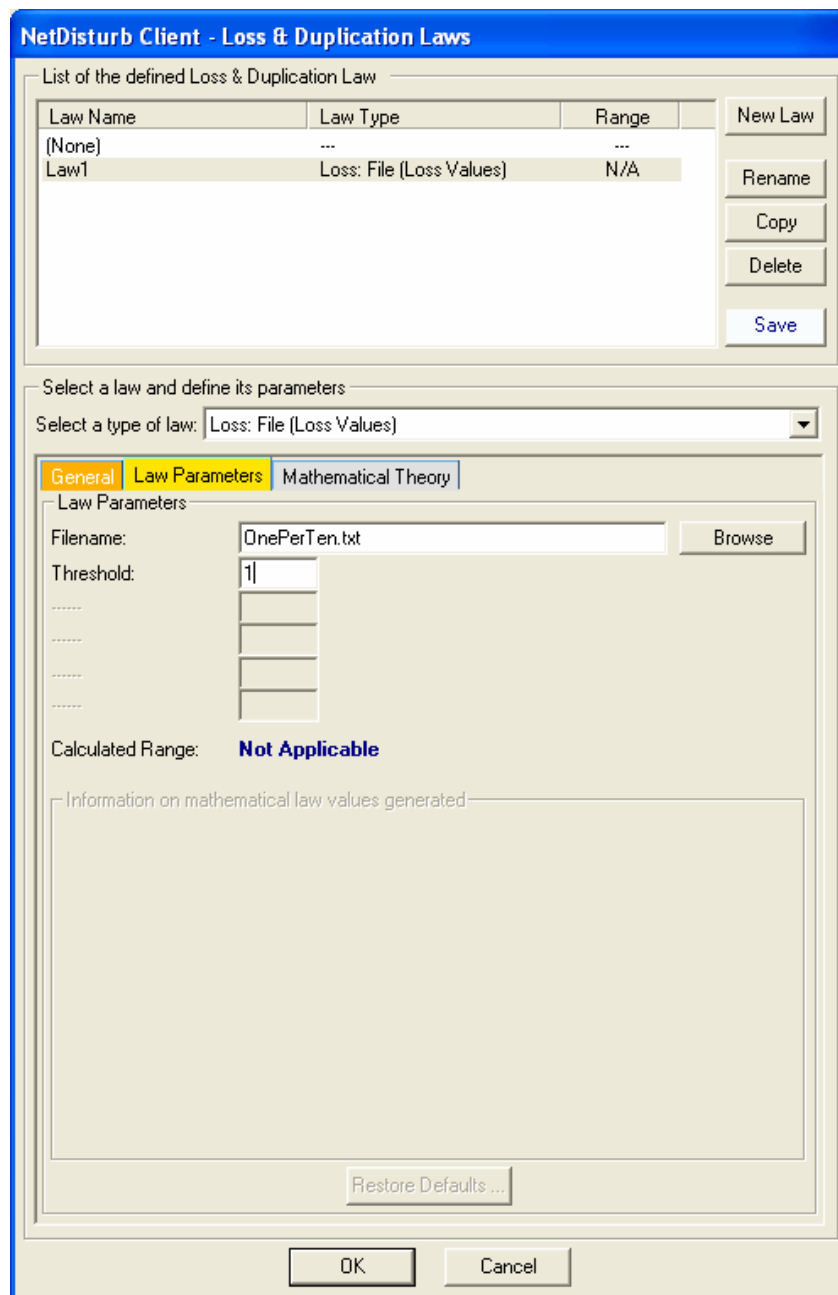
For this law, five parameters are defined:

- **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.



7.4.3.6 Loss: User-defined File



The dialog box is titled "NetDisturb Client - Loss & Duplication Laws". It contains a table listing defined laws and a section for defining parameters for a selected law.

Law Name	Law Type	Range
(None)	---	---
Law1	Loss: File (Loss Values)	N/A

Buttons on the right: New Law, Rename, Copy, Delete, Save.

Select a law and define its parameters:

Select a type of law: Loss: File (Loss Values)

General | **Law Parameters** | Mathematical Theory

Law Parameters:

Filename: OnePerTen.txt [Browse]

Threshold: 1

Calculated Range: **Not Applicable**

Information on mathematical law values generated:

[Restore Defaults ...]

OK Cancel

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 7.4.3.1) for each selected packet. If this number is greater or equal than the threshold, then the packet is lost. When the end of the file is reached, 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 τ is $0 < \tau < 100$.

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

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

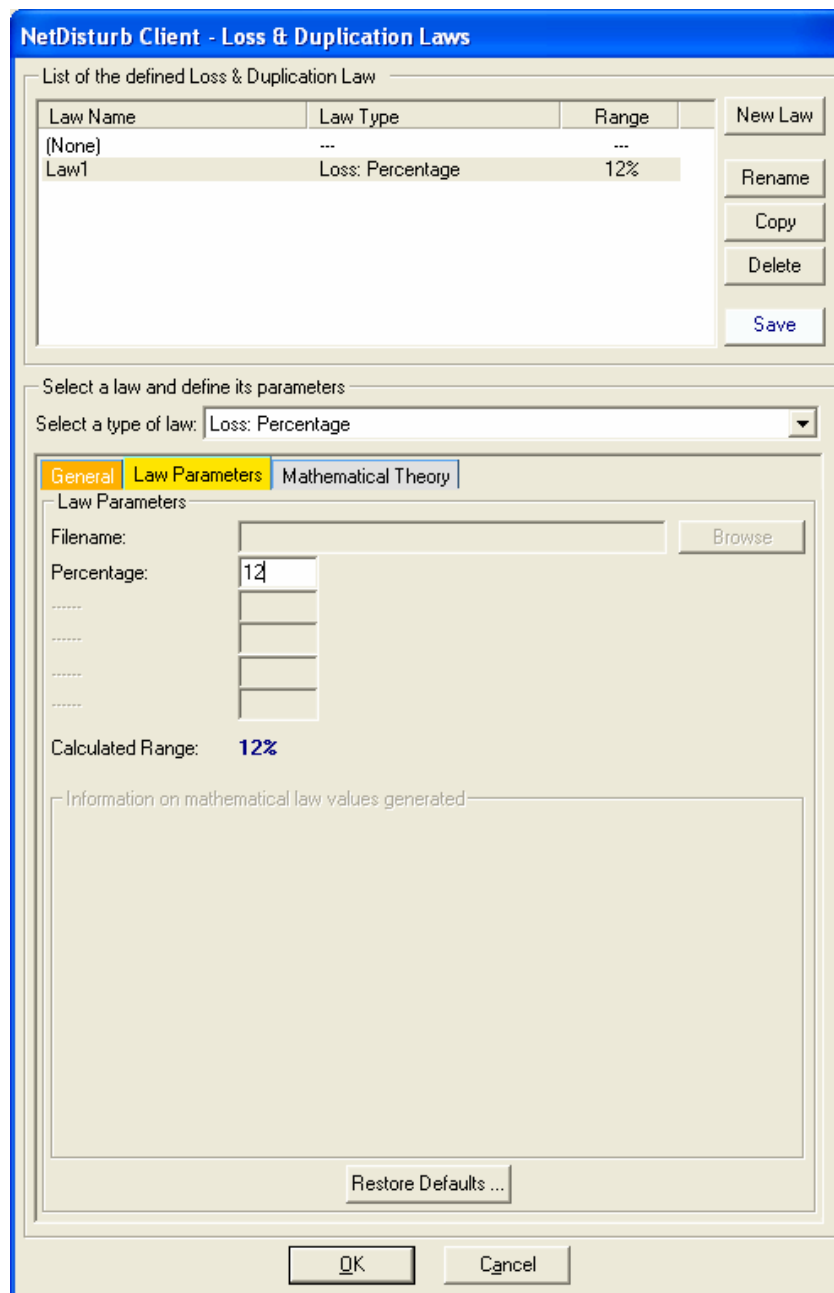
Here is another example of the impact of the threshold value. The content of the file is: 10 20 30 40 50 60 70 80 90 100

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

7.4.3.7 Loss: Percentage



The dialog box is titled "NetDisturb Client - Loss & Duplication Laws". It contains a table listing defined laws and a section for defining parameters for a selected law.

Law Name	Law Type	Range
(None)	---	---
Law1	Loss: Percentage	12%

Buttons on the right: New Law, Rename, Copy, Delete, Save.

Select a law and define its parameters:

Select a type of law: Loss: Percentage

General | **Law Parameters** | Mathematical Theory

Law Parameters

Filename: Browse

Percentage:

Calculated Range: 12%

Information on mathematical law values generated

Restore Defaults ...

OK Cancel

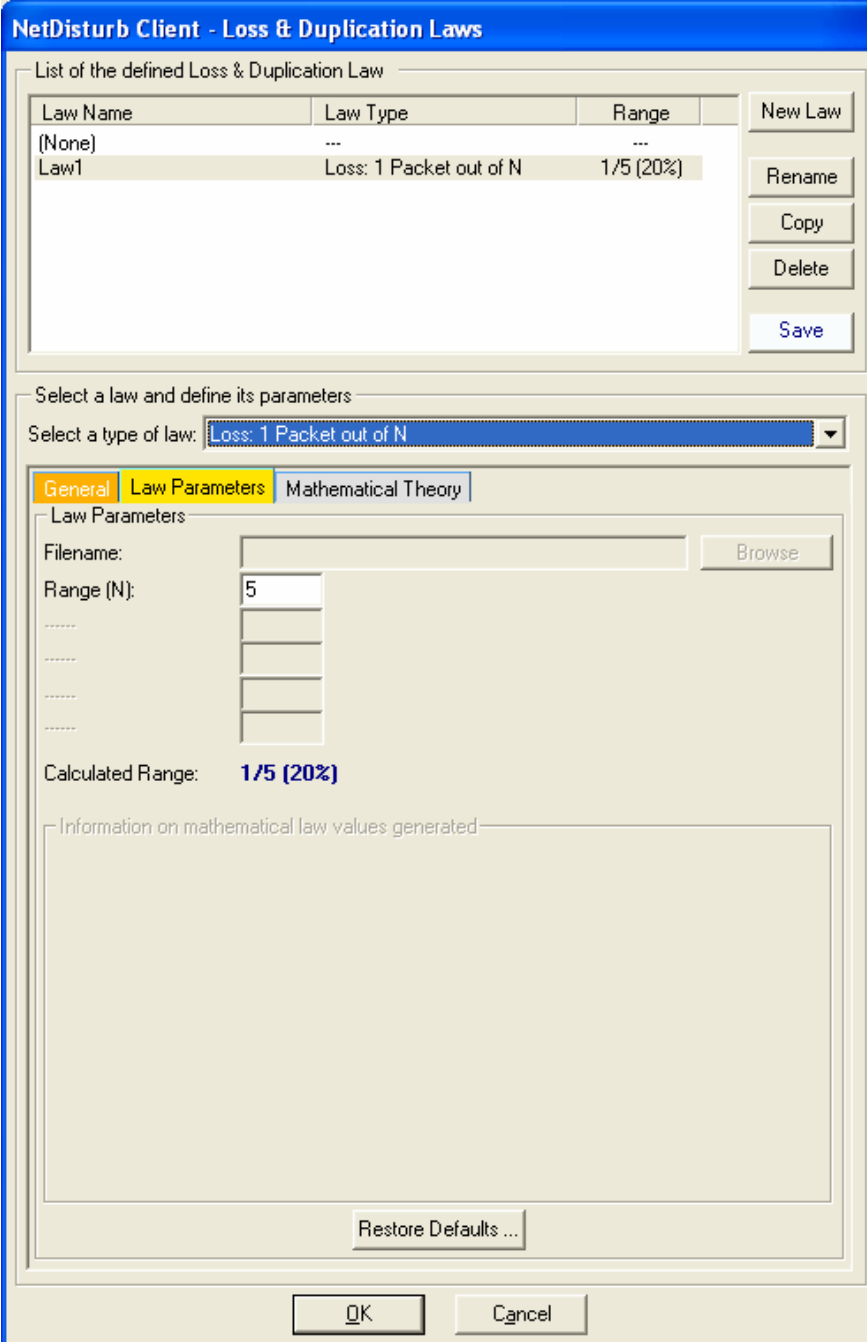
When this law is selected, a percentage of packets are lost and the packets to lose are randomly selected.

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.

7.4.3.8 Loss: 1 Packet out of N



The dialog box is titled "NetDisturb Client - Loss & Duplication Laws". It contains a table of defined laws and a section for defining a new law's parameters.

List of the defined Loss & Duplication Law

Law Name	Law Type	Range
(None)	---	---
Law1	Loss: 1 Packet out of N	1/5 (20%)

Buttons on the right: New Law, Rename, Copy, Delete, Save.

Select a law and define its parameters

Select a type of law: **Loss: 1 Packet out of N**

Tabbed interface: General (selected), Law Parameters, Mathematical Theory.

Law Parameters

Filename: Browse

Range (N):

Calculated Range: **1/5 (20%)**

Information on mathematical law values generated:

Restore Defaults ...

OK Cancel

This law allows losing 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 ... packet and so on are lost.

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

7.4.3.9 Loss: Percentage & Duration

NetDisturb Client - Loss & Duplication Laws

List of the defined Loss & Duplication Law

Law Name	Law Type	Range
(None)	---	---
Law1	Loss: Percentage & Duration	N/A

Buttons: New Law, Rename, Copy, Delete, Save

Select a law and define its parameters

Select a type of law: Loss: Percentage & Duration

General | **Law Parameters** | Mathematical Theory

Law Parameters

Packet Loss of % during milliseconds. Add

Packet Loss of 10% during 30000 milliseconds to be followed by a
 Packet Loss of 0% during 120000 milliseconds to be followed by a
 Packet Loss of 5% during 10000 milliseconds to be followed by a
 Packet Loss of 8% during 5000 milliseconds

Delete Move Up Move Down

Calculated Range: **Not Applicable**

Information on mathematical law values generated

OK Cancel

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.

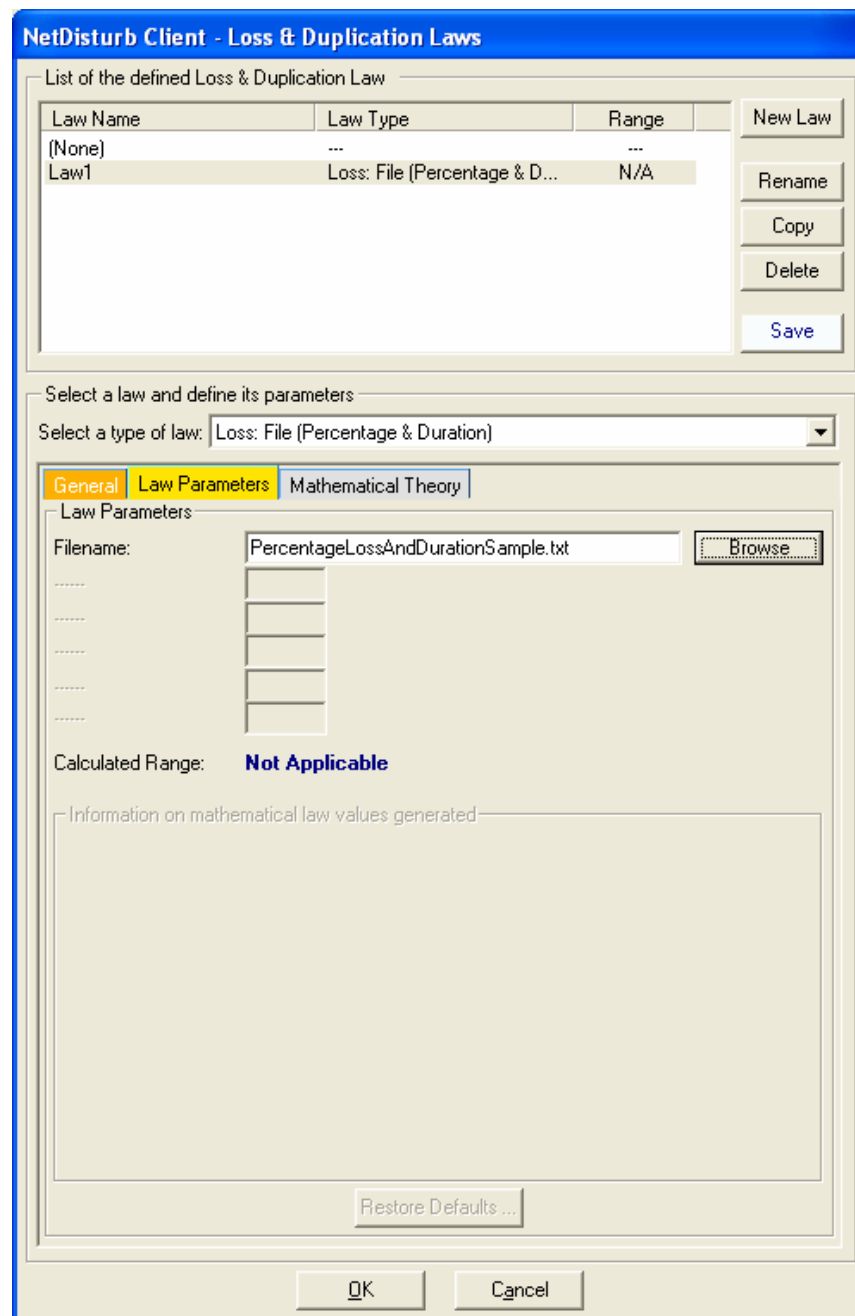
The percentage of lost packets is calculated on the basis of 100 received packets or a multiple of 100.

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.

7.4.3.10 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

7.4.3.11 General Rules concerning the Duplication of Packets

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

7.4.3.11.1 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.

7.4.3.11.2 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”.

7.4.3.12 Duplication: Percentage

NetDisturb Client - Loss & Duplication Laws

List of the defined Loss & Duplication Law

Law Name	Law Type	Range
(None)	---	---
Law1	Duplication: Percentage	5%

Buttons: New Law, Rename, Copy, Delete, Save

Select a law and define its parameters

Select a type of law: Duplication: Percentage

General | Law Parameters | Mathematical Theory

Law Parameters

Filename: [] Browse

Percentage: 5

Minimum Duplication: 1

Maximum Duplication: 3

Calculated Range: 5%

Information on mathematical law values generated

Restore Defaults ...

OK Cancel

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.

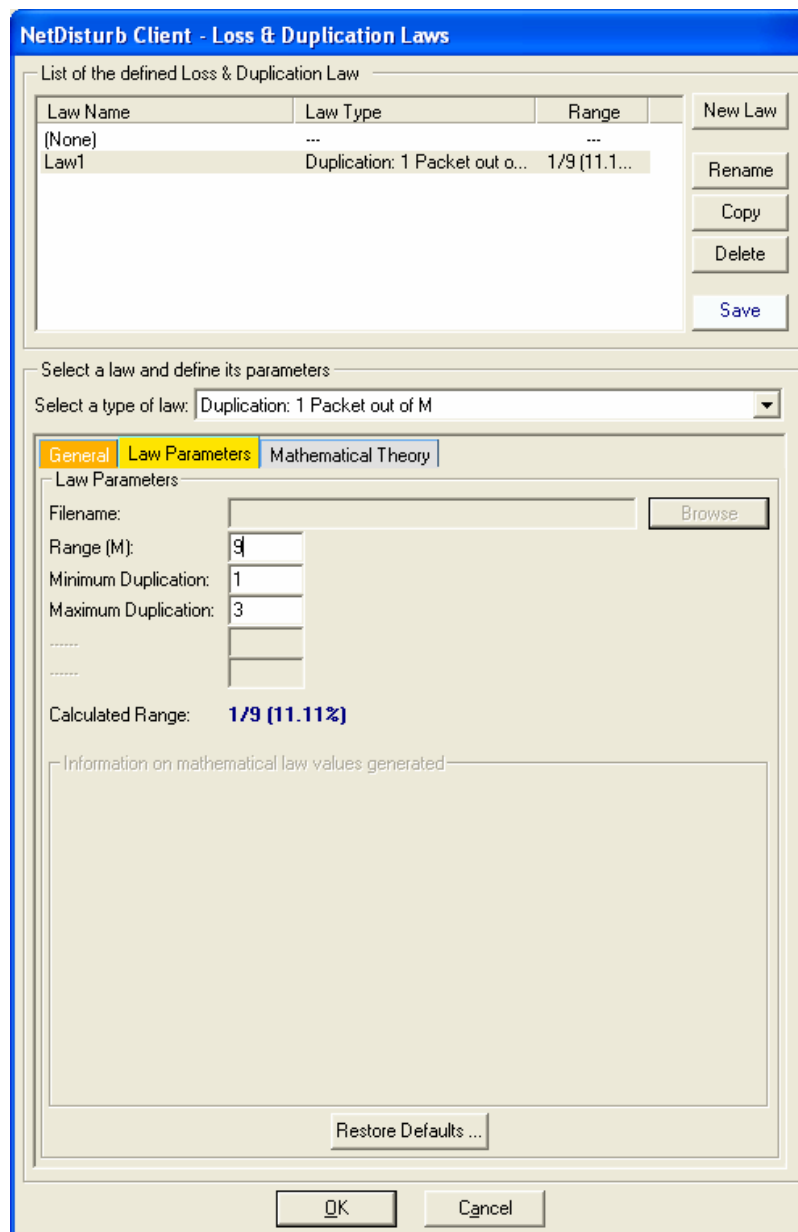
When '**Minimum Duplication**' equals '**Maximum Duplication**', all the eligible packets during the process of duplication are copied the same number of times.

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 7.4.3.11 for the general rules and terms relevant to the duplication of packets.

7.4.3.13 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 9th, 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 7.4.3.11 for the general rules and terms relevant to the duplication of packets.

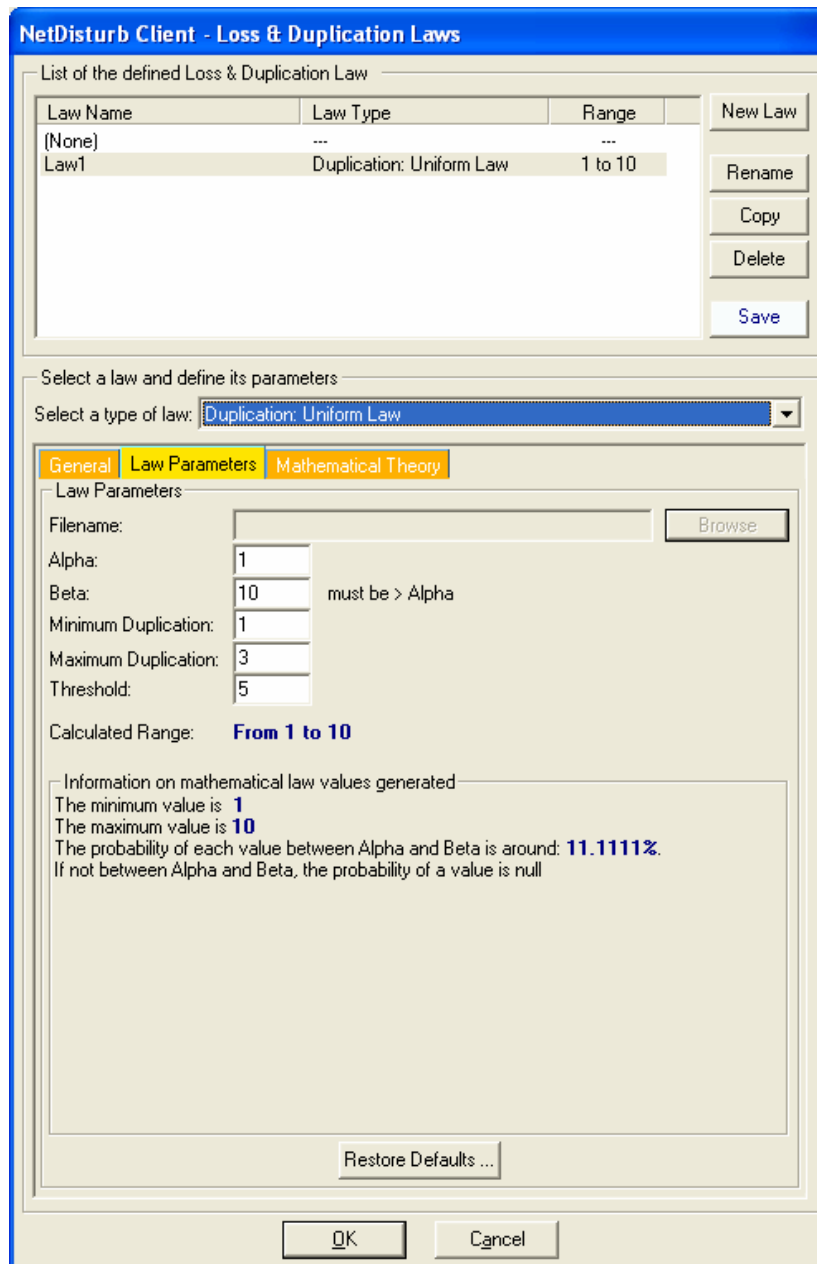
7.4.3.14 Duplication: Uniform Law

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.



The dialog box is titled "NetDisturb Client - Loss & Duplication Laws". It contains a table listing defined laws and a section for configuring a selected law.

List of the defined Loss & Duplication Law

Law Name	Law Type	Range
(None)	---	---
Law1	Duplication: Uniform Law	1 to 10

Buttons: New Law, Rename, Copy, Delete, Save

Select a law and define its parameters

Select a type of law: Duplication: Uniform Law

General | Law Parameters | Mathematical Theory

Law Parameters

Filename: Browse

Alpha:

Beta: must be > Alpha

Minimum Duplication:

Maximum Duplication:

Threshold:

Calculated Range: **From 1 to 10**

Information on mathematical law values generated

The minimum value is **1**

The maximum value is **10**

The probability of each value between Alpha and Beta is around: **11.1111%**

If not between Alpha and Beta, the probability of a value is null

Restore Defaults ...

OK Cancel

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

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

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

For this law, three parameters are defined:

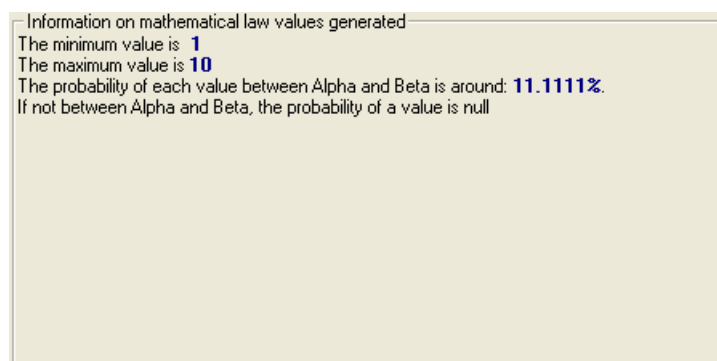
Alpha: min value of the range

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 7.4.3.11 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 this values using the user-defined parameters. Moreover, the probability of each value that can be generated is also available.



7.4.3.15 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)**. Refer to paragraph 7.4.3.8 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**. Refer to paragraph 7.4.3.13 Duplication: 1 Packet out of M for more details.

NetDisturb Client - Loss & Duplication Laws

List of the defined Loss & Duplication Law

Law Name	Law Type	Range
(None)	---	---
Law1	Loss (1 out of N) then Dupli...	1/5 & 1/10

Buttons: New Law, Rename, Copy, Delete, Save

Select a law and define its parameters

Select a type of law: Loss (1 out of N) then Duplication (1 out of M)

General | **Law Parameters** | Mathematical Theory

Law Parameters

Filename: Browse

Loss Range (N):

Duplication Range (M):

Minimum Duplication:

Maximum Duplication:

Calculated Range: **1/5 & 1/10**

Information on mathematical law values generated:

Restore Defaults ...

OK Cancel

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 20 packet set is the 45th) and the 88th (because packet #70 and #80 have been lost with a 20 packets set starting at 67th).

See also paragraph 7.4.3.11 for the general rules and terms relevant to the duplication of packets.

7.4.4 The Delay & Jitter Law Configuration

NetDisturb can delay the IP packets following a mathematical law configured by the user or using values extracted from an input file. These values apply to the IP packets matching to the selected mask, 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	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 & F.(Jitter)	Constant Delay & File (Jitter)	The file Random_delay.txt contains jitter values to add to the constant 10 ms delay.
F.(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 & F.(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 & F.(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).

7.4.4.1 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 mask that haven't been lost. For each packet, a new Delay & Jitter value is extracted from the law or from the file, depending on the type of law selected. These values are stored in a global table by 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 mask 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.

7.4.4.2 Delay & Jitter Accuracy

The **NetDisturb** driver accuracy is ± 2 milliseconds.

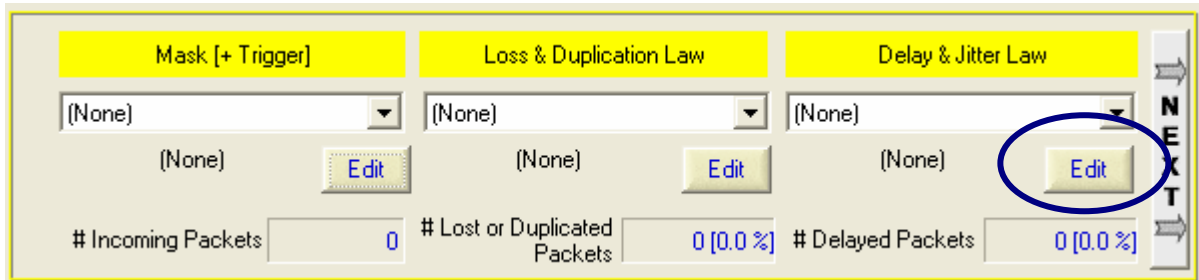
It means that a delay variation of one millisecond between two packets can't be taken into account. With such Delay & Jitter, the result is either no Delay & Jitter or a Delay & Jitter of 2ms at least.



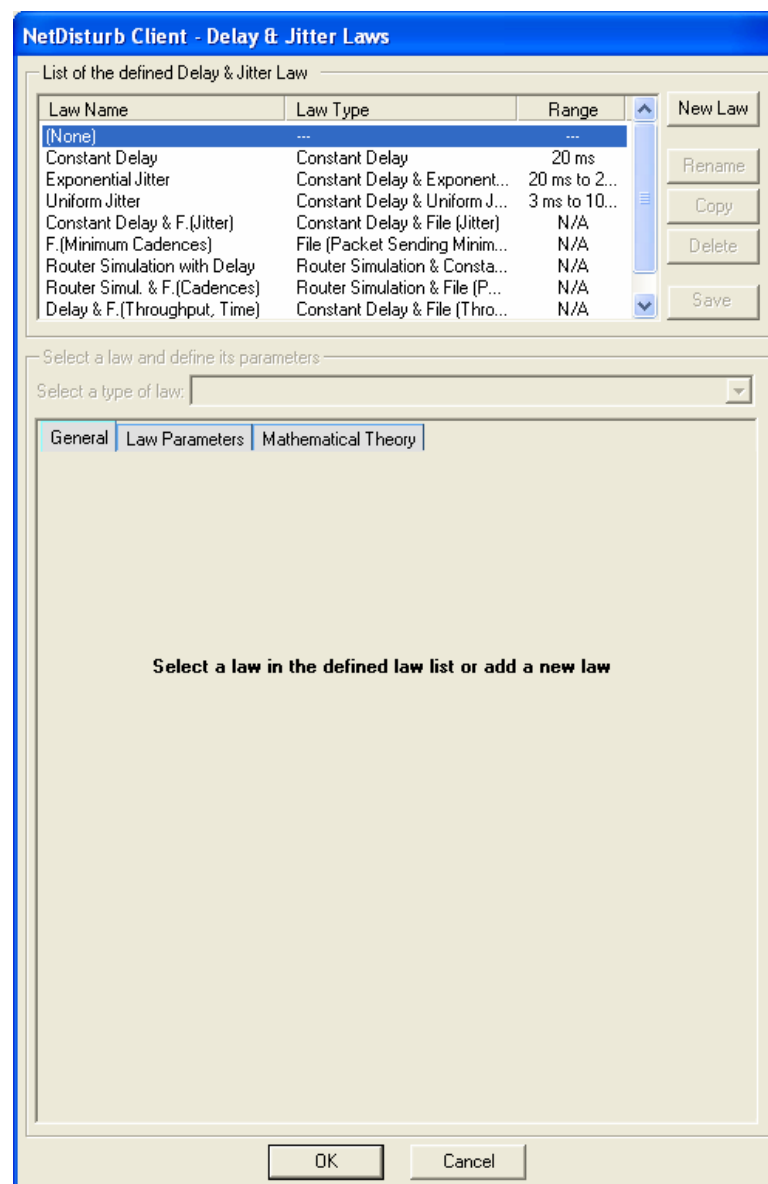
*The **NetDisturb** driver uses the OS timer accuracy to delay the packets. Because Windows is not a real-time OS, it may append Windows is not able to wake up the **NetDisturb** driver in the timely manner. In such case, the delay and/or jitter value is increased unexpectedly.*

7.4.4.3 How to create or edit the Delay & Jitter Law

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



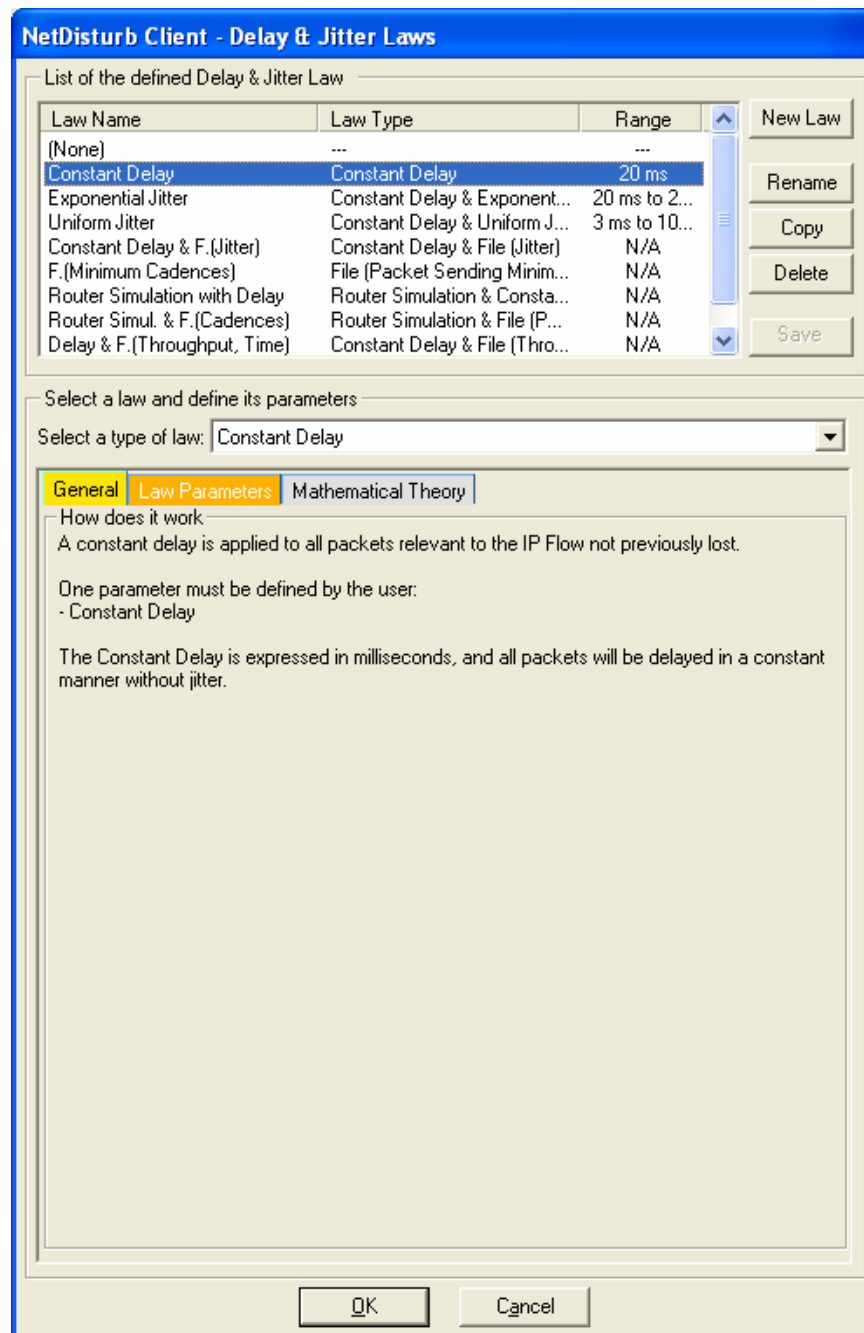
The following window is then displayed:



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

7.4.4.3.1 List of the Delay Laws defined

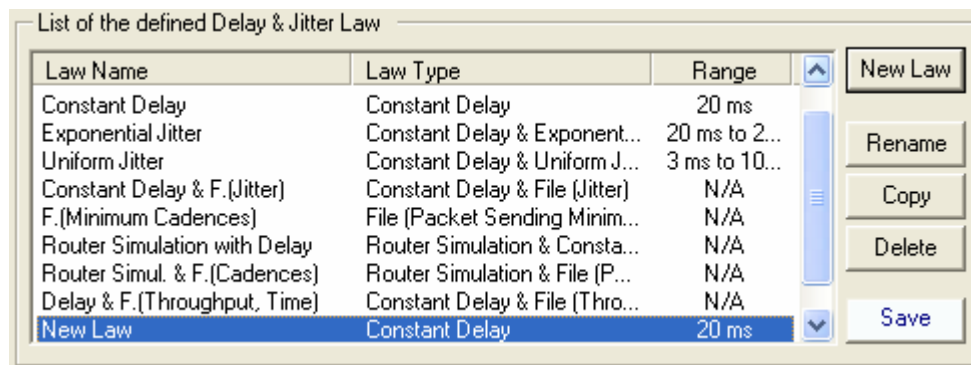
The list-box displays for each defined law the summary of the characteristics, except for (None) corresponding to 'No Delay & Jitter Law' selected:

- Law Name: name of the law
- Law Type: the type of Delay law chosen amongst the pre-defined list (more details available in paragraph 7.4.4.3.2 Select a law and define its parameters)
- Range: range of values generated by the specified laws.

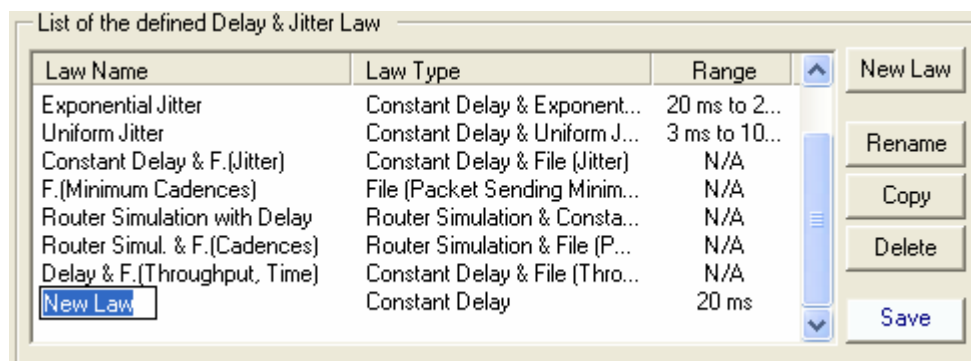
To manage the Law list, various buttons are available:

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:

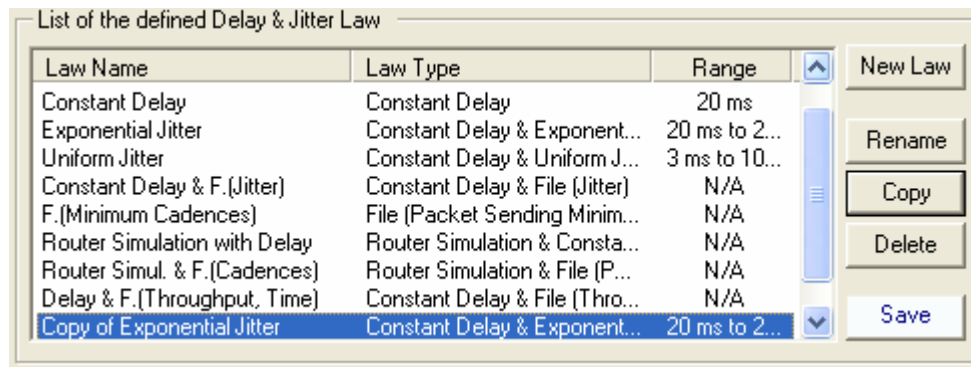


Then click on 'New Law' label to rename this entry or press the Rename button:

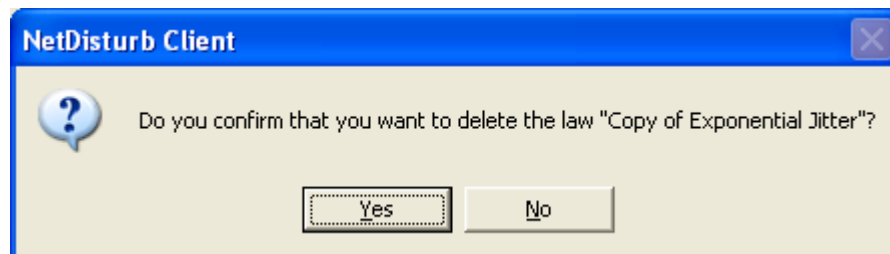


Rename: to rename the Law. This button should be used to change the Law name.

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.

7.4.4.3.2 *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 Content Impairment 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.

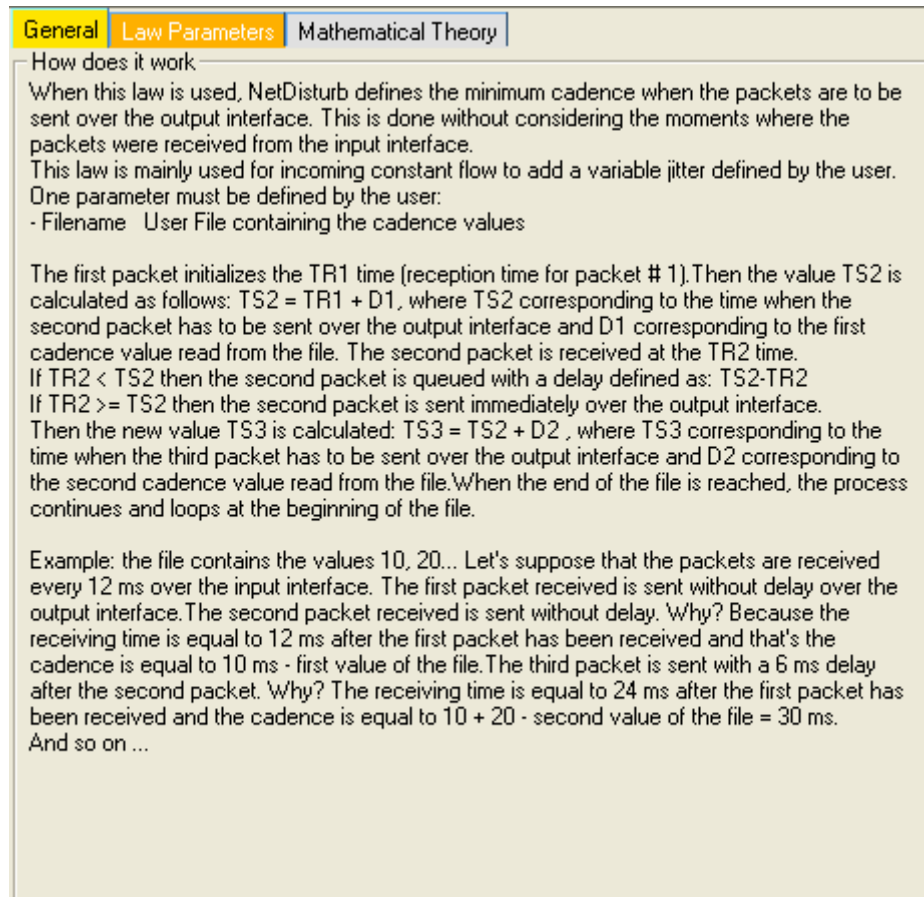
⇒ **Select a type of law**

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)

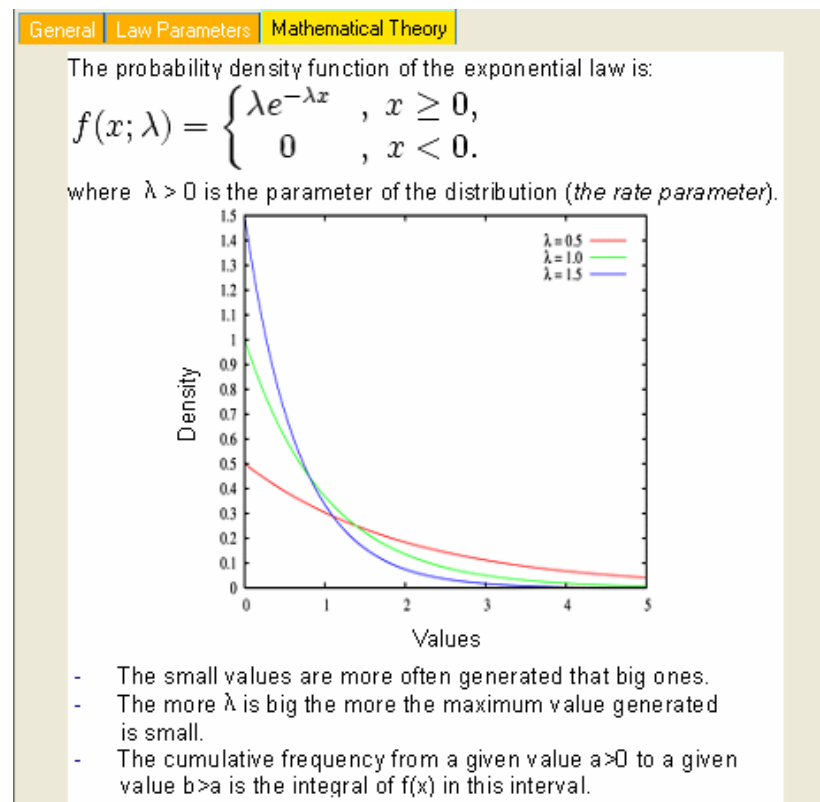
This tab is described for each law type here after.

⇒ 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:



⇒ Action buttons

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

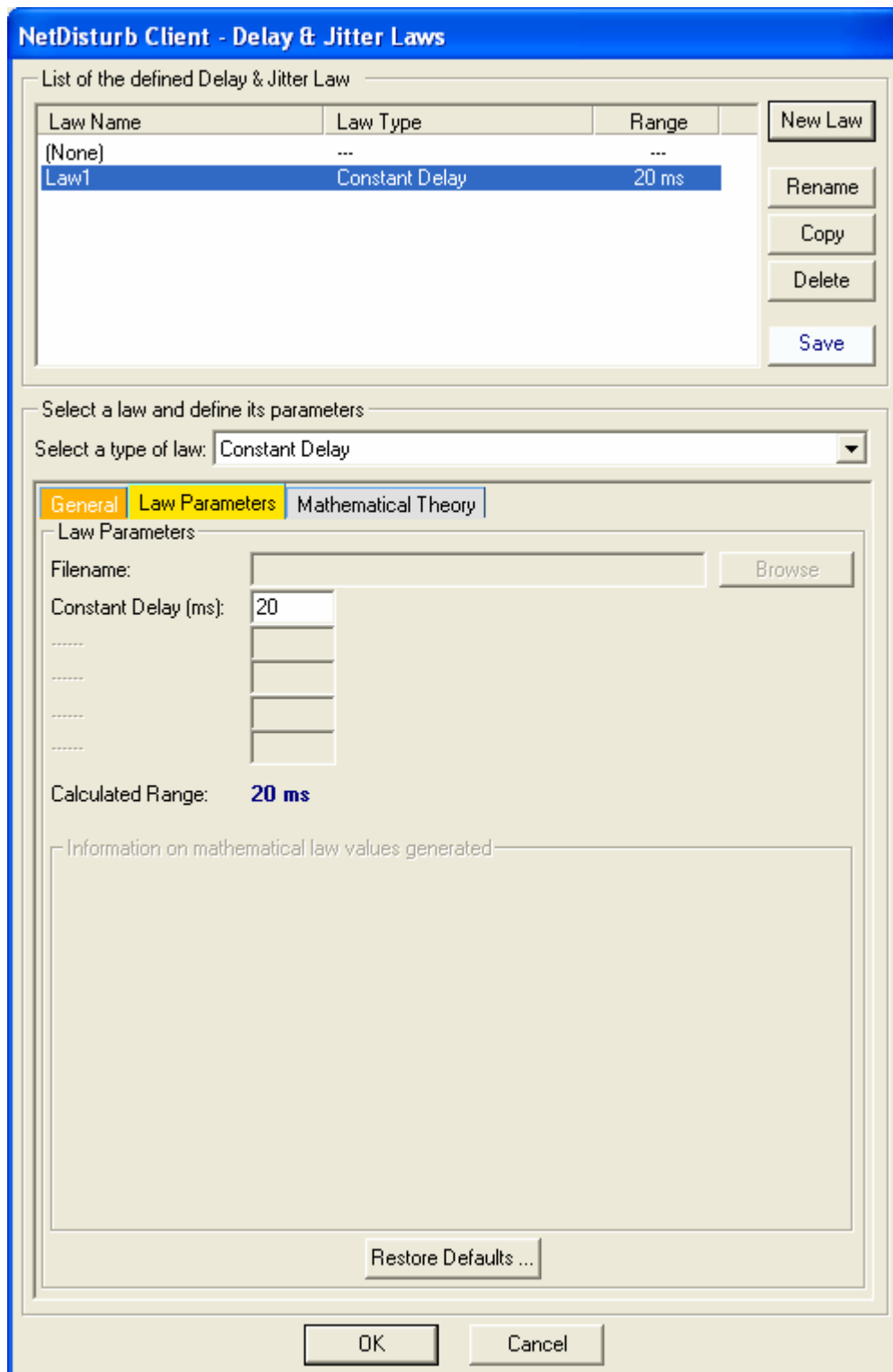
<i>Button</i>	<i>Action</i>
Restore Defaults ...	resets all parameters of the current law.
OK	saves all modifications made if you didn't save them before. Moreover, the selected law in the list of the defined laws becomes the selected law in the combo-box of the IP Flow window.
Cancel	ignores all modifications 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 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 IP Flow.

7.4.4.4 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.

7.4.4.5 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.

NetDisturb Client - Delay & Jitter Laws

List of the defined Delay & Jitter Law

Law Name	Law Type	Range
(None)	---	---
Law1	Constant Delay & Exponent...	20 ms to 1...

Buttons: New Law, Rename, Copy, Delete, Save

Select a law and define its parameters

Select a type of law: Constant Delay & Exponential Jitter

General | Law Parameters | Mathematical Theory

Law Parameters

Filename: Browse

Lambda:

Constant Delay (ms):

Calculated Range: **From 20 ms to 124 ms**

Information on mathematical law values generated

The minimum value is: **0**

The maximum value is: **104**

0.005 % of generated values are sitted after the value: **99**

The probability of the integer value (> 0) is around: **9.9574%**

For a cumulative frequency:

from (integer > 0) equal to % you should choose a lambda equal to: **0.0100503**

from (integer > 0) to infinity equal to % you should choose a lambda equal to: **4.6051702**

Restore Defaults ...

OK Cancel

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

Exponential law ($\lambda > 0$)

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

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

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 are 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.

Information on mathematical law values generated

The minimum value is: **0**

The maximum value is: **104**

0.005 % of generated values are sitted after the value: **99**

The probability of the integer value **1** (> 0) is around: **9.9574%**

For a cumulative frequency:

from **1** (integer > 0) equal to **1** % you should choose a
lambda equal to: **0.0100503**

from **1** (integer > 0) to infinity equal to **1** % you should choose a
lambda equal to: **4.6051702**

7.4.4.6 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.

NetDisturb Client - Delay & Jitter Laws

List of the defined Delay & Jitter Law

Law Name	Law Type	Range
(None)	---	---
Law1	Constant Delay & Uniform J...	21 ms to 1...

New Law
Rename
Copy
Delete
Save

Select a law and define its parameters

Select a type of law: **Constant Delay & Uniform Jitter**

General **Law Parameters** **Mathematical Theory**

Law Parameters

Filename: Browse

Alpha:

Beta:

Constant Delay (ms):

Calculated Range: **From 21 ms to 120 ms**

Information on mathematical law values generated

The minimum value is: **1**

The maximum value is: **100**

The probability of each value between Alpha and Beta is around: **1.0101%**

If not between Alpha and Beta, the probability of a value is null

Restore Defaults ...

OK Cancel

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

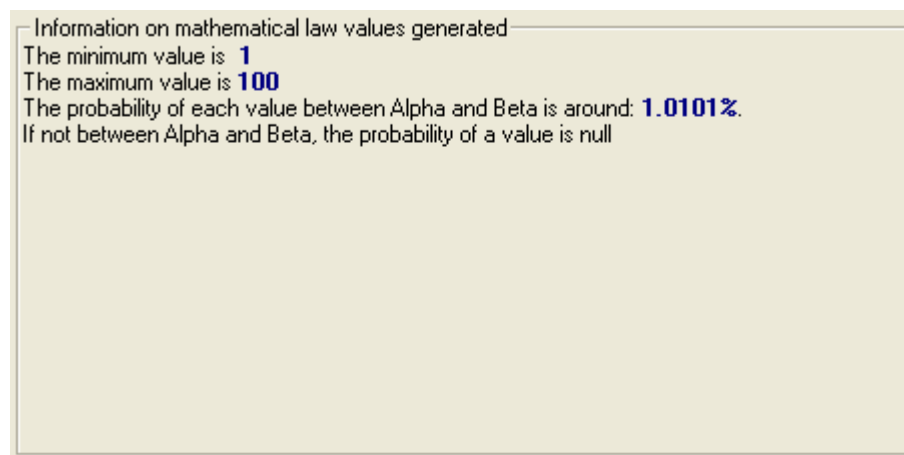
Uniform law on (α, β) range

$$f(x) = 1/(\beta - \alpha) \quad \text{if } \alpha < x < \beta$$
$$f(x) = 0 \quad \text{else}$$

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 are 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.



7.4.4.7 Constant Delay & File (Jitter)

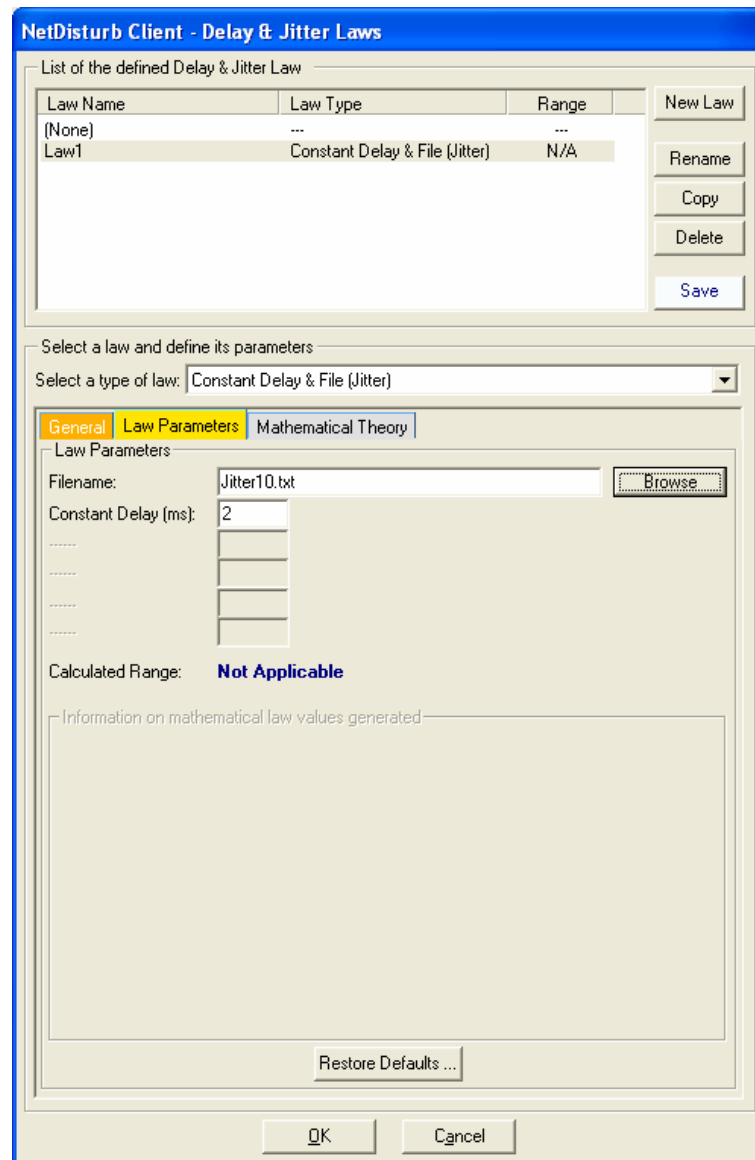
When this law is selected, the delay rate is obtained from a file.

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 law IP 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 read back the file from its beginning.

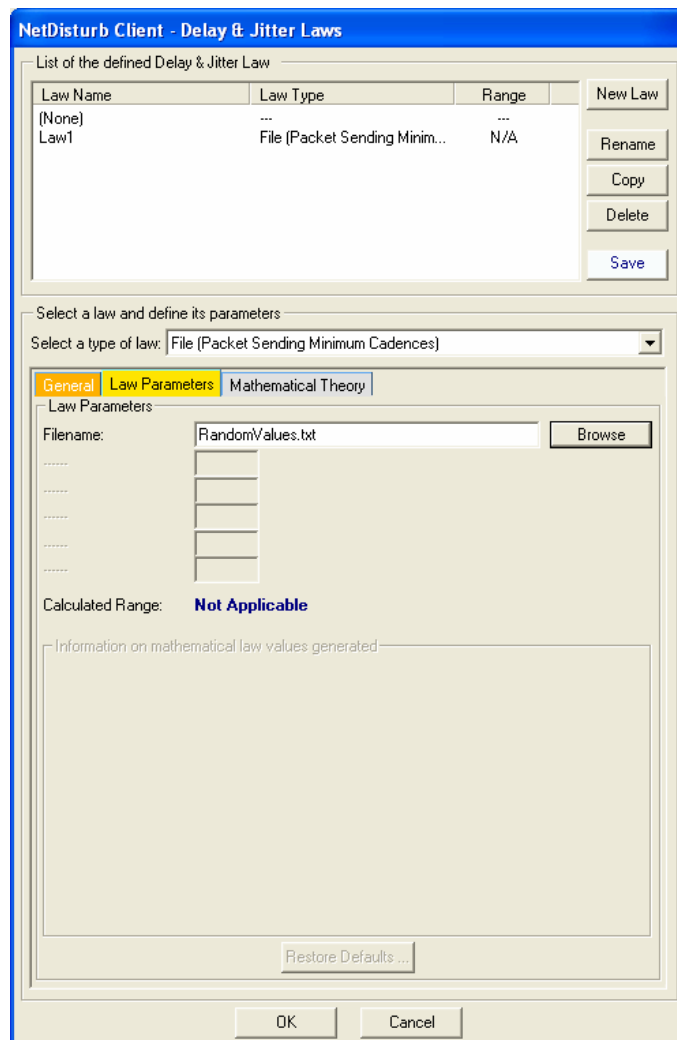
7.4.4.8 File (Packet Sending Minimum Cadences)

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 corresponding to the time when the second packet has to be sent over the output interface and D1 corresponding 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 $TR2 \geq TS2$ then the second packet is sent immediately over the output interface.

Then the new value $TS3$ is calculated: $TS3 = TS2 + D2$, where $TS3$ corresponding to the time when the third packet has to be sent over the output interface and $D2$ corresponding 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 equal to 12 ms after the first packet has been received and that's the cadence is equal 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 equal to $10 + 20$ - second value of the file = 30 ms.

And so on ...

7.4.4.9 Router Simulation & Constant Delay

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

- A limited **IP Throughput** on the output interface in Kbps.
- A **Constant Delay** (to simulate a network transit delay)
- 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**.

NetDisturb Client - Delay & Jitter Laws

List of the defined Delay & Jitter Law

Law Name	Law Type	Range
(None)	---	---
Law1	Router Simulation & Consta...	N/A

Buttons: New Law, Rename, Copy, Delete, Save

Select a law and define its parameters

Select a type of law: Router Simulation & Constant Delay

General | Law Parameters | Mathematical Theory

Law Parameters

Filename: Browse

IP Throughput (Kb/s):

Constant Delay (ms):

Maximum Memory (KB):

Calculated Range: **Not Applicable**

Information on mathematical law values generated

Restore Defaults ...

OK Cancel

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

(continue)

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

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

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

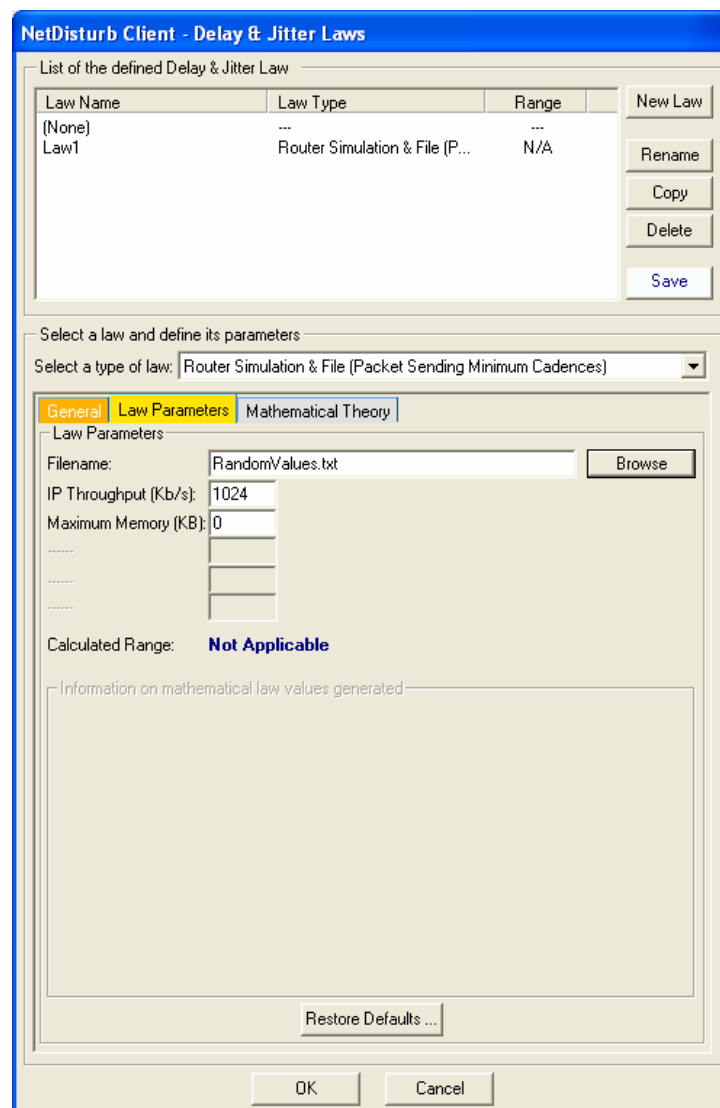
You shouldn't be surprised if packets continue to be sent even if no packet has been received: it is in most cases the **output queue** that is not yet empty.

7.4.4.10 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**.



7.4.4.11 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.

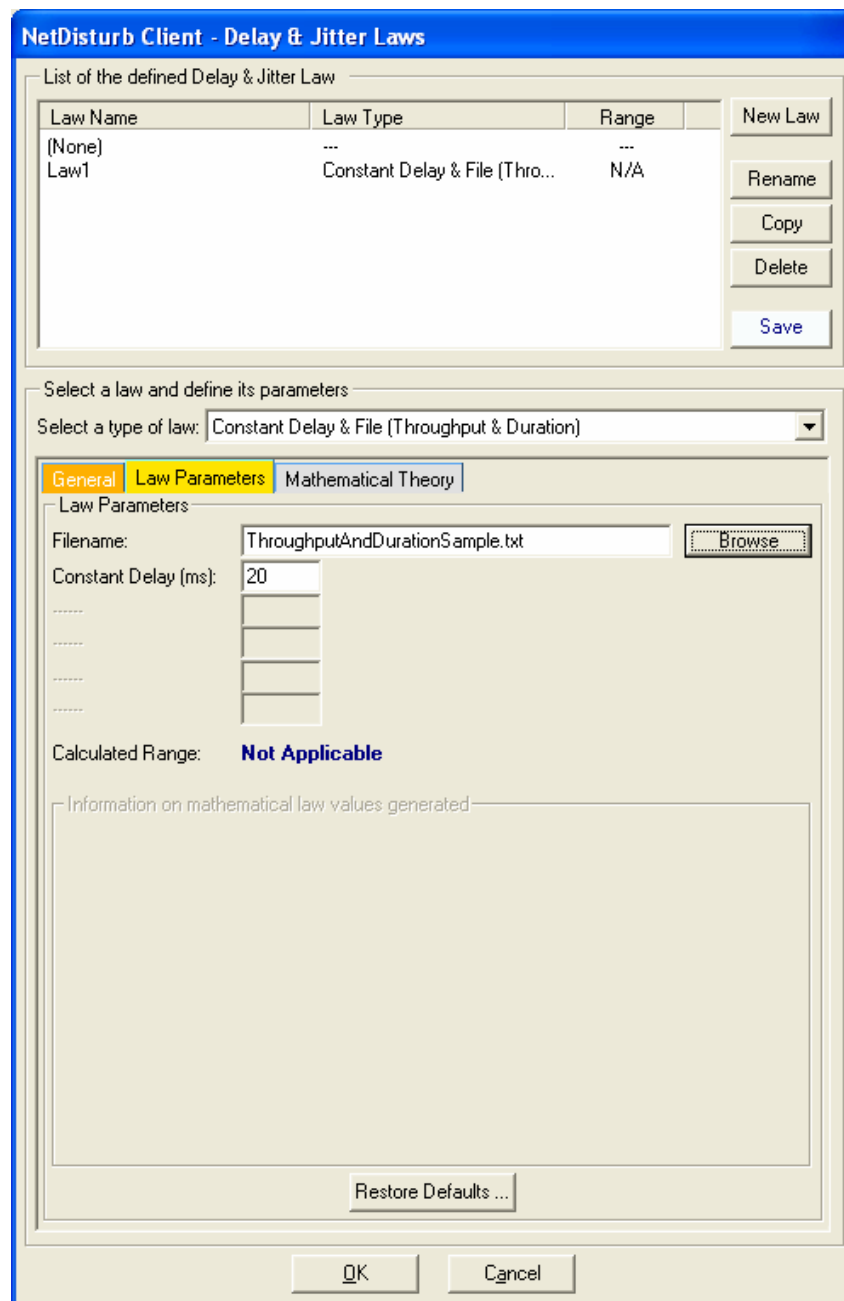
To assure performance, the file is read in one shot and stored in memory at law selection time. The values extracted from the file fill a table transmitted to the **NetDisturb** driver. In order to not overload the memory resources, the maximum read number of values is limited to 40,960 i.e. 20,480 couples.

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.

7.4.5 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 IP packets matching to the selected mask, 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	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 : <ul style="list-style-type: none"> 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 7.4.5.7 Packet Content Impairment Type for more details.

7.4.5.1 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 IP Flow, the law applies to all packets matching the mask. 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.

7.4.5.2 How to create or edit the Content Impairment Law

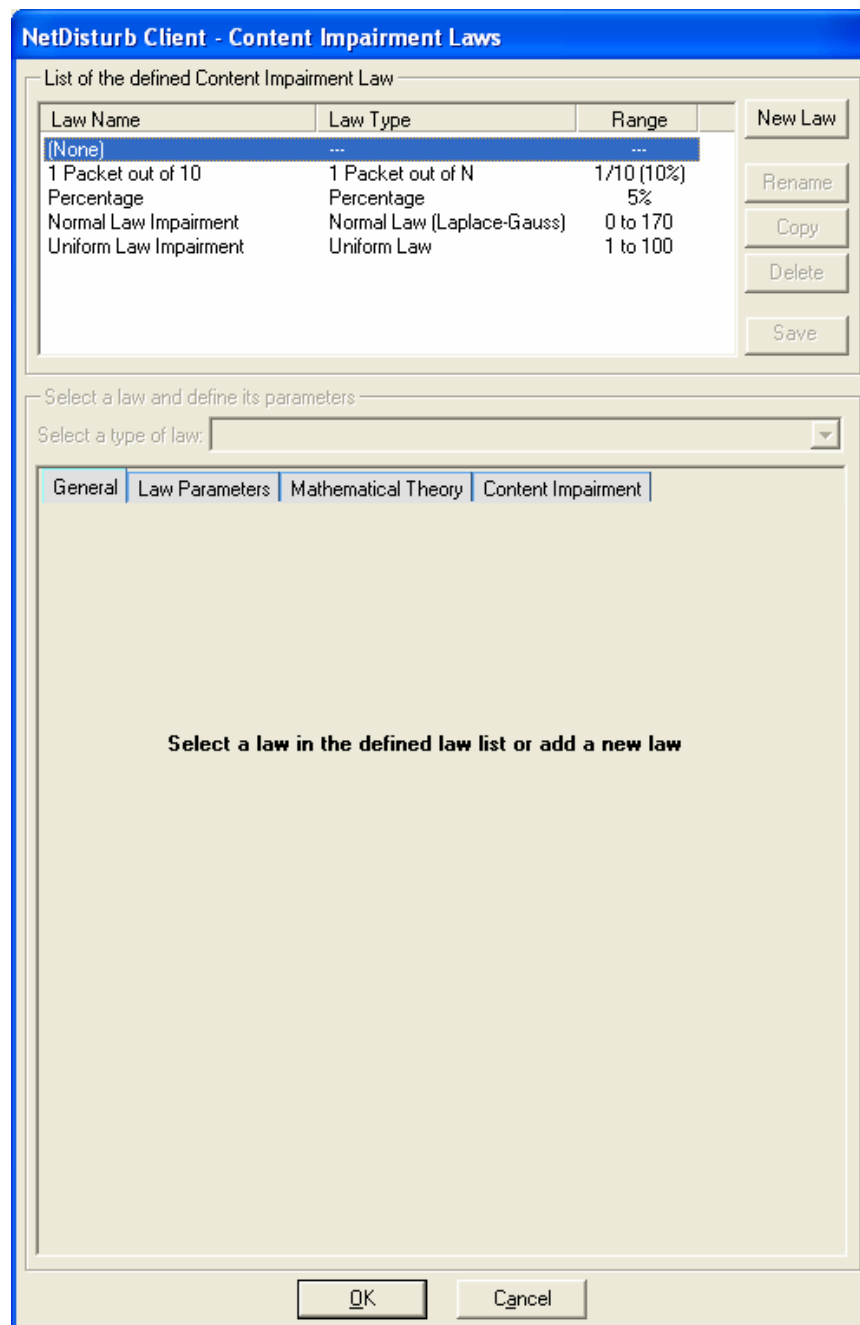
To create or configure a Packet Content Impairment Law click on the “Edit” button at the top or bottom part of the main window.

Click on the right arrow to access the edit button of the Content Impairment Law.

The first screenshot shows the top part of the main window with three tabs: "Mask [+ Trigger]", "Loss & Duplication Law", and "Delay & Jitter Law". Each tab has a dropdown menu set to "(None)", an "Edit" button, and a status display. The "Mask [+ Trigger" status is "# Incoming Packets 0". The "Loss & Duplication Law" status is "# Lost or Duplicated Packets 0 [0.0 %]". The "Delay & Jitter Law" status is "# Delayed Packets 0 [0.0 %]". A vertical "NEXT" button with right-pointing arrows is on the right, with the right arrow circled in blue.

The second screenshot shows the bottom part of the main window with three tabs: "Loss & Duplication Law", "Delay & Jitter Law", and "Content Impairment Law". Each tab has a dropdown menu set to "(None)", an "Edit" button, and a status display. The "Loss & Duplication Law" status is "# Lost or Duplicated Packets 0 [0.0 %]". The "Delay & Jitter Law" status is "# Delayed Packets 0 [0.0 %]". The "Content Impairment Law" status is "# Modified Packets 0 [0.0 %]". A vertical "NEXT" button with left-pointing arrows is on the left, and the "Edit" button for the "Content Impairment Law" tab is circled in blue.

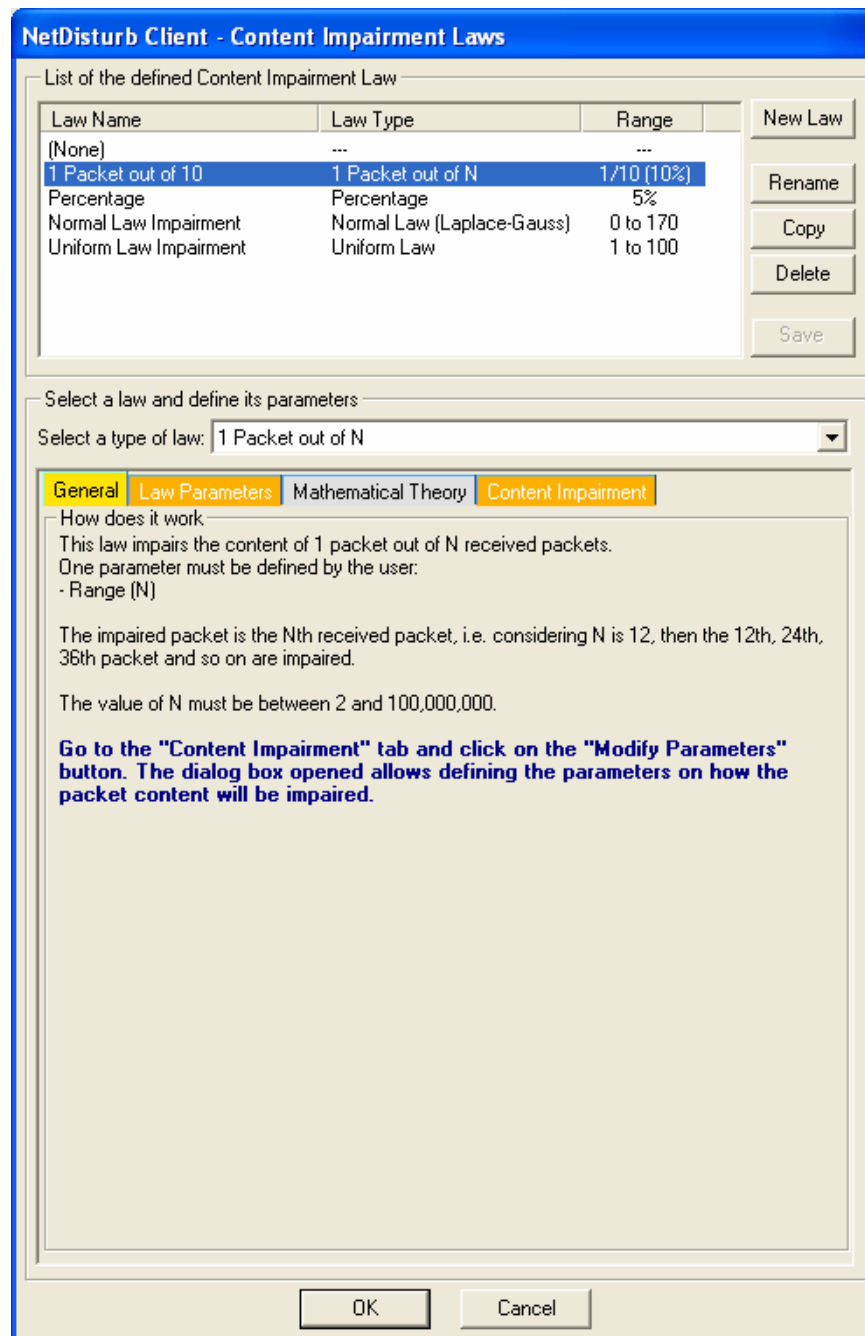
The following window is then displayed:



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 Content Impairment Law: a list-box displays the defined laws and five buttons allow managing the laws: New Law, Rename, Copy, Delete and Save.
- 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)
 - (tab 4) Content Impairment

7.4.5.2.1 List of the Content Impairment Laws defined

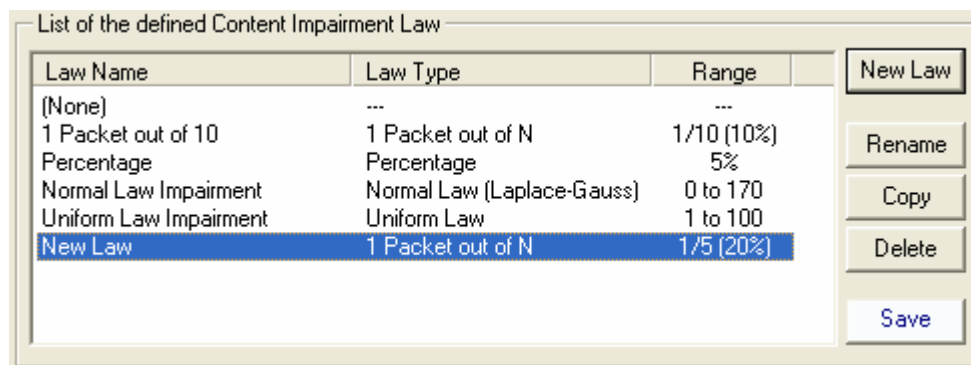
The list-box displays for each defined law the summary of the characteristics, except for (None) corresponding to 'No Content Impairment Law' selected:

- Law Name: Name of the law
- Law Type: The type of Content Impairment law chosen amongst the pre-defined list (more details available in 7.4.5.2.2 Select a law and define its parameters)
- Range: Range of values generated by the specified laws.

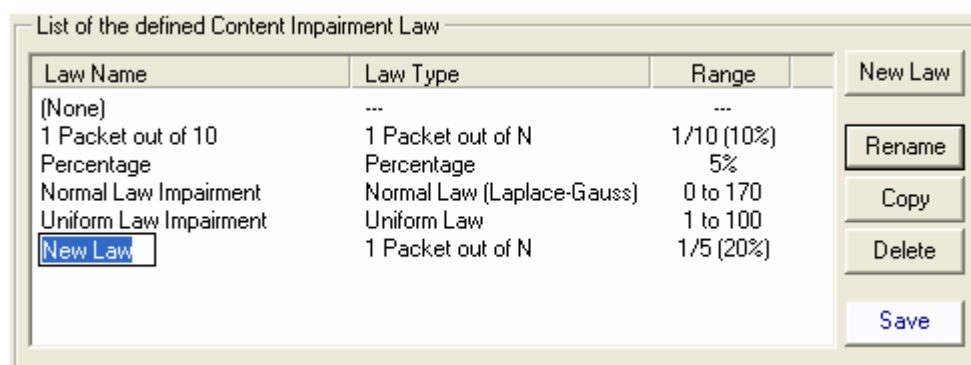
To manage the Law list, various buttons are available:

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:

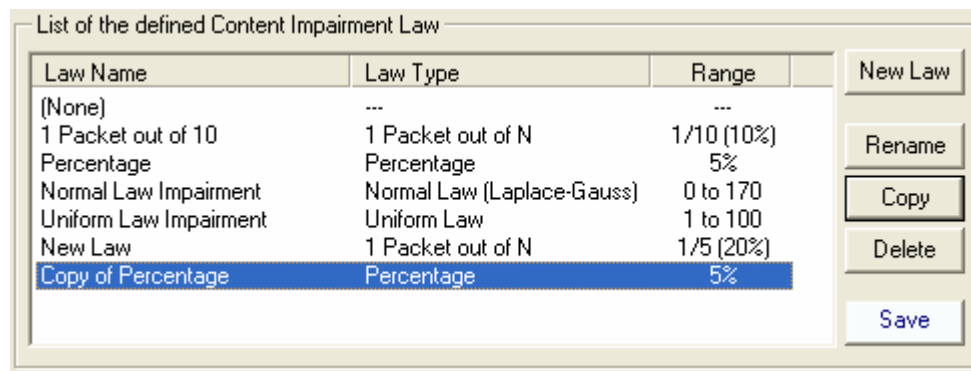


Then click on 'New Law' label to rename this entry or press the Rename button:

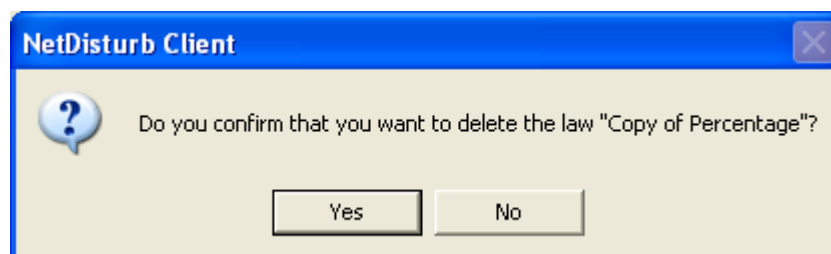


Rename: to rename the Law. This button should be used to change the Law name.

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.

7.4.5.2.2 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

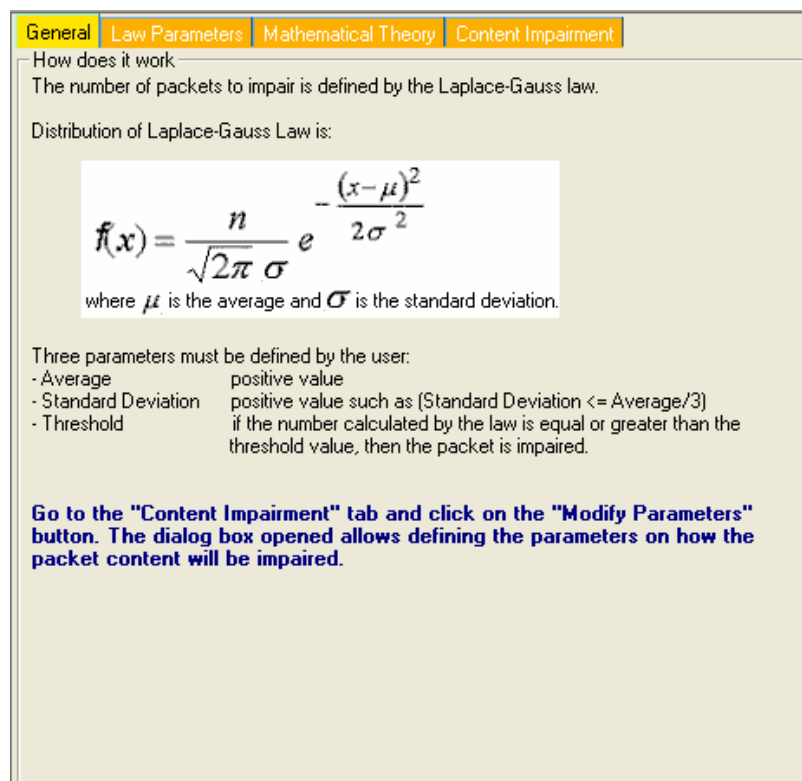
⇒ Select a type of law

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)

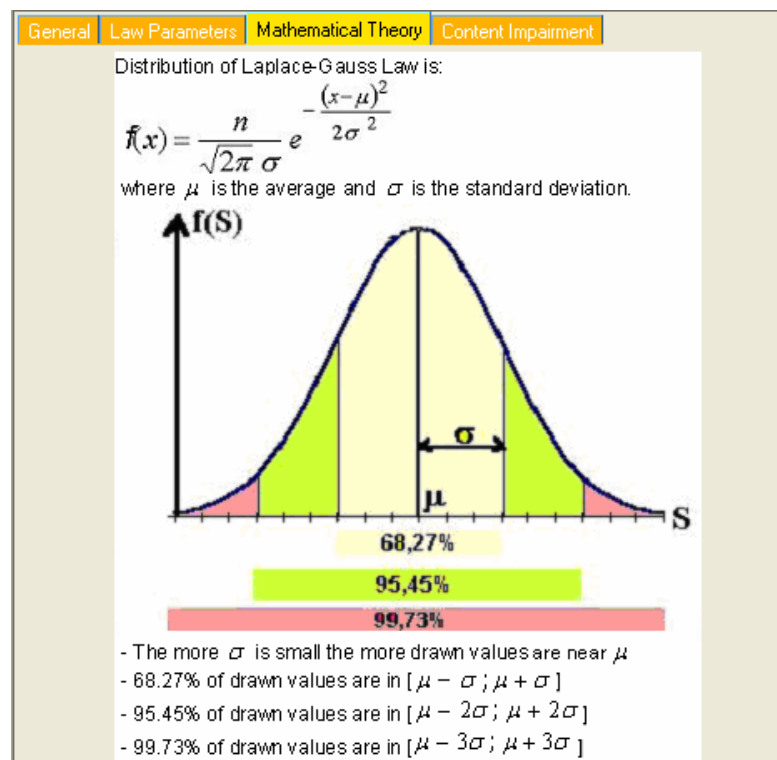
This tab is described for each law type here after.

⇒ 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 7.4.5.7 Packet Content Impairment Type.

⇒ Action buttons

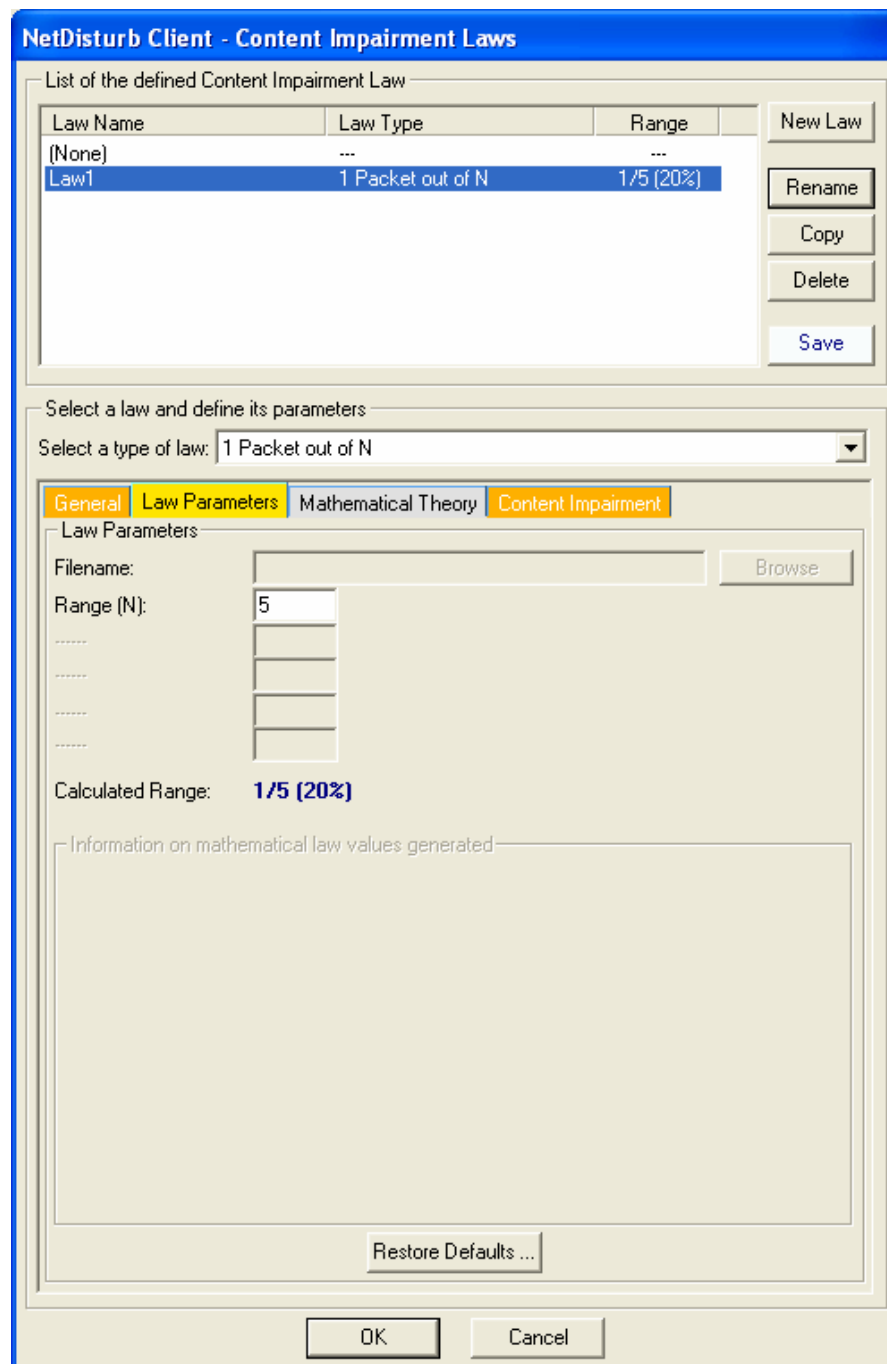
The "Content Impairment Laws" window handles a temporary list of laws until the user press the **OK** or **Cancel** button.

Button	Action
Restore Defaults ...	resets all parameters of the current law.
OK	saves 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	ignores 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 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 IP Flow.

7.4.5.3 1 Packet out of N

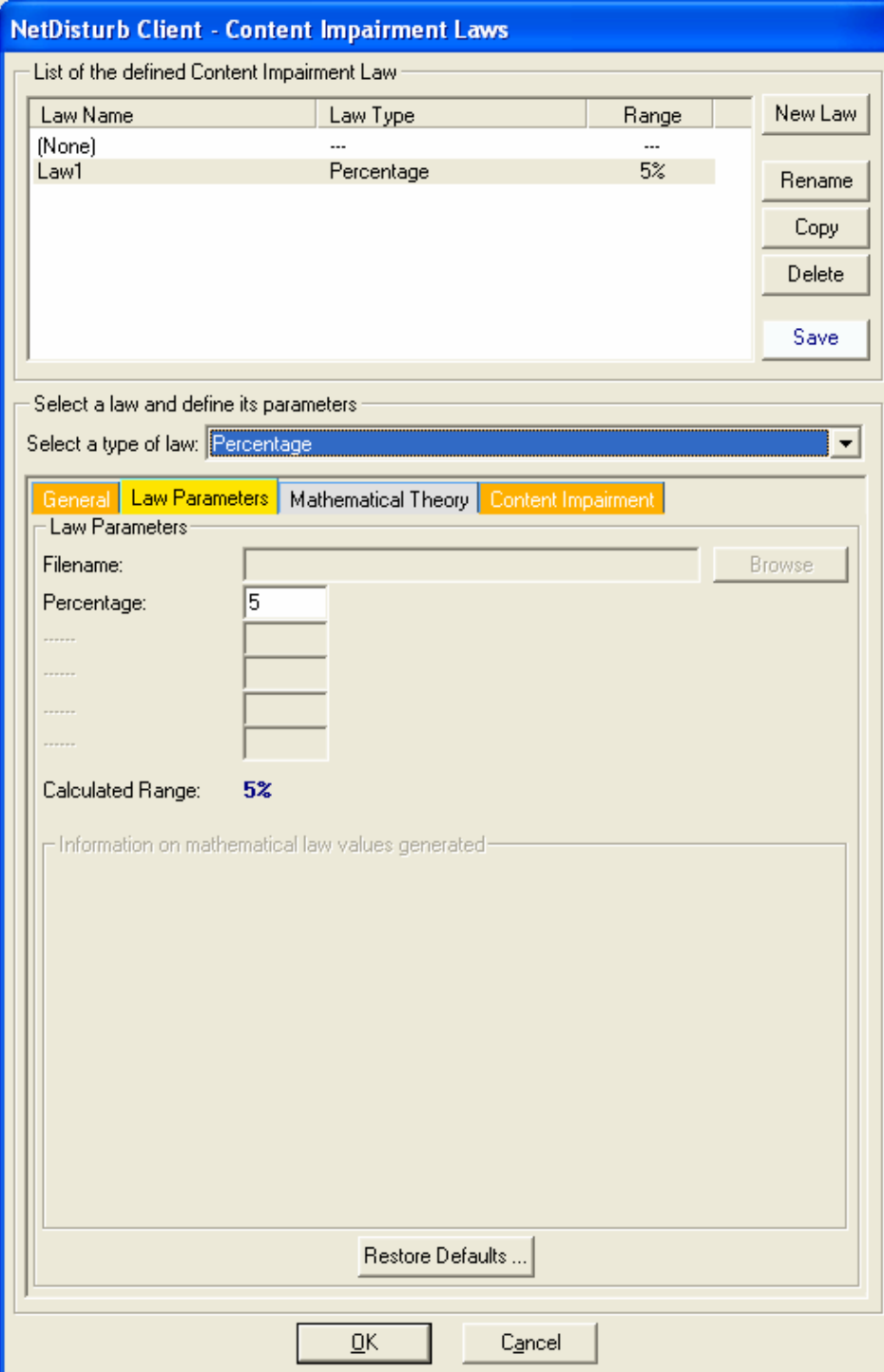


This law allows impairing the content of 1 packet out of N received packets. It affects a same packet based on its order.

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.

7.4.5.4 Percentage



The dialog box is titled "NetDisturb Client - Content Impairment Laws". It contains a table listing defined laws and a section for configuring a selected law.

List of the defined Content Impairment Law

Law Name	Law Type	Range
(None)	---	---
Law1	Percentage	5%

Buttons on the right: New Law, Rename, Copy, Delete, Save.

Select a law and define its parameters:

Select a type of law: **Percentage**

Tabbed interface with four tabs: General, Law Parameters, Mathematical Theory, Content Impairment. The "Law Parameters" tab is active.

Law Parameters

Filename: Browse

Percentage:

Calculated Range: **5%**

Information on mathematical law values generated:

Restore Defaults ...

OK Cancel

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.

7.4.5.5 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.

NetDisturb Client - Content Impairment Laws

List of the defined Content Impairment Law

Law Name	Law Type	Range
(None)	---	---
Law1	Uniform Law	1 to 10

Buttons: New Law, Rename, Copy, Delete, Save

Select a law and define its parameters

Select a type of law: Uniform Law

General | **Law Parameters** | Mathematical Theory | Content Impairment

Law Parameters

Filename: Browse

Alpha:

Beta:

Threshold:

Calculated Range: **From 1 to 10**

Information on mathematical law values generated

The minimum value is **1**

The maximum value is **10**

The probability of each value between Alpha and Beta is around: **11.1111%**

If not between Alpha and Beta, the probability of a value is null

Restore Defaults ...

OK Cancel

The **NetDisturb** driver picks a number in the table (see also 7.4.3.1) 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

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

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

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.

Information on mathematical law values generated

The minimum value is **1**

The maximum value is **10**

The probability of each value between Alpha and Beta is around: **11.1111%**.

If not between Alpha and Beta, the probability of a value is null

7.4.5.6 Normal (Laplace-Gauss) Law

NetDisturb Client - Content Impairment Laws

List of the defined Content Impairment Law

Law Name	Law Type	Range
(None)	---	---
Law1	Normal Law (Laplace-Gauss)	0 to 17

New Law
Rename
Copy
Delete
Save

Select a law and define its parameters

Select a type of law: **Normal Law (Laplace-Gauss)**

General **Law Parameters** **Mathematical Theory** **Content Impairment**

Law Parameters

Filename: Browse

Average:

Standard Deviation:

Threshold:

Calculated Range: **From 0 to 17**

Information on mathematical law values generated

The minimum value is: **0**

The maximum value is: **17**

99.73% of the values are included in **[7:13]**

The probability of the integer value is around: **< 0.0001%**

Restore Defaults ...

OK Cancel

The **NetDisturb** driver picks a number in the table (see also 7.4.3.1) 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

$$f(x) = 1/(\beta - \alpha) \quad \text{if } \alpha < x < \beta$$
$$f(x) = 0 \quad \text{else}$$

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.

Information on mathematical law values generated

The minimum value is: **0**
The maximum value is: **17**
99.73% of the values are included in **[7;13]**

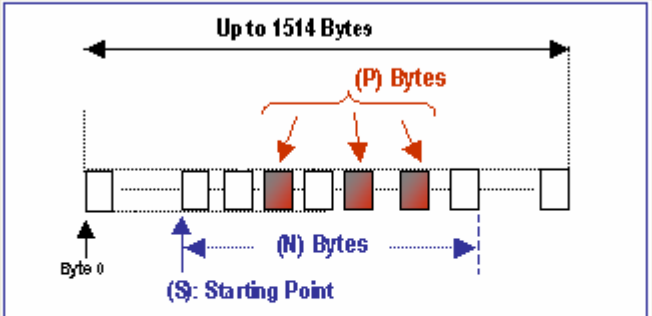
The probability of the integer value is around: **< 0.0001%**

7.4.5.7 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.

General Law Parameters Mathematical Theory **Content Impairment**

(P) Bytes impaired are randomly chosen by NetDisturb among **(N) Bytes** which are selected from the **Starting Point (S)**



Byte 0

Defined Parameters

(S): 0
(N): Random Value between (1) and (1513-S)
(P): Random Value between (1) and (N)
Impairment summary: One bit randomly selected and modified for each of the (P) Bytes
CRC recalculations after impairment: Yes

Modify Parameters

The following window is then displayed when you click on the "Modify Parameters" button:

NetDisturb - Content Impairment Type

[P] Bytes impaired are randomly chosen by NetDisturb among [N] Bytes which are selected from the Starting Point [S]

Up to 1514 Bytes

Byte 0

(S) Starting Point

(N) Bytes

(P) Bytes

1

2 Define the Starting Point (S) from where the impairments will start
[S]: 0 (Value from 0 to 1513)

3 Define the number of Bytes (N) to be selected from the Starting Point
☒ Random Value between (1) and (1513 - S)
[N]: 0 (Value from 0 to 1514-[S]) [see the parameter above]
0 means up to the end of the frame

4 Define the number of Bytes (P) to be impaired
☒ Random Value between (1) and (N)
[P]: 0 (Value from 0 to N)
0 means that all Bytes should be impaired

5 Type of impairment to apply
☐ Invert bits [0] (1 to 8) for each of the (P) Bytes
☐ Invert bits per pair (1-2, 3-4, 5-6, 7-8) for each of the (P) Bytes
☐ Invert Bytes per pair
☒ One bit randomly selected and modified for each of the (P) Bytes
☐ Use this pattern to replace the content of the (P) Bytes that should be impaired
(hexadecimal value)

6 Option
☒ CRC recalculations [IP & Protocol (TCP, UDP, IGMP, ICMP)] after applying the impairments

OK Cancel

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):

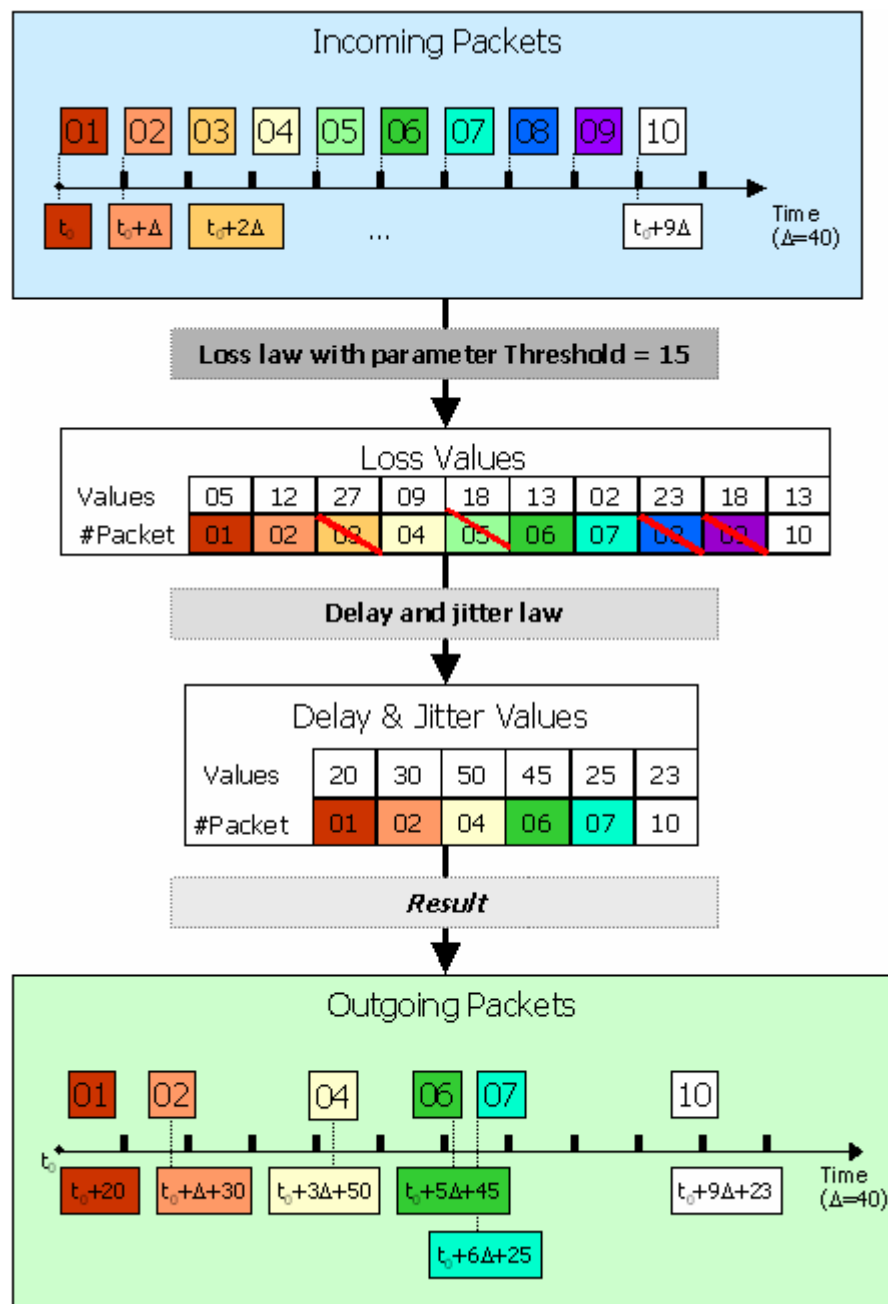
10101011 (Bin)
AB (Hex)
 - Use a V pattern to replace the content of the (P) Bytes that should be impaired.
 If the V pattern is bigger than (P) Bytes to replace, only the (P) first Bytes of the V pattern are used. If the V pattern is smaller than (P) bytes, all or part of the V pattern is used several 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

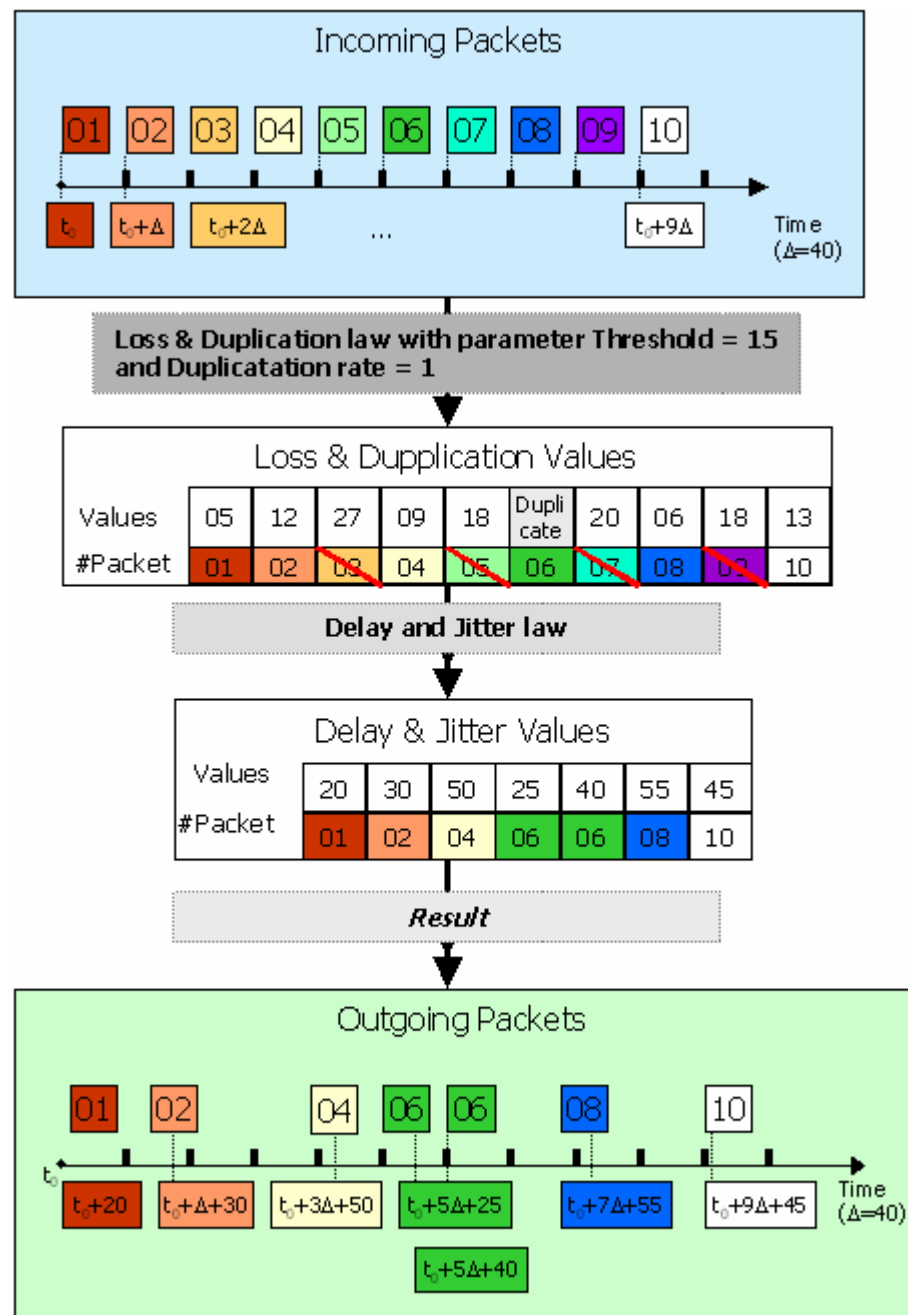
7.4.6 Loss/Duplication, Delay/Jitter Dynamics

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



7.4.7 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 ($A \rightarrow B$ and/or $B \rightarrow A$).

The IP Flow order in the aggregate defines the priority of packets to delay. While the top IP Flow packets gets the highest priority, the other IP Flows packets are queuing until there are no higher priority packets.

All the IP Flows related to the aggregate must have their own Mask 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 this 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 mask.

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.

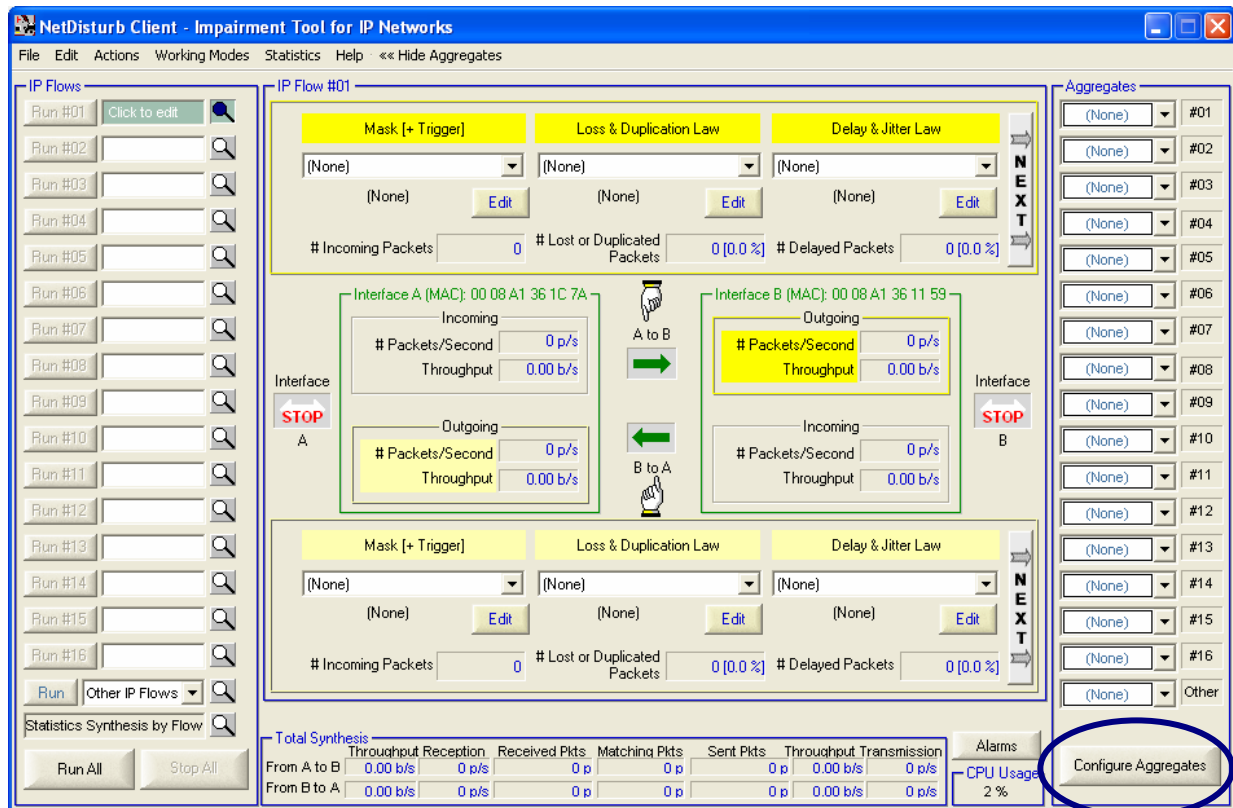
So the HTTP packets are first processed with the IP Flow # 01, then the TCP packets are handled with the IP Flow # 02 and the UDP packets are finally processed with the IP Flow # 03.

To implement this example, take the following steps:

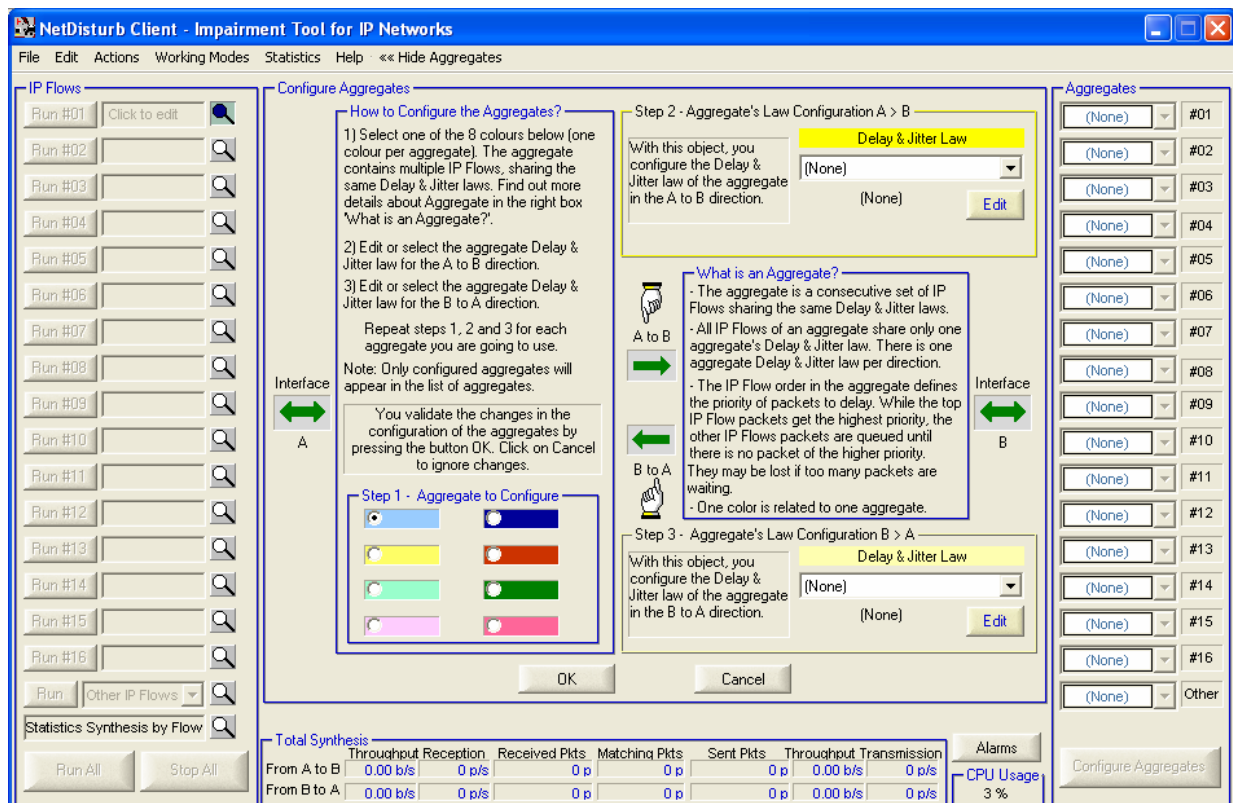
- **Step 1:** you must define the Mask and the Loss & Duplication Law for the three IP Flows:
 - IP Flow #01:
 - Mask: Source Port List = 80
 - Loss & Duplication Law: select 1 predefined loss law
 - IP Flow #02:
 - Mask: Protocol = TCP
 - Loss & Duplication Law: select 1 predefined duplication law
 - IP Flow #03:
 - Mask: Protocol = UDP
 - No Loss & Duplication Law
- **Step 2:** you 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:** you can now apply 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:

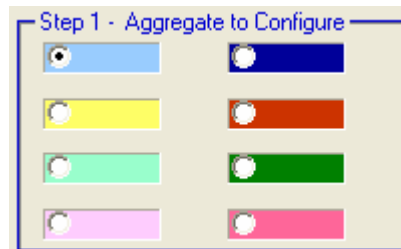


You can define up to 8 aggregates and one aggregate is associated with one color.

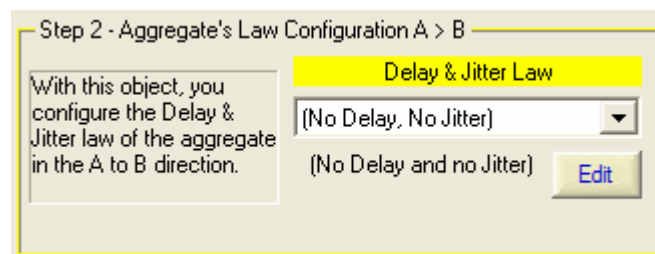
Four steps are necessary to parameter an aggregate.

The step 2 and the step 3 are optional, but at least one Delay & Jitter Law should be defined.

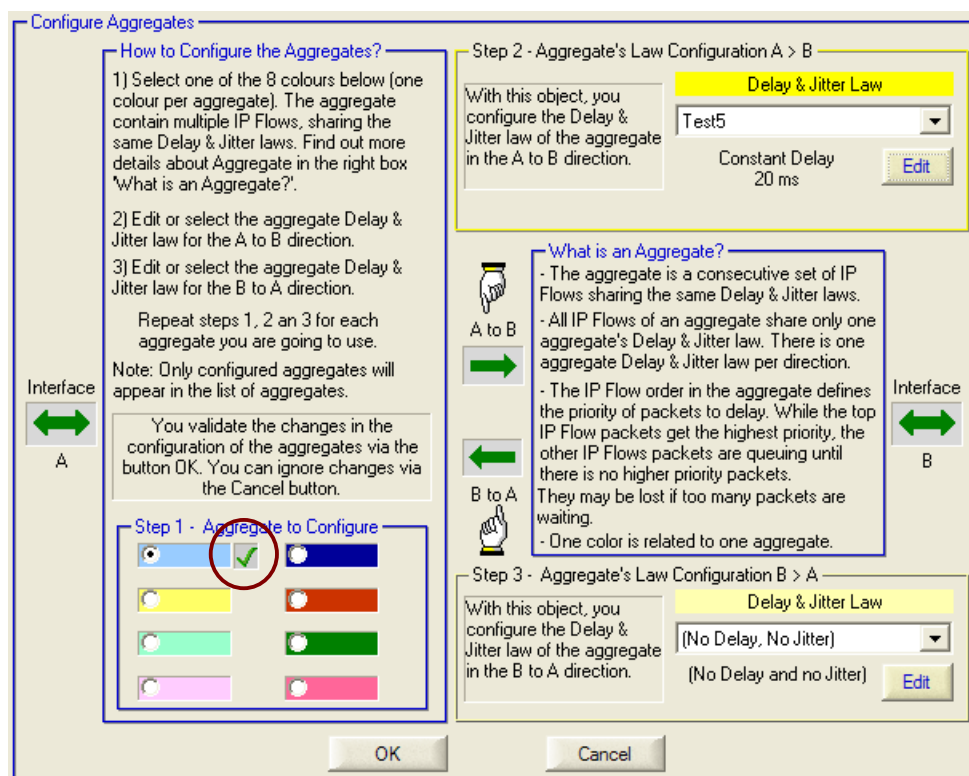
- Step 1: Select first a color among 8 for the aggregate



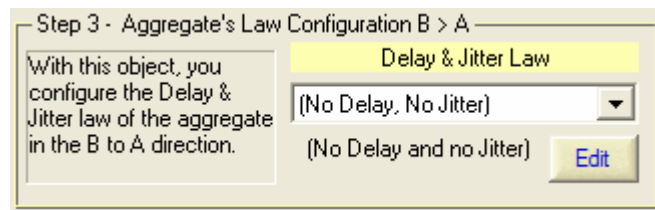
- Step 2 (optional): Select or define a Delay & Jitter Law in the A → B direction



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

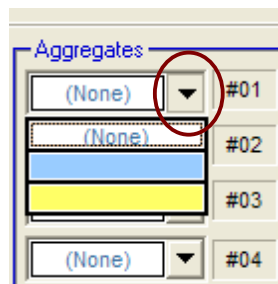


Once the law has been selected or defined, if the tick mark was not already present, it will be displayed on the right of the color box, as shown above.

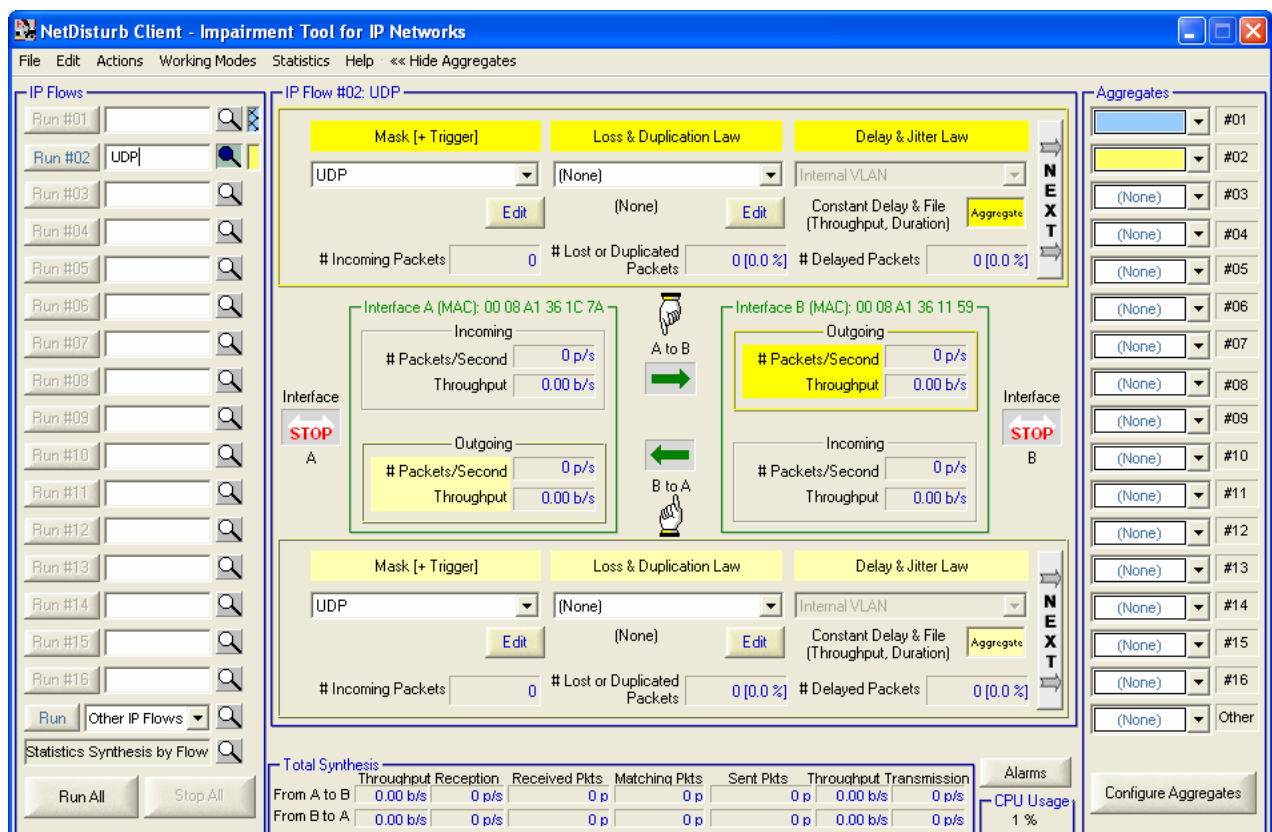
- Step 4: Click OK to save the aggregate

7.5.4 How to associate a colored aggregate to an IP Flow

Click the combo-box as shown below - in this example two aggregates have been defined: light Bleu and Yellow. Then select the colored aggregate:





Once the aggregate is selected, a colored mark is displayed on the right of the IP Flow. 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.



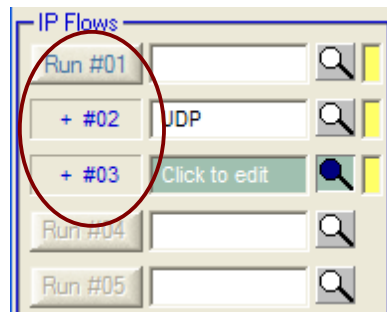
For the following example, the light Blue aggregate is associated to the IP Flow # 01, and the yellow aggregate is related to the IP Flow # 02.



The colored mark located on the right may have two states:

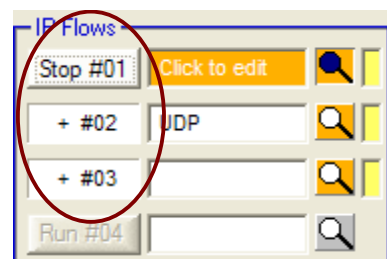
- full color, for example  meaning that a mask is defined for this IP Flow
- or hatched color, for example  meaning that a mask is not defined for this IP Flow and can't be started.

You can associate the same colored aggregate to several IP Flows as in the example below where 3 IP Flows are associated to the yellow aggregate:



Note that the label of the buttons change when an aggregate is associated to several IP 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.



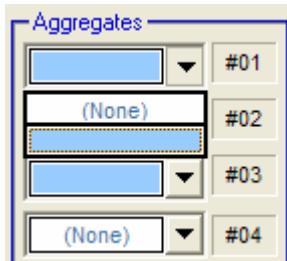
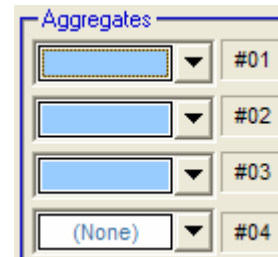
To stop the aggregate, press the "Stop #xx" button.

7.5.5 How to disassociate an IP Flow belonging to a colored aggregate

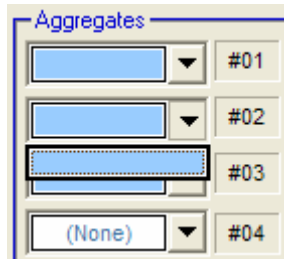
Example:

A light blue light aggregate is associated with three IP Flows (#01, #02 et #03).

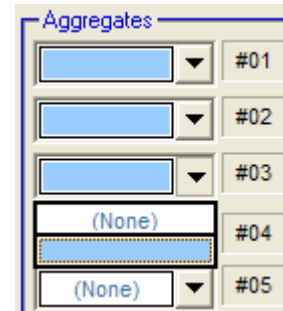
You can only dissociate an IP Flow belonging to an aggregate if this IP Flow is the first or the last of the aggregate



With this configuration you can disassociate the IP Flow #01.



The IP Flow #02 can't be disassociated because the previous IP Flow (#01) and the next IP Flow (#03) are associated to the aggregate.

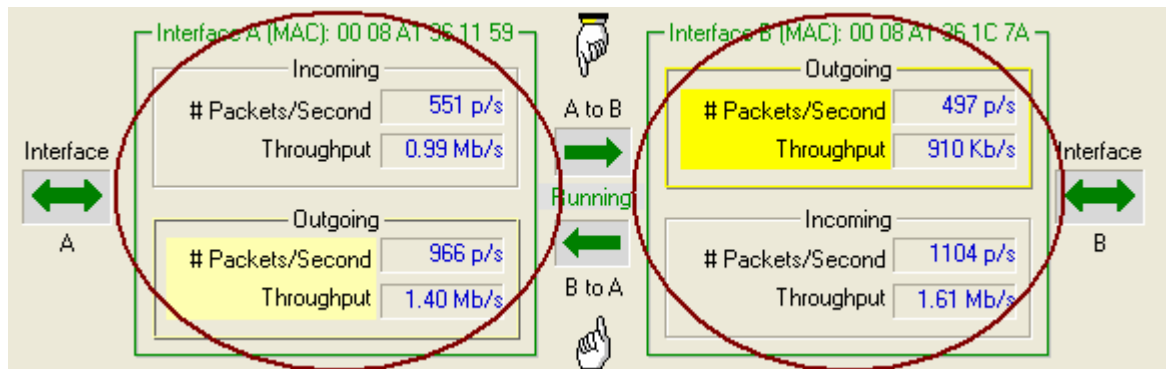


With this configuration, you can disassociate the IP Flow #03.

7.6 The NetDisturb Client Statistics

The traffic on the two interfaces is displayed in the central part of the window when an IP 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/Second	This field presents the instant number of packets per second for the IP 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.

7.7 The Errors Detected by the NetDisturb Driver

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

Total Synthesis							
	Incoming Throughput	Incoming Pkts	Matching Pkts	Outgoing Pkts	Outgoing Throughput		
From A to B	6.53 Mb/s	4174 p/s	169345 p	169344 p	169344 p	6.53 Mb/s	4174 p/s
From B to A	36.7 Kb/s	17 p/s	3386 p	3228 p	3386 p	36.7 Kb/s	17 p/s

Alarms

CPU Usage
24 %

Click on the "Alarms" button to get details about the errors and the following window is displayed:

NetDisturb Client - Alarms Summary

Alarms Linked to the Direction from Interface A to Interface B

Incoming from A		Outgoing to B	
# Lost Packets:	0	# Lost Packets:	0
# Lost Bytes:	0	# Lost Bytes:	0
# Driver Errors:	0	# Driver Errors:	0
# Missing Buffer Errors:	0		
# Lost TCP/UDP Connections:	0		

A to B

Details

Alarms Linked to the Direction from Interface B to Interface A

Outgoing to A		Incoming from B	
# Lost Packets:	0	# Lost Packets:	0
# Lost Bytes:	0	# Lost Bytes:	0
# Driver Errors:	0	# Driver Errors:	0
		# Missing Buffer Errors:	0
		# Lost TCP/UDP Connections:	0

B to A

Details

OK Clear Alarms Update Alarms Summary

The alarms are classified per direction: **A → B** and **B → A**.

The Information displayed is different depending of the direction (incoming or outgoing).

Incoming from A

# Lost Packets:	0
# Lost Bytes:	0
# Driver Errors:	0
# Missing Buffer Errors:	0
# Lost TCP/UDP Connections:	0

For the incoming direction:

- Number of lost packets
- Number of lost bytes
- Number of errors returned by the driver of the Interface
- Number of buffers that were missing to keep all packets
- Number of ignored connections

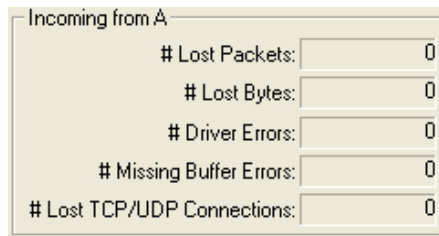
Outgoing to B

# Lost Packets:	0
# Lost Bytes:	0
# Driver Errors:	0

For the outgoing direction:

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

7.7.1 Details for the Incoming Errors



The screenshot shows a window titled "Incoming from A" with five rows of error counters, each with a label and a numeric value in a text box. The values are all 0.

Label	Value
# Lost Packets:	0
# Lost Bytes:	0
# Driver Errors:	0
# Missing Buffer Errors:	0
# Lost TCP/UDP Connections:	0

► **# 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

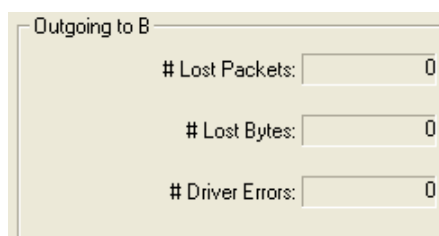
► **# Missing Buffer Errors**

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



The screenshot shows a window titled "Outgoing to B" with three rows of error counters, each with a label and a numeric value in a text box. The values are all 0.

Label	Value
# Lost Packets:	0
# Lost Bytes:	0
# Driver Errors:	0

► **# 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

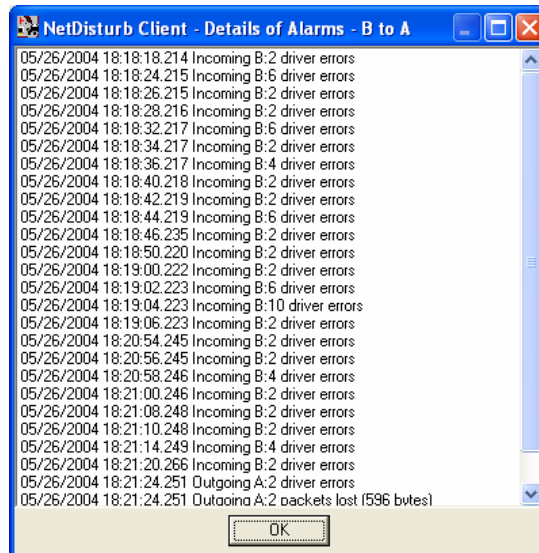
7.7.3 Alarm Management

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  to gray  until new errors occur.

Part 8 Using the NetDisturb Command Line Interface

NetDisturb version 4.6 is offering a Command Line Interface (CLI) allowing the integration of **NetDisturb** in test beds which are controlled through batch processes. The Command Line Interface is provided by **NetDisturbCLI.exe** which is located in the **NetDisturb** Client directory.

With the Command Line Interface, you can load a context, start and/or stop the IP 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 IP 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 /?

Displays the commands list which describes each command and its parameters.

Result:

```

C:\Program Files\NetDisturb\Client>NetDisturbCLI.exe /?
NetDisturb Command Line Interface Version 1.0.1
Copyright © ZTI 2007

NetDisturbCLI Usage:
  Command      Parameter      Explanation
  -----
  /?           This help
  /Context     PATH           Load the context from the file 'PATH'
  /Start       ALL           Run all IP Flows i.e. 'Start All' button
  /Start       X             Run IP Flow X where X is in the range [1..17]
  /Stop        ALL           Stop all IP Flows i.e. 'Stop All' button
  /Stop        Y             Stop IP Flow Y where Y is in the range [1..17]
  /Trace       Start          Start to save Statistics
  /Trace       Stop           Stop to save Statistics
  /Trace       PATH          Set the target Statistics file using the 'PATH' parameter
  /Run         Load and Start NetDisturb Server
  /Quit        Quit (NetDisturb Client and NetDisturb Server)
  /Quit        CClient1      Quit (NetDisturb Client only)

C:\Program Files\NetDisturb\Client>

```

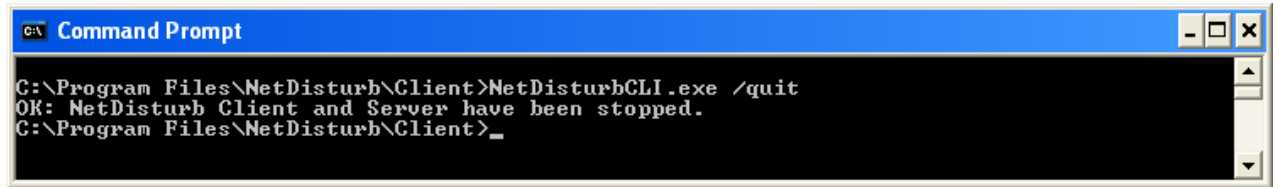
Figure 10 - Command Line Interface Help

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
Stops **NetDisturb Server** and **NetDisturb Client** then shutdowns both applications.

Result:



```
C:\Program Files\NetDisturb\Client>NetDisturbCLI.exe /quit
OK: NetDisturb Client and Server have been stopped.
C:\Program Files\NetDisturb\Client>_
```

Figure 11 – Stops NetDisturb Server and NetDisturb Client, then shutdowns both applications

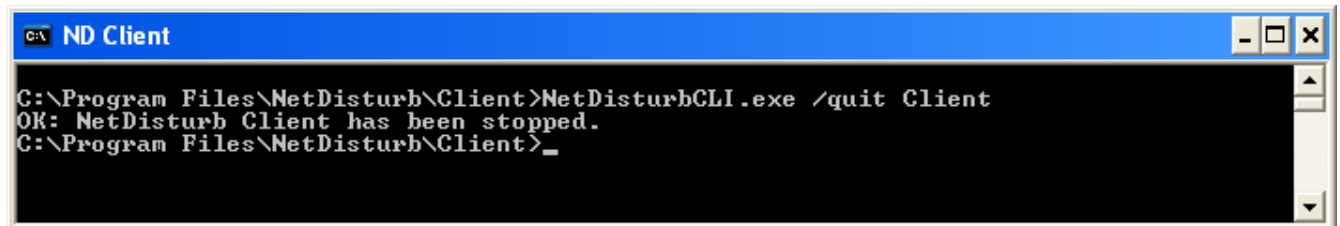
Error message: None

Warning message: None

8.2.3 Stop and shutdown NetDisturb Client only (/Quit Client)

Command: NetDisturb /Quit Client
Stops and shutdowns **NetDisturb Client**.

Result:



```
C:\Program Files\NetDisturb\Client>NetDisturbCLI.exe /quit Client
OK: NetDisturb Client has been stopped.
C:\Program Files\NetDisturb\Client>_
```

Figure 12 – Stops and shutdowns NetDisturb Client

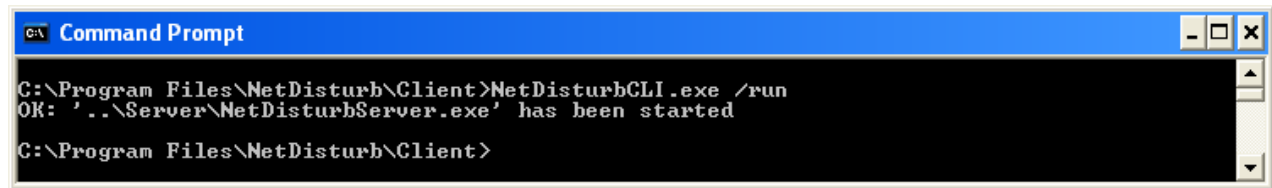
Error message: None

Warning message: None

8.2.4 Open and Start NetDisturb Server (/Run)

Command: `NetDisturb /run`
Opens and starts **NetDisturb Server**.

Result:



```
C:\Program Files\NetDisturb\Client>NetDisturbCLI.exe /run
OK: '..\Server\NetDisturbServer.exe' has been started
C:\Program Files\NetDisturb\Client>
```

Figure 13 – Opens and starts NetDisturb Server

Error message:

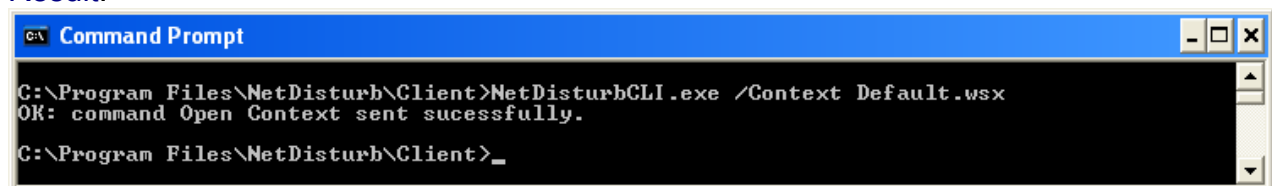
- **Error: Can't create '..\Server\NetDisturbServer.exe': Windows error message**
The <Windows error message> gives the reason why **NetDisturb Server** did not start.

Warning message: None

8.2.5 Load the context file (/Context filename)

Command: `NetDisturb /context filename`
Loads a **NetDisturb** context like in the menu File/Open of the **NetDisturb Client** GUI.

Result:



```
C:\Program Files\NetDisturb\Client>NetDisturbCLI.exe /Context Default.wsx
OK: command Open Context sent sucessfully.
C:\Program Files\NetDisturb\Client>_
```

Figure 14 – Defines the context file and loads 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 IP Flows to be able to change the context.**

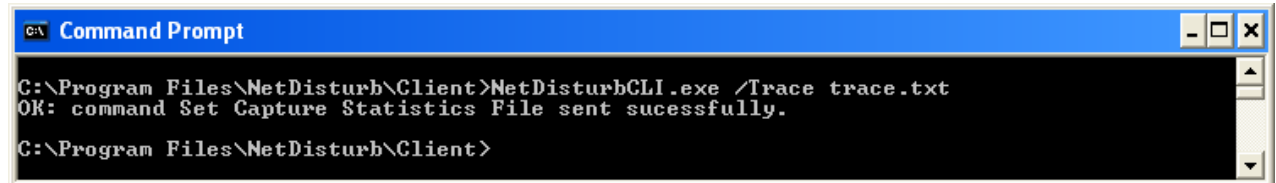
Warning message: None

8.2.6 Set the file name where to store the statistics (/Trace filename)

Command: NetDisturb /trace *filename*

Defines 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:



```
C:\Program Files\NetDisturb\Client>NetDisturbCLI.exe /Trace trace.txt
OK: command Set Capture Statistics File sent sucessfully.
C:\Program Files\NetDisturb\Client>
```

Figure 15 – Defines 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.

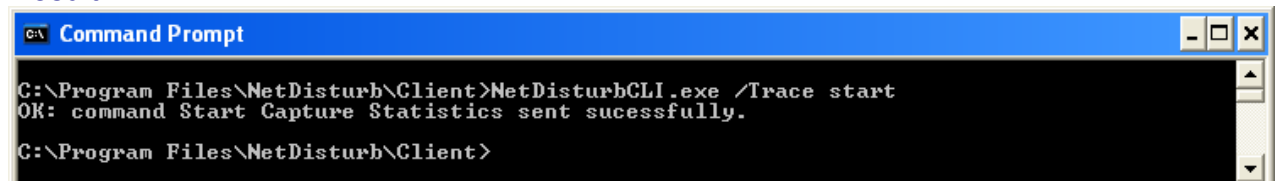
Warning message: None

8.2.7 Start saving the statistics (/Trace start)

Command: NetDisturb /trace start

Sends a request to **NetDisturb Client** to start saving statistics into a file.

Result:



```
C:\Program Files\NetDisturb\Client>NetDisturbCLI.exe /Trace start
OK: command Start Capture Statistics sent sucessfully.
C:\Program Files\NetDisturb\Client>
```

Figure 16 – Starts 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:

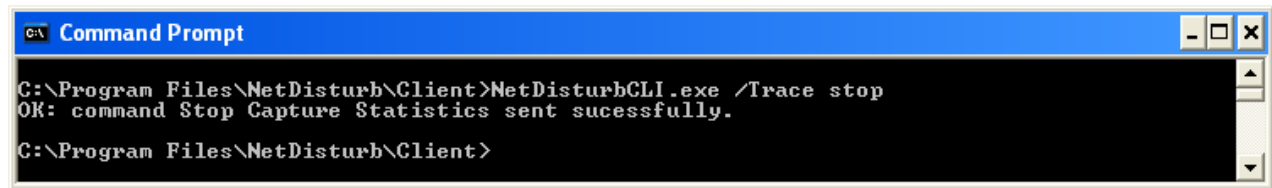
- **Warning: NetDisturb Client is already saving the statistics.**

8.2.8 Stop saving the statistics (/Trace stop)

Command: NetDisturb /trace stop

Sends a request to **NetDisturb Client** to stop saving statistics into a file.

Result:



```
C:\Program Files\NetDisturb\Client>NetDisturbCLI.exe /Trace stop
OK: command Stop Capture Statistics sent sucessfully.
C:\Program Files\NetDisturb\Client>
```

Figure 17 – Stops 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:

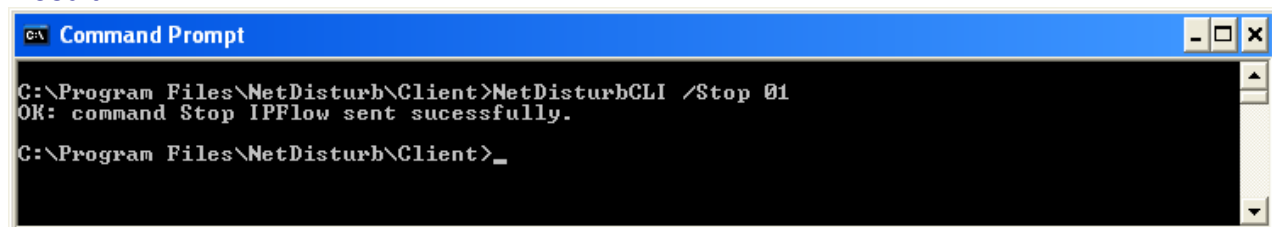
- **Warning: NetDisturb Client is not saving the statistics.**

8.2.9 Stop an IP Flow (/Stop X)

Command: NetDisturb /stop X

Sends a request to **NetDisturb Client** to stop the IP Flow X, where X should be in the range [1..17] (the value 17 corresponds to 'Other IP Flows'/'Other Frames' flow).

Result:



```
C:\Program Files\NetDisturb\Client>NetDisturbCLI /Stop 01
OK: command Stop IPFlow sent sucessfully.
C:\Program Files\NetDisturb\Client>_
```

Figure 18 – Stops the IP 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 an IP Flow.
- **Error: The IP Flow X is out of range. Allowed range: from 1 to 17 included.**
The IP Flow number must be in the range from 1 to 17.
- **Error: NetDisturb Client was unable to stop the IP Flow X.**
More details should be available into the internal log file about the reason why NetDisturb Client couldn't stop the IP Flow.

Warning message:

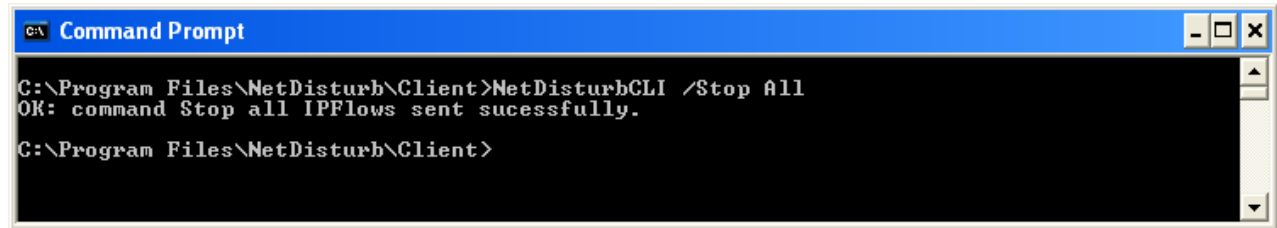
- **Warning: The IP Flow X is already stopped.**
The command doesn't change the status of the IP Flow because it was stopped.

8.2.10 Stop all IP Flows (/Stop all)

Command: NetDisturb /stop all

Send a request to **NetDisturb Client** to stop all IP Flows.

Result:



```
C:\Program Files\NetDisturb\Client>NetDisturbCLI /Stop All
OK: command Stop all IPFlows sent successfully.
C:\Program Files\NetDisturb\Client>
```

Figure 19 – Stops 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 an IP Flow.

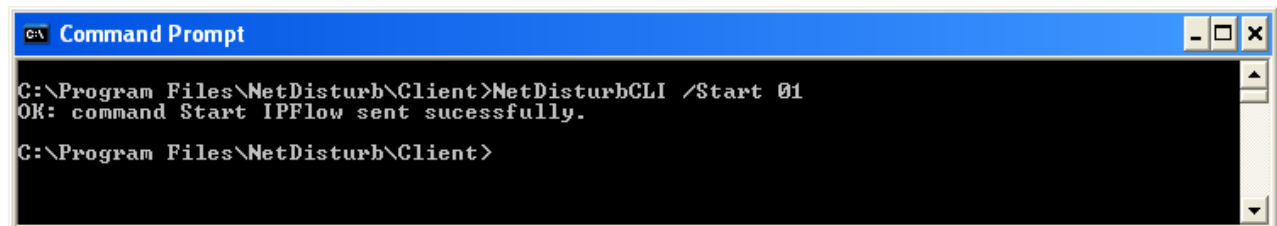
Warning message: None

8.2.11 Start an IP Flow (/Start X)

Command: NetDisturb /start X

Send a request to **NetDisturb Client** to run the IP Flow X, where X should be in the range [1..17] (the value 17 corresponds to 'Other IP Flows'/'Other Frames' flow).

Result:



```
C:\Program Files\NetDisturb\Client>NetDisturbCLI /Start 01
OK: command Start IPFlow sent successfully.
C:\Program Files\NetDisturb\Client>
```

Figure 20 – Runs the IP 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 an IP Flow.
- **Error: The IP Flow X has no mask defined..**
A mask should be selected before starting an IP Flow.

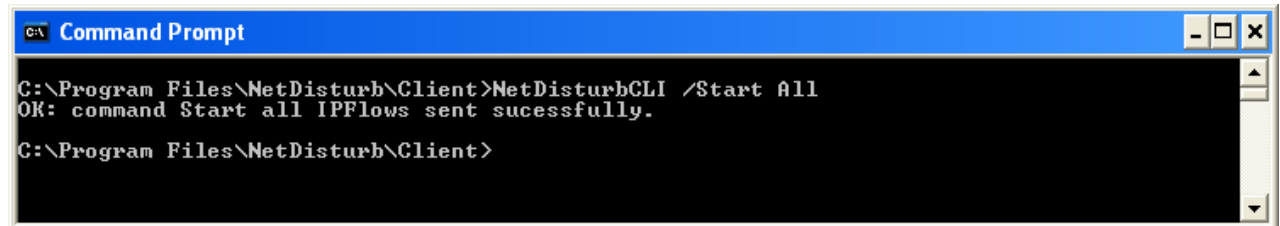
Warning message:

- **Warning: The IP Flow X is already started.**
The command doesn't change the status of the IP Flow because it is running already.

8.2.12 Start all IP Flows (/Start all)

Command: NetDisturb /start all
Send a request to **NetDisturb Client** to start all IP Flows.

Result:



```

C:\Program Files\NetDisturb\Client>NetDisturbCLI /Start All
OK: command Start all IPFlows sent sucessfully.
C:\Program Files\NetDisturb\Client>

```

Figure 21 – Runs 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 starting IP Flows.
- **Error: The IP Flow X has no mask defined..**
A mask should be selected before starting an IP 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 (<i>highest->lowest</i>)	Command	Ignore other commands
Highest ↓ Lowest	/?	Yes
	/Quit	Yes
	/Run	No
	/Context	No
	/Trace	No
	/Stop # or All	No
	/Start # or All	No

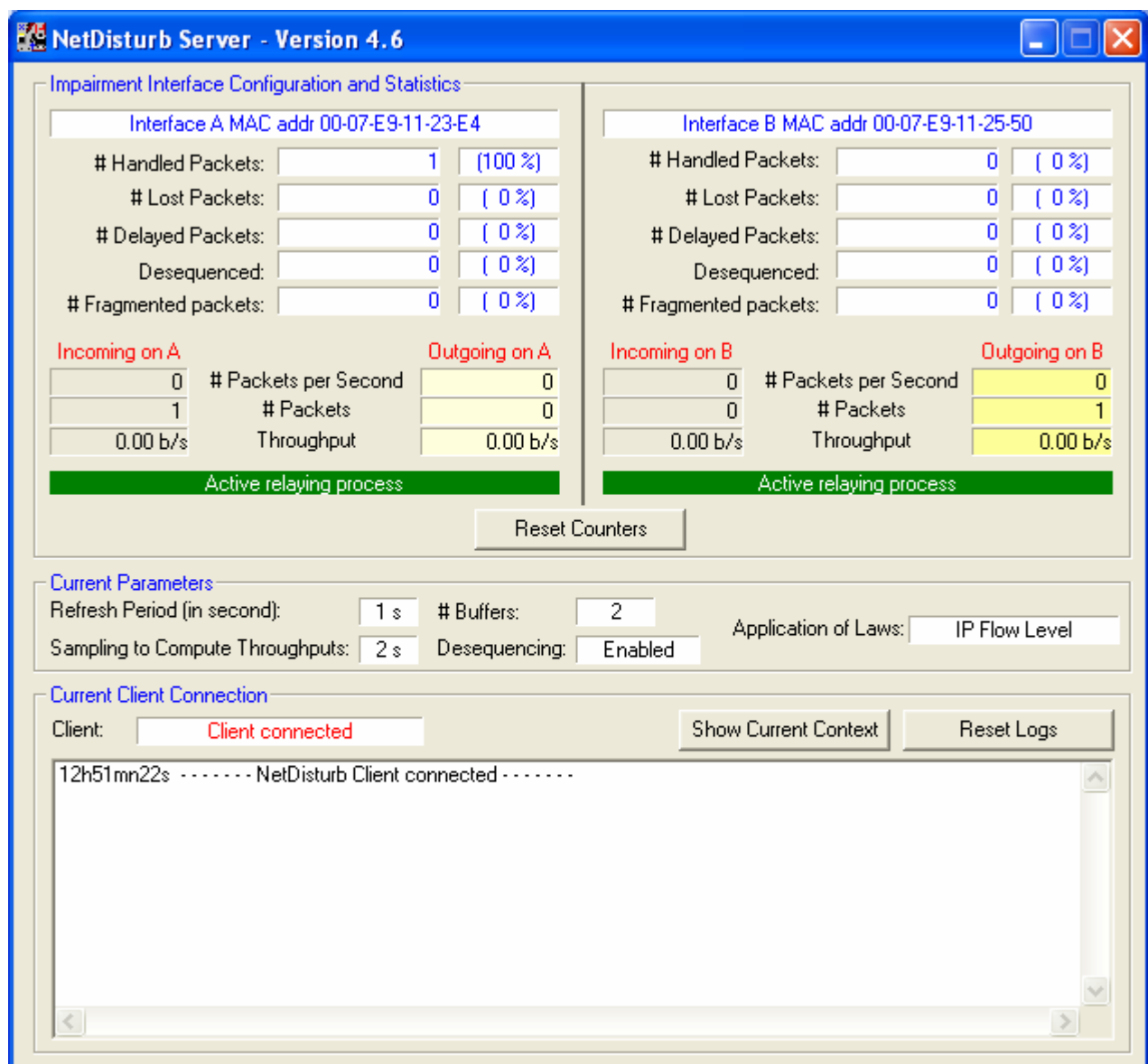
Table 1 - Commands execution order

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 mask 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, desequenced 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 masks 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-order i.e. desequencing mode: Enabled or Disabled
- (5) The method to apply the laws:
 - 'IP Flow level' means **Laws apply to the IP Flow**
 - or 'TCP/UDP connections' means **Laws apply to each TCP/UDP connection of the IP Flow**

⇒ Current Client Connection

This section shows the currently connected client, 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 Desequencing Packets Laws apply to the IP Flow
• Traces	Active
• Driver relaying status	Running
• Buffer number	2
• Flow mode	Mono-flow
• For the 16 definable masks	
Mask	<i>Not defined</i>
Loss & Duplication law	<i>Not defined</i>
Delay & Jitter law	<i>Not defined</i>
Content Impairment law	<i>Not defined</i>
• Other IP Flows	
Loss & Duplication law	<i>Not defined</i>
Delay & Jitter law	<i>Not defined</i>
Content Impairment law	<i>Not defined</i>

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)
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: trace 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
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

Key (Windows NT only) = HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disturb

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

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).



*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

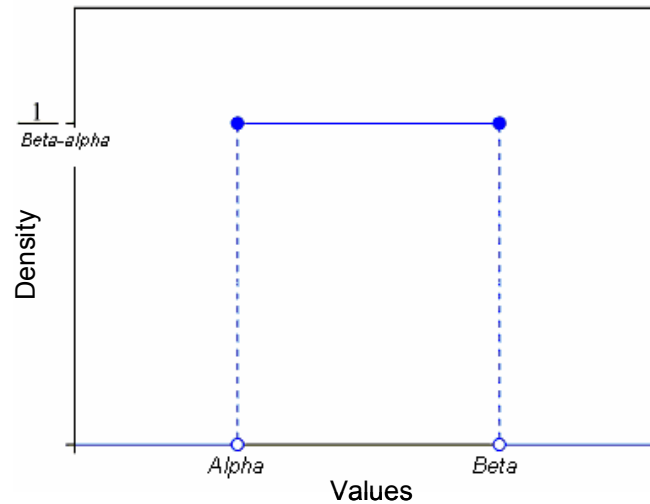
10.3.1 Uniform law

Distribution of Uniform Law is:

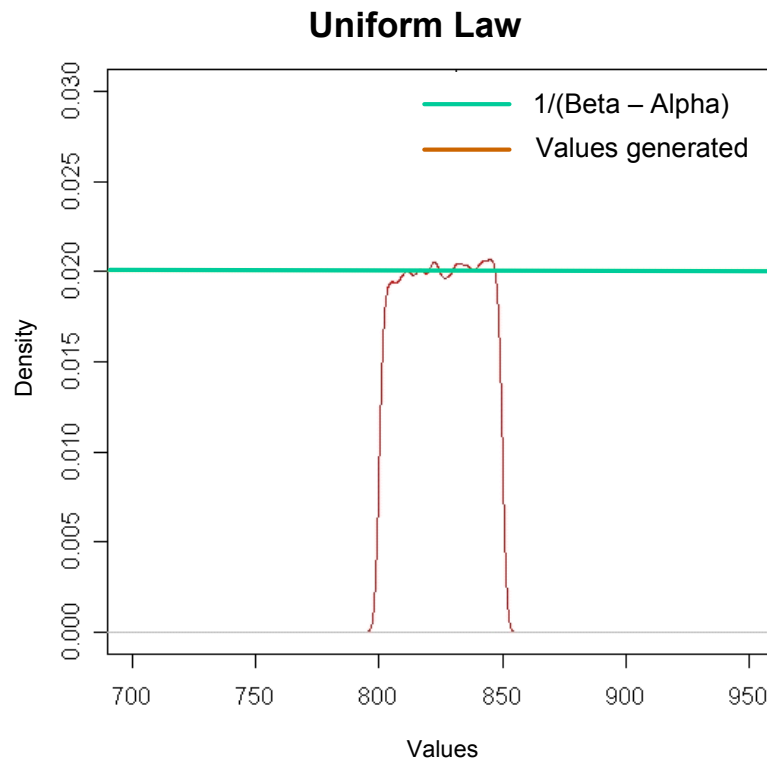
$$f(x) = \frac{1}{Beta - Alpha} \quad \text{for } Alpha < x < Beta$$

$$f(x) = 0 \quad \text{for } x < Alpha \text{ or } x > Beta$$

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]**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).

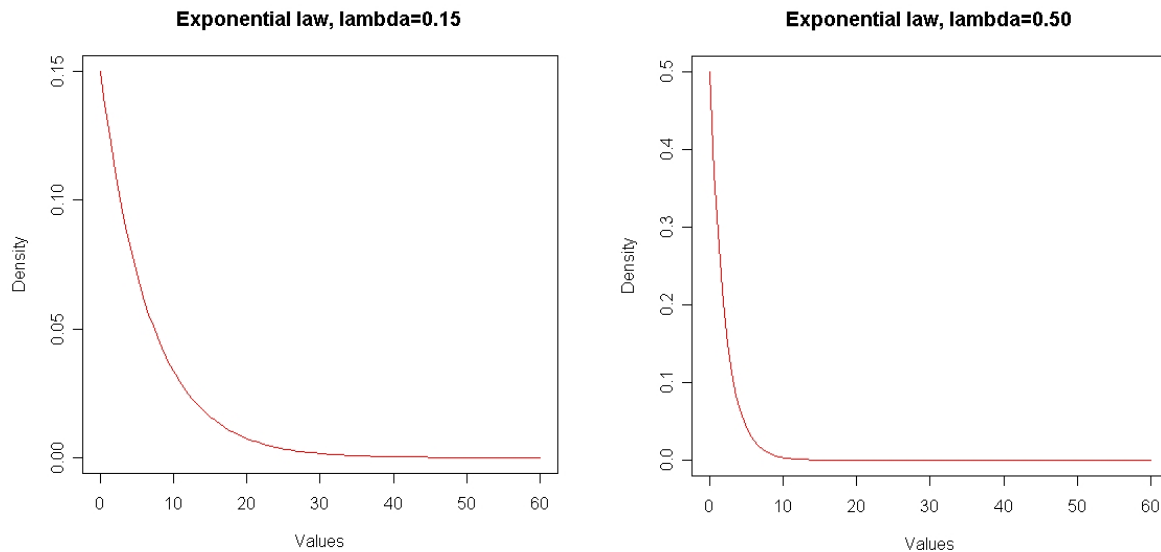
10.3.3 Exponential law

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 $\lambda=0.15$ and $\lambda=0.50$.

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.

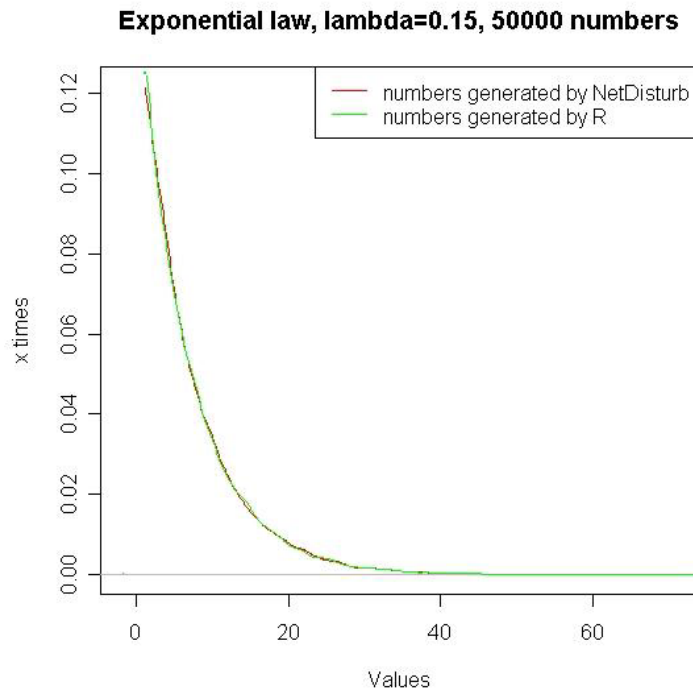
As a result of the increase of λ , the incline of the distributions curve increases. Therefore the probability to draw small numbers is bigger than the one to draw big numbers.

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.

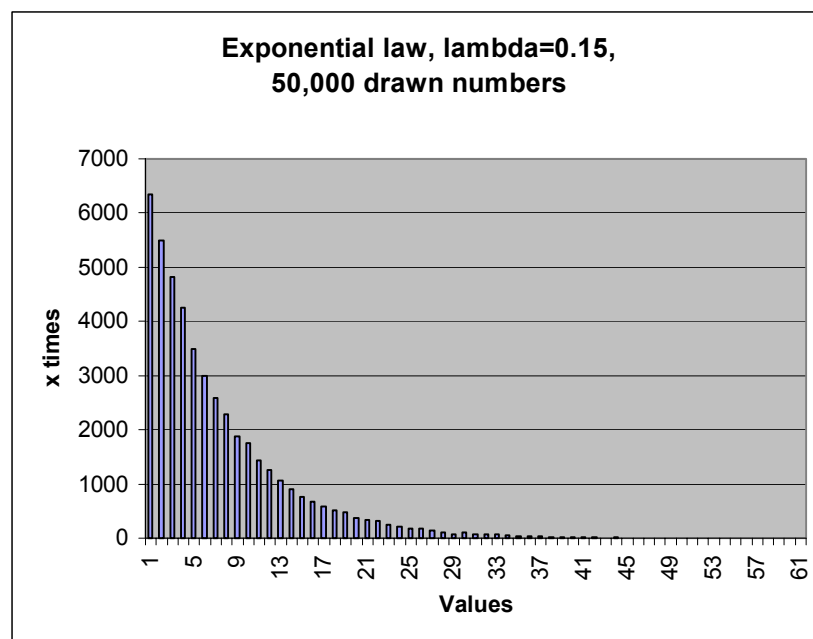
Using this function with $\lambda=0.15$ as a parameter, we drew such numbers and then we plotted, by using a mathematical tool (*R* software), the distribution of those. Then we got the following graph.



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.

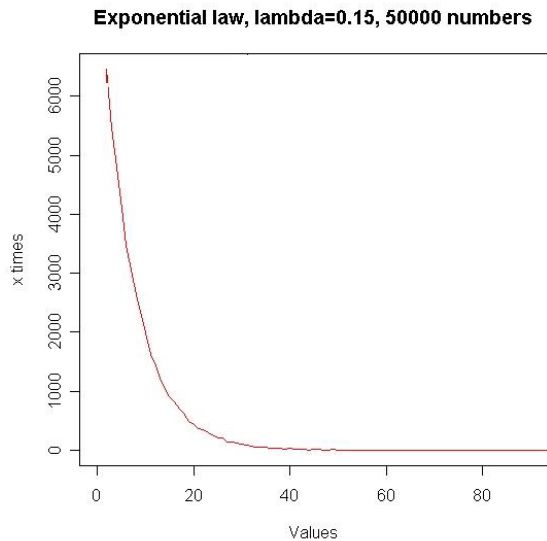
As shown in the theoretical part, the probability to have small numbers is much bigger than the probability to have big ones.

For example, we generate 50000 numbers following the exponential law with $\lambda=0.15$. 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.

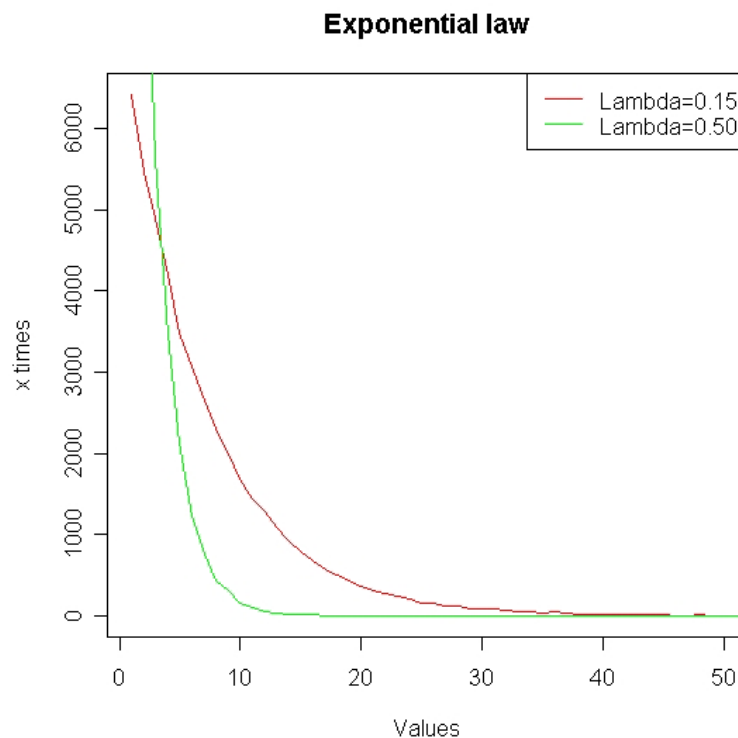


The generated values are on the abscissa axis, and how many times each value is generated on the ordinate axis.

Otherwise, we can represent the same result by a curve.



In order to see the effect of the parameter λ we repeat the same operation as before with $\lambda=0.15$ and $\lambda=0.50$ and we plot both curves:



As the legend shows, the red curve represents the result of using the exponential law with $\lambda=0.15$ as parameter, and the green one the result of using the same law with $\lambda=0.50$. 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
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
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 $\lambda = 0.1$:

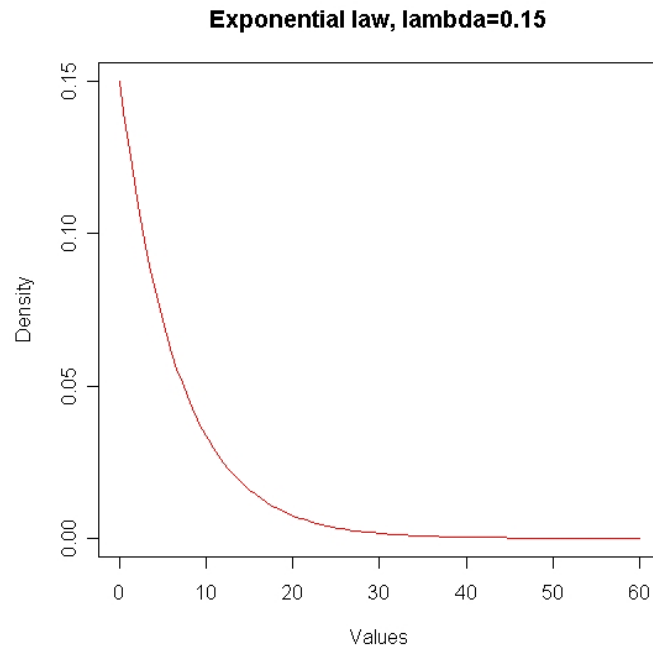
0.227489
1.961810
1.217468
13.854097
0.474025
5.870118
2.353334
0.766254
4.868133
0.802894

To represent those values in a simple way we round up double to the nearest integer, for example:

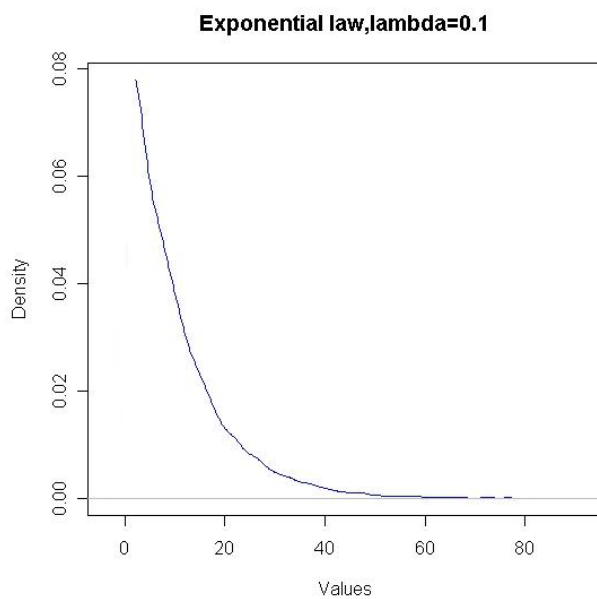
real values	represented values
0.227489	0
1.961810	2
1.217468	1
13.854097	14
0.474025	0
5.870118	6
2.353334	2
0.766254	1
4.868133	9
0.802894	1

As a result, the values of the first column **approximately** correspond to the “x” in the theoretical representation of the exponential law.

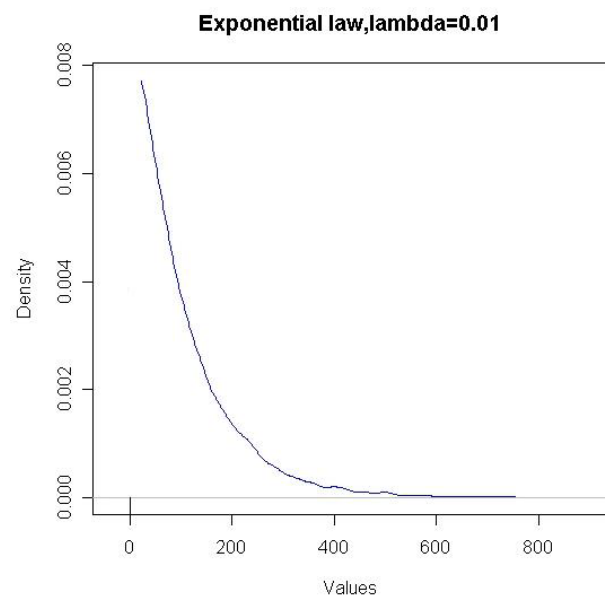
The effect of this approximation is more important when we draw values near “0”. Thus the probability in the table to generate “0” is smaller than “1”.



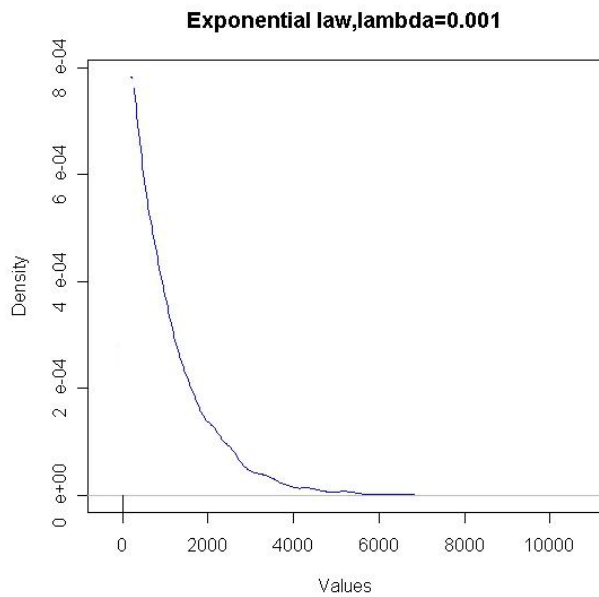
This graph is plotted with real values generated by **NetDisturb**. We observe that the probability for $x=0$ ($=\lambda$) is bigger than for $x=1$. Here are below graphs plotted with small values for λ .



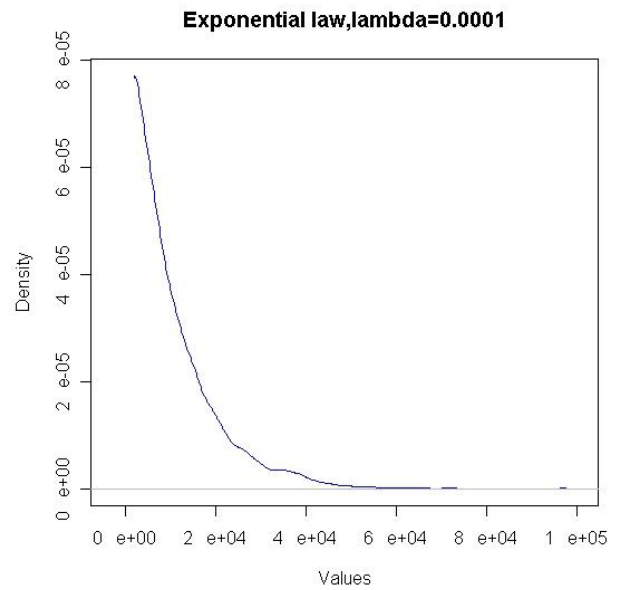
Maximum* drawn value = 221



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!*

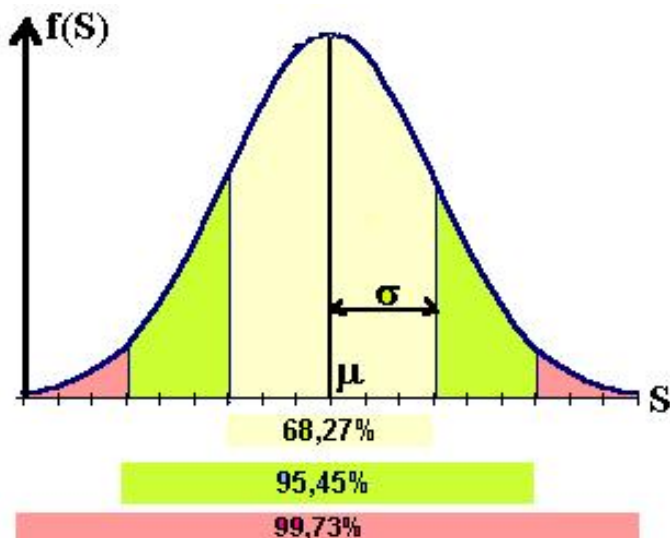
10.3.4 Laplace-Gauss law

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 $\sigma > 0$