



# LanTraffic V2

**Version 2.3**

***Traffic Generator for IP Networks (IPv4 & IPv6)***  
***LAN, MAN, WAN, WLAN, Cellular, Satellite, PLC ...***

**LanTrafficV2**

File Edit Configuration File Downloading Automation Tool Help

Sender - Parameters | Sender - Traffic + Statistics | Receiver - Traffic + Statistics | Throughput Graphics

Destination Parameters

	IP Address or Host Name	Protocol	Port
Connection #01	NO_ADDRESS	TCP	2009
Connection #02	NO_ADDRESS	TCP	2009
Connection #03	NO_ADDRESS	TCP	2009
Connection #04	NO_ADDRESS	TCP	2009
Connection #05	NO_ADDRESS	TCP	2009
Connection #06	NO_ADDRESS	TCP	2009
Connection #07	NO_ADDRESS	TCP	2009
Connection #08	NO_ADDRESS	TCP	2009
Connection #09	NO_ADDRESS	TCP	2009
Connection #10	NO_ADDRESS	TCP	2009
Connection #11	NO_ADDRESS	TCP	2009
Connection #12	NO_ADDRESS	TCP	2009
Connection #13	NO_ADDRESS	TCP	2009
Connection #14	NO_ADDRESS	TCP	2009
Connection #15	NO_ADDRESS	TCP	2009
Connection #16	NO_ADDRESS	TCP	2009

Save the Received Data

Filename

Browse #01
Browse #02
Browse #03
Browse #04
Browse #05
Browse #06
Browse #07
Browse #08
Browse #09
Browse #10
Browse #11
Browse #12
Browse #13
Browse #14
Browse #15
Browse #16

Unitary Mode

Traffic Generator

Generator	Parameters	On
Generator	Parameters #01	On
Generator	Parameters #02	On
Generator	Parameters #03	On
Generator	Parameters #04	On
Generator	Parameters #05	On
Generator	Parameters #06	On
Generator	Parameters #07	On
Generator	Parameters #08	On
Generator	Parameters #09	On
Generator	Parameters #10	On
Generator	Parameters #11	On
Generator	Parameters #12	On
Generator	Parameters #13	On
Generator	Parameters #14	On
Generator	Parameters #15	On
Generator	Parameters #16	On

[P]

Sender Statistics (based on application data)

Active Connections: [ ] (TCP Connections: 0 - UDP Connections: 0)

Total Sending Throughput: [ ] Total Receiving Throughput: [ ]

Start Receiver

Stop Receiver

Receiver Statistics (based on application data)

Active Connections: [ ] (TCP Connections: 0 - UDP Connections: 0)

Total Sending Throughput: [ ] Total Receiving Throughput: [ ]

## 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's guide imperfection.*

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

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  
B.P. 154  
22302 Lannion Cedex  
France

Phone: +33 2 96 48 43 43

Fax: +33 2 96 48 14 85

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

Email: [contact@zti-telecom.com](mailto:contact@zti-telecom.com) (marketing & sales)  
[support@zti-telecom.com](mailto:support@zti-telecom.com) (technical support)

---

**Copyrights**

Copyright 1997-2004 ZTI. 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, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form 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 ZTI property. French copyright laws and international treaties protect the products. ZTI grants you the right to use the products according to the following:

- **USE OF THE SOFTWARE**

You may:

- Install the software on hard disk of your system accordingly with the software protection described in the next paragraph.
- Make 1 backup copy of the software, provided this copy is not used or install on any computer.
- Use the Products properly.

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 Products reputation.

- **SOFTWARE PROTECTION**

The "LanTraffic V2" software is licensed on a per 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, which requires the corresponding unique Site Key to be entered before the tool is operational.

- **LIMITED WARRANTY**

Software is supplied without any warranty express or implied regarding the performance or results obtained by the use of the Products.

ZTI warrants that software media (i.e. CD-ROM) will be free of material defects for a ninety (90) days period following purchase. The limited warranty applies to the media and not the information contained on it. If the media does not comply with this limited warranty, the sole 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.

- **JURISDICTION**

French laws will govern this agreement.

The court of GUINGUAMP-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  
1Boulevard d'Armor  
B.P. 154  
22302 Lannion Cedex  
France

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

Email: [support@zti-telecom.com](mailto:support@zti-telecom.com) or [support@zti.fr](mailto:support@zti.fr)  
Web: <http://www.zti-telecom.com> or <http://www.zti.fr>

## Table of Contents

<b>PART 0</b>	<b>Preface .....</b>	<b>7</b>
0.1	Organization of this manual .....	7
0.2	Minimum System Requirements .....	8
0.3	Technical Support .....	8
<b>PART 1</b>	<b>Product Overview .....</b>	<b>9</b>
1.1	Key Features .....	9
1.2	Reference .....	11
1.3	Terms used in this document .....	11
<b>PART 2</b>	<b>Install LanTraffic V2 .....</b>	<b>12</b>
2.1	Install from a downloaded trial version .....	12
2.2	Install from the CD-ROM .....	14
<b>PART 3</b>	<b>License configuration .....</b>	<b>15</b>
3.1	To configure a license .....	15
3.2	License Transfers .....	17
3.2.1	Direct transfer: move the license from one local directory to another .....	17
3.2.2	Transfer by media (floppy disk or USB key) from a source PC to a target PC .....	18
3.3	To kill a license .....	24
<b>PART 4</b>	<b>Uninstall LanTraffic V2 .....</b>	<b>25</b>
<b>PART 5</b>	<b>Graphical User Interface .....</b>	<b>26</b>
5.1	Main Window .....	26
5.2	Display general rules of "LanTraffic V2" GUI .....	27
5.3	Used units in information display .....	28
5.3.1	Volume units .....	28
5.3.2	Throughput units .....	28
<b>PART 6</b>	<b>Using "LanTraffic V2" .....</b>	<b>29</b>
6.1	Main steps .....	29
6.2	Menu description .....	30
6.2.1	File menu .....	30
6.2.1.1	File/New .....	30
6.2.1.2	File/Open .....	30
6.2.1.3	File/Save .....	30
6.2.1.4	File/Save as ... ..	30
6.2.1.5	File/Recent Contexts ... ..	31
6.2.1.6	File/Exit .....	31
6.2.2	Edit menu .....	31
6.2.2.1	Edit/Destination Parameters: IP Address or Host Name .....	31
6.2.2.2	Edit/Destination Parameters: Protocol .....	31
6.2.2.3	Edit/Destination Parameters: Port .....	31
6.2.3	Configuration menu .....	32
6.2.3.1	Configuration/Stack Parameters .....	32
6.2.3.2	Configuration/General Parameters .....	34
6.2.3.3	Configuration/AutoComplete ... ..	35
6.2.4	File Downloading menu .....	37
6.2.5	Automation Tool menu .....	40
6.2.5.1	Automation Tool/Open .....	40
6.2.5.2	Automation Tool/Close .....	40

6.2.5.3	Automation Tool/Bring to the top.....	40
6.2.6	"Help" menu .....	40
6.2.6.1	Help/Help.....	40
6.2.6.2	Help/Forewarnings .....	41
6.2.6.2.1	Inter-packet delay .....	41
6.2.6.2.2	Echoer modes.....	41
6.2.6.2.3	UDP connections .....	41
6.2.6.3	Help/About LanTrafficV2 .....	42
<b>6.3</b>	<b>Total statistics .....</b>	<b>43</b>
6.3.1	Sender statistics.....	43
6.3.2	Receiver statistics .....	43
<b>6.4</b>	<b>Sender part .....</b>	<b>45</b>
6.4.1	Sender - Parameters tab.....	45
6.4.1.1	Destination parameters .....	46
6.4.1.1.1	Summary of connection parameters.....	46
6.4.1.1.2	Select the network interface, IP version and source IP address .....	47
6.4.1.1.3	IP Address translation mechanism .....	49
6.4.1.1.4	Duplicate parameters of a connection onto others .....	49
6.4.1.1.5	IP address floating menu .....	50
6.4.1.1.6	Protocol floating menu .....	50
6.4.1.1.7	Port floating menu.....	51
6.4.1.2	Save the Received Data .....	51
6.4.1.3	Configure the Unitary Mode .....	52
6.4.1.3.1	Step 1: select the traffic generator type for this connection.....	53
6.4.1.3.1.1	Packets generator .....	53
6.4.1.3.1.2	Mathematical law.....	54
6.4.1.3.1.3	File to send .....	56
6.4.1.3.2	Step 2: Specify data size and packets parameters .....	57
6.4.1.3.2.1	Data size.....	57
6.4.1.3.2.2	Inter Packet Delay .....	58
6.4.1.3.2.3	RTT option.....	58
6.4.1.3.2.4	The TOS field (IPv4 only).....	59
6.4.1.3.2.5	The TTL field .....	60
6.4.1.3.3	Step 3 (optional): Activate a throughput limit.....	60
6.4.1.4	Configure the Automatic Mode.....	61
6.4.1.4.1	Starting time connections generation laws .....	62
6.4.1.4.2	Data volume to send laws.....	63
6.4.1.4.3	Packets size.....	64
6.4.2	Sender - Traffic + Statistics tab.....	65
6.4.2.1	Destination Parameters.....	65
6.4.2.2	Sender statistics .....	66
6.4.2.3	Export statistics into a file.....	69
6.4.2.3.1	Sender statistics file format.....	70
6.4.2.3.2	Export Sender file sample.....	71
6.4.2.4	Run the Unitary Mode .....	73
6.4.2.5	Run the Automatic Mode.....	74
<b>6.5</b>	<b>Receiver part.....</b>	<b>75</b>
6.5.1	Duplicate parameters of a connection onto others .....	75
6.5.2	Listening To .....	76
6.5.2.1	Summary of connection parameters .....	76
6.5.2.2	Select the network interface, IP version and local IP address.....	77
6.5.2.3	Port floating menu .....	79
6.5.2.4	Protocol floating menu .....	79
6.5.3	Coming From .....	79
6.5.3.1	IP address floating menu .....	80
6.5.3.2	IP Address translation mechanism.....	80
6.5.4	Working Mode.....	81
6.5.4.1	Absorber mode.....	81
6.5.4.2	Absorber File mode.....	81
6.5.4.3	Echoer mode .....	81

6.5.4.4	Echoer File mode .....	81
6.5.4.5	Absorber + Generator mode .....	82
6.5.4.6	Disable mode .....	82
6.5.5	Statistics.....	83
6.5.6	Export statistics into a file .....	86
6.5.6.1	Receiver statistics file format .....	87
6.5.6.2	Export Receiver file sample .....	88
<b>6.6</b>	<b>The Throughput Graphics tab.....</b>	<b>90</b>
6.6.1	The Graphical Display object.....	91
6.6.2	The Display Configuration object.....	93
<b>PART 7</b>	<b>Command Line Parameters.....</b>	<b>94</b>
<b>PART 8</b>	<b>How To Do ... ..</b>	<b>96</b>
<b>8.1</b>	<b>Checking router configuration.....</b>	<b>96</b>
8.1.1	PC #2 parameters.....	96
8.1.2	PC #1 parameters.....	97
8.1.3	What should happened .....	98
<b>8.2</b>	<b>Checking a firewall configuration.....</b>	<b>99</b>
8.2.1	LanTraffic V2 parameters on the server .....	99
8.2.2	LanTraffic V2 parameters for the Remote PC .....	101
8.2.3	What result can you expect.....	102
<b>8.3</b>	<b>Checking the best throughput.....</b>	<b>102</b>
8.3.1	PC #2 parameters.....	102
8.3.2	PC #1 parameters.....	103
<b>8.4</b>	<b>ADSL connection simulation .....</b>	<b>104</b>
8.4.1	PC #2 parameters.....	104
8.4.2	PC #1 parameters.....	105
<b>8.5</b>	<b>Generating multicast IP traffic.....</b>	<b>106</b>
8.5.1	PC #2 and PC #3 parameters.....	106
8.5.2	PC #1 parameters.....	107
<b>8.6</b>	<b>IPV6 connection .....</b>	<b>108</b>
8.6.1	PC #2 parameters.....	108
8.6.2	PC #1 parameters.....	109
<b>8.7</b>	<b>Source/Local IP Address and Interface requirements .....</b>	<b>112</b>
<b>PART 9</b>	<b>Annexes .....</b>	<b>114</b>
<b>9.1</b>	<b>Mathematical laws used by "LanTraffic V2".....</b>	<b>114</b>
9.1.1	Uniform law .....	114
9.1.2	Exponential law.....	115
9.1.3	Pareto Law .....	117
9.1.4	Gauss law .....	118
<b>9.2</b>	<b>"LanTraffic V2" Traces .....</b>	<b>119</b>
<b>9.3</b>	<b>"LanTraffic V2" configuration parameters saved in the registry .....</b>	<b>119</b>
9.3.1	General configuration parameters .....	119
9.3.2	Help configuration parameters.....	120
<b>9.4</b>	<b>Default values of a context.....</b>	<b>121</b>

## PART 0 Preface

### 0.1 Organization of this manual

This user guide is aimed at helping you to discover and use “LanTraffic V2”. This manual is organized as follows:

- **Part 1: Product Overview**

Briefly describes the “LanTraffic V2” software and its features.

- **Part 2: Install, Uninstall, License Configuration and Transfer**

Explains how to install and uninstall the software, configure a license and move a license between the source and the target PCs.

- **Part 3: Graphical User Interface**

Presents the “LanTraffic V2” Graphical User Interface, i.e. the main rules and principles of representation and display.

- **Part 4: Using LanTraffic V2**

Explains how to use the “LanTraffic V2” software. This part includes menu and functionality description. It is based on Windows and Tabs description. Each Tab is presented separately.

- **Part 5: Command Line Parameters**

Explains how to use a command line with parameters to start the “LanTraffic V2” software.

- **Part 6: How To Do ...**

Gives some samples about how and where to use LanTraffic V2.

- **Part 7: Annexes**

Describes additional information about the mathematical laws used by “LanTraffic V2”, “LanTraffic V2” traces, configuration parameters saved in the Registry database, and default values of a new context.

In this document, you will find the following symbols:



**Warning**



*Zoom or Advice*



*Note or Remark*

## 0.2 Minimum System Requirements

“LanTraffic V2” requires the following minimum system requirement to operate properly:

- Windows 98 (SE recommended), Me, NT4 (SP6 recommended), 2000 or XP
- Pentium processor with 128 Kb memory
- 1024 x 768 display
- 10 MB free hard disk space



***To use IPv6, Windows XP or Windows 2003 server is required.***



*Acrobat Reader is needed to display the «LanTraffic V2» Help. If Acrobat reader hasn't been installed, a warning message is displayed to inform that «LanTraffic V2» is available without the help.*

## 0.3 Technical Support

ZTI Technical support can assist you with all your technical problems, from installation to troubleshooting.

Before contacting technical support, please read the relevant sections of the product documentation and the “Read Me First” file.

You can contact Technical Support by:

Email	Send as many details as possible to <a href="mailto:support@zti-telecom.com">support@zti-telecom.com</a> or <a href="mailto:support@zti.fr">support@zti.fr</a>
Fax	Send as many details as possible to +33 2 96 48 14 85
Telephone	Telephone support is available from 09:00 am to 06:00 pm (GMT Time +1 or +2), Monday to Friday. Call +33 2 96 48 43 43

Before contacting Technical Support, please record the following information:

- Product name and version.
- Demo version or licensed product.
- System configuration.
- Problem details: settings, error messages...
- If the problem is repeatable, the details of how to create the problem.



## PART 1 Product Overview

### 1.1 Key Features

"LanTraffic V2" is a connection and data generation tool for IP networks. Data flows use TCP (Transmission Control Protocol) or UDP protocol (User Datagram Protocol), which is used by mailing exchanges, file transfer and World Wide Web transmission.

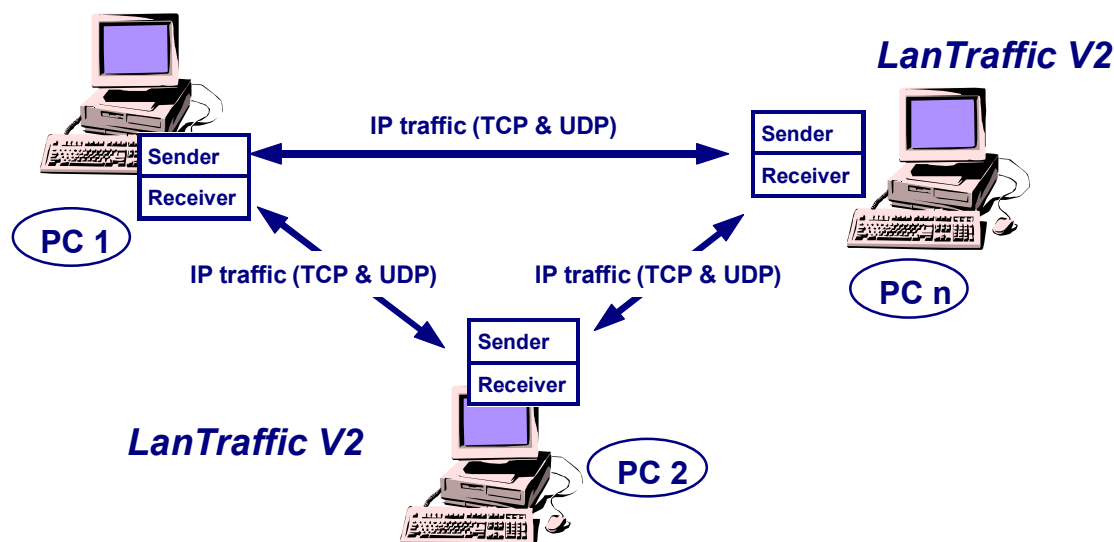
"LanTraffic V2" needs at least two PCs running on Windows XP Home or Professional, Windows 2000 Professional or Server, Windows NT 4 Service Pack 6 Workstation or Server, Windows 98 or Me. Screen resolution must be at least 1024 x 768.

Each PC shall have at least one Ethernet connection (LAN card i.e. NIC, remote access...).

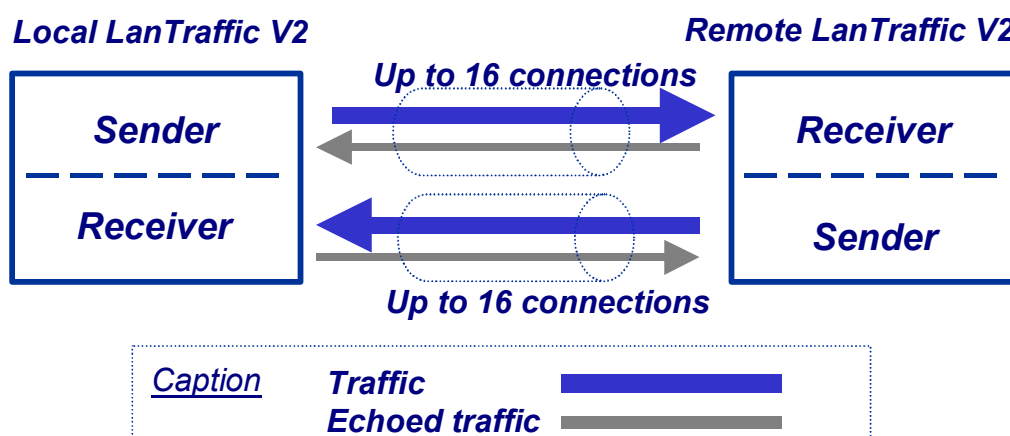
Acrobat Reader is needed to display the Help.

Various testing configurations can be implemented using more than two PCs. "LanTraffic V2" establishes TCP or UDP connections between PCs through the IP network.

#### LanTraffic V2



The "LanTraffic V2" testing tool is composed of a **Sender** part and a **Receiver** part.



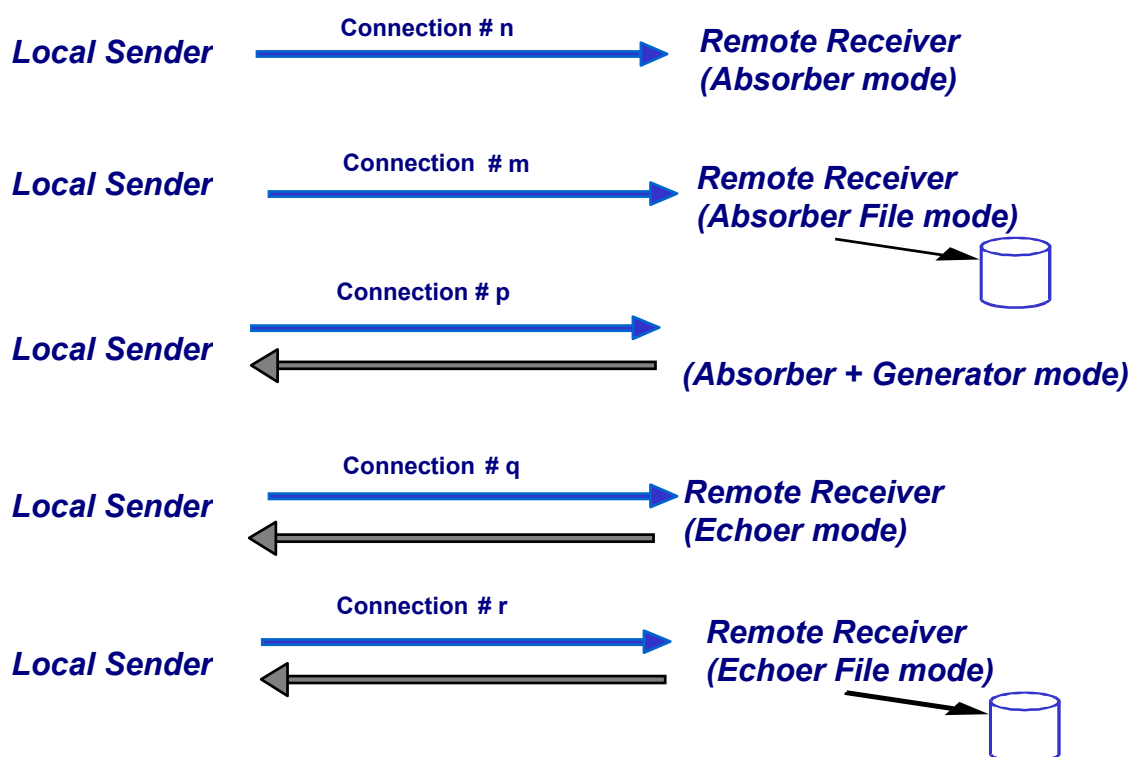
- The **Sender** part generates up to 16 simultaneous connections. Connections can be generated following two different testing modes:
  - ⇒ In the unitary mode you can select the traffic generator data source and configure packets size and inter-packet delay for each connection

"LanTraffic V2" offers three different data sources:

- Automatic data generator by using mathematical laws,
- Packets generator: many parameters can be defined (number of packets to send, inter packet delay, packet contents, ...)
- File: selection of a file to send.

⇒ In the automatic mode you select one mathematical law for connections generation starting time and another mathematical law for data volume to send to generate up to 16 connections.

- The **Receiver part** receives traffic (up to 16 simultaneous connections) and operates following different working modes: Absorber, Absorber file, Absorber + Generator, Echoer, Echoer File.



In this user guide, we will consider that the local machine is used for sending and remote one is used for receiving.

### Multicast feature



The "LanTraffic V2" software is able to generate and receive Unicast and Multicast IP traffic. The multicast feature is used only for the UDP protocol. Used only with UDP protocol, IPv4 addresses from 224.0.0.0 to 239.255.255.255 are MULTICAST IP addresses.

These addresses can be used to generate multicast IP traffic (define the multicast IP address in the Sender part) or to receive multicast IP traffic (define the multicast IP address in the Receiver part).

For information: these IPv4 addresses 224.0.0.0 to 224.255.255.255 don't generate IGMP JOIN /LEAVE messages

## IP version selection (Windows XP and later)

Microsoft has included the IPv6 protocol stack in Windows XP. IPv6 is not commercially available with older Windows version. A research - partial - implementation was available for Windows 2000. Microsoft does not support it. ZTI doesn't offer the use of the Windows 2000 IPv6 stack with "LanTraffic V2".

IPv6 is not installed by default: it should be added on the interface you want to use.

"LanTraffic V2" supports the IPv6 numerical address format (128 bits long) as well as canonical addresses. The IPv6 multicast is available with "LanTraffic V2", in accordance to RFC 2373 where a multicast IPv6 address starts with FF.

With IPv6, the maximum size of the TCP packet is 1440 bytes whereas it is 1460 bytes with IPv4.

## Interface selection

The interface selection of a LAN card (NIC), a virtual NIC such as an IP tunneling protocol or a remote access is useful to control the data traffic hardware route.

The "LanTraffic V2" software is able to generate and receive Unicast and Multicast IP traffic on a selected interface, giving the user a deeper control where data are exchanged with and to reduce ambiguity when multiple routes are defined.

## Statistics values

Statistics values presented by 'LanTraffic V2' are computed at the Application level. They don't include the protocol header, the IP header nor data link header and/or trailer.

## 1.2 Reference

[WINSOCK2] « Windows Socket 2 - Application Programming Interface » Revision 2.2.0 - May 10, 1996

[IPV6-XP] <http://www.microsoft.com/windowsserver2003/technologies/ipv6/ipv6.mspx>

[RFC2460] "Internet Protocol, Version 6 (IPv6) - Specification"

[RFC2373] "IP Version 6 Addressing Architecture"

## 1.3 Terms used in this document

Interface	Generic term used to reference a NIC (LAN adapter), a connected RAS connection (ISDN, ADSL, Modem) or a tunneling path.
Tooltip	A tooltip is a popup window displayed when you move the mouse over a sensitive area. "LanTraffic V2" displays the tooltip during 5 seconds.
Automation	Automation is an add-on scripting tool used in addition to "LanTrafficV2".

## PART 2 Install LanTraffic V2

The "LanTraffic V2" software needs less than of ten megabytes free disk-space. By default, the setup folder will be C:\Program files\LanTrafficV2.

The "Automation Tool for LanTraffic V2" add-on software is automatically installed with the "LanTraffic V2" software.



***\* To run "LanTraffic V2" your computer's screen resolution must be configured on 1024 X 768 (at least).***

***\* For Windows NT, 2000 and XP you must be logged on with administrator privileges.***



*It is advisable to first close anti-virus application before installing "LanTraffic V2". Please note that you should mask the task bar in a 1024x768 screen resolution, so you could have an optimal view of the software interface.*

The "LanTraffic V2" software is configured by default with a 15-day limited license. When the time limit expires, "LanTraffic V2" will cease to run. See paragraph III below for more information about the license program.

The installation procedure is a standard installation program for Windows 98, Me, NT4, 2000 and XP.

### 2.1 Install from a downloaded trial version



***The installation procedure under Windows NT4, 2000 or XP requires to be logged on with administrator privileges.***

If you have downloaded the "LanTraffic V2" software trial version from our website, you have downloaded the file "Setup\_LanTrafficV2Bundle.exe".

Run "Setup\_LanTrafficV2Bundle" and follow the "LanTraffic V2" setup instructions to proceed with the installation.

By default, the "LanTraffic V2" software will be installed in the following directory: C:\Program Files\LanTrafficV2

The "LanTraffic V2" installation procedure will install the following files on your disk, in particular:

- LanTrafficV2.exe: program file
- LanTraffic V2 User Guide: PDF format. (You can use for example the free Adobe® Acrobat® Reader® software. See [www.adobe.com](http://www.adobe.com)).
- Aut\_LTV2.exe: program file (Automation tool)
- Automation Tool for LanTraffic V2 User Guide: PDF format
- LanTrafficV2 license help file
- Version.txt: text file, which contains information about versions and Registry commands.



*At LanTraffic V2 launch, all files created by the application will be saved in the folder where LanTraffic V2 has been installed.*

### Start Menu shortcuts created:

Start > Programs > **LanTraffic V2**

- ⇒ **LanTraffic V2** (click to run the software)
- ⇒ **LanTrafficV2 User Guide** (PDF format)
- ⇒ **Automation Tool for LanTrafficV2** (click to run the software)
- ⇒ **Automation Tool for LanTrafficV2 User Guide** (PDF format)
- ⇒ **License help**
- ⇒ **Uninstall LanTrafficV2**

With a “LanTraffic V2” trial version, when you run it for the first time, a message is displayed showing remaining days of use (for example, 15 days left out of 15 in the following example):



*Please refer to the third paragraph to configure your license.*

## 2.2 Install from the CD-ROM

The installation procedure is a standard installation program.



***The installation procedure under Windows NT4, 2000 or XP requires to be logged on with administrator privileges.***

- First, insert the “LanTraffic V2” CD-ROM on disk drive.
- Click on “Start”, “Execute” and type “CD-ROM unit>:\Setup\_LanTrafficV2Bundle.exe”. Follow the “LanTraffic V2” setup instructions to proceed with the installation. By default, the “LanTraffic V2” software will be installed in the following directory:  
C:\Program Files\LanTrafficV2.

### Start Menu shortcuts created:

Start > Programs > **LanTraffic V2**

- ⇒ **LanTraffic V2** (click to run the software)
- ⇒ **LanTrafficV2 User Guide** (PDF format)
- ⇒ **Automation Tool for LanTrafficV2** (click to run the software)
- ⇒ **Automation Tool for LanTrafficV2 User Guide** (PDF format)
- ⇒ **License help**
- ⇒ **Uninstall LanTrafficV2**

When you launch “LanTraffic V2” for the first time, a message is displayed showing remaining days of use, even if you have bought an unlimited license (for example, 15 days left out of 15 in the following example):



*Please refer to the next paragraph to configure your unlimited license.*

## PART 3 License configuration

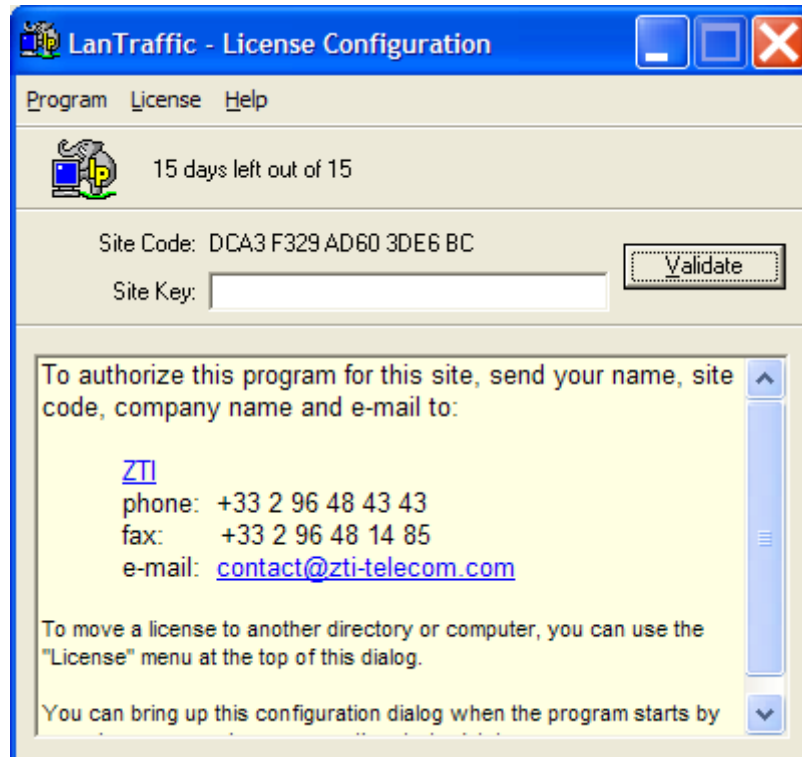
### 3.1 To configure a license

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

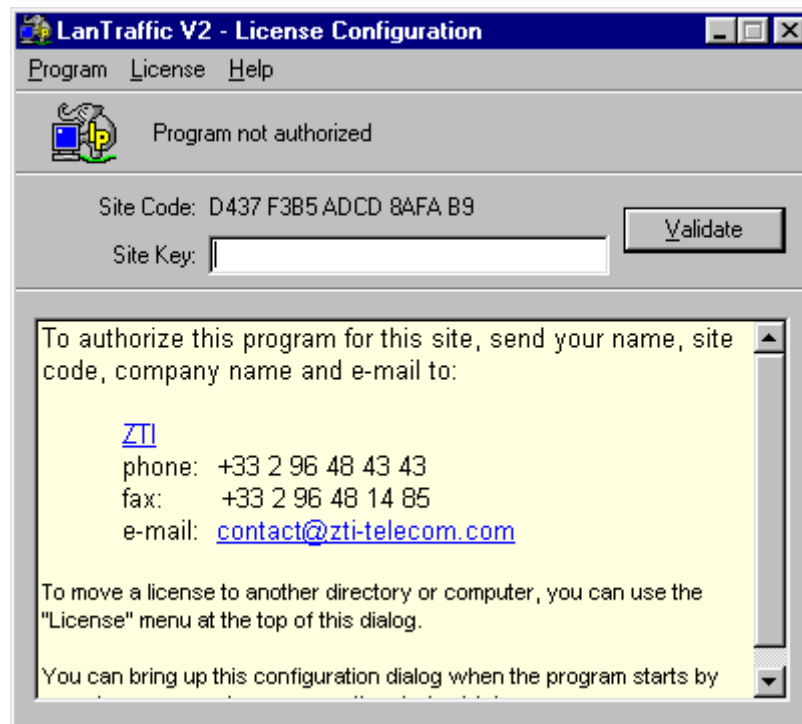
If you wish to configure your license before trial period end, please press **Enter** when the following message is displayed:



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



At the end of the trial period when you launch "LanTraffic V2", the same license configuration dialog appears, with a specific mention instead of the remaining days of use: "Program not authorized".

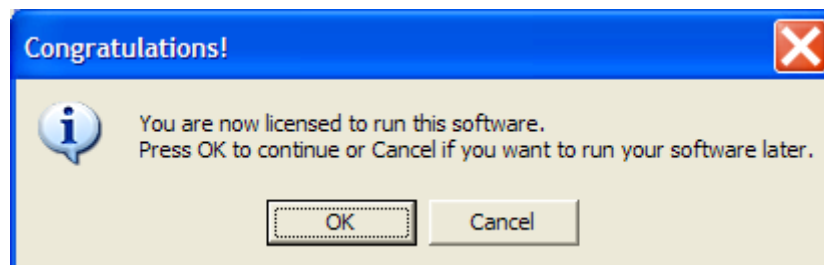


To get the 'Site Key' and obtain an unlimited version, please send your name, 'Site Code' (specific to your installation), company name, e-mail and preferred method of payment (if you haven't bought the "LanTraffic V2" software yet) to: [contact@zti-telecom.com](mailto:contact@zti-telecom.com) or [contact@zti.fr](mailto:contact@zti.fr).

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

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

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







You will see the following dialog when you launch “LanTraffic V2” if you have an unlimited license:



## 3.2 License Transfers



***A license transfer is not a duplication of any type.***

***Please contact ZTI or your authorized distributor for site license information and for several licenses purchase.***

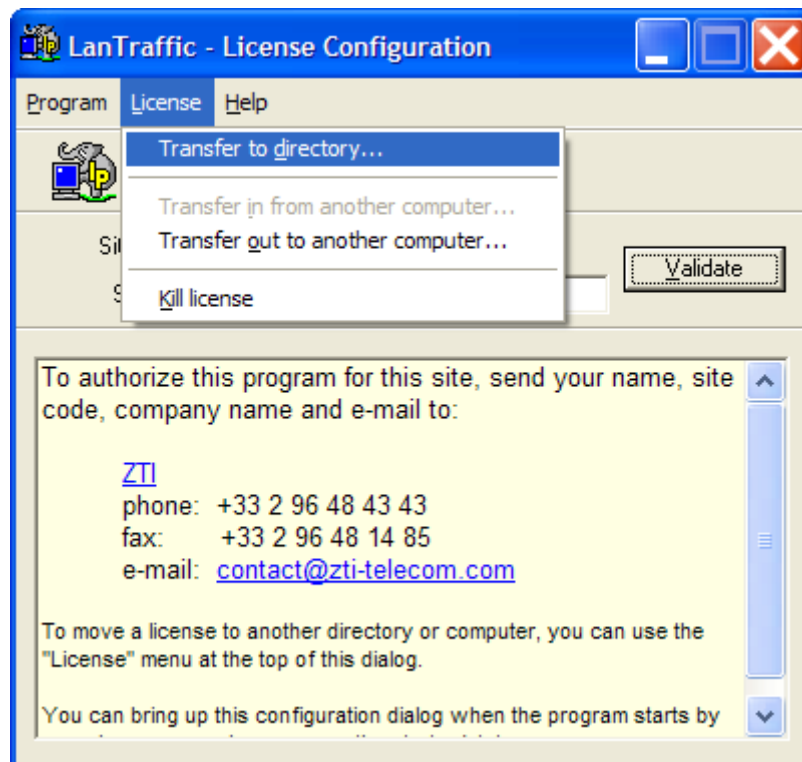
Licenses can be transferred using one of the following methods:

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

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

This transfer mechanism must be used to move a license in two cases:

- from a source to a target directory of the same PC
  - from a source to a target directory of networked PCs
- First, copy the program (copy the folder “LanTraffic V2”) to the target directory.  
*For example from “C:\Program Files\LanTrafficV2” to “C:\Temp\LanTrafficV2”*
  - Then run the program in the original directory (from “C:\Program Files\LanTrafficV2”). When the license configuration window appears, press **Enter** and select in the menu “License > Transfer to directory ...”, as shown below:



- Provide the path name of the target program (for example *C:\Program Files\LanTrafficV2\LanTrafficV2.exe*).  
The program copy now has the license awarded the original.

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



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

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

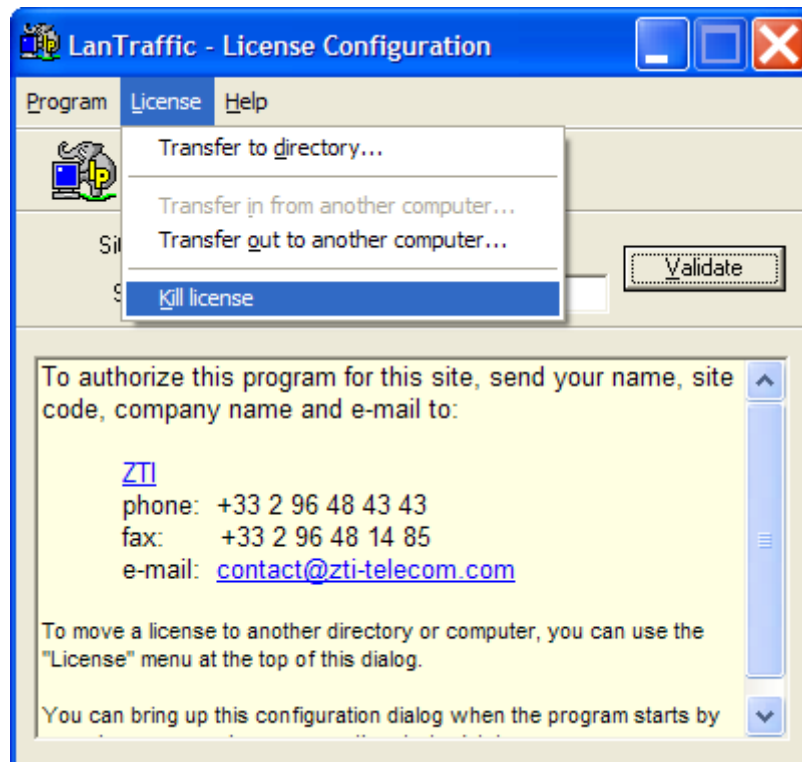
**Point 1:** First install the program on the target PC (PC# 2).

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

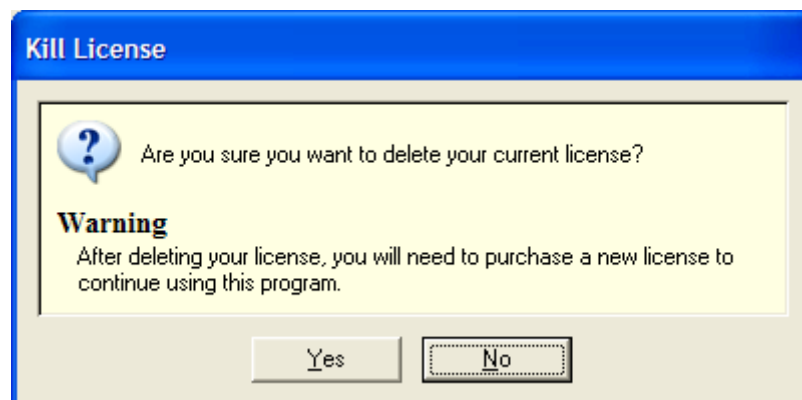
You need to kill the license if the "Transfer in from another computer ..." item of the license menu is disabled.

**To kill the license, please proceed as follows.**

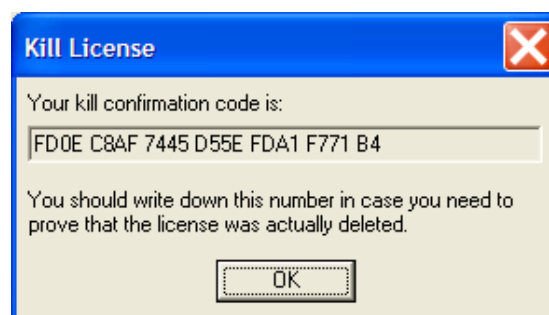
When the license configuration window appears, press **Enter** and select in the menu "License > Kill license".



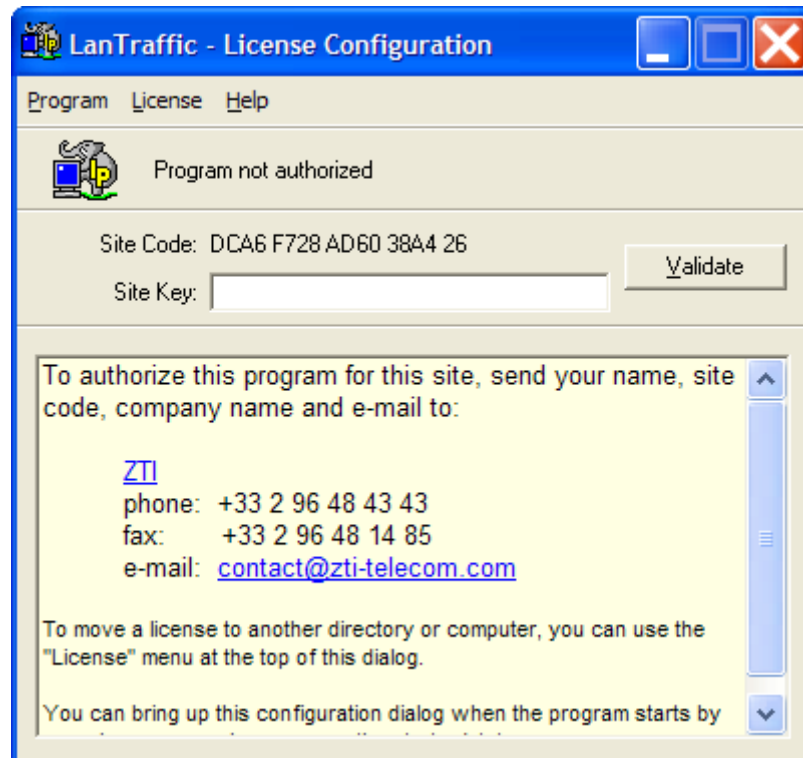
A message box appears, press 'Yes' to kill the license.



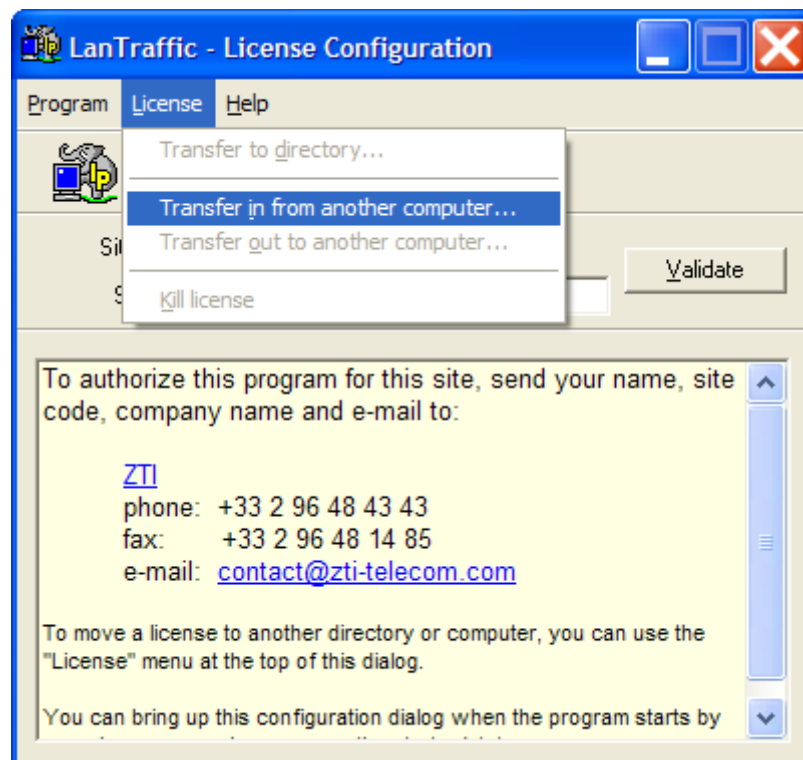
And a kill confirmation code is displayed.



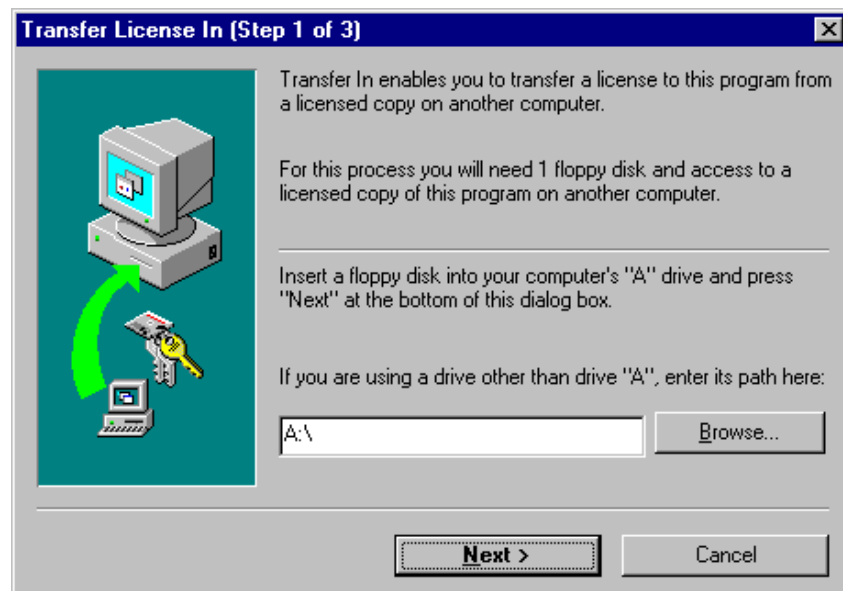
The license window displays now "Program not authorized" as following:



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



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

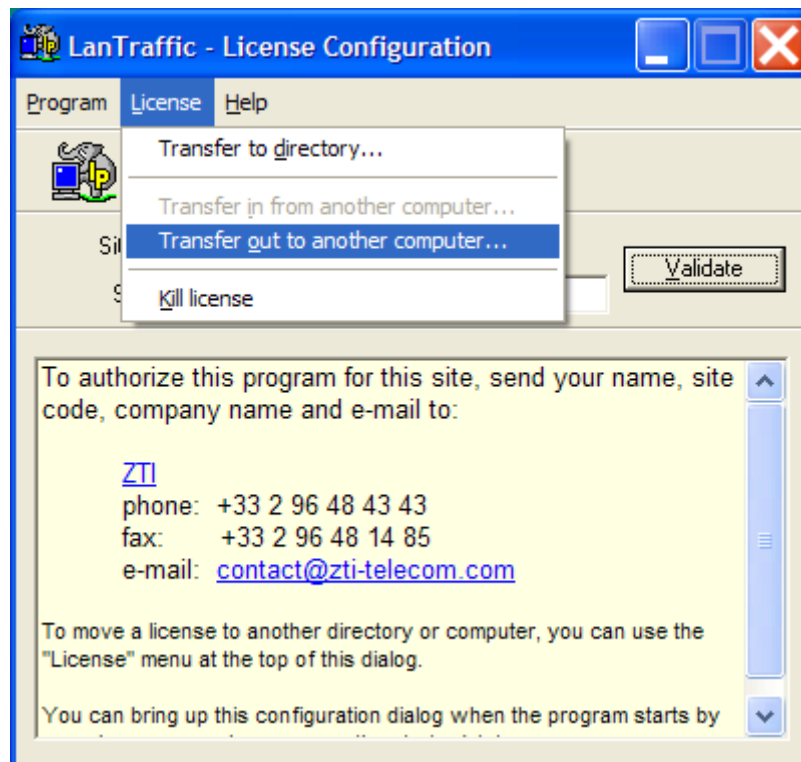


**Point 4:** Insert a floppy disk or use a USB key as requested in step 1 of 3 and specify the path.

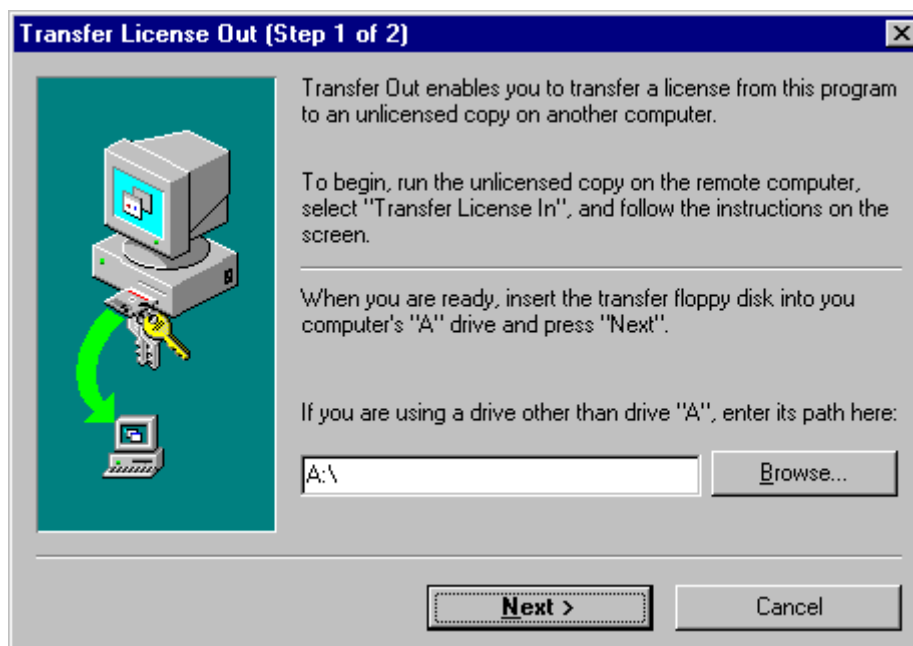
Then press "Next >" and the "Transfer License In (Step 2 of 3)" window is displayed:



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

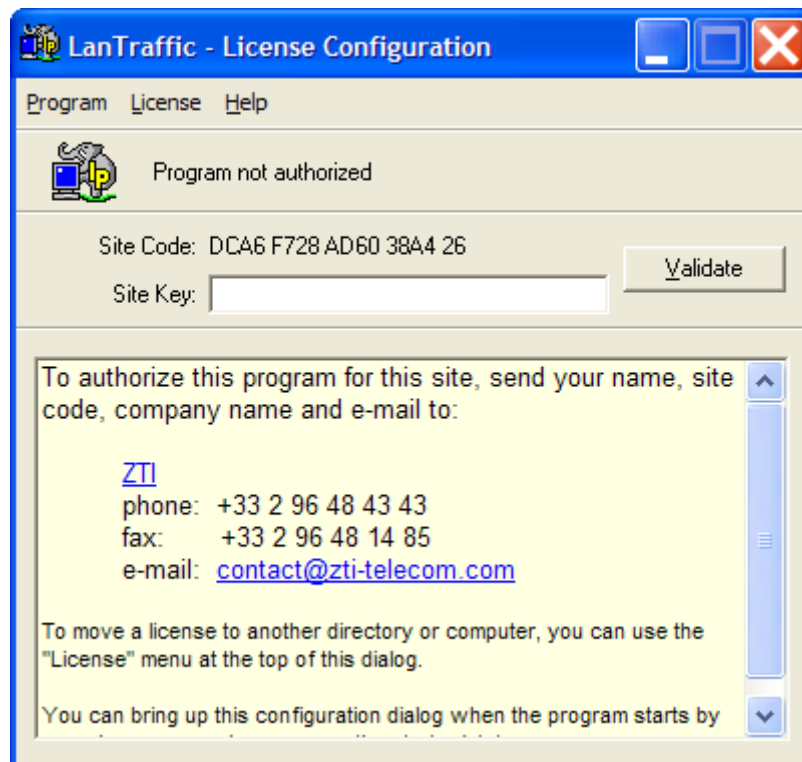


Then the following window is displayed:



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

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



You can check that the license is no more available on the source PC since the LanTraffic V2 software license is on a per workstation basis. Contact us to get information on site license ([contact@zti.fr](mailto:contact@zti.fr) or [contact@zti-telecom.com](mailto:contact@zti-telecom.com)).

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

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

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



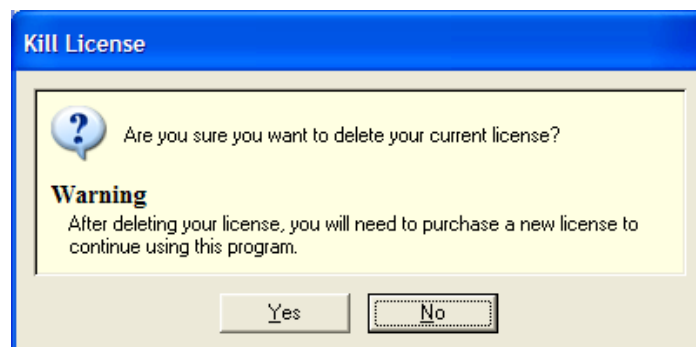
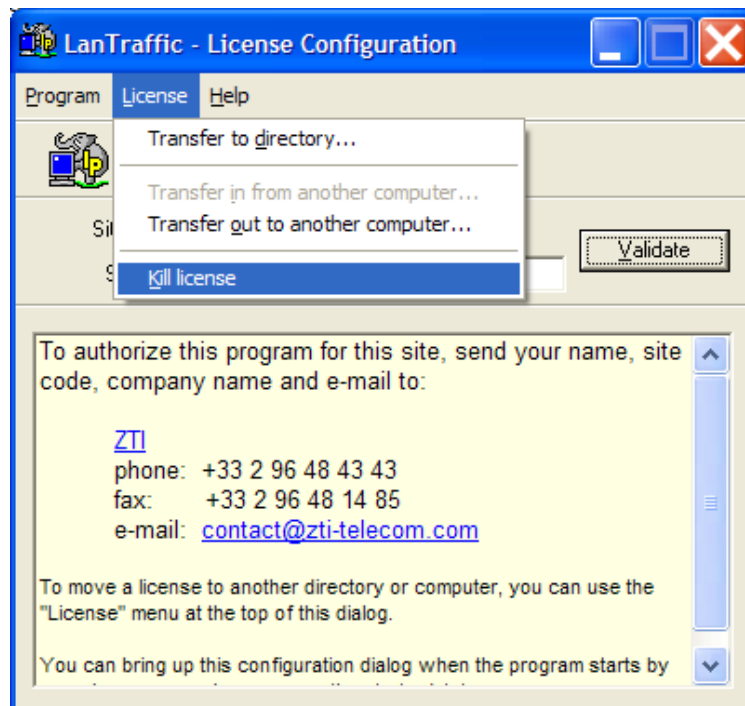
Click Finish to continue.

### 3.3 To kill a license

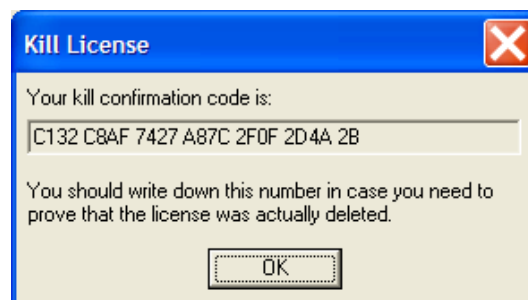
If you would like to transfer an unlimited license key onto a PC where a trial period is still active, you should first kill the active trial period. If you don't kill the active trial period, you will not be able to transfer an unlimited license.

To kill the trial license, you should proceed as follows:

- On the license configuration window, select in the menu "License > Kill License" as shown below. A message box appears, press OK.



- Press Yes and then your license is now killed. Please, write down the kill confirmation code. This code may be requested by ZTI.





## **PART 4   Uninstall LanTraffic V2**

The uninstall procedure is a standard uninstall program.

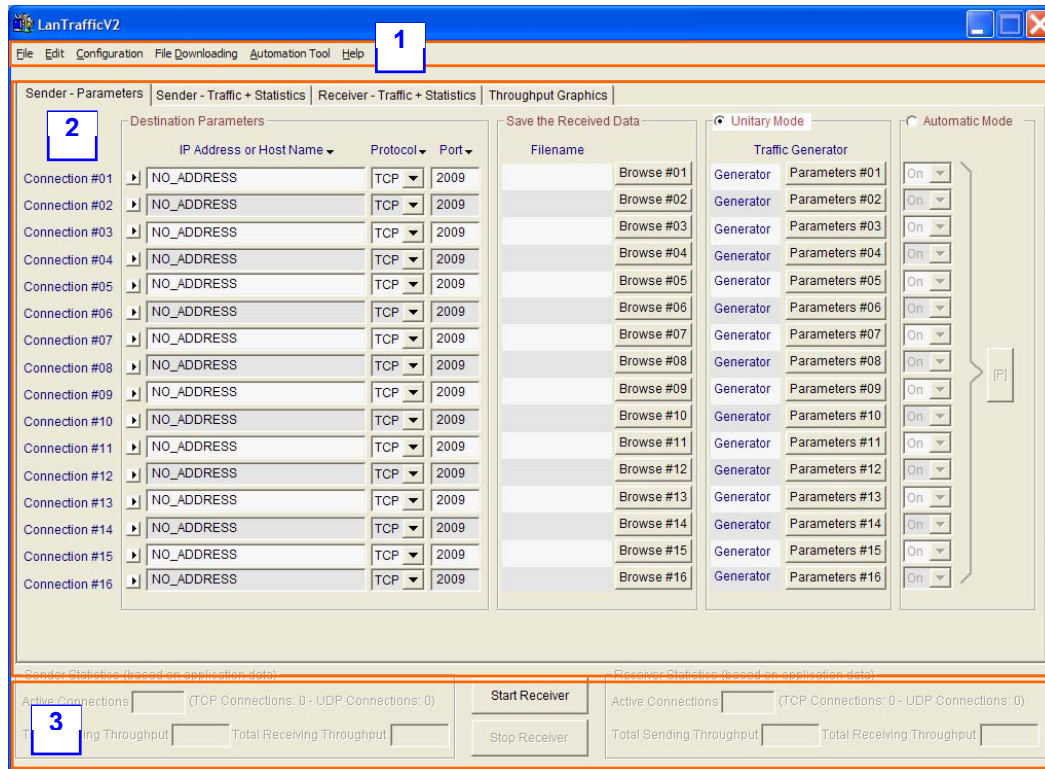
In the “Start > Programs > LanTraffic V2” menu, select “Uninstall LanTraffic V2”.

You must then delete all remaining files in the directory: C:\Program Files\LanTrafficV2.

## PART 5 Graphical User Interface

### 5.1 Main Window

When “LanTraffic V2” is started, the following main window is displayed:



"LanTraffic V2" main window

The “LanTraffic V2” main window is composed of three areas:

#### Area 1: Menu bar

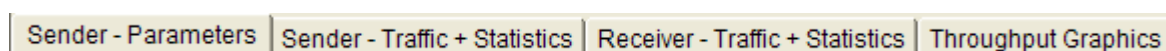
**Area 2:** this main area displays the **four tabs** of “LanTraffic V2”.  
To view a tab, click on the tab title you want to view.

**Area 3: Statistics** for the Sender and Receiver parts and general command buttons.

'Menu bar' and 'Statistics' are always visible whatever tab is displayed

#### Tabs general presentation:

“LanTraffic V2” GUI is composed of four tabs:



"LanTraffic V2" - tabs titles

- The first two tabs are related to the Sender part: “Sender - Parameters” and “Sender - Traffic + Statistics”.
- The third one is related to the Receiver part: “Receiver Traffic + Statistics”.
- In the first three tabs related to Sender and Receiver parts, each one of the 16 connections is represented by one line (from “connection # 01” to “connection #16”). Columns represent parameters or status of connections and statistics.
- The fourth tab allows displaying throughput graphs: “Throughput Graphics”.

Each tab is composed of several areas. For each tab, we will present in this guide each area separately.

## 5.2 Display general rules of “LanTraffic V2” GUI

“LanTraffic V2” fields can be filled following four situations:

- Fields in which you can enter values

All the fields in which you can enter or choose values are recognizable by black writing on white background colors. If an address is not valid, the red color is displayed instead of black.

- Statistics fields

Statistics fields are automatically filled. They are identifiable by blue writing on white background colors. You can only configure the refresh time of statistics display or reset statistics display by pressing the “Reset Display” buttons.

When a statistic value cannot be computed “N / S” for No Sense value is displayed in the field.

- Fields generated further to user action and displayed as information use only

These fields are filled automatically by “LanTraffic V2” further to use enter or parameters selection. They are displayed as reminder and will be modified by another user action.

These fields are recognizable by black writing on gray background.

- Fields turned out of reach further to user action

User actions and parameters selection may turn some “LanTraffic V2” GUI fields and action buttons out of reach. Usually, all the out of reach fields are grayed.

### **Fields can become out of reach in several cases, for example:**

- As soon as a connection is running, it is impossible to change its parameters. You must stop the connection in order to change the connection’s parameters.
- When a testing mode (unitary or automatic) is selected, it is impossible to change parameters of the unselected testing mode.
- If you enter a no valid value in a field, the connection could be disabled or actions button in configuration windows could become out of reach.

### 5.3 Used units in information display

All information used by “LanTraffic V2” is displayed with its unit and unit is changing in order to limit figure size.

#### 5.3.1 Volume units

Display	Meaning
10 B	10 Bytes
1 KB	1 Kilo Bytes (1,024 Bytes)
1 MB	1 Mega Bytes (1,048,576 Bytes)
1 GB	1 Giga Bytes (1,073,741,824 Bytes)
1 TB	1 Tera Bytes (1,099,511,627,776 Bytes)
1.23^65	1.23 x 10^65 Bytes

#### 5.3.2 Throughput units

Display	Meaning
10 b/s	10 bits per second
1 Kb/s	1 Kilo bits per second (1,024 b/s)
1 Mb/s	1 Mega bits per second (1,048,576 b/s)
1 Gb/s	1 Giga bits per second (1,073,741,824 b/s)
1 Tb/s	1 Tera bits per second (1,099,511,627,776 b/s)
1.23^65	1.23 x 10^65 bits per second



#### *Throughput computing*

*The “LanTraffic V2” displayed throughputs correspond to payload data on the sampling period (defined in the “LanTraffic V2” configuration menu) and bring back to a bits/second number.*

*The displayed throughput is an “application” throughput.*

*At some instant, it could be different from the physical network throughput because data can be split and buffered at various system levels.*

## PART 6 Using “LanTraffic V2”

### 6.1 Main steps

The main steps to use “LanTraffic V2” are:

⇒ **To send data:**

1. *In Tab 1 “Sender – parameters”:*  
Configure Sender parameters i.e. IP address, port number, and protocol. You can select optionally the interface and the IP protocol.  
Select, and configure testing mode,
2. *In Tab 2 “Sender – Traffic+ Statistics”:*  
Run connections,
3. Result: exploit statistics and throughput graphs.

⇒ **To receive data:**

1. *In Tab 3 “Receiver - Traffic + Statistics”*  
Configure Receiver parameters i.e. connected senders, working mode, and optionally you can select the interface and the IP protocol.
2. *In Tab 3 “Receiver - Traffic + Statistics”:*  
Start receiving connections,
3. Result: exploit statistics and throughput graphs.



#### *About the context file*

*In order to avoid entering again all parameters for a new testing session, or to create again mathematical laws, all the “LanTraffic V2” parameters can be saved in a context file (see File menu description below).*

*So, if you want to repeat a test session with the same parameters later, do not forget to save the current parameters in a context file before changing some parameters.*

## 6.2 Menu description

The menu bar is composed of 6 items:

File Edit Configuration File Downloading Automation Tool Help

The options for each item are described in this chapter.

### 6.2.1 File menu



#### 6.2.1.1 File/New

This command opens a new default context in “LanTraffic V2”. Before opening a new default context, running connections must be stopped. The default values of a new context are presented in Annex part.

#### 6.2.1.2 File/Open

“Open” command allows reading a context file (.CTX file), which contains a previously saved configuration. Before opening a context, running connections must be stopped.

The context format varies from versions to versions. A context saved with “LanTraffic V2” version 2.0.12 or 2.1 is silently read by “LanTraffic V2” version 2.2. Older context cannot be read: an error message is displayed when you attempt to open such a file.



*A context file contains configuration parameters and a copy of the laws defined by the user. Reading of a context file will delete currently used laws and replace them by the laws saved in the context file.*

#### 6.2.1.3 File/Save

“Save” option allows saving all the configuration parameters and the laws defined by the user in the opened context file.



*If versions 2.0.12 or 2.1 contexts were opened, the context file saved get the new format used by “LanTraffic V2” version 2.2: it will not be available for reuse with an older version of “LanTraffic V2”*

#### 6.2.1.4 File/Save as ...

This option allows saving all the configuration parameters and laws defined in a context file (.CTX file).

The context file saved by the "LanTraffic V2" version 2.2 can't be read by versions 2.1 and older.

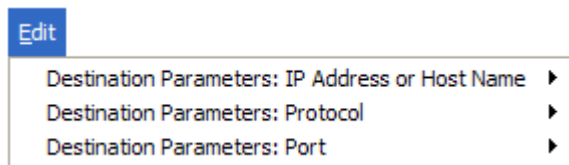
#### 6.2.1.5 File/Recent Contexts ...

This option allows opening a context file previously loaded. The 4 most recent context files are shown in the list.

#### 6.2.1.6 File/Exit

This command allows quitting "LanTraffic V2". To quit "LanTraffic V2", all active connections (Sender and Receiver) must be stopped. A message box will ask you to save or not changes made to parameters in a context file.

### 6.2.2 Edit menu



#### 6.2.2.1 Edit/Destination Parameters: IP Address or Host Name

1 option is available:

Copy the IP Address from Connection #01 to all Connections

By selecting this item, the IP Address field from connection #01 is recopied for all connections from #02 to #16.

#### 6.2.2.2 Edit/Destination Parameters: Protocol

2 options are available:

Select TCP for all Connections  
Select UDP for all Connections

By selecting one option, the 'Protocol' field for the connections #01 to #16 are set to TCP or UDP.

#### 6.2.2.3 Edit/Destination Parameters: Port

4 options are available:

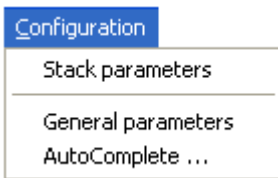
Increase only UDP Ports (from first UDP Connection)  
Decrease only UDP Ports (from first UDP Connection)  
Increase all Ports (from Connection #01)  
Decrease all Ports (from Connection #01)

With this menu, you can:

- Set the port number increasingly or decreasingly for all UDP connections, based on the port number of the first UDP connection.

- Set the port number increasingly or decreasingly for all connections, based on the port number of the first connection without taking into account the protocol in use.

## 6.2.3 Configuration menu

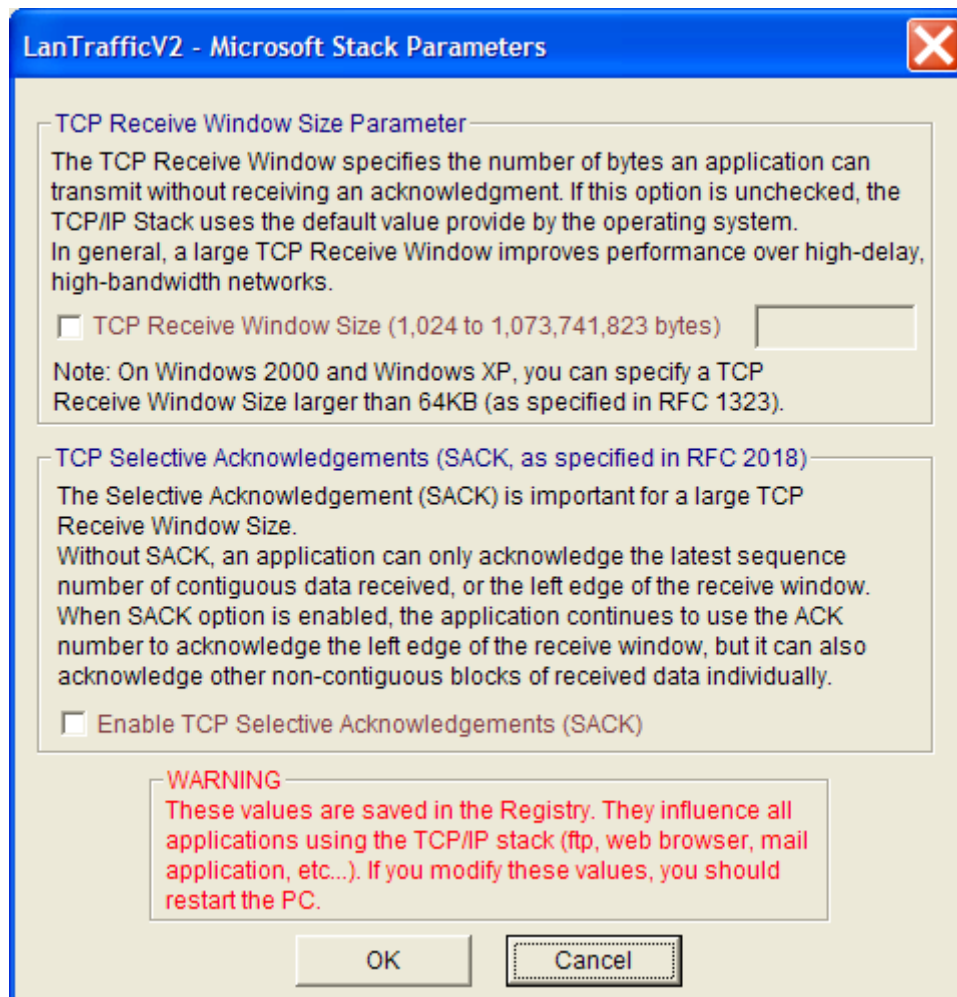


### 6.2.3.1 Configuration/Stack Parameters

“LanTraffic V2” uses the Microsoft TCP/IP stack via the Winsock2 interface (or API). This interface enables modifying some parameters of the Microsoft TCP/IP stack.

“LanTraffic V2” enables modifying the TCP Receive Window size and enable the TCP Selective Acknowledgements.

When the Stack Parameters command is selected, the following window is pop up:



*Stack Parameters window*



*The TCP Receive Window Size value must be included between 1,024 and 1,073,741,823 bytes.*



“OK” button allows saving changes made to the TCP/IP stack Parameters. If some changes have been made, you must restart your PC.



***Important: these values are saved in the Registry and influence all applications using the TCP/IP stack***

Paths to these parameters on the registry depend on the operating system:

- Windows NT4, 2000 and XP Key is:  
HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\TCPIP\Parameters  
Name: TcpWindowSize & Tcp1323Opts & SackOpts.
- Windows 98 Key is:  
HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\VXD\MSTCP  
Name: DefaultRcvWindow & Tcp1323Opts (no SACK).

TCP WINDOW SIZE value is saved in the Registry, and so saved for all contexts. It affects all applications that use the Windows TCP stack (ftp, etc).



***Note for Windows 98: the TCP window size is the DEFAULTRECEIVE-WINDOW parameter.***

### 6.2.3.2 Configuration/General Parameters

This command allows configuring parameters applying to graphical display, timeouts for echoed connections and the size of buffers used by the "LanTraffic V2" software. When selected, the following window is pop up:

**LanTrafficV2 - General Parameters**

**Refresh Time and Throughput Sampling Period**  
The refresh time parameter defines the frequency of statistics updates on "LanTrafficV2". This parameter applies also to the statistics exportation processes. The Throughput Sampling Period defines the number of seconds of traffic to take in account to calculate the throughput.

Refresh time (1 to 60 seconds)

Throughput sampling period (1 to 60 seconds)

**TCP and UDP received Data Timeout**  
These parameters concern the Sender Part only. When there are no more data to send, "LanTrafficV2" continues to receive data until the timeout expires. Then the connection is released. When the timeout is 0, the connection is stopped as soon as there are no data to send.

Timeout for TCP packets echoed (1 to 9,999 ms)

Timeout for UDP packets echoed (1 to 9,999 ms)

**LanTrafficV2 Buffer Size (SO\_RCVBUF and SO\_SNDBUF)**  
The buffers used by "LanTrafficV2" to dialog with the Winsock API influence the throughput performance for high speed network. The best performance can be reached with a high buffer size. Change in one of these sizes concerns the new connections only.

Receive buffer size (1,024 to 65,535 bytes)

Transmit buffer size (1,024 to 65,535 bytes)

General parameters window

#### *Parameters applying to GUI display*

- **Refresh time:** value entered in this field configures display refresh time for all statistics displayed in "LanTraffic V2".
- **Throughput sampling period:** value entered in this field is used to compute throughput for statistics display.

#### *Parameters applying to echoed connections*

- **Timeout for TCP packets echoed (ms):** value entered in milliseconds. This field is used for echoed TCP connections. When the connection is stopping, "LanTraffic V2" continues TCP data acquisition during a time defined by this timeout. If this value equals zero, "LanTraffic V2" don't handle any TCP incoming traffic on this connection as soon as the connection is stopped.

- **Timeout for UDP packets echoed (ms):** value entered in milliseconds. This field is used for echoed UDP connections. When the connection is stopping, “LanTraffic V2” continues UDP data acquisition during a time defined by this timeout. If this value equals zero, “LanTraffic V2” don’t handle any UDP incoming traffic on this connection as soon as the connection is stopped.

#### *Parameters applying to the data buffer size*

- **Receive buffer size:** this value is saved in the current context only and is used when receiving data from the Microsoft Winsock2 interface.
- **Transmit buffer size:** this value is saved in the current context only and is used when sending data to the Microsoft Winsock2 interface.

### 6.2.3.3 Configuration/AutoComplete ...

The AutoComplete option is a help mechanism to input values for the user. It lists possible entries that match user entries typed before. The AutoComplete mechanism with “LanTraffic V2” is available for IP address entries in the “Sender – Parameters” and “Receiver – Traffic + Statistics” tabs.

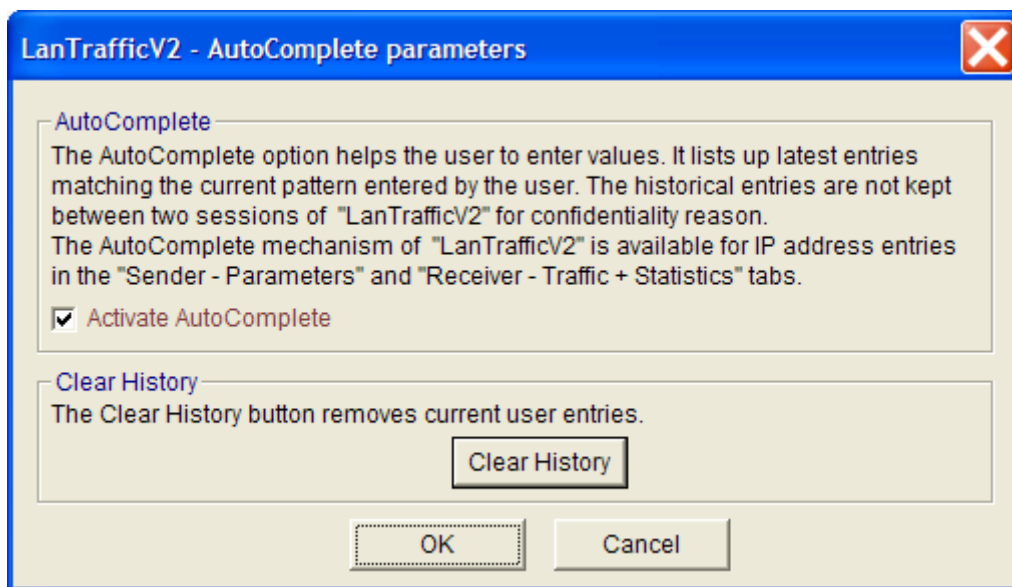


*Example of AutoComplete entry in the "Sender – Parameters" tab.*

There are 3 different historical records:

- Historical record for IP address entry in the Sender tab,
- Historical record for IP address entry in the Receiver tab
- Historical record for IP address in the File Downloading dialog box.

The AutoComplete parameters dialog is used to enable/disable and to clear all historical records.



*AutoComplete parameters.*

Up to 30 entries can be kept in the historical record. When a 31<sup>st</sup> entry is typed, the 1<sup>st</sup> entry is deleted: the historical record is handled like a FIFO list.

The **Clear History** button removes user entries from historical records leaving two predefined entries:

- NO\_ADDRESS: this is the default Sender IP address - a void address, used to disable the connection.
- ANY\_ADDRESS: this is the default Receiver IP address, used to accept any incoming connection.

When AutoComplete is disabled, the historical record doesn't continue to be filled. User entries before AutoComplete deactivation will be available when AutoComplete is activated again.



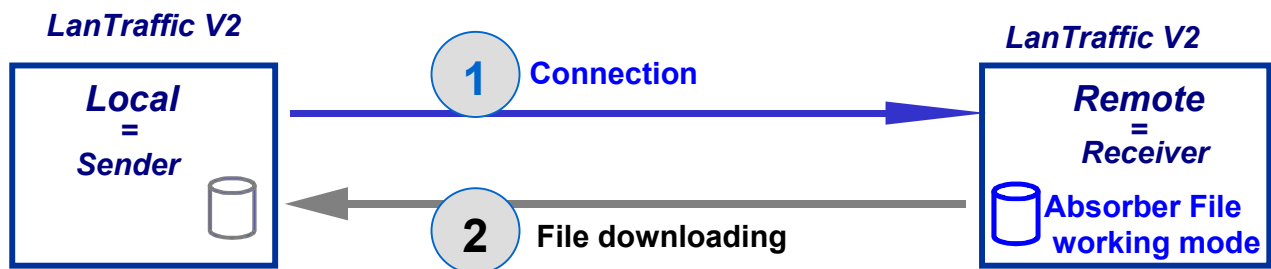
*The historical record is associated to the "LanTraffic V2" session. For confidential reasons, the historical record is not kept between sessions and is lost at the end of the "LanTraffic V2" session.*

## 6.2.4 File Downloading menu

### File Downloading

This command allows downloading a file from one “LanTraffic V2” machine to another one. In order to avoid confusion, “Local” and “Remote” terms are used to design the machines for this command.

File Downloading is mainly used when a receiving connection is operating in the Absorber File working mode. It is aimed to repatriate the absorbed file from Receiver to Sender, as shown in the following scheme. (Though any file from the remote machine can be downloaded).



*Example of File downloading in File absorber receiving working mode environment*

**1:** Remote receiver stores received data in a file (working mode = Absorber File).

**2:** The user of the Local Sender machine can get the file back by using File downloading function.

### Example of File downloading usage:

File Downloading may be used when a receiving connection at the Remote side is operating in Absorber File working mode. It is aimed to repatriate the absorbed file from Receiver to compare it to the file sent by the Sender, as shown in the following scheme. The Remote receiver is configured in Absorber file Mode, for TCP connection. The Local sender establishes a TCP connection and sends data from a file. When the connection is finished, the Sender uses the File downloading function to get received data from the Remote Receiver. So you can check if data transfer was successful.

### Process to download a file:

When clicking on the File Downloading command, the following window is pop up:

**LanTrafficV2 - File downloading Parameters**

This function allows file downloading from a remote "LanTrafficV2" PC to the local "LanTrafficV2" by using a specific TCP port number. The remote and the local PCs must have the same port number. This function uses IPv4.

File downloading Port Number  
Local port number (1 to 65,535)  1

File downloading from a Remote

Remote source filename  2

IP Address or Host Name  3

Local destination filename  4

0  100

5

*File downloading window***To process a file transfer, proceed as follows:**

On the local and remote machines:

(1) Configure port number – Port number must be the same for local and remote machines.

On the local machine:

(2) Give the name and path of the remote file to download. To be downloaded, the file must be not be written or enriched on the remote machine at the same time.

(3) Give the IP address or Host name of the remote machine from where the file is downloaded

(4) Give the local name of the destination file

(5) Press “Start” button to begin the file downloading from the remote machine

“OK” button allows saving the entered parameters and closes the window.



*When “Start” button is pushed, it is impossible to press OK or to close the window. You should press “Stop” or wait the end of file transfer operation or abort it.*

On the remote machine, the following message box will warn that a file downloading is in progress:

LanTrafficV2 - File downloading in progress from a remote			
Remote IP address	192.168.0.37	Port number	2500
Local filename downloaded by the remote		E:\Temp\FileReceived.bin	
Data volume to send	49684357	Data remaining volume	24117125

*Warning message displayed on the remote machine from which file is downloaded*

- Remote IP address is the IP address of the machine where the file to download is. This address is never in canonical format.
- Port number is the port number chosen for file downloading (it must be the same for the remote and local machines).
- Local filename downloaded by remote is the name of the downloaded file.
- Data volume to send is the total volume of the file to download.
- Data remaining volume is the volume still to send.

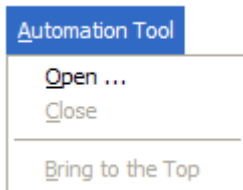


***During a file transfer, you will not be allowed to close the application on the Remote machine.***

#### File downloading is working as follows:

- Local requests the file that is sent by the Remote machine.
- Local establishes the connection.
- Remote accepts the connection and waits for the filename (with a time-out - default 5 s).
- When connected, Local sends the filename.
- When Remote receives the filename, it checks if the file exists and send the size (0 means no file or file access error) and data.
- When Local wants to stop the reception of the file, it disconnects.
- When Remote has sent the file, it waits for an ACK (with a timeout - 5s by default).
- When reception of the file is complete, Local send an ACK.
- When Remoter receives an ACK (or expiration of the Timeout), it disconnects.

## 6.2.5 Automation Tool menu

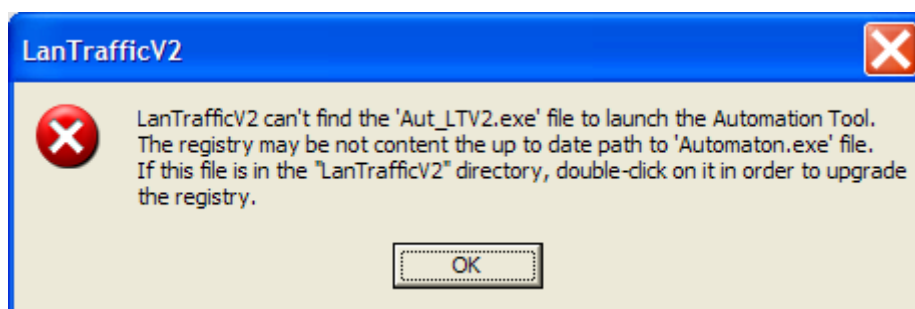


### 6.2.5.1 Automation Tool/Open...

This command starts the “Automation tool for LanTraffic V2”.

The “Open...” command is grayed when the “Automation tool for LanTraffic V2” is already started because only one instance can run at the same time.

If the Aut\_LTV2.exe file is not located in the same directory than “LanTraffic V2”, an error message is displayed:



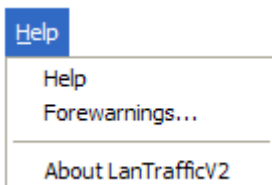
### 6.2.5.2 Automation Tool/Close

This command stops the running “Automation tool for LanTraffic V2”.

### 6.2.5.3 Automation Tool/Bring to the top

This command displays the “Automation tool for LanTraffic V2” window at the top of the other opened applications, except applications that can’t be masked e.g. task manager when this option is selected.

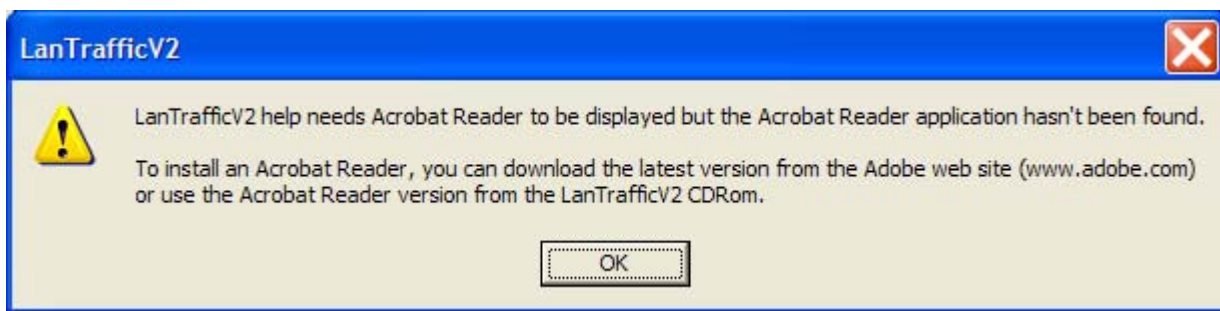
## 6.2.6 “Help” menu



### 6.2.6.1 Help/Help

Help command displays help on “LanTraffic V2”. Pressing **F1** key can also activate help. To display “LanTraffic V2” Help, Acrobat Reader should be installed. If Acrobat reader is not installed, a warning message is displayed:





You can download the latest version from <http://www.adobe.com>, or use the version of Acrobat Reader provided with the “LanTraffic V2” CD ROM and install Acrobat Reader.



***“LanTraffic V2” doesn’t support other PDF readers than Acrobat Reader version 4 or 5.***

### 6.2.6.2 Help/Forewarnings ...

This command is aimed to inform of “LanTraffic V2” special behaviors due to system limits. “LanTraffic V2” leans on the Microsoft Winsock 2 Interface to generate and receive TCP or UDP traffic. Therefore the “LanTraffic V2” application behavior, as any Winsock 2 application, is dependent of the Winsock 2 Interface, Microsoft TCP/IP stack and operating system working modes.

#### 6.2.6.2.1 *Inter-packet delay*

When defining the inter-packet delay, you must consider that the minimum resolution handled by “LanTraffic V2” is related to the timer resolution of the operating system. This timer resolution varies according to the operating system and PC used, as well as CPU and network load when “LanTraffic V2” is operating.

The best timer resolution that “LanTraffic V2” can provide is one millisecond.

“LanTraffic V2” operates in the best effort mode to provide the inter-packet delay requested by the user.

#### 6.2.6.2.2 *Echoer modes*

When the Receiver is configured in Echoer mode (‘Echoer’, ‘Echoer file’ or ‘Absorber + Generator’) it is recommended to use the most powerful PC of the test bed as Receiver (more CPU is required to send back data).

#### 6.2.6.2.3 *UDP connections*

When several UDP connections are running and according to the traffic level and to the system load, “LanTraffic V2” could behave particularly due to the TCP/IP stack limits and working modes.

The current release of the Winsock2 API doesn’t provide any system limit information to applications such as “LanTraffic V2”, so the following situations may occur.

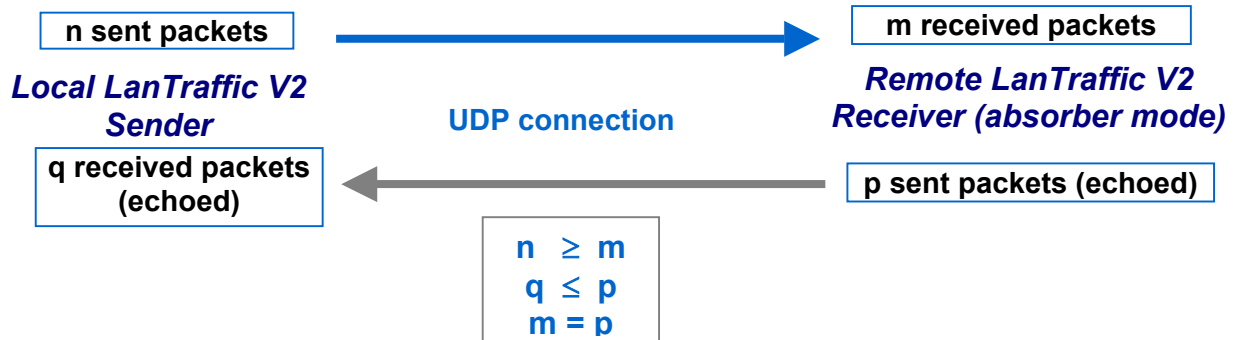
- **Loses of packets**

The Winsock2 interface doesn’t transmit all received packets to the “LanTraffic V2” Receiver.

a) UDP connection from Local sender to Remote receiver - the working mode of the remote Receiver is absorber.



b) UDP connection from Local sender to Remote receiver - the working mode of the remote Receiver is echoer.



In this case, number of received packets (m) will be equal to the number of echoed packets (p) in the Receiver part. Nevertheless, the number of received packets (q) in the Sender part could be inferior to the number of packets (p) sent by the remote Receiver in echoer mode.

#### ▪ UDP connection distribution

When several UDP connections are running together, the TCP/IP stack may favor some connections. It has been noticed that echoed connections are favored.

Throughput of connections for the Receiver working in absorber mode may decrease to zero for a variable while.

#### ▪ UDP total throughput

The total sending throughput could indicate a higher value than the face value of the physical link throughput

*When these situations occur, they can be limited by regulating connections throughput according to the face value of the physical link throughput.*

*To regulate throughput you can reduce the packet size or increase the inter-packet delay for the connections. Another way to curb these limits is to configure the buffer size in the “Configuration / Stack parameters” menu or to tune the Microsoft TCP/IP stack.*

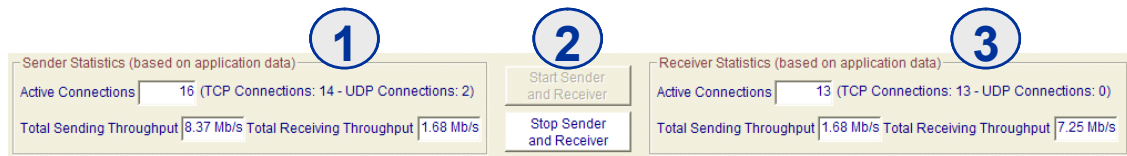
### 6.2.6.3 Help/About LanTrafficV2

The “About” command display the version number and copyright of the “LanTraffic V2” application.

## 6.3 Total statistics

Total statistics for the Sender ① and Receiver ③ are displayed in the lower part of the “LanTraffic V2” main window.

Statistics display refresh time and sampling period to compute the throughputs are configured in the “Configuration / General Parameters” menu, as described in 6.2.3.2.



*Total statistics displayed in the main window lower part*

Two general command buttons ② are also available to start and stop the Sender and the Receiver parts, and the label of these buttons vary according to the activity state of each entity:

<b>Sender inactive</b> <b>Receiver inactive</b>	<b>Sender active</b> <b>Receiver active</b>	<b>Sender active</b> <b>Receiver inactive</b>	<b>Sender inactive</b> <b>Receiver active</b>
<div>Start Sender and Receiver</div> <div>Stop Sender and Receiver</div>	<div>Start Sender and Receiver</div> <div>Stop Sender and Receiver</div>	<div>Start Receiver</div> <div>Stop Sender</div>	<div>Start Sender</div> <div>Stop Receiver</div>

### 6.3.1 Sender statistics

For the Sender tab, the following statistics are displayed:

- **Active connections:** Number of current running connections on the Sender part. More details are displayed: number of TCP Sender connections and number of UDP Sender connections.
- **Total Sending Throughput:** Instant throughput of data sent for all connections of the Sender.
- **Total Receiving Throughput:** Instant throughput of data received. These statistics are available only when some connections are configured in the Echoer or Absorber-Generator working mode on the Remote Receiver part.

### 6.3.2 Receiver statistics

For the Receiver tab, following statistics are displayed:

- **Active connections:** Number of current running connections on the Local Receiver part. More details are displayed: number of TCP Receiver connections and number of UDP Receiver connections.

- **Total Sending Throughput:** Instant throughput of all echoing connections sent back from Local Receiver to Remote Sender, or Absorber-Generator.
- **Total Receiving Throughput:** Instant throughput of all receiving connections.


## 6.4 Sender part

The Sender generates up to 16 simultaneous connections. Connections can be generated following two different testing modes: Unitary or Automatic. These modes are exclusive.

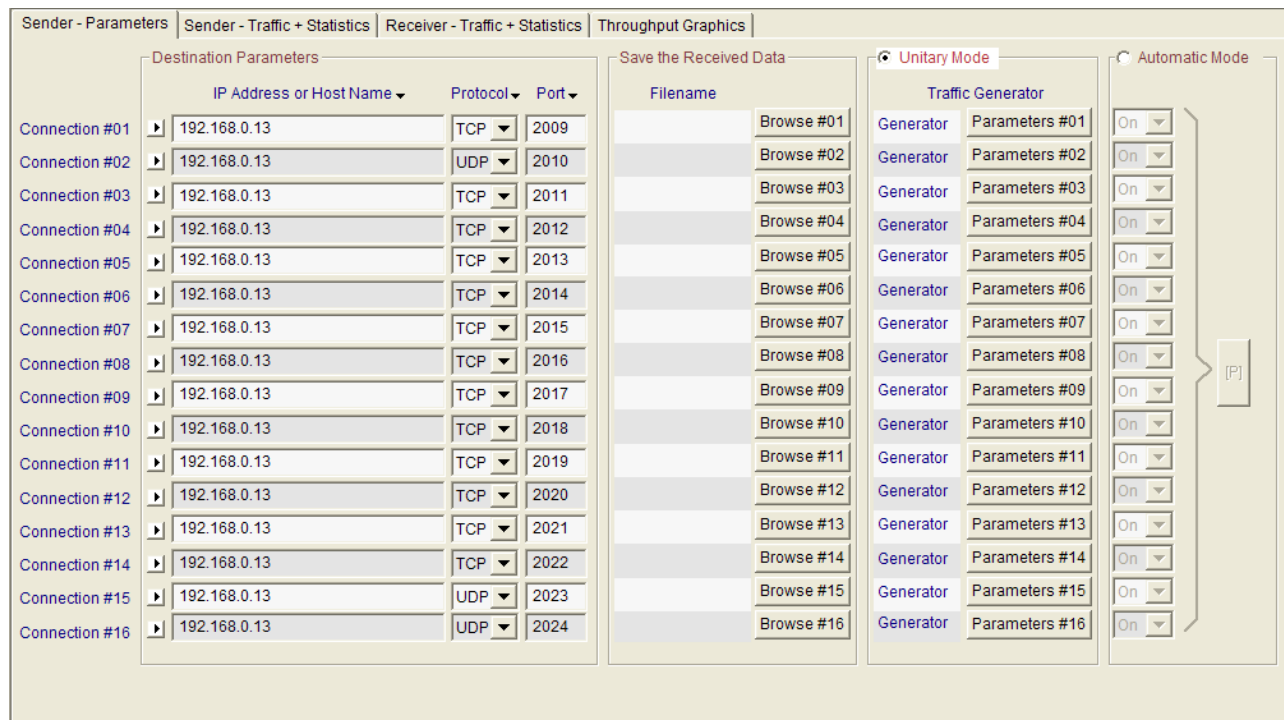
Sender part is represented in two tabs. The first one “Sender-Parameters” is used to configure connections and testing mode. The second one “Sender-Traffic + Statistics” is used to command the traffic generation and visualize the traffic statistics.

### 6.4.1 Sender - Parameters tab

The first tab of “LanTraffic V2” allows:

- Selecting the interface and the IP version (when IPv6 is installed) for each connection, by clicking the black arrow .
- Entering destination parameters (IP address, protocol and port number) for each connection.
- Selecting files to save received data when connections are working in Echoer mode or Absorber-Generator mode for the Remote Receiver part.
- Selecting and configuring the testing mode: Unitary or Automatic.
- Configuring the generator: for each connection when the Unitary mode is selected or globally when the Automatic mode is selected.

These actions are represented by the “Sender-Parameters” tab in 4 distinct areas and detailed below.




Destination Parameters				Save the Received Data		Traffic Generator		Automatic Mode
	IP Address or Host Name	Protocol	Port	Filename		Generator	Parameters	
Connection #01	192.168.0.13	TCP	2009		Browse #01	Generator	Parameters #01	On
Connection #02	192.168.0.13	UDP	2010		Browse #02	Generator	Parameters #02	On
Connection #03	192.168.0.13	TCP	2011		Browse #03	Generator	Parameters #03	On
Connection #04	192.168.0.13	TCP	2012		Browse #04	Generator	Parameters #04	On
Connection #05	192.168.0.13	TCP	2013		Browse #05	Generator	Parameters #05	On
Connection #06	192.168.0.13	TCP	2014		Browse #06	Generator	Parameters #06	On
Connection #07	192.168.0.13	TCP	2015		Browse #07	Generator	Parameters #07	On
Connection #08	192.168.0.13	TCP	2016		Browse #08	Generator	Parameters #08	On
Connection #09	192.168.0.13	TCP	2017		Browse #09	Generator	Parameters #09	On
Connection #10	192.168.0.13	TCP	2018		Browse #10	Generator	Parameters #10	On
Connection #11	192.168.0.13	TCP	2019		Browse #11	Generator	Parameters #11	On
Connection #12	192.168.0.13	TCP	2020		Browse #12	Generator	Parameters #12	On
Connection #13	192.168.0.13	TCP	2021		Browse #13	Generator	Parameters #13	On
Connection #14	192.168.0.13	TCP	2022		Browse #14	Generator	Parameters #14	On
Connection #15	192.168.0.13	UDP	2023		Browse #15	Generator	Parameters #15	On
Connection #16	192.168.0.13	UDP	2024		Browse #16	Generator	Parameters #16	On

Tab 1: “Sender – Parameters”

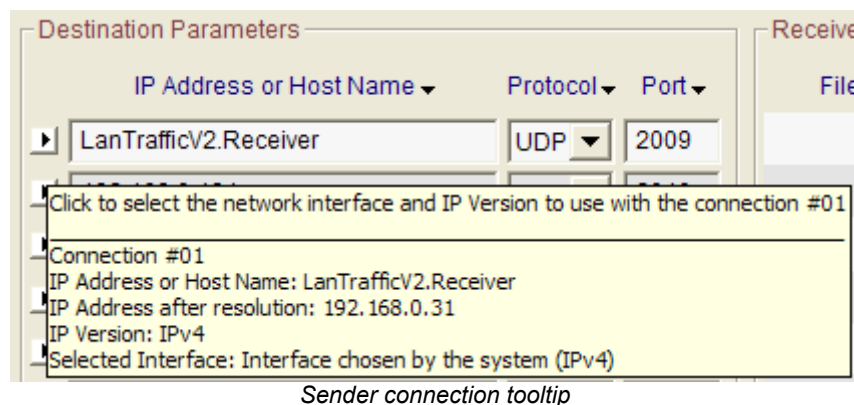
### 6.4.1.1 Destination parameters

Located at left part of the tab, this area allows configuring destination parameters of each sending connection. You can enter the following information:

<b>Network interface selection and IP version</b> 	<p>The black arrow has two purposes:</p> <ul style="list-style-type: none"> <li>• To display a summary of the connection's parameters.</li> <li>• To select the network interface, the IP version or the IP source address for a connection.</li> </ul>
<b>IP address or Host Name</b>	<p>IP address should be entered following the numerical writing of IP address (i.e. xxx.xxx.xxx.xxx) or using the canonical format (e.g. an URL).</p> <p>The default IP address is NO_ADDRESS (0.0.0.0 for IPv4).</p> <p>Once the value entered, a verification is made and the field is red colored if the value is invalid.</p>
<b>Protocol</b>	TCP or UDP protocol (default = TCP protocol).
<b>Port</b>	<p>The port number is limited to 65,535.</p> <p>By default, the entered port number is 2009.</p> <p>In case of invalid value, the value is <b>red</b> colored.</p>

#### 6.4.1.1.1 Summary of connection parameters

When you move the mouse over the black arrow, a popup window - called a **tooltip** – is displayed.



Sender connection tooltip

The tooltip for the Sender connection includes 5 items:

- First item is the connection number the tooltip refers to.
- Next item is the IP address defined by the user.
- Next item is the IP address translated when IP Translation address has succeeded (e.g. the address is not NO\_ADDRESS or 0.0.0.0).
- Next item is the IP version currently selected.
- Last item is the interface name selected. The name displayed is the name of the connection presented in the “Settings/Network and Dial-up Connections” Start menu of the operating system (Default is “Interface chosen by the system”).

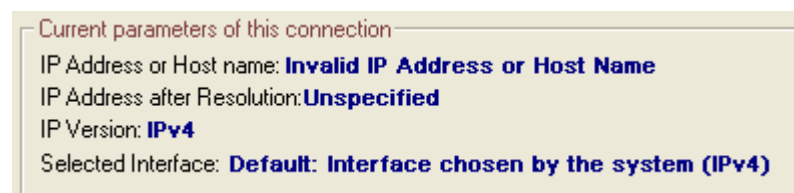
### 6.4.1.1.2 Select the network interface, IP version and source IP address

When you click on the black arrow, a window is displayed:



*Network interface, IP version and IP source address for a Sender's connection*

- (1) The **network interface** selection is optional. It is used to select the IPv6 or to force connections to be established using a specific interface.
- By default:
    - IP version 4 is used.
    - The IP stack resolves the interface selection to send packets to the remote.  
The IP stack uses the destination IP address to select the correct interface. IP address and netmask related to each interface are checked against the remote IP address to reach. When an interface that matches the remote IP address is found, it is used. To understand how the IP stack selects the interface, you may enter 'route print' console command to list interface order, IP address and network address mask.
  - You can select one interface from the list of connected interfaces. "LanTraffic V2" will only use the selected interface to translate IP address and to make connection. You must select the interface compatible with the remote IP address you want to reach. When the IP address translation failed, current connection parameters area is updated as follows:



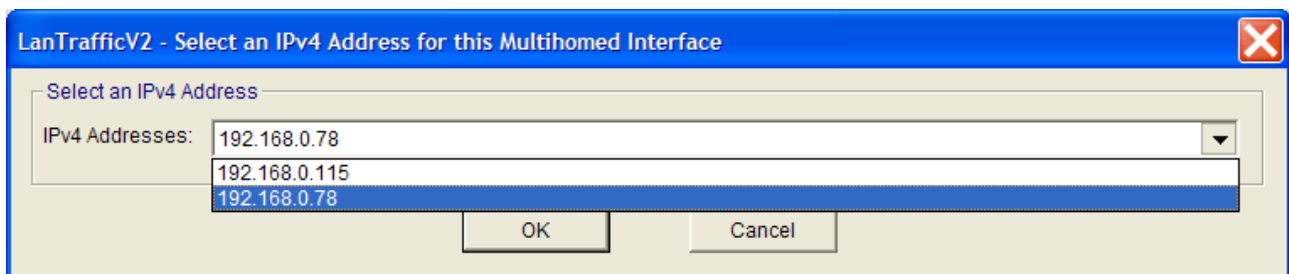
- Use of IPv6 requires the selection of an interface.
- Interface types are restricted: only Ethernet and PPP are listed.  
A PPP interface should be in 'connected' state to belong to the interface list.



- (2) **IP version** selection is available:
- with Windows XP (or later)
  - when IPv6 is attached to the interface e.g. current Windows versions doesn't offer IPv6 over PPP.
  - when an interface has been selected with IPv6 attached e.g. 'interface chosen by the system' can't be used.

The IP address translation (see 6.4.1.1.3) uses the current IP version to get the IP address numerical form.

- (3) **Select IP address** is available when multiple IP addresses are attached to the network interface. This interface configuration is also known as 'multihomed' interface. Selection of a Source IP address is generally not required: "LanTraffic V2" uses the default IP address of the interface to establish connections. It may be useful when routing priority or policy is defined. Example of IP address selection for a multihomed interface:



*Select IP address is not available if the default interface 'Interface chosen by the system' is selected.*

- (4) **Current parameters of this connection** area are an abstract for the connection. It summarizes IP address, numerical IP address format, IP version and interface selection.
- IP addresses are static. The IP address translation will process only when you click on OK.
  - IP version field is dynamically updated with the user selection.
  - Current interface is dynamically updated with the user selection.



*When you click on the OK button, if the interface selected or IP version has changed, the IP address translation is automatically started. It may be time consuming.*



### 6.4.1.1.3 IP Address translation mechanism

“LanTraffic V2” tries to translate – e.g. to resolve - the IP address from a canonical to a numerical format. This operation is called the *IP address translation mechanism*. When the ‘IP Address or Host Name’ field or Interface parameters changes, when you move from ‘IP Address or Host Name’ field to another field, to another tab, when the Enter key is pressed or when Interface parameters change, automatically starts the IP address translation mechanism.

Because the IP address translation mechanism is CPU consuming, a particular attention should apply when using IP canonical addresses. CPU consumption depends on the DNS answer speed, the number of DNS configured and the network load when the DNS request is sent.

If network environment changes – e.g. a new DNS has been defined - you should press the Enter key in the ‘IP Address or Host Name’ field to force “LanTraffic V2” restart the translation mechanism for this connection.



*When the IP address translation failed, the IP address is written **red** on white. This connection cannot be started: the “Run” button in the ‘Sender – Traffic + Statistics’ tab is grayed.*



*To summarize, the **IP address translation mechanism** is activated when:*

- *the focus leaves the ‘IP Address or Host Name’ field,*
- *another tab is selected,*
- *you duplicate parameters from one connection to another,*
- *you change the Interface parameters.*

### 6.4.1.1.4 Duplicate parameters of a connection onto others

In order to facilitate input of these parameters, a *copy/paste mechanism* for all parameters of a connection is available. This mechanism is not available when the canonical IP address cannot be translated in numerical format.

Duplication of connection’s parameters doesn’t copy the interface information. When you copy a connection to another one, the IP address translation mechanism is started.

Step 1: first, input parameters for a connection (by example, connection #01)

Sender - Parameters				Sender - Traffic + Statistics		Receiver - Traffic + Statistics	
Destination Parameters							
	IP Address or Host Name	Protocol	Port				
Connection #01	192.168.0.13	TCP	2010				
Connection #02	NO_ADDRESS	TCP	2009				
Connection #03	NO_ADDRESS	TCP	2010				

Step 2: move the mouse cursor on the ‘Connection #1’ label (source). The mouse cursor appears as shown beside.

	IP Address or Host Name	Protocol	Port
Connection #01	192.168.0.13	TCP	2010

Step 3: mouse click left. Then the 'Connection #1' label is blue colored.

	IP Address or Host Name ▾	Protocol ▾	Port ▾
Connection #01	192.168.0.13	TCP	2010

Step 4: when you move the mouse cursor on one another 'Connection #02' label for example, the mouse cursor changes.

	IP Address or Host Name ▾	Protocol ▾	Port ▾
Connection #01	192.168.0.13	TCP	2010
Connection #02	NO_ADDRESS	TCP	2009

(Copy mode)

Step 5: then you can paste all parameters of connection #01 to the desired connection (#02 for example as target). Put the mouse cursor on the 'Connection #02' label and then use the left mouse button.

	IP Address or Host Name ▾	Protocol ▾	Port ▾
Connection #01	192.168.0.13	TCP	2010
Connection #02	192.168.0.13	TCP	2010

*Note: this copy/paste mechanism allows copying parameters from one connection (source) to another one (target). Repeat this process for others connections if needed.*

#### 6.4.1.1.5 IP address floating menu

When the mouse is located on the 'IP address' text area, the color changes to white and the following tooltip is displayed:

IP Address or Host Name ▾	Protocol ▾	Port ▾	Filename
192.168.0.13	TCP	2010	

Click to copy the IP address from connection #01 to all connections

Click on the left mouse button to display the short menu as below:

Destination Parameters			Save the Receiver
IP Address or Host Name ▾	Protocol ▾	Port ▾	Filename
Connection #01	192.168.0.13	TCP	2009

Copy the IP Address from Connection #01 to all Connections

With this function, the IP Address field from connection #01 is recopied for all connections from #02 to #16.

#### 6.4.1.1.6 Protocol floating menu

When the mouse is located on the 'Protocol' text area, the color changes to white and the following tooltip is displayed:

IP Address or Host Name ▾	Protocol ▾	Port ▾	Filename
192.168.0.13	TCP	2010	

Click to select the same protocol for all connections

Click on the left mouse button to display the short menu as below:

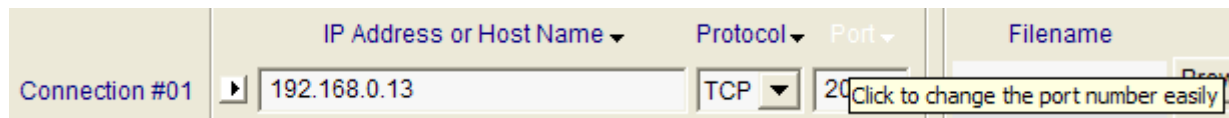
IP Address or Host Name ▾	Protocol ▾	Port ▾	Filename
192.168.0.13	TCP	2010	

Select TCP for all Connections  
Select UDP for all Connections

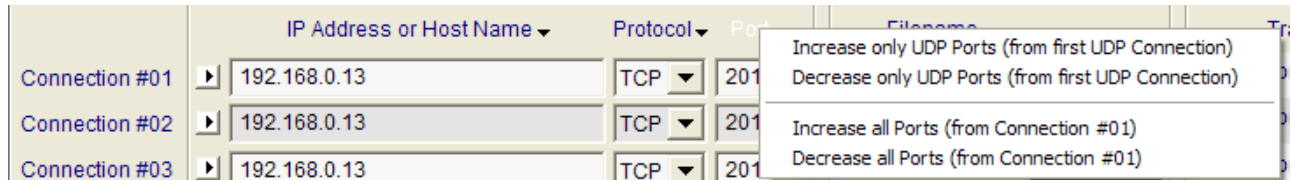
This menu helps to set the same protocol for all connections.

#### 6.4.1.1.7 Port floating menu

When the mouse is located on the ‘Port’ text area, the color changes to white and the following tooltip is displayed:



Click on the left mouse button to display four items menu as following:



With this menu, you can:

- Set the port number increasingly or decreasingly for all UDP connections, based on the port number of the first UDP connection,
- Set the port number increasingly or decreasingly for all connections, based on the port number of the first connection without taking into account the protocol in use.

#### 6.4.1.2 Save the Received Data

When the Remote Receiver part is operating in echoer working mode for a connection, you can select from this area a file name where received data for this connection will be saved.

A “Browse” button allows selecting a file easily.

### 6.4.1.3 Configure the Unitary Mode

Unitary mode is one of the two testing mode offered by the “LanTraffic V2” Sender part. Notice that each testing mode is exclusive, i.e. it is impossible to mix connections in unitary testing and automatic testing modes.

The Unitary Mode is configured in Tab 1 “Sender parameters” and run from Tab 2 “Sender Traffic + Statistics”.

To run or configure unitary testing session, you must first select “Unitary Mode”.

By pressing “Parameter # n” buttons, the following parameters can be configured for each connection:

- Traffic generator type: Packets generator, mathematical law or file to send,
- Data size and packets parameters: data size, inter packet delay, RTT option (RTT: Round Trip Time), TOS value (Type Of Service) – TTL (Time To Live) value if IPv4 or Hop Limit if IPv6.
- Optional: activate a throughput limit.

The traffic generator **Type** of a connection #n is reminded beside the 'Parameters #n' button: **Generator**, **File** or **Law**.

When you click on 'Parameter #n' in Tab 1 “Sender – Parameters”, the Parameters window is pop up.

This window is divided in several areas: Traffic generator type, Data size and packet parameters, and the optional throughput limit.

The connection number is reminded in the window title.

“OK” button allows validating new entered parameters for the connection and closes the window.

**LanTrafficV2 - Traffic Generator Parameters - Sender Unitary Testing Mode (connection #01)**

**Step 1: Select the traffic generator type**  
First of all, select the traffic generator which is going to be used on this connection.

☒ Packets generator

**Packets Generator Parameters**

Packets number (0 to 99,999,999)  (0 = infinite value)

**Packet Contents (00 to FF hexa byte)**

☒ Fix

☐ Random  min  max

☐ Alternate  value-1  value-2

☐ Increasing / Decreasing  min  max  step

☐ Mathematical law

Law : data volume to send

Uniform law  
Range : [9.77 KB , 2.38 MB]

☐ File to send

Filename

Loop counter (1 to 99)  Idle time between each loop (0 to 99 s)

**Step 2: Specify Data size and packets parameters**  
In this step, define Data Size and packets parameters as well as the delay between each sent packet or specify values for some IP Header fields.

**Data Size (1 to 65,535 bytes)**

☒ Fix

☐ Random  min  max

☐ Alternate  size-1  size-2

☐ Increasing / Decreasing  min  max  step

**Inter Packet Delay (0 to 9,999 ms)**

☒ Fix  (See Forewarnings menu please)

☐ Random  min  max

☐ Alternate  value-1  value-2

☐ Increasing / Decreasing  min  max  step

☐ Mathematical law

**RTT Option** ☐ Yes ☒ No

**TOS (1 hexa byte)** Value

**Time To Live (TTL)** Value

**Step 3 (Optional): Activate a throughput limit**  
When one of these two options is selected, "LanTrafficV2" generates the traffic in best effort to respect the throughput chosen.

**Average Throughput (8 to 999,999 Kb/s)**

☐ Use value

☒ Data size adjustable

☐ Inter packet delay adjustable

**Average Throughput (1 to 99,999 Pkts/s)**

☐ Use value (only for UDP connection)

Unitary testing parameters window (IPv4)**6.4.1.3.1 Step 1: select the traffic generator type for this connection**

The first parameter to configure is the data source type. Three exclusive types of data source are offered:

- Packets generator (Packets generator parameters)
- Mathematical law (Law: Data volume to send)
- File to send (Filename)

**6.4.1.3.1.1 Packets generator**

When the Packet Generator data source is selected, “LanTraffic V2” will generate n user-defined contents packets for this connection.

**Packets Generator Parameters**

Packets number (0 to 99,999,999)  (0 = infinite value)

**Packet Contents (00 to FF hexa byte)**

☒ Fix

☐ Random  min  max

☐ Alternate  value-1  value-2

☐ Increasing / Decreasing  min  max  step

Packets generator parameters

- Packets number

Number of packets to send is limited to 99,999,999. Zero value means infinite and is the default value.

- Packet contents (00 to FF hex byte)

The Content is in hex-byte. Accepted values are all combinations from 00 to FF.

The packet contents can be configured as follows:

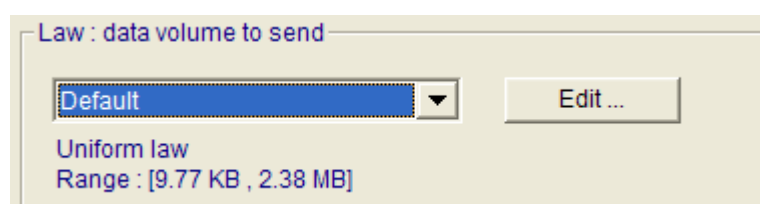
- **Fix:** each packet has the same content.
- **Random:** "LanTraffic V2" computes random packet content included in a user-defined range (min to max).
- **Alternate:** "LanTraffic V2" uses the first value (value-1) for odd packets and the second value (value-2) for even packets.
- **Increasing/Decreasing:** the content of each packet varies in a user-defined range from the minimal to the maximal value. Each following packet content is incremented by the step value (0 is an invalid value). When the maximal value is reached, the packet content decreases down to the minimal value by the step value.



*Statistics: when the traffic generator type is selected, the 'Volume to send' and the 'Remaining volume' statistics cannot be computed. In statistics fields of the "Sender- Traffic + statistics" tab, "N/A" will be displayed.*

#### 6.4.1.3.1.2 Mathematical law

For the unitary testing mode, the mathematical law is a data volume to send law. Volume will impact the duration of the connection.



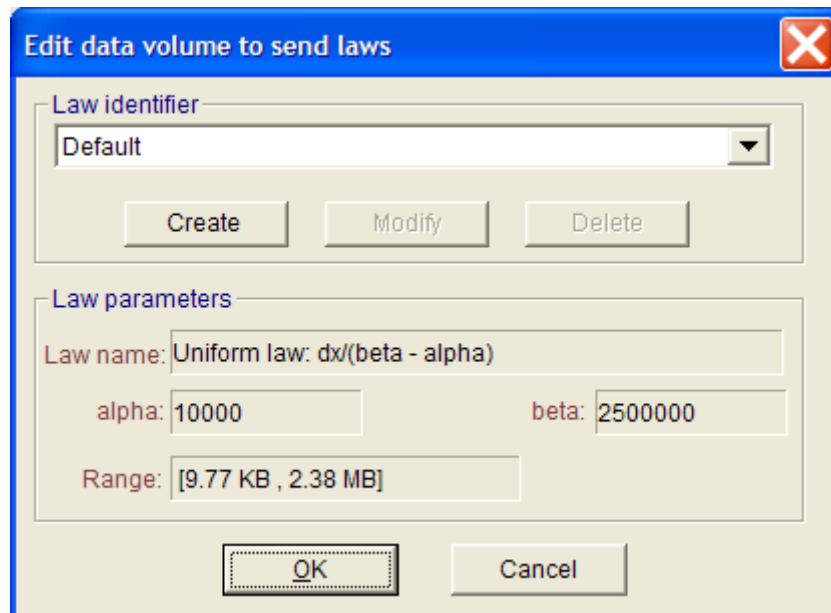
"LanTraffic V2" unitary testing mode offers four mathematical laws related to the data volume:

- Uniform law
- Exponential law
- Pareto's law
- Gauss law

These laws are presented in details in Annex PART 9.

In the “Law: data volume to send” sub-area, a list box allows to select an existing law. The main features (type of mathematical law and values range) of the selected law are reminded below the List box.

You can add, modify or delete a law by pressing the “Edit” button. Then a new window is pop up:



**Edit data volume to send laws**

Law identifier  
Default

Create Modify Delete

Law parameters

Law name: Uniform law:  $dx/(beta - alpha)$

alpha: 10000 beta: 2500000

Range: [9.77 KB , 2.38 MB]

OK Cancel

Edit data volume to send law

### To add a new data volume to send law:

1. Press the "Create" button, then a new window is displayed:

2. Select one mathematical law name: Exponential, Uniform, Pareto or Gauss.
3. Enter parameters value for the selected mathematical law (1 or 2 parameters are required depending on the selected law),
4. Save and close the window by pressing the "OK" button.
5. Your new law is selected in the parent window.
6. Repeat operation 1 to 5 to create other laws.



*Range is computed automatically each time you modify the parameters of the law.*



*Laws created from this window will also be available in the Automatic testing mode.*

#### 6.4.1.3.1.3 File to send

With this selection, "LanTraffic V2" will send the file defined in the 'Filename' sub-area. The 'Browse' button allows selecting easily the file to send.

The **Loop counter** should be greater than 0. Each time the file is sent, the loop counter decreases and when the 0 value is reached, the traffic generator stops.

**Idle time between each loop** is expressed in seconds. It defines a pause between two file transfers. It is recommended to define a value lower than the remote TCP/IP timeout if TCP protocol is used (default TCPTIMEOUT value is 5 seconds) because the remote will disconnect due to the idle timeout.



### 6.4.1.3.2 Step 2: Specify data size and packets parameters

#### 6.4.1.3.2.1 Data size

This parameter defines the size of data transmitted for each packet.

Data Size (1 to 65,535 bytes)

<input checked="" type="radio"/> Fix	<input type="text" value="1460"/>				
<input type="radio"/> Random	<input type="text" value="128"/>	min	<input type="text" value="1460"/>	max	
<input type="radio"/> Alternate	<input type="text" value="128"/>	size-1	<input type="text" value="1460"/>	size-2	
<input type="radio"/> Increasing / Decreasing	<input type="text" value="1"/>	min	<input type="text" value="1460"/>	max	<input type="text" value="1"/> step

The maximum accepted value is 65,535. 0 (null) is not a valid value. By default, the entered value is 1,460. This value is the default payload for TCP with IPv4. When IPv6 is selected, the payload should be shorter. Packet size can be configured as follows:

- **Fix:** each packet has the same size. The last packet may have an inferior size to fit the data volume to send when mathematical law or file to send data source is selected.
- **Random:** “LanTraffic V2” computes a random packet size included in a range specified by the user for each packet to send.
- **Alternate:** two values must be defined. “LanTraffic V2” uses the first value for odd packets and the second value for even packets.
- **Increasing/Decreasing:** the size of each packet varies in a range defined by the user, from the minimal to the maximal value. Each size is incremented by the step value (0 is an invalid value). When the maximal value is reached, the packet size decreases step by step until the minimal value.



*It is important to note that “LanTraffic V2” requires a minimal packet size when the RTT mode is selected, to add a CRC, a sequence number and the timestamp. Therefore, the minimal packet size with RTT mode active is 14 bytes (see paragraph 6.4.1.3.2.3 about RTT option).*

#### 6.4.1.3.2.2 Inter Packet Delay

This parameter allows defining the time interval between two packets. Values are limited to 9,999 milliseconds i.e. 10 seconds. A value of zero means no inter-packet delay.

The inter-packet delay can be configured as follows:

- **Fix:** inter-packet delay is the same for all transmitted packets.
- **Random:** “LanTraffic V2” computes a random inter-packet delay included in a range specified by the user for each packet to send.
- **Alternate:** two values must be defined. “LanTraffic V2” uses the first value for odd packets and the second value for even packets.
- **Increasing/Decreasing:** inter-packet delay varies in a range defined by the user, from the minimal to the maximal value. Each inter-packet delay is incremented by the step defined by the user (0 is not an accepted value for step). When the maximal value is reached, inter-packet delay decreases by the step value down to the minimal value.
- **Mathematical law:** the user chooses between one of the fourth available laws (Uniform, Exponential, Pareto and Gauss).

#### 6.4.1.3.2.3 RTT option

When ‘Yes’ is selected, “LanTraffic V2” will add RTT (Round Trip Time) header information into packets without changing the data size defined.

The RTT header format is:

- 4 bytes    magic number
- 4 bytes    sequence number
- 4 bytes    time when sent
- 4 bytes    length (without the RTT header)

This information will be used in conjunction with connections running in echoer mode on the Remote Receiver part. Each echoed packet is analyzed by the Local Sender part. When RTT header is found, RTT is computed and can be saved in a file specified in Tab 1 “Sender - Traffic+Statistics” (see in paragraph 6.4.2).

At the Remote Receive side, RTT information is checked to update ‘sequencing errors’ statistics.

#### 6.4.1.3.2.4 The TOS field (IPv4 only)

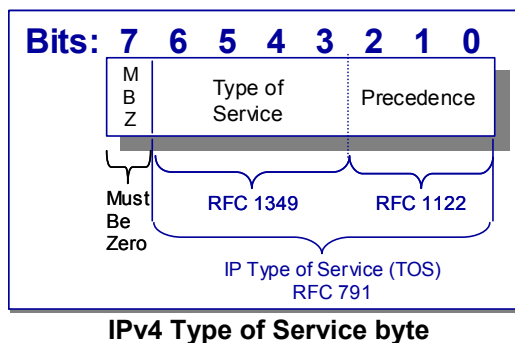
The TOS field is available only if IPv4 is selected for the connection.

You can input the TOS value (by default, TOS = 00) used for each packet sent on the IP connection.

Example: value = 14 (or in binary: **0001 0100**) means:

**Type of Service bits 3-6 (TOS)** = 0100 (maximize throughput)

**Precedence bits 0-2 (COS)** = 001 (priority)



**For Windows 2000 and XP:** to allow for behavior similar to Windows NT 4.0 IP\_TOS on Windows 2000/XP0 for backward compatibility, a new registry key is added on Windows 2000. It is necessary to edit the Registry and modify this key in order to use the TOS byte of "LanTraffic V2"



**Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved.**

**For information about how to edit the registry, view the "Changing Keys and Values" Help topic in Registry Editor (regedit.exe) or the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in regedit.exe.**

**Note that you should back up the registry before you edit it. If you are running Windows NT, Windows 2000 or XP you should also update your Emergency Repair Disk (ERD).**

**Follow these steps to enable the IP\_TOS option for the Winsock setsockopt function and the -v option for the ping utility on Windows 2000/XP:**

**Start Registry Editor (regedit.exe). Go to the following key on Local Machine:**

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\

**NOTE: The registry key is one path.**

**On the Edit menu, click Add Value, and then type DisableUserTOSSetting.**

**Click REG\_DWORD in the Data Type box, and then click OK. Enter 0 in the prompt box. Quit Registry Editor, and then restart the computer.**

#### 6.4.1.3.2.5 The TTL field

<div>Time To Live (TTL)</div> <div>Value <input type="text" value="00"/></div> <div>IPv4</div>	or	<div>Hop Limit</div> <div>Value <input type="text" value="00"/></div> <div>IPv6</div>	<p>The user can input the TTL/Hop Limit value (hexadecimal) used for each packet sent on the connection.</p> <p>Default value = 00</p>
--	----	---	--

#### 6.4.1.3.3 Step 3 (optional): Activate a throughput limit

For the TCP connection, the average throughput limit is expressed in Kb/s (or Kbps):

Step 3 (Optional): Activate a throughput limit

When one of these two options is selected, "LanTrafficV2" generates the traffic in best effort to respect the throughput chosen.

Average Throughput (8 to 999,999 Kb/s)

☐ Use value

☒ Data size adjustable

☐ Inter packet delay adjustable

Average Throughput (1 to 99,999 Pkts/s)

☐ Use value (only for UDP connection)

With this feature, you can define a throughput limit for this connection (in Kilo bits per second) with the check box 'Use value'. You specify the average throughput in Kbps in the edit box and select one of the two parameters (packet size or inter packet delay). "LanTraffic V2" will automatically adapt data traffic generation with adjustment of packet size or inter packet delay (user choice) up to the throughput requested by the user.

For the UDP connection, the average throughput is expressed in Kb/s or can also be expressed in number of packets per second (Pkts/s):

Step 3 (Optional): Activate a throughput limit

When one of these two options is selected, "LanTrafficV2" generates the traffic in best effort to respect the throughput chosen.

Average Throughput (8 to 999,999 Kb/s)

☐ Use value

☒ Data size adjustable

☐ Inter packet delay adjustable

Average Throughput (1 to 99,999 Pkts/s)

☐ Use value (only for UDP connection)



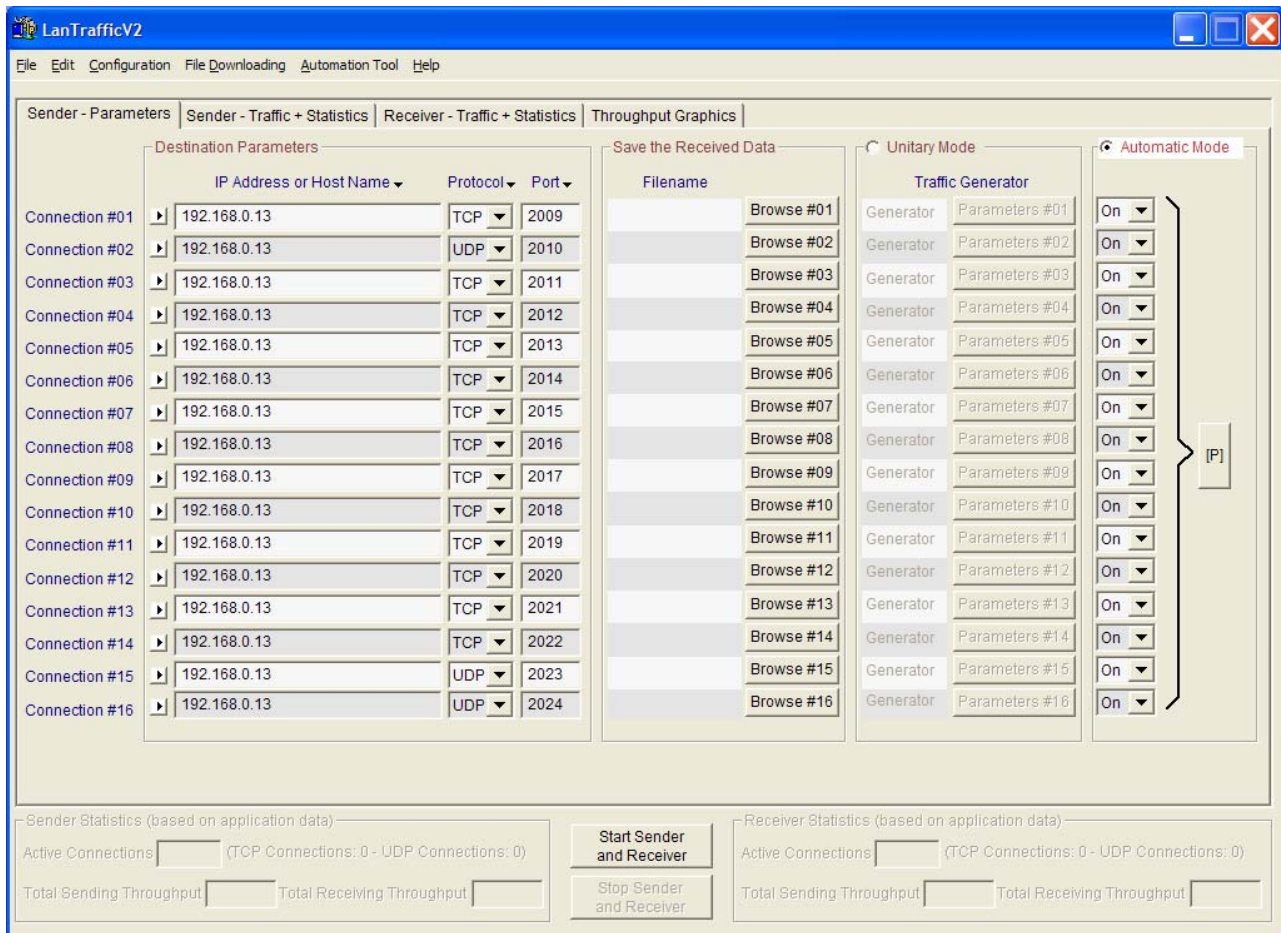
*The throughput value must be greater than or equal to 8 Kbps.*

#### 6.4.1.4 Configure the Automatic Mode

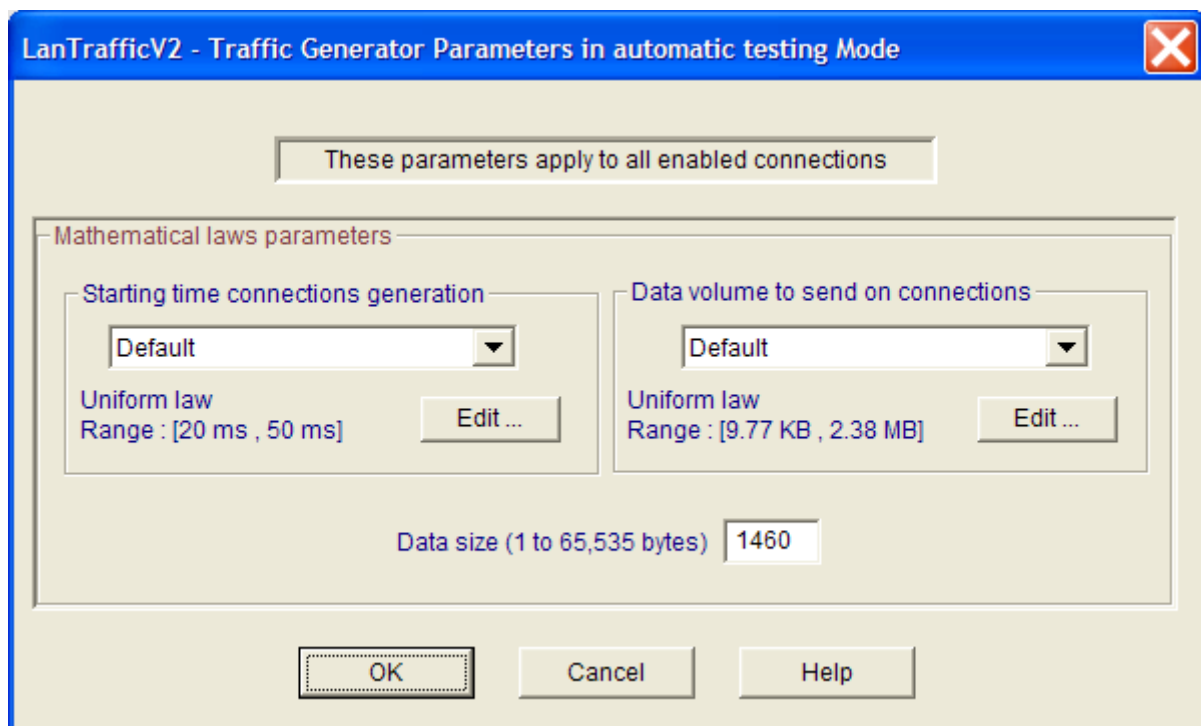
The Automatic Mode is a mode in which all enabled connections are generated together following a “Starting time connections generation” law and a “Data volume to send” law.

As unitary testing mode, automatic testing mode is configured in Tab 1 “Sender – Parameters” and run in Tab 2 “Sender Traffic +Statistics”.

Once automatic mode is selected in Tab 1, you can choose to enable or disable each connection by using the ON/OFF list box.



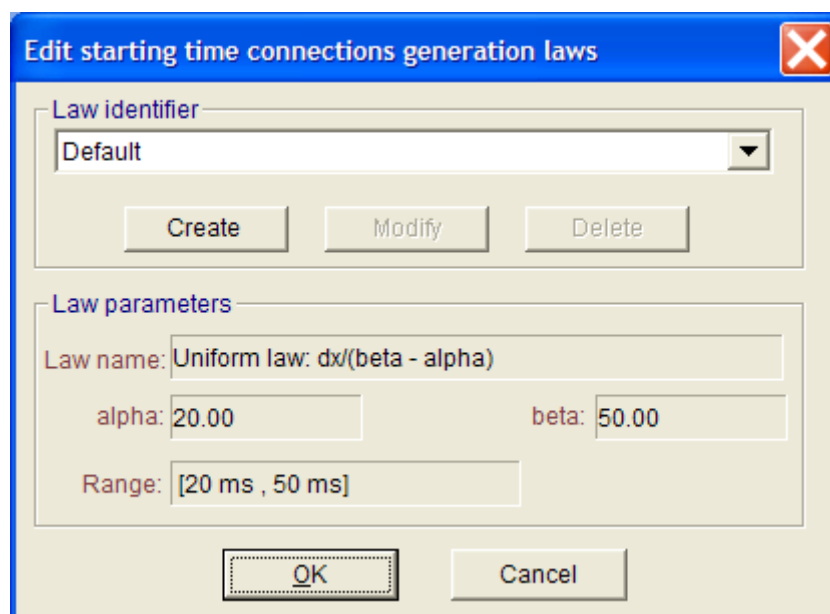
By clicking on the '[P]' button (P as Parameters), the following window is pop up allowing to configure the automatic testing mode parameters:



*Automatic testing parameters window*

#### 6.4.1.4.1 Starting time connections generation laws

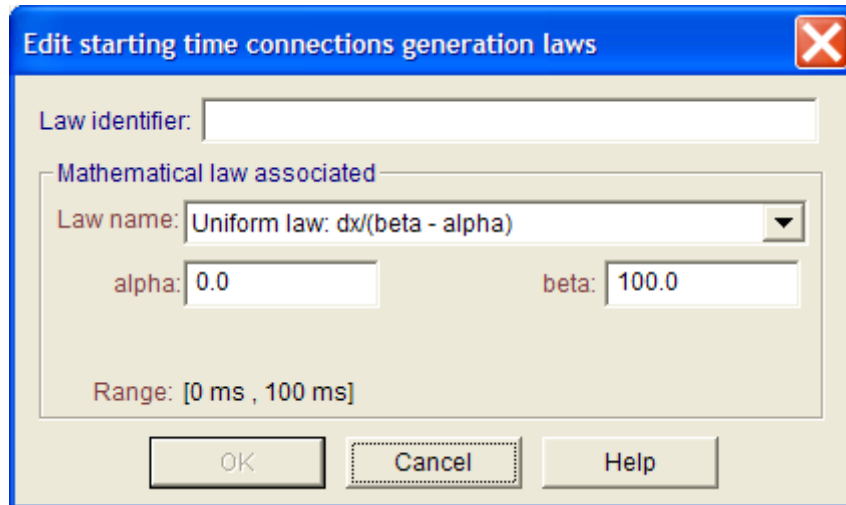
Starting time connection laws regulate the timing between starting of two connections. The available mathematical laws for starting time connection are Uniform and Exponential laws. (Mathematical laws are presented in details in Annex part). You can add, modify or delete a law by pressing the "Edit" button. Then a new window is pop up:



*Starting time connections generation law window*

To add a new *Starting time connections generation law*:

- 1) Press the "Create" button, then a new window is pop up

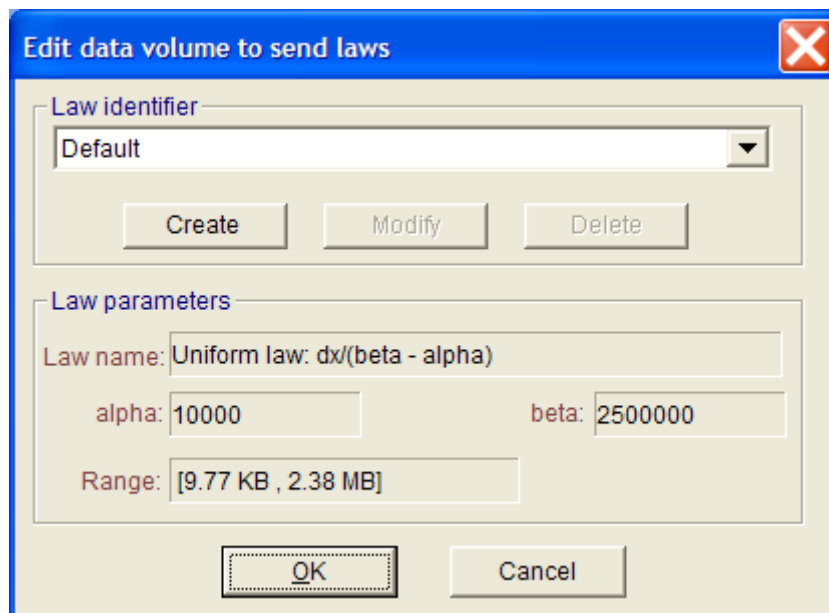
The dialog box has a blue title bar with the text "Edit starting time connections generation laws" and a red close button. Inside, there is a "Law identifier:" text box. Below it is a section titled "Mathematical law associated" containing a "Law name:" dropdown menu showing "Uniform law: dx/(beta - alpha)". Below the dropdown are two text boxes: "alpha:" with the value "0.0" and "beta:" with the value "100.0". At the bottom of this section is a "Range:" text box showing "[0 ms , 100 ms]". At the very bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

Edit starting time connections generation law window

- 2) Select one mathematical law: Uniform or Exponential.
- 3) Enter parameters values for the selected mathematical law (1 or 2 parameters are required depending on the selected law).
- 4) Save and close the window by pressing "OK" button.
- 5) Your new law is selected in the parent window.
- 6) Repeat operation 1 to 5 to create other laws.

#### 6.4.1.4.2 Data volume to send laws

Data volume laws regulate the data volume to send for connection. The available mathematical laws for data volume to send are: Uniform, Exponential and Pareto laws. (Mathematical laws are presented in details in Annex Part). You can add, modify or delete a law by pressing the "Edit" button. Then a new window is pop up:

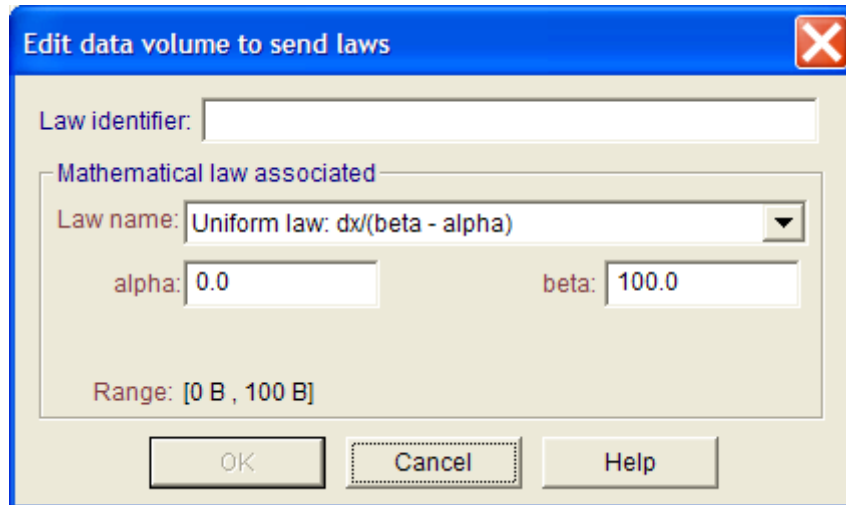
The dialog box has a blue title bar with the text "Edit data volume to send laws" and a red close button. Inside, there is a "Law identifier:" dropdown menu showing "Default". Below this are three buttons: "Create", "Modify", and "Delete". Below these buttons is a section titled "Law parameters" containing a "Law name:" text box showing "Uniform law: dx/(beta - alpha)". Below the text box are two text boxes: "alpha:" with the value "10000" and "beta:" with the value "2500000". At the bottom of this section is a "Range:" text box showing "[9.77 KB , 2.38 MB]". At the very bottom of the dialog are two buttons: "OK" and "Cancel".

Volume law window



**To add a new data volume to send law:**

1. Press the "Create" button and the following window is pop up:



Edit data volume law window

2. Select one mathematical law: Uniform, Exponential, Pareto or Gauss.
3. Enter parameters value for the selected mathematical law (1 or 2 parameters are required depending on the selected law).
4. Save and close the window by pressing "OK" button.
5. Your new law is selected in the parent window.
6. Repeat operation 1 to 5 to create other laws.



*Up to the used machine (Windows 95, 98, Me, NT4, 2000 or XP), the WinSock 2 Interface could present number-limits of the incoming simultaneous calls. Consequence for "LanTraffic V2" is the presence of "connection failed", particularly when connections frequency is very near (inferior to 150 ms), and when the data volume to transmit is very small which implies to make many connections. These connection failures do not disturb "LanTraffic V2". To reduce these failures, decrease the frequency of connections or increase the data volume.*

**6.4.1.4.3 Packets size**

In the automatic testing mode, entering a value in bytes in the «Mathematical Laws Parameters» window configures the packet size.

Packet size is limited to 65,535 bytes.



## 6.4.2 Sender - Traffic + Statistics tab

This second tab related to the Sender allows:

- Displaying destination parameters of each connection,
- Displaying traffic statistics for each connection,
- If unitary testing mode is selected in Tab 1, to command traffic generation in unitary testing mode i.e. to run and stop each connection, including a tooltip summary,
- If automatic testing mode is selected in Tab 1, to command traffic generation in automatic testing mode i.e. to run and stop all enabled connections.



***The cursor can be changed to the hourglass during the time needed to this tab to process IP address translation.***

The Tab 2 “Sender - Traffic + Statistics” is divided in four areas:

- Destination Parameters
- Statistics (based on application data)
- Buttons to start/stop connections in the Unitary or Automatic mode selected in the “Sender – Parameters” tab
- Export statistics into a File

Each area is presented in the following paragraphs.

The screenshot displays the 'Sender - Traffic + Statistics' tab. It features a table with 16 connections. The first two connections are active, showing traffic statistics. The remaining 14 connections are in a 'NO\_ADDRESS' state. On the right side, there are buttons to start/stop individual connections and 'Start All Connections' / 'Stop All Connections'. At the bottom, there are buttons for 'Export Statistics into a File' and 'Choose Columns'.

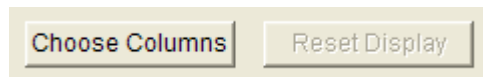
Connection #	IP Address or Host Name	Port	Tx Throughput	Tx Volume	Tx Packets	Rx Throughput	Rx Volume	Rx Packets	Jitter
Connection #01	192.168.0.77	2009	1.12 Mb/s	1.44 MB	1023 p	1.13 Mb/s	1.44 MB	1016 p	3 ms
Connection #02	192.168.0.77	2010	576 Kb/s	737 KB	512 p	576 Kb/s	737 KB	512 p	1 ms
Connection #03	NO_ADDRESS	2009							
Connection #04	NO_ADDRESS	2009							
Connection #05	NO_ADDRESS	2009							
Connection #06	NO_ADDRESS	2009							
Connection #07	NO_ADDRESS	2009							
Connection #08	NO_ADDRESS	2009							
Connection #09	NO_ADDRESS	2009							
Connection #10	NO_ADDRESS	2009							
Connection #11	NO_ADDRESS	2009							
Connection #12	NO_ADDRESS	2009							
Connection #13	NO_ADDRESS	2009							
Connection #14	NO_ADDRESS	2009							
Connection #15	NO_ADDRESS	2009							
Connection #16	NO_ADDRESS	2009							

*Tab 2: “Sender - Traffic + Statistics”*

### 6.4.2.1 Destination Parameters

In this area, the destination parameters (IP address and port number) are displayed as information for each connection. These parameters can be modified in the tab 1 “Sender – Parameters” if the connection is stopped.

### 6.4.2.2 Sender statistics



By using the "Choose Columns" button at the bottom, you can select the parameters to display.

Up to 7 parameters can be simultaneously displayed among 13 parameters described later in this paragraph, and at least one parameter must be selected.

*These statistics are computed at the application level (and based on application data sent or received). No MAC, IP and TCP/UDP headers and trailers are taken into account.*

To reset the statistics displayed, two methods can be used:

- by clicking on the "Reset Display" button (this button is enabled when all connections are stopped).
- by checking the "Clear on Stop" option (when the connection stops, the statistics for this connection are automatically cleared).



The "**N/A**" (Not Applicable) mention can be displayed instead of a value in the cell of the statistics table if the parameter cannot be calculated.

Statistics (based on application data)						<input type="checkbox"/> Clear on Stop
Tx Packets	Tx Throughput	Rx Packets	Rx Throughput	Jitter	Seq. Num. Errors	
Connection failed: no response from the Remote. Please check your parameters.						
4817 p	2.23 Mb/s	0 p	0.00 b/s	N/A	N/A	

If a connection is in progress or cannot be activated (in case of invalid parameters or connection problem), a warning message is displayed.

Examples:

- Connection failed: no response from the Remote. Please check your parameters.
- Connection pending: LanTrafficV2 is waiting for the Remote response.
- Connection reset: the Remote has reset the connection.

Statistics (based on application data)						<input checked="" type="checkbox"/> Clear on Stop
Tx Packets	Tx Throughput	Tx Volume	Rx Packets	Rx Throughput	Jitter	Seq. Num. Errors
Connection failed: no response from the Remote. Please check your parameters.						
Connection reset: the Remote has reset this connection.						

*Note: the warning message isn't erased if the "Clear on Stop" option is selected.*

## List of the 13 statistic parameters calculated for the Sender

### Transmitting statistics

<b>Tx Packets</b>	Tx Packets (Tx = Transmit) is the number of packets that "LanTraffic V2" has sent since the connection is started.
<b>Tx Pkts Throughput</b>	Tx Pkts Throughput (Tx = Transmit) is the mean number of packets that "LanTraffic V2" is sending per second. This value is only available with UDP connections. The calculation of this value is based on the sampling period defined by the throughput sampling period in the 'Configuration/General Parameters' menu.
<b>Tx Throughput</b>	Tx Throughput (Tx = Transmit) is the mean throughput of data sent. The calculation of this value is based on the sampling period defined by the throughput sampling period in the 'Configuration/General Parameters' menu.
<b>Tx Volume</b>	Tx Volume (Tx = Transmit) is the number of bytes that "LanTraffic V2" has sent since the connection is started.

### Receiving statistics

<b>Rx Packets</b>	Rx Packets (Rx = Receive) is the number of packets that "LanTraffic V2" has received since the connection is started.
<b>Rx Pkts Throughput</b>	Rx Pkts Throughput (Rx = Receive) is the mean number of packets that "LanTraffic V2" is receiving per second. This value is only available with UDP connections. The calculation of this value is based on the sampling period defined by the throughput sampling period in the 'Configuration/General Parameters' menu.
<b>Rx Throughput</b>	Rx Throughput (Rx = Receive) is the mean throughput of data received. The calculation of this value is based on the sampling period defined by the throughput sampling period in the 'Configuration/General Parameters' menu.
<b>Rx Volume</b>	Rx Volume (Rx = Receive) is the number of bytes that "LanTraffic V2" has received since the connection is started.

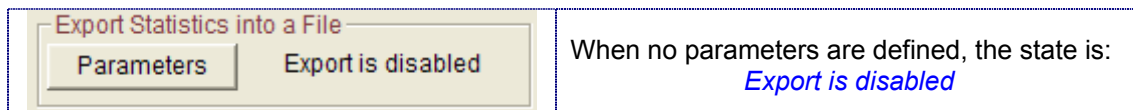
### Other statistics

<b>Jitter</b>	Jitter is the mean variation of delays on packets received. This value is only available when RTT option is selected (on the Local Sender: see Traffic Generator Parameters). This value corresponds to either the mean one-way variation (remote Receiver = Absorber Generator mode) or the mean two-ways variation (remote Receiver = Echoer mode).
<b>Remaining Volume</b>	'Remaining Volume' is the number of bytes that "LanTraffic V2" has still not sent. This information is only available for two Traffic Generator types (Mathematical Law and File to Send).
<b>RTT</b>	'RTT' is the Round Trip Time of a packet which was sent by "LanTraffic V2". This value is calculated if the RTT option is selected on the local Sender Traffic Generator and if the remote Receiver works in Echoer mode.

<b>Seq. Numb. Errors</b>	'Seq. Numb. Errors' (Sequence Number Errors) is the sum of the Out Of Sequence packets number (OOS) and the number of lost packets. This value is only available if the RTT option is selected (on local Sender: see Traffic Generator Parameters) and if the working mode of the remote Receiver is Absorber Generator or Echoer.
<b>Volume To Send</b>	'Volume To Send' is the number of bytes that "LanTraffic V2 should send. This information is only available for two Traffic Generator Types (Mathematical law and File to Send).

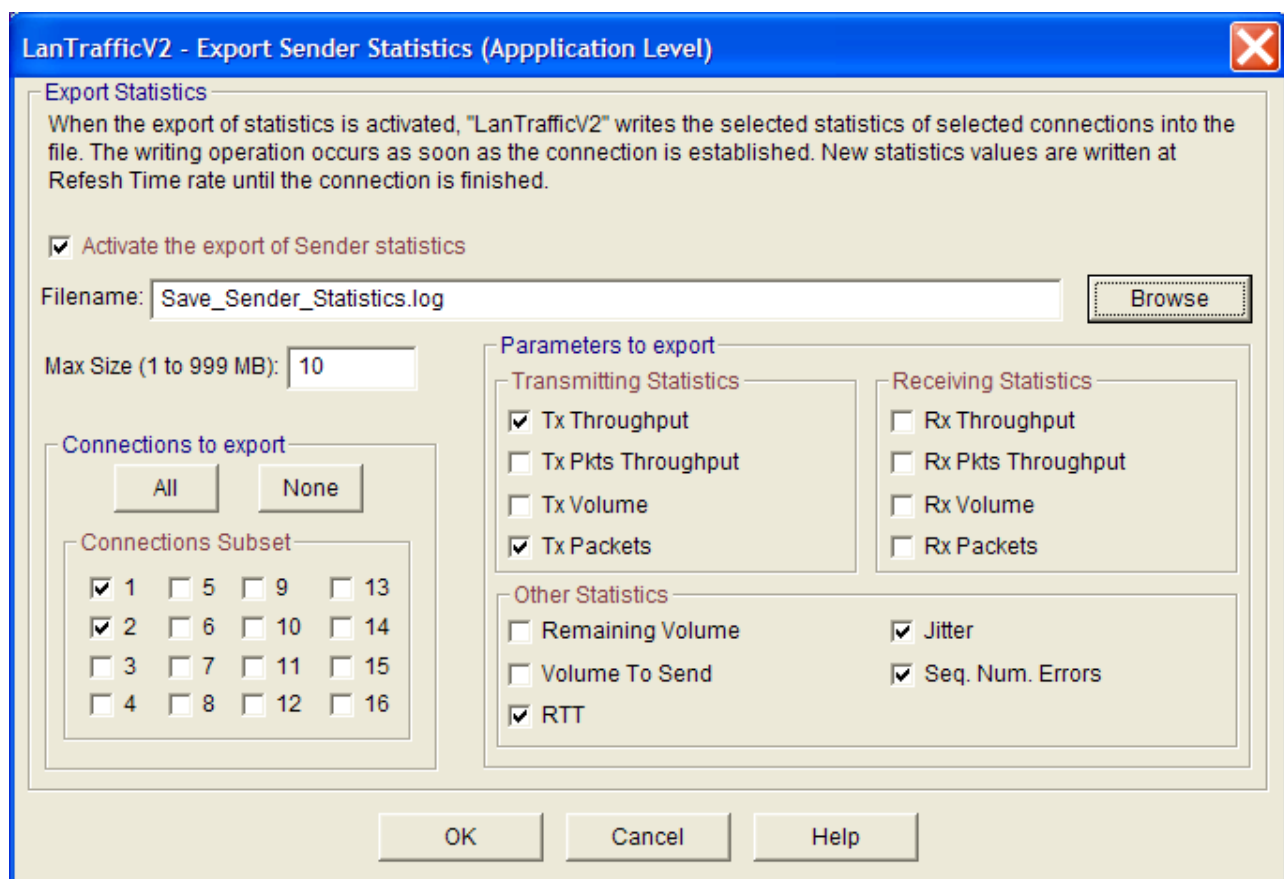
### 6.4.2.3 Export statistics into a file

To export all or part of **statistics** into a file, click on the 'Parameters' button when enabled (i.e. if connections of the Sender are not active):



Then a new window allows defining parameters for the export process:

- Enable or disable the export process,
- The filename (.log extension) of the export file,
- The maximum size of the export file (*when the maximum size of the file is reached, statistics are not saved anymore*),
- The identification of the needed connections,
- The parameters to export (up to 13).



Then press OK to validate, and a new state is displayed:

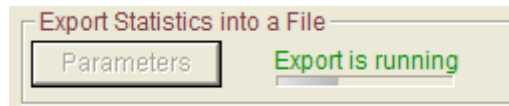


*Do not specify the same filename to save statistics for the Sender and the Receiver parts; else a warning message is displayed.*

The statistics file is updated with the same refresh period than the statistics displayed. A special mark is added to keep special TCP and UDP events e.g. Begin and End of sending traffic.

When you reset statistics, the displayed values and the exported values are reset.

Statistics are saved into the file as soon as connections of the Sender are started and the 'Export is running' state is displayed:



When all connections are stopped, then the export process is automatically suspended and the following idle state is displayed:



#### 6.4.2.3.1 Sender statistics file format

The Sender statistics file is formatted line by line as follows:

First line: Starting session MM/DD/YYYY at HH:MM:SS,mmm (**UTC time**)

Second line: LanTrafficV2 Sender

Third line: this line contains the labels of columns

Connection #nn (Protocol)	Date	Time	Parameter i	Parameter i	Parameter ...
---------------------------	------	------	-------------	-------------	---------------

with:

- nn is the number of the connection
- Protocol is UDP or TCP,
- Date (MM/DD/YYYY)
- Time (HH:MM:SS.mmm) **UTC time**
- Parameter i, Parameter j ... are the statistics chosen by the user (up to 13 parameters can be selected)  
Example: Parameter i = Tx (Transmit) Throughput, Parameter j = Tx (Transmit) Packets ...

Next lines: numerical values

Connection #nn (Protocol)	MM/DD/YYYY	HH:MM:SS.mmm	nnn.nn	nnn.nn	...
---------------------------	------------	--------------	--------	--------	-----

#### Additional marks for TCP and UDP connection events

##### Connection #nn (TCP or UDP) Begin

This indicates the beginning of sending traffic for the connection #nn (nn: from 01 to 16). Numerical values are latest values computed by "LanTraffic V2" for the line.

##### Connection #nn (TCP or UDP) End

This indicates the end of traffic for the connection #nn. Numerical values are latest values computed by "LanTraffic V2" for the line.



- ▶ When a value cannot be computed, the "N/A" mention is indicated.
- ▶ The delimiter mark used between each field is the tabulation character.

#### 6.4.2.3.2 *Export Sender file sample*

In the following example, 3 connections (#01, #02 et #15) have been selected for the local Sender with 7 parameters exported: Tx (Transmit) Packets, Tx (Transmit) Throughput, Tx (Transmit) Volume, Rx (Receive) Packets, Rx (Receive) Throughput, Jitter and Seq. Num. Errors (Sequence Number errors):

- Connection #01: Protocol = TCP & Traffic Generator type = Packets generator  
[Size Packet = 1460, Inter Packet Delay = 20, RTT option = Yes]
- Connection #02: Protocol = UDP & Traffic Generator type = Packets generator  
[Size Packet = 1460, Inter Packet Delay = 30, RTT option = Yes]
- Connection #15: Protocol = TCP & Traffic Generator type = File to send (816 KB) with Loop counter = 15 and idle time between each loop = 3 seconds.  
[Size Packet = 1460, Inter Packet Delay = 50, RTT option = No]

The remote Receiver has been configured with 3 enabled connections working in the following modes:

- Connection #01: working mode = Absorber
- Connection #02: working mode = Echoer
- Connection #03: working mode = Absorber + Generator

Parameters set In the General Parameters of the Configuration menu:

- Refresh time = 1 second
- Throughput sampling period = 1 second

The 3 connections are started all together; and then the connections #01, #02 and #15 are manually stopped.

Starting session 07/16/2004 at 15:58:11.856 (UTC Time)

LanTrafficV2 Sender

Connection #i (Protocol)	Date	Time	Tx Throughput (Kb/s)	Tx Volume (KB)	Tx Packets (Pkts)	Rx Throughput (Kb/s)	Rx Packets (Pkts)	Jitter (ms)	Seq. Num. Errors
Connection #02 (UDP) BEGIN	07/16/2004	15:58:11.876	0	0	0	0	0	N/A	0
Connection #01 (TCP) BEGIN	07/16/2004	15:58:11.926	0	0	0	0	0	N/A	0
Connection #15 (TCP) BEGIN	07/16/2004	15:58:11.926	0	0	0	0	0	N/A	N/A
Connection #01 (TCP)	07/16/2004	15:58:12.307	0	27.35	19	0	0	N/A	0
Connection #02 (UDP)	07/16/2004	15:58:12.307	0	18.71	13	0	12	0	1
Connection #15 (TCP)	07/16/2004	15:58:12.307	0	11.41	8	0	15	0	N/A
Connection #01 (TCP)	07/16/2004	15:58:13.308	276.38	99.32	69	0	0	N/A	0
Connection #02 (UDP)	07/16/2004	15:58:13.308	195.77	67.65	47	172.73	45	1	1
Connection #15 (TCP)	07/16/2004	15:58:13.308	114.06	39.92	28	228.13	63	0	N/A
Connection #01 (TCP)	07/16/2004	15:58:14.310	575.78	171.29	119	0	0	N/A	0
Connection #02 (UDP)	07/16/2004	15:58:14.310	380.02	115.16	80	391.53	79	1	1
Connection #15 (TCP)	07/16/2004	15:58:14.310	228.13	68.44	48	536.09	110	0	N/A
Connection #01 (TCP)	07/16/2004	15:58:15.311	575.78	243.27	169	0	0	N/A	0
Connection #02 (UDP)	07/16/2004	15:58:15.311	380.02	162.66	113	380.02	112	2	1
Connection #15 (TCP)	07/16/2004	15:58:15.311	228.13	96.95	68	536.09	157	0	N/A
Connection #01 (TCP)	07/16/2004	15:58:16.313	575.78	315.24	219	0	0	N/A	0
Connection #02 (UDP)	07/16/2004	15:58:16.313	391.53	211.6	147	380.02	145	1	1
Connection #15 (TCP)	07/16/2004	15:58:16.313	228.13	125.47	88	547.5	205	0	N/A
Connection #01 (TCP)	07/16/2004	15:58:17.314	575.78	387.21	269	0	0	N/A	0
Connection #02 (UDP)	07/16/2004	15:58:17.314	380.02	259.1	180	391.53	179	0	1
Connection #15 (TCP)	07/16/2004	15:58:17.314	228.13	153.98	108	536.09	252	0	N/A
Connection #01 (TCP)	07/16/2004	15:58:18.315	575.78	459.19	319	0	0	N/A	0
Connection #02 (UDP)	07/16/2004	15:58:18.315	380.02	306.6	213	380.02	212	1	1
Connection #15 (TCP)	07/16/2004	15:58:18.315	228.13	182.5	128	547.5	300	0	N/A
Connection #01 (TCP)	07/16/2004	15:58:19.317	575.78	531.16	369	0	0	N/A	0
Connection #02 (UDP)	07/16/2004	15:58:19.317	380.02	355.54	247	380.02	246	0	1
Connection #15 (TCP)	07/16/2004	15:58:19.317	228.13	211.02	148	547.5	348	0	N/A
Connection #01 (TCP)	07/16/2004	15:58:20.318	575.78	604.57	420	0	0	N/A	0
Connection #02 (UDP)	07/16/2004	15:58:20.318	391.53	403.05	280	391.53	279	1	1
Connection #15 (TCP)	07/16/2004	15:58:20.318	228.13	239.53	168	536.09	395	0	N/A
Connection #01 (TCP)	07/16/2004	15:58:21.320	575.78	676.54	470	0	0	N/A	0
Connection #02 (UDP)	07/16/2004	15:58:21.320	380.02	451.99	314	380.02	312	0	1
Connection #15 (TCP)	07/16/2004	15:58:21.320	228.13	268.05	188	536.09	442	0	N/A
Connection #01 (TCP)	07/16/2004	15:58:22.331	575.78	748.52	520	0	0	N/A	0
Connection #02 (UDP)	07/16/2004	15:58:22.331	391.53	499.49	347	391.53	346	0	1
Connection #15 (TCP)	07/16/2004	15:58:22.331	228.13	296.56	208	536.09	490	0	N/A
Connection #01 (TCP) END	07/16/2004	15:58:22.852	575.78	784.5	545	0	0	N/A	0
Connection #02 (UDP)	07/16/2004	15:58:23.323	380.02	546.99	380	380.02	379	1	1
Connection #15 (TCP)	07/16/2004	15:58:23.323	228.13	325.08	228	547.5	537	0	N/A
Connection #02 (UDP)	07/16/2004	15:58:24.324	380.02	595.93	414	380.02	413	1	1
Connection #15 (TCP)	07/16/2004	15:58:24.324	228.13	353.59	248	536.09	585	0	N/A
Connection #02 (UDP)	07/16/2004	15:58:25.325	391.53	643.44	447	380.02	446	0	1
Connection #15 (TCP)	07/16/2004	15:58:25.325	228.13	382.11	268	547.5	632	0	N/A
Connection #02 (UDP)	07/16/2004	15:58:26.327	380.02	692.38	481	391.53	480	1	1
Connection #15 (TCP)	07/16/2004	15:58:26.327	228.13	410.63	288	536.09	680	0	N/A
Connection #15 (TCP)	07/16/2004	15:58:27.328	228.13	439.14	308	547.5	727	0	N/A
Connection #02 (UDP) END	07/16/2004	15:58:27.949	380.02	734.12	510	310.92	509	0	1
Connection #15 (TCP)	07/16/2004	15:58:28.330	228.13	467.66	328	536.09	775	0	N/A
Connection #15 (TCP)	07/16/2004	15:58:29.331	228.13	497.6	349	536.09	822	0	N/A
Connection #15 (TCP) END	07/16/2004	15:58:30.843	228.13	524.69	368	547.5	894	0	N/A



#### 6.4.2.4 Run the Unitary Mode

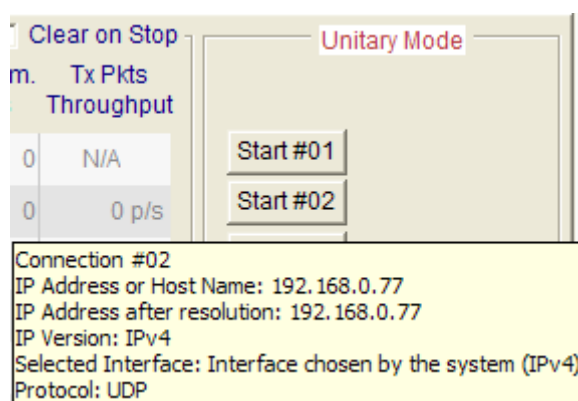


The unitary mode is chosen in the "Sender – Parameters" tab. The unitary testing mode can be launched from the 'Unitary Mode' area as shown opposite.

You can run or stop connections separately (by using the command buttons 'Start #nn' or 'Stop #nn'), or all together ('Start All Connections' or 'Stop All Connections').

**Tooltip to get a summary of connection parameters:**

You can view a summary of the main parameters of a connection when moving the mouse over the 'Start #nn' button, and then a tooltip is displayed:



*Tab 2 “Sender - Traffic + Statistics” – Connection summary*

The “Sender – Traffic + Statistics” summary tooltip displays:

- Connection number
- IP address or Host Name entered by the user
- IP address in numerical format after resolution
- IP version
- The interface used
- The protocol selected.

**To carry out the unitary testing session:**

1. In Tab 2: “Sender Traffic + Statistics”  
⇒ If Sender connections are active, stop all running connections by pressing the “Stop All Connections” button.
2. In Tab 1: “Sender Parameters”  
⇒ Select the Unitary Mode.
3. In Tab 1: “Sender Parameters”  
⇒ If necessary configure unitary parameters of each connection by pressing the “Parameters #n” button.
4. In Tab 2: “Sender Traffic + Statistics”  
⇒ Press the “Start all Connections” button to start all connections together or press the “Start #nn” buttons to start connections one by one.

### 6.4.2.5 Run the Automatic Mode

The Automatic mode is chosen in the "Sender – Parameters" tab.

The automatic testing mode can be launched from the 'Automatic Mode' area as shown opposite.

In this area, there are two buttons to start and stop all enabled connections: 'Start All Connections' and 'Stop All Connections'.

**To carry out the automatic testing session:**

- 1 *In Tab 2: "Sender - Traffic + Statistics"*  
⇒ If Sender connections are active, stop all running connections by pressing the "Stop All Connections" button.
- 2 *In Tab 1: "Sender - Parameters"*  
⇒ Select the Automatic Mode.
- 3 *In Tab 1 "Sender - Parameters":*  
⇒ If necessary, configure automatic parameters by pressing the "[P]" button and enable or disable connections by using the ON/OFF combo box.
- 4 *In Tab 2: "Sender - Traffic + Statistics":*  
⇒ Press the "Start All Connections" button to start all enabled connections.

## 6.5 Receiver part

The Receiver part allows receiving UDP and TCP traffic following five different working modes: 'Absorber' or 'Absorber File', 'Echoer' or 'Echoer file', and 'Absorber + Generator'.

### Receiver - Parameter + Statistics tab

By using this tab, you can:

- configure unitarily up to 16 connections in order to receive traffic from one or many remote Senders,
- configure the receiving working mode for each connection,
- select the statistics to display (5 among 13 parameters) and save into a file.

The tab is divided in four areas: 'Listening To ...', 'Coming From ...', receiving 'Working Mode' and 'Statistics'.

Tab 3 “Receiver - Traffic + Statistics”

### 6.5.1 Duplicate parameters of a connection onto others

In order to facilitate input of the parameters for a connection, a *copy/paste mechanism* for all parameters of a connection is available (identical to the *copy/paste mechanism* for the Sender part – see 6.4.1.1.4).

This mechanism is not available when the canonical IP address cannot be translated in numerical format.

Duplication of connection’s parameters doesn’t copy the interface information. When you copy a connection to another one, the IP address translation mechanism is started.

## 6.5.2 Listening To ...

In this area, you configure each receiving connection with the following parameters corresponding to the connected sender from which connections are received:

### Network interface selection and IP version

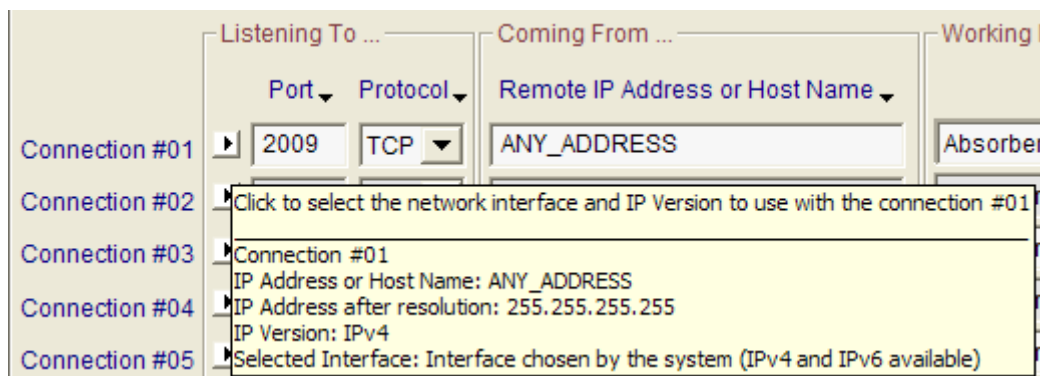
*The black arrow has two purposes:*

- *To display a summary of the connection's parameters*
- *To select the network interface and the IP version for a connection.*

<b>Port</b>	The port number is limited to 65,535. By default, the entered port number is 2009. In case of invalid value, the value is <b>red</b> colored.
<b>Protocol</b>	TCP or UDP protocol (default = TCP protocol).

### 6.5.2.1 Summary of connection parameters

When you move the mouse over the black arrow, a popup window - called a **tooltip** – is displayed.



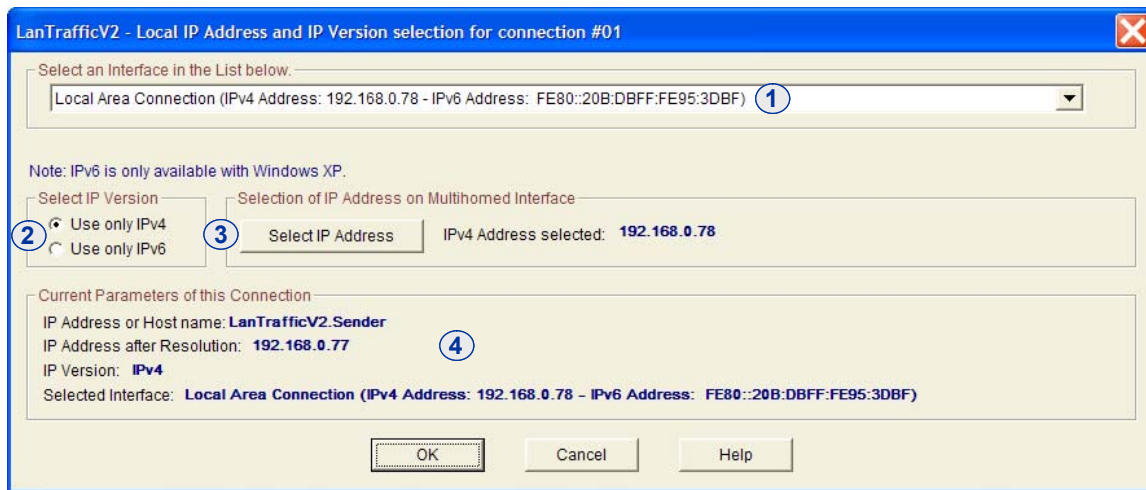
*Receiver connection tooltip*

The tooltip for the Receiver connection includes 5 items:

- First item is the connection number the tooltip refers to.
- Next item is the IP address defined by the user.
- Next item is the IP address translated when IP Translation address has succeeded (e.g. the address is not NO\_ADDRESS or 0.0.0.0).
- Next item is the IP version currently selected.
- Last item is the interface name selected. The name displayed is the name of the connection presented in the “*Settings/Network and Dial-up Connections*” Start menu of the operating system (Default is “Interface chosen by the system”).

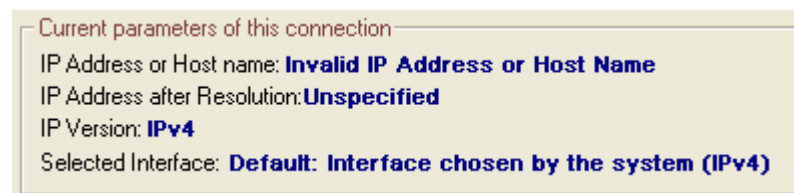
### 6.5.2.2 Select the network interface, IP version and local IP address

When you click on the black arrow, a window is displayed:



*Network interface, IP version and IP local address for a Receiver's connection*

- (1) The **network interface** selection is optional. It is used to select the IPv6 or to force connections to use a specific interface.
- By default:
    - IP version 4 is used.
    - The IP stack resolves the interface selection to receive packets from the remote.  
The IP stack uses the destination IP address to select the correct interface. IP address and netmask related to each interface are checked against the remote IP address to reach. When an interface that matches the remote IP address is found, it is used. To understand how the IP stack selects the interface, you may enter 'route print' console command to list interface order, IP address and network address mask.
  - You can select one interface from the list of connected interfaces. "LanTraffic V2" will only use the selected interface to translate IP address and to make connection. You must select the interface compatible with the remote IP address you want to receive. When the IP address translation failed, current connection parameters area is updated as follows:

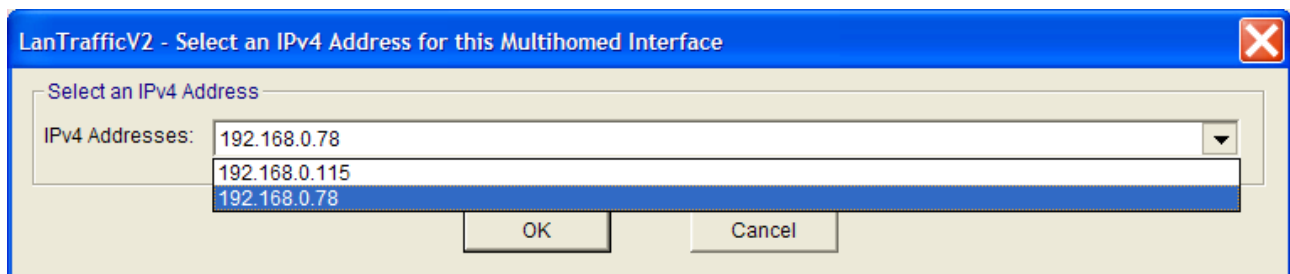



- Use of IPv6 requires the selection of an interface.
- Interface types are restricted: only Ethernet and PPP are listed.  
A PPP interface should be in 'connected' state to belong to the interface list.

- (2) **IP version** selection is available:
- with Windows XP (or later)
  - when IPv6 is attached to the interface e.g. current Windows versions doesn't offer IPv6 over PPP.
  - when an interface has been selected with IPv6 attached e.g. 'interface chosen by the system' can't be used.

The IP address translation (see 6.4.1.1.3) uses the current IP version to get the IP address numerical form.

- (3) **Select IP address** is available when multiple IP addresses are attached to the network interface. This interface configuration is also known as 'multihomed' interface. Selection of an IP address is generally not required: "LanTraffic V2" uses the default IP address of the interface to establish connections. It may be useful when routing priority or policy is defined. Example of IP address selection for a multihomed interface:



 *Select IP address is not available if the default interface 'Interface chosen by the system' is selected.*

- (4) **Current parameters of this connection** area are an abstract for the connection. It summarizes IP address, numerical IP address format, IP version and interface selection.
- IP addresses are static. The IP address translation will process only when you click on OK.
  - IP version field is dynamically updated with the user selection.
  - Current interface is dynamically updated with the user selection.



*When you click on the OK button, if the interface selected or IP version has changed, the IP address translation is automatically started. It may be time consuming.*

So, you can configure various incoming connection criteria:

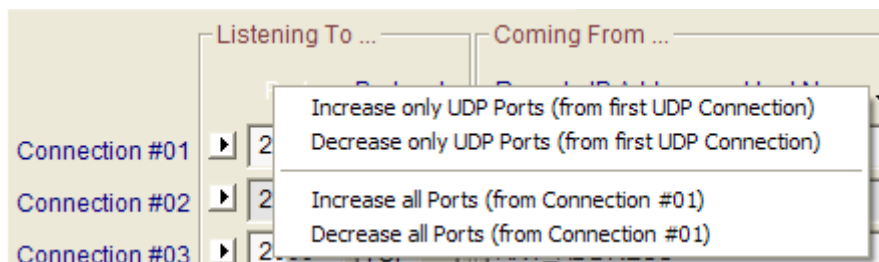
- **Interface:** you limit a connection to a specific Interface or let the Operating System to return connections from any interfaces.
- **IP version:** when an Interface offers the two IP versions, you should select the IP version expected. By default, IPv4 is selected.
- **When multiple IP addresses are attached to one interface,** you should select the destination IP address the incoming connection should refer to. By default, the first IP address returned by the system is selected.

### 6.5.2.3 Port floating menu

When the mouse is located on the ‘Port’ text area, the color changes to white and the following tooltip is displayed:



Click on the left mouse button to display four items menu as following:

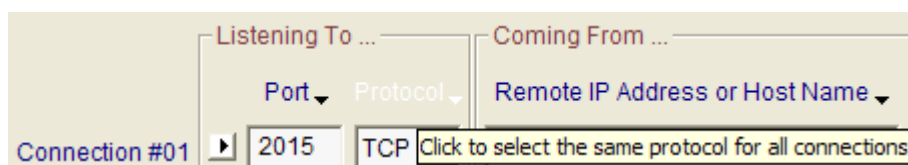


With this menu, you can:

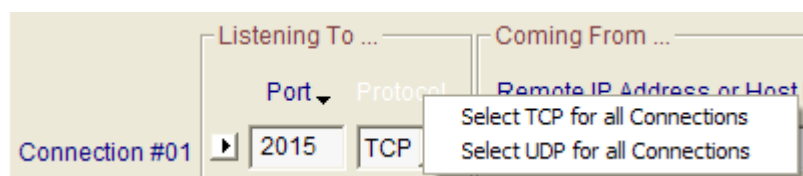
- Set the port number increasingly or decreasingly for all UDP connections, based on the port number of the first UDP connection,
- Set the port number increasingly or decreasingly for all connections, based on the port number of the first connection without taking into account the protocol in use.

### 6.5.2.4 Protocol floating menu

When the mouse is located on the ‘Protocol’ text area, the color changes to white and the following tooltip is displayed:



Click on the left mouse button to display the short menu as below:



This menu helps to set the same protocol for all connections.

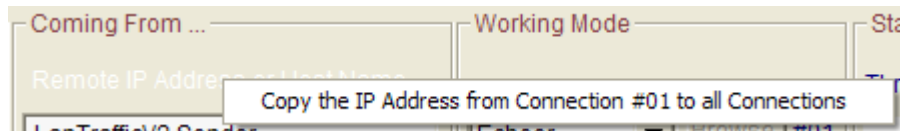
## 6.5.3 Coming From ...



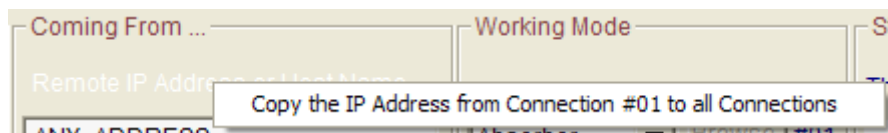
**Remote IP address or Host Name:** Enter the IP address (numerical format) or Host Name (canonical format), with the help of AutoComplete when active.  
By default, the value is ANY\_ADDRESS (This address is a mask to accept connection from any source address. It applies on both IPv4 and IPv6).

### 6.5.3.1 IP address floating menu

When the mouse is located on the ‘IP address’ text area, the color changes to white and the following tooltip is displayed:



Click on the left mouse button to display the short menu as below:



With this function, the IP Address field from connection #01 is recopied for all connections from #02 to #16.

### 6.5.3.2 IP Address translation mechanism

“LanTraffic V2” tries to translate – e.g. to resolve - the IP address from a canonical to a numerical format. This operation is called the *IP address translation mechanism*. When the ‘IP Address or Host Name’ field or Interface parameters changes, when you move from ‘IP Address or Host Name’ field to another field, to another tab, when the Enter key is pressed or when Interface parameters change, automatically starts the IP address translation mechanism.

Because the IP address translation mechanism is CPU consuming, a particular attention should apply when using IP canonical addresses. CPU consumption depends on the DNS answer speed, the number of DNS configured and the network load when the DNS request is sent.

If network environment changes – e.g. a new DNS has been defined - you should press the Enter key in the ‘IP Address or Host Name’ field to force “LanTraffic V2” restart the translation mechanism for this connection.



When the IP address translation failed, the IP address is written red on white. This connection cannot be started: the “Run” button in the ‘Sender – Traffic + Statistics’ tab is grayed.





To summarize, the **IP address translation** mechanism is activated when:

- the focus leaves the 'IP Address or Host Name' field,
- another tab is selected,
- you duplicate parameters from one connection to another,
- you change the Interface parameters.

## 6.5.4 Working Mode

“LanTraffic V2” offers five different active working modes for the Receiver part: 'Absorber', 'Absorber file', 'Echoer', 'Echoer File', 'Absorber + Generator'.

A 'Disable' (or inactive) mode is also available.

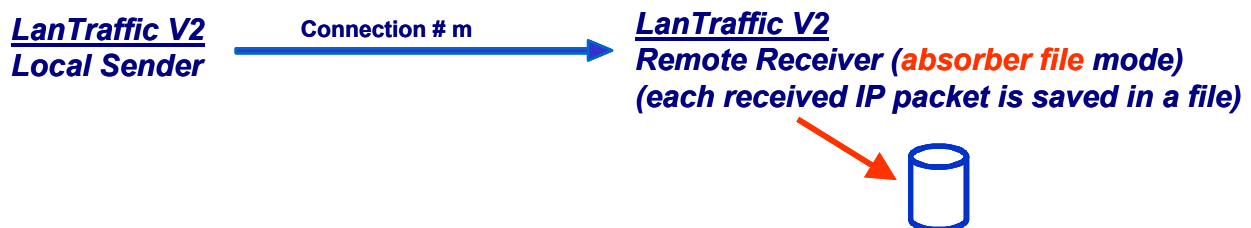
### 6.5.4.1 Absorber mode

With this working mode, data received by “LanTraffic V2” is only used for statistics.



### 6.5.4.2 Absorber File mode

When a receiving connection is operating in the Absorber File mode, the Receiver will save received data in a file. The name of the file must be entered in the Filename field. A 'Browse' button allows selecting the file easily.



### 6.5.4.3 Echoer mode

When a receiving connection is operating with the echoer mode, the received data are sent back to the Sender.



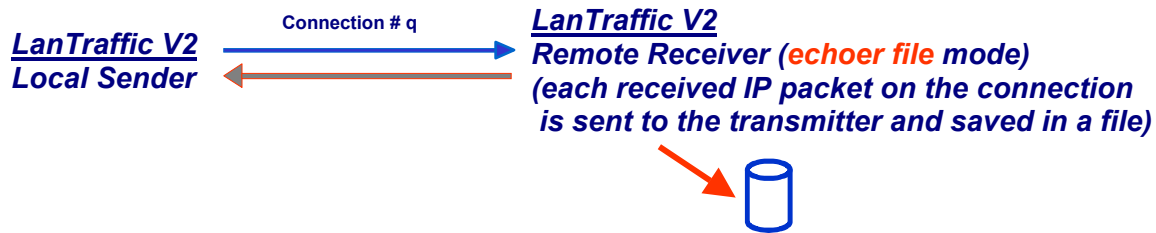
With UDP protocol, echoer mode is available only if a connected sender IP address is specified.



Echoed data can be saved into a file on the remote Sender via the "Sender - Parameters" tab.

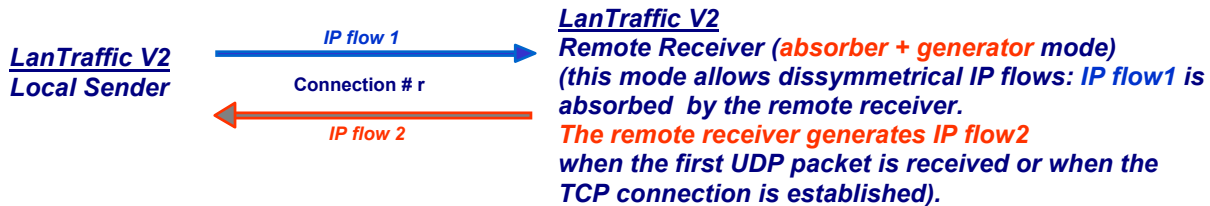
### 6.5.4.4 Echoer File mode

When a receiving connection is operating in this mode, the received data are sent back to the Sender and saved into a file. The name of the file must be entered in the Filename field. A 'Browse' button allows selecting the file easily.



#### 6.5.4.5 Absorber + Generator mode

This mode is displayed as 'Absorber Gen.' in the combo-box mode.



Properties of the *IP flow 1* are defined at the "LanTraffic V2" Local Sender level and each IP packet received by the remote IP answering module is only used to compute statistics.

Connection #01	Port 2009	Protocol TCP	Remote IP Address or Host Name ANY_ADDRESS	Absorber Gen	Param. #01
----------------	--------------	-----------------	---	--------------	------------

When you select the “Absorber gen.” mode for a connection (#01 in the example above), a 'Param.' Button is displayed in order to specify traffic parameters generated by the 'Remote Receiver' entity (i.e. *IP flow 2*).

When the 'Param.' Button is pressed, a “LanTrafficV2 - Traffic generator parameters in unitary testing mode” window is displayed (the same as Sender part – configure unitary testing mode).

So you can input parameters for this *IP flow 2* as you like (for example, generate 10,000 packets with a mean throughput of 250 Kbps).

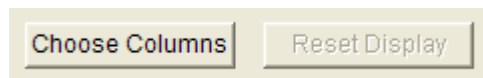
For a TCP connection, *IP flow 2* is generated as soon as the TCP connection will be established between the 'Local Sender' and the 'Remote Receiver' modules. It stops when 'Local Sender' stops the connection or at the end of the 'Remote Receiver' Traffic generator.

For a UDP connection, *IP flow 2* is generated as soon as the 'Remote Receiver' will receive the first UDP packet. It stops when the traffic from the 'Local Sender' is void during 5 seconds (default value) or at the end of the 'Remote Receiver' Traffic generator.

#### 6.5.4.6 Disable mode

When this mode is selected for a connection, “LanTraffic V2” does not establish the connection. The disabled connections are grayed when you start generating traffic. Statistics fields of disabled connections are filled with the following message: “Connection has been disabled”.

### 6.5.5 Statistics



By using the "Choose Columns" button at the bottom, you can select the parameters to display.

Up to 5 parameters can be simultaneously displayed among 13 parameters described later in this paragraph, and at least one parameter must be selected.

*These statistics are computed at the application level (and based on application data sent or received). No MAC, IP and TCP/UDP headers and trailers are taken into account.*

To reset the statistics displayed, you can use the 'Reset Display' button at any time.

The "**N/A**" (Not Applicable) mention can be displayed instead of a value in the cell of the statistics table if the parameter cannot be calculated.

Statistics (based on application data)				
Rx Packets	Rx Pkts Throughput	Rx Throughput	Jitter	Seq. Num. Errors
2769 p	47 p/s	536 Kb/s	N/A	N/A
1044 p	N/A	1.03 Mb/s	0 ms	0

If a problem is detected for a connection, a warning message is displayed.

Example:

- Problem: disconnection due to TCP inactivity (cf registry).  
*The Receiver has ended the TCP connection because no data has been received (timeout defined with the TCPINACTIVITY parameter of LanTraffic V2 in the registry).*

Statistics (based on application data)				
Rx Packets	Rx Pkts Throughput	Rx Throughput	Jitter	Seq. Num. Errors
524 p	46 p/s	525 Kb/s	N/A	N/A
Problem: disconnection due to TCP inactivity (cf registry).				

## List of the 13 statistic parameters calculated for the Sender

### Transmitting statistics

<b>Tx Packets</b>	Tx Packets (Tx = Transmit) is the number of packets that "LanTraffic V2" has sent since the connection is started.
<b>Tx Pkts Throughput</b>	Tx Pkts Throughput (Tx = Transmit) is the mean number of packets that "LanTraffic V2" is sending per second. This value is only available with UDP connections. The calculation of this value is based on the sampling period defined by the throughput sampling period in the 'Configuration/General Parameters' menu.
<b>Tx Throughput</b>	Tx Throughput (Tx = Transmit) is the mean throughput of data sent. The calculation of this value is based on the sampling period defined by the throughput sampling period in the 'Configuration/General Parameters' menu.
<b>Tx Volume</b>	Tx Volume (Tx = Transmit) is the number of bytes that "LanTraffic V2" has sent since the connection is started.

### Receiving statistics

<b>Rx Packets</b>	Rx Packets (Rx = Receive) is the number of packets that "LanTraffic V2" has received since the connection is started.
<b>Rx Pkts Throughput</b>	Rx Pkts Throughput (Rx = Receive) is the mean number of packets that "LanTraffic V2" is receiving per second. This value is only available with UDP connections. The calculation of this value is based on the sampling period defined by the throughput sampling period in the 'Configuration/General Parameters' menu.
<b>Rx Throughput</b>	Rx Throughput (Rx = Receive) is the mean throughput of data received. The calculation of this value is based on the sampling period defined by the throughput sampling period in the 'Configuration/General Parameters' menu.
<b>Rx Volume</b>	Rx Volume (Rx = Receive) is the number of bytes that "LanTraffic V2" has received since the connection is started.

### Other statistics

<b>Data Not Echoed</b>	'Data Not Echoed' is the number of bytes that the Receiver couldn't echo. This value is only available if the Receiver works in the Echoer mode.
<b>Jitter</b>	Jitter is the mean variation of delays on packets received. This value is only available when RTT option is selected (on the remote Sender: see Traffic Generator Parameters). This value corresponds to the mean one-way variation only.
<b>Remaining Volume</b>	'Remaining Volume' is the number of bytes that "LanTraffic V2" has still not sent. This information is only available for two Traffic Generator types (Mathematical Law and File to Send).

<b>Seq. Numb. Errors</b>	'Seq. Numb. Errors' (Sequence Number Errors) is the sum of the Out Of Sequence packets number (OOS) and the number of lost packets. This value is only available if the RTT option is selected (on local Sender: see Traffic Generator Parameters) and if the working mode of the remote Receiver is Absorber Generator or Echoer.
<b>Volume To Send</b>	'Volume To Send' is the number of bytes that "LanTraffic V2 should send. This information is only available for two Traffic Generator Types (Mathematical law and File to Send).

**By pressing the 'Start Receiving Traffic' button**, all connected sender information and working mode information are grayed,  
Disabled connections statistics fields are empty on gray background,  
UDP enabled connections statistics fields are filled with "00" value on white background,  
TCP connections statistics fields are empty on white background (they will be filled only when the connection is established).

**By pressing the 'Stop Receiving Traffic' button**, statistics fields are cleared up, connected sender and working mode parameters become available. ***This button also stops Receiver statistics exported into a file.***

**By pressing the 'Reset Display' button**, statistics displayed are reset. The Receiver part statistics displayed can be reset at any time.

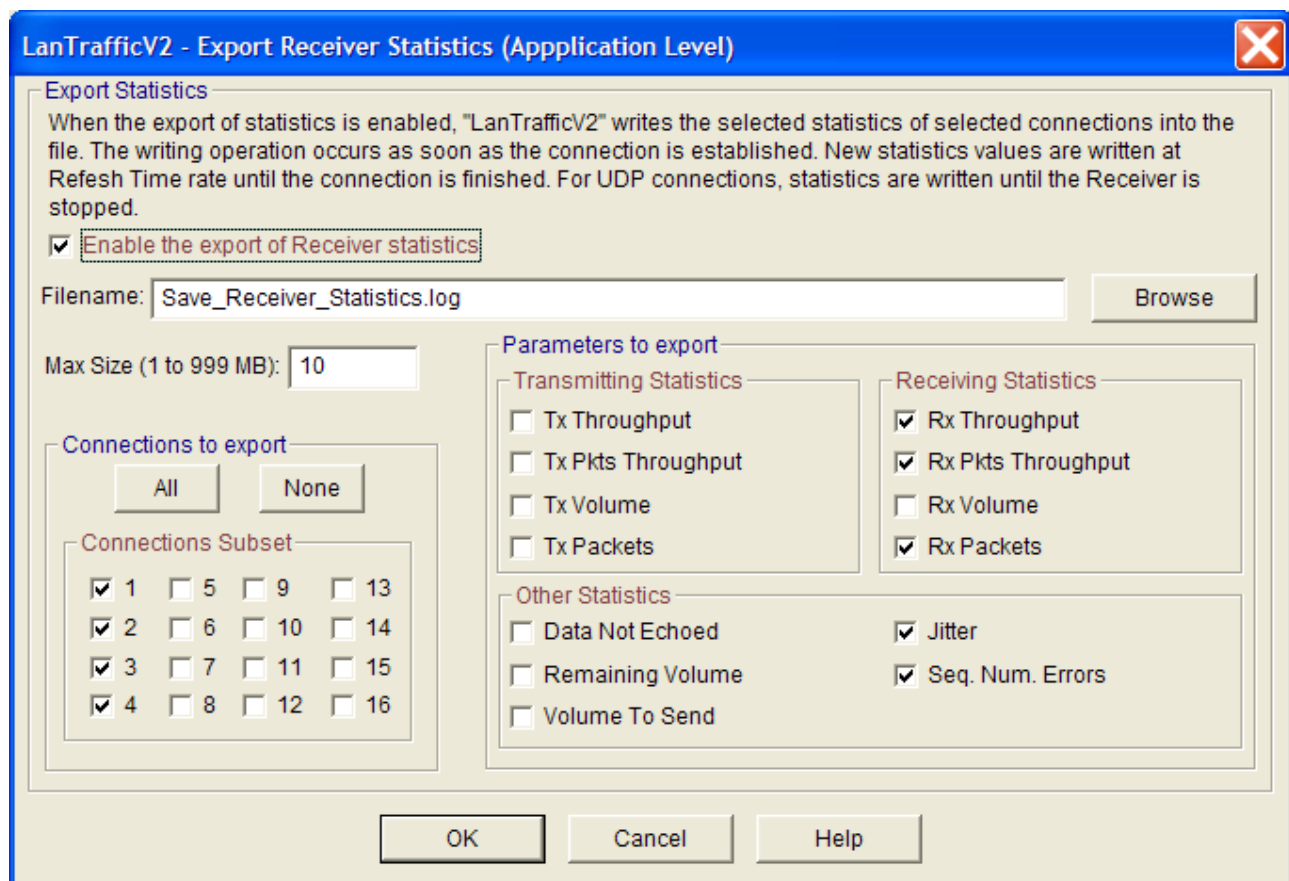
### 6.5.6 Export statistics into a file

To export all or part of **statistics** into a file, click on the 'Parameters' button when enabled (i.e. if the Receiver is not active):



Then a new window allows defining parameters for the export process:

- Enable or disable the export process,
- The filename (.log extension) of the export file,
- The maximum size of the export file (*when the maximum size of the file is reached, statistics are not saved anymore*),
- The identification of the needed connections,
- The parameters to export (up to 13).



Then press OK to validate, and a new state is displayed:

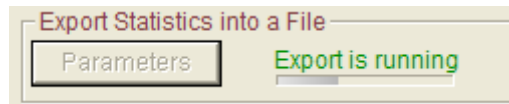


*Do not specify the same filename to save statistics for the Sender and the Receiver parts; else a warning message is displayed.*

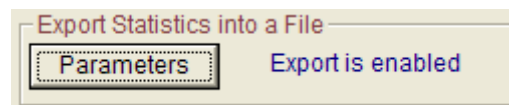
The statistics file is updated with the same refresh period than the statistics displayed.  
A special mark is added to keep special TCP and UDP events e.g. Begin and End of sending traffic.

When you reset statistics, the displayed values and the exported values are reset.

Statistics are saved into the file as soon as the 'Start Receiving Traffic' button of the Receiver has been pressed and the 'Export is running' state is displayed:



When the 'Start Receiving Traffic' button of the Receiver has been pressed, then the export process is automatically suspended and the following idle state is displayed:



#### 6.5.6.1 Receiver statistics file format

The Receiver statistics file is formatted line by line as follows:

First line: Starting session MM/DD/YYYY at HH:MM:SS,mmm (**UTC time**)

Second line: LanTrafficV2 Receiver

Third line: this line contains the labels of columns

Connection #nn (Protocol)	Date	Time	Parameter i	Parameter i	Parameter ...
---------------------------	------	------	-------------	-------------	---------------

with:

- nn is the number of the connection
- Protocol is UDP or TCP,
- Date (MM/DD/YYYY)
- Time (HH:MM:SS.mmm) **UTC time**
- Parameter i, Parameter j ... are the statistics chosen by the user (up to 13 parameters can be selected)  
Example: Parameter i = Tx (Transmit) Throughput, Parameter j = Tx (Transmit) Packets ...

Next lines: numerical values

Connection #nn (Protocol)	MM/DD/YYYY	HH:MM:SS.mmm	nnn.nn	nnn.nn	...
---------------------------	------------	--------------	--------	--------	-----

#### Additional marks for TCP and UDP connection events

##### Connection #nn (TCP or UDP) Begin

This indicates for the connection #nn (nn: from 01 to 16):

- UDP connection: ready to receive traffic.
- TCP connection: beginning of receiving traffic

Numerical values are latest values computed by "LanTraffic V2" for the line.

### Connection #nn (TCP or UDP) End

This indicates the end of traffic for the connection #nn.

Numerical values are latest values computed by "LanTraffic V2" for the line.



- ▶ When a value cannot be computed, the "N/A" mention is indicated.
- ▶ The delimiter mark used between each field is the tabulation character.

### Convention for 'Seq. Num. Errors' and 'RTT'

'Seq. Num. Errors' and 'RTT' are filled with the "N/A" symbol when the 'RTT' option is not found for at least one packet and when TCP connection is stopped.

#### 6.5.6.2 Export Receiver file sample

In the following example, 3 connections (#01, #02 et #15) have been selected for the local Receiver with 5 parameters exported: Rx (Receive) Throughput, Rx (Receive) Pkts (Packets) Throughput, Rx (Receive) Packets, Jitter and Seq. Num. Errors (Sequence Number errors):

- Connection #01: Protocol = TCP & Working Mode = Echoer
- Connection #02: Protocol = TCP & Working Mode = Echoer
- Connection #03: Protocol = UDP & Working Mode = Echoer

The remote Sender has been configured with 3 connections:

- Connection #01: Protocol = TCP & Traffic Generator type = Packets generator  
[Size Packet = 1460, Inter Packet Delay = 20, RTT option = Yes]
- Connection #02: Protocol = TCP & Traffic Generator type = Packets generator  
[Size Packet = 1460, Inter Packet Delay = 20, RTT option = No]
- Connection #03: Protocol = UDP & Traffic Generator type = Packets generator  
[Size Packet = 1460, Inter Packet Delay = 50, RTT option = Yes]

Parameters set In the General Parameters of the Configuration menu:

- Refresh time = 2 seconds
- Throughput sampling period = 5 seconds

First the local Receiver is started and then the 3 connections of the remote Sender are started all together. Then the connections #01, #02 and #03 of the remote Sender are manually stopped.

Starting session 07/18/2004 at 20:49:49.342 (UTC Time)

LanTrafficV2 Receiver

Connection #i (Protocol)	Date	Time	Rx Throughput (Kb/s)	Rx Pkts Throughput (Pkts/s)	Rx Packets (Pkts)	Jitter (ms)	Seq. Num. Errors
Connection #03 (UDP) BEGIN	07/18/2004	20:49:49.502	0	0	0	N/A	N/A
Connection #03 (UDP)	07/18/2004	20:49:49.512	0	0	0	N/A	N/A
Connection #03 (UDP)	07/18/2004	20:49:50.433	0	0	0	N/A	N/A
Connection #03 (UDP)	07/18/2004	20:49:52.436	0	0	0	N/A	N/A
Connection #03 (UDP)	07/18/2004	20:49:54.439	0	0	0	N/A	N/A
Connection #02 (TCP) BEGIN	07/18/2004	20:49:55.500	0	N/A	0	N/A	N/A
Connection #01 (TCP) BEGIN	07/18/2004	20:49:55.500	0	N/A	0	N/A	N/A
Connection #01 (TCP)	07/18/2004	20:49:56.442	99.03	N/A	45	0	N/A
Connection #02 (TCP)	07/18/2004	20:49:56.442	100.38	N/A	45	0	N/A
Connection #03 (UDP)	07/18/2004	20:49:56.442	99.03	8	44	0	N/A
Connection #01 (TCP)	07/18/2004	20:49:58.445	320.13	N/A	141	0	N/A
Connection #02 (TCP)	07/18/2004	20:49:58.445	317.09	N/A	140	0	N/A
Connection #03 (UDP)	07/18/2004	20:49:58.445	317.83	27	140	0	N/A
Connection #01 (TCP)	07/18/2004	20:50:00.448	541.23	N/A	236	0	N/A
Connection #02 (TCP)	07/18/2004	20:50:00.448	533.81	N/A	236	0	N/A
Connection #03 (UDP)	07/18/2004	20:50:00.448	538.93	46	236	0	N/A
Connection #01 (TCP)	07/18/2004	20:50:02.460	550.45	N/A	332	0	N/A
Connection #02 (TCP)	07/18/2004	20:50:02.460	542.94	N/A	331	0	N/A
Connection #03 (UDP)	07/18/2004	20:50:02.460	548.14	47	330	0	N/A



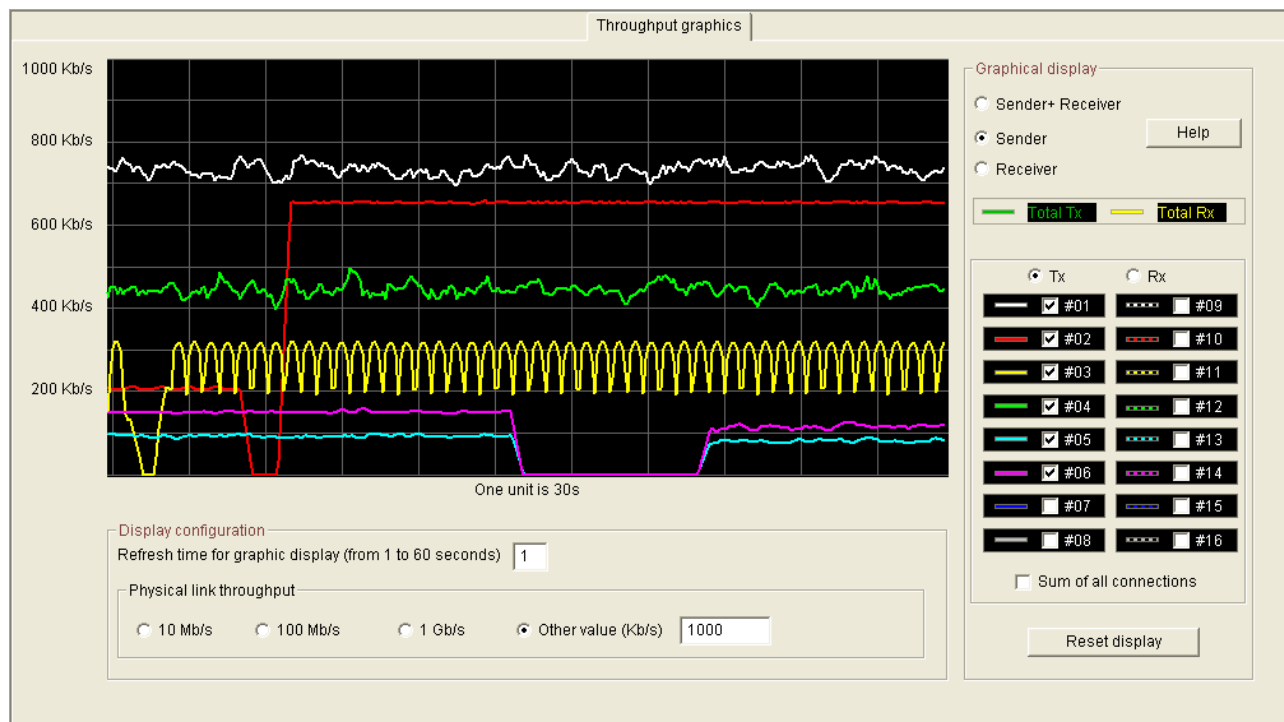
Connection #01 (TCP) END	07/18/2004	20:50:04.113	550.45	N/A	384	0	N/A
Connection #02 (TCP)	07/18/2004	20:50:04.453	542.94	N/A	427	0	N/A
Connection #03 (UDP)	07/18/2004	20:50:04.453	548.14	47	426	0	N/A
Connection #02 (TCP)	07/18/2004	20:50:06.456	545.22	N/A	523	0	N/A
Connection #03 (UDP)	07/18/2004	20:50:06.456	545.84	47	521	0	N/A
Connection #02 (TCP) END	07/18/2004	20:50:07.788	545.22	N/A	560	0	N/A
Connection #03 (UDP)	07/18/2004	20:50:08.459	550.45	47	617	0	N/A
Connection #03 (UDP)	07/18/2004	20:50:10.472	548.14	47	713	0	N/A
Connection #03 (UDP)	07/18/2004	20:50:12.465	548.14	47	807	0	N/A
Connection #03 (UDP)	07/18/2004	20:50:14.468	548.14	47	902	0	N/A
Connection #03 (UDP)	07/18/2004	20:50:16.471	366.2	31	917	0	N/A
Connection #03 (UDP)	07/18/2004	20:50:18.473	147.4	12	917	0	N/A
Connection #03 (UDP)	07/18/2004	20:50:20.486	0	0	917	0	N/A
Connection #03 (UDP)	07/18/2004	20:50:21.017	0	0	917	0	N/A

## 6.6 The Throughput Graphics tab

This fourth tab allows displaying the throughputs for the Receiver and Sender parts, and configuring the graphics display,

This tab is divided in three areas:

- The ‘**Graphic area**’ where curves are displayed (up to 16 curves simultaneously),
- The ‘**Graphical Display**’ object to select curves to display,
- And the ‘**Display configuration**’ object to change the scale parameters.



This snapshot shows 6 curves for connections #01 up to #06 for the Tx (Transmit) part of the Sender.

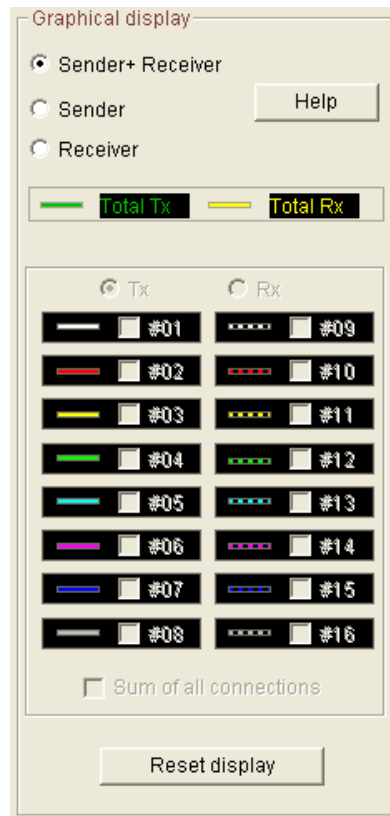
### 6.6.1 The Graphical Display object

This object allows selecting curves to display.

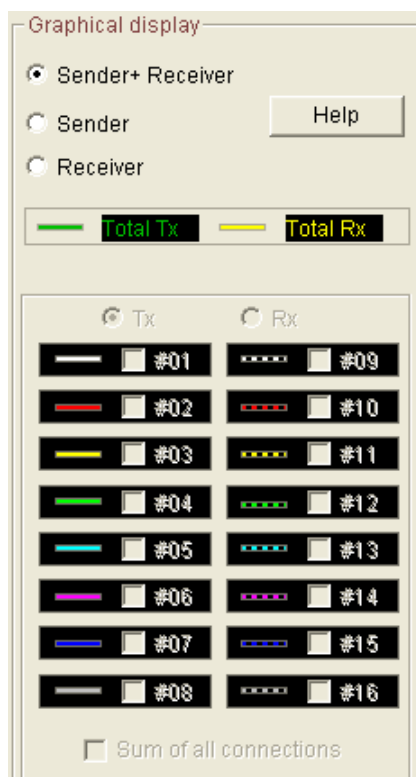
The user has three choices:

- Sender + Receiver (for all connections: the 16 connections for the Sender + the 16 connections for the Receiver),
- Sender,
- Receiver.

The 'Reset Display' button allows clearing the graphic display.



**When you select 'Sender + Receiver', two curves are displayed:**

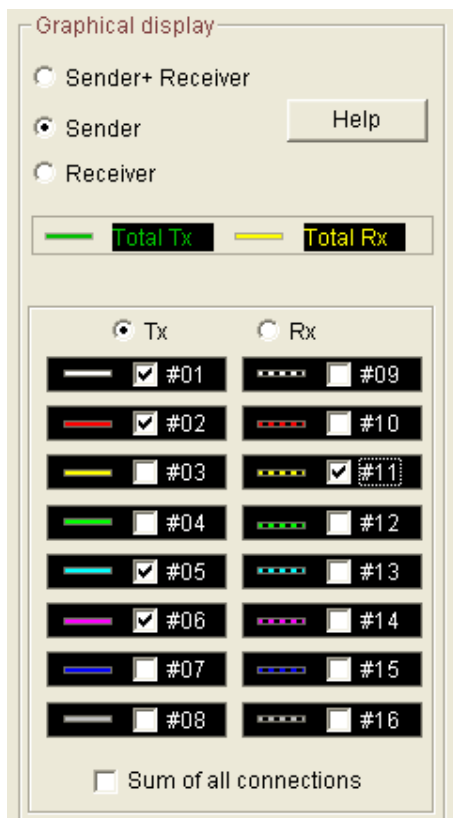


Total Tx (green curve) represents 'Total LanTraffic V2 sending throughput' = total sending throughput of the Sender + total echoing throughput of the Receiver.

Total RX (yellow curve) represents 'Total LanTraffic V2 receiving throughput' = total receiving throughput of the Sender + total receiving throughput of the Receiver.

If the total "LanTraffic V2" sending throughput and the total "LanTraffic V2" receiving throughput are equal, only the green line is visible. If the throughput is superior to the values represented in graph scale, a red line informs the user.

When you select 'Sender' or 'Receiver', a choice is offered: 'Tx' (Transmit) or 'Rx' (Receive) as shown below:



For example, the user has selected 'Tx' for the Sender part.

One or more connections can be selected (via the #i check box) and a colored curve is displayed for each selected connection. Up to 16 connections can be displayed on the graphic.

The check box 'Sum of all connections' allows displaying a curve that is the throughput sum of all connections (in the example above, sum of all Transmit throughput for the sender part).

So, you can graph:

- ▶ for the **Sender** part:
  - ⇒ Transmit (Tx):
    - 1 curve for each connection (up to 16 curves)
    - 1 curve for the sum of all connections
  - ⇒ Receive (Rx):
    - 1 curve for each connection (up to 16 curves)
    - 1 curve for the sum of all connections
- ▶ for the **Receiver** part:
  - ⇒ Transmit (Tx):
    - 1 curve for each connection (up to 16 curves)
    - 1 curve for the sum of all connections
  - ⇒ Receive (Rx):
    - 1 curve for each connection (up to 16 curves)
    - 1 curve for the sum of all connections

## 6.6.2 The Display Configuration object



Display Configuration

Refresh time for graphic display (1 to 60 seconds)

Physical Link Throughput

☒ 10 Mb/s    ☐ 100 Mb/s    ☐ 1 Gb/s    ☐ Other value (5 to 1,000,000 Kb/s)

**Refresh time** defines the time represented by one pixel on the graph. With value = 1, a new point is drawn every second. In this case, the graph shows an approximately 3-min period. Notice that "LanTraffic V2" offers up to 3 hours historic, by entering 60 as value in the Refresh time field.

You can configure the **Physical Link Throughput**: used as scale of the throughput graph: 10 Mb/s, 100 Mb/s, 1 Gb/s or any other value expressed in Kb/s limited to 1,000,000.

## PART 7 Command Line Parameters

The "LanTraffic V2" software can be started by using a command line with parameters.

Example of a script

```
Line 1: C:>LanTrafficV2 -SALL -R
Line 2: pause
Line 3: C:>LanTrafficV2 -STOP
Line 4: pause
Line 5: C:>LanTrafficV2 -Context:"C:\Program Files\LanTraffic V2\Test1.ctx" -S1 -S2
Line 6: pause
Line 7: C:>LanTrafficV2 -UNLOAD
```

### General rule

Parameters should be separated by a space. "LanTraffic V2" is not case sensitive.

### Context filename

The context filename is a set of parameters for "LanTraffic V2". This set can be saved in a file and reloaded later in such a way the user has not to re-enter addresses and configuration parameters.

Command line parameter to define and load this context: **-Context**

Syntax:

**-Context:filename**

Where filename may be c:\temp\file.ctx or "c:\Program Files\LanTrafficV2\file.ctx".

The " symbol is necessary to use spaces in filenames or directories.

### Starting the "LanTraffic V2" Receiver part

There is only one command parameter to start the Receiver part.

Syntax:

**-R**

### Starting the "LanTraffic V2" Sender part

The Sender part can be operated following 2 modes: 'Unitary testing mode' and 'Automatic testing mode'.

Syntax for the 'Automatic testing mode': **-SAutomatic**

Syntax for the 'Unitary testing mode': **-SOption**

Where **Option** may be:

- All: all connections defined are started. To start, a connection should have the IP address defined.
- 1..16: only the connection defined is started.

### Stopping the "LanTraffic V2" Sender and Receiver parts

There is only one command parameter to stop the Sender and the Receiver.

Syntax:

**-STOP**

**Unload the "LanTraffic V2" application**

This command parameter allows unloading the "LanTraffic V2" instance.

Syntax:       **-UNLOAD**

**Command line samples**

- **LanTrafficV2 -r**

This command line starts "LanTraffic V2" with default parameters and starts the Receiver part.

- **LanTrafficV2 -context:c:\temp\20030607.ctx -SAutomatic**

This command line launches "LanTraffic V2" and loads the file context named c:\temp\20030607.ctx. Then the Sender is started in 'Automatic testing mode' (for defined connections).

- **LanTrafficV2 -context:c:\temp\20030607.ctx -SAI**

This command line starts "LanTraffic V2" and loads the file context named c:\temp\20030607.ctx. Then the Sender is started in 'Unitary testing mode' for every connection defined.

- **LanTrafficV2 -context:c:\temp\20030607.ctx -R -S1 -S2 -S4 -S16 -S12**

This command line starts "LanTraffic V2" and load the file context named c:\temp\20030607.ctx. Then the receiver is started, and for the Sender connections #01, #02, #04, #12, #16 are started in the 'Unitary testing mode' (if they are defined).

**Error return code**

"LanTraffic V2" does not return an error code if a syntax error is found in parameters, or if an unknown parameter is used.

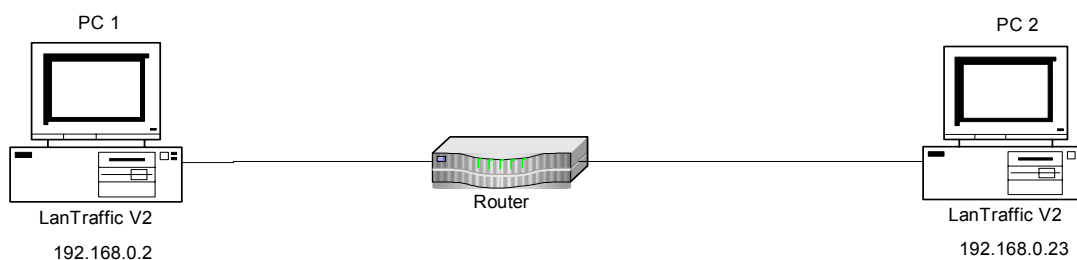
## PART 8 How To Do ...

This part presents simple but real examples of some "LanTraffic V2" usages. Each sample is detailed to help you to reproduce it.

The list is not exhaustive. You may find specific usage of "LanTraffic V2" by your own as it may apply to various network configurations.

### 8.1 Checking router configuration

With this sample, it is shown how to check if a router is able to handle the TOS field in the IP header ([see The TOS field](#) paragraph 6.4.1.3.2.4).



PC #1 is the Sender and PC #2 is the Receiver.

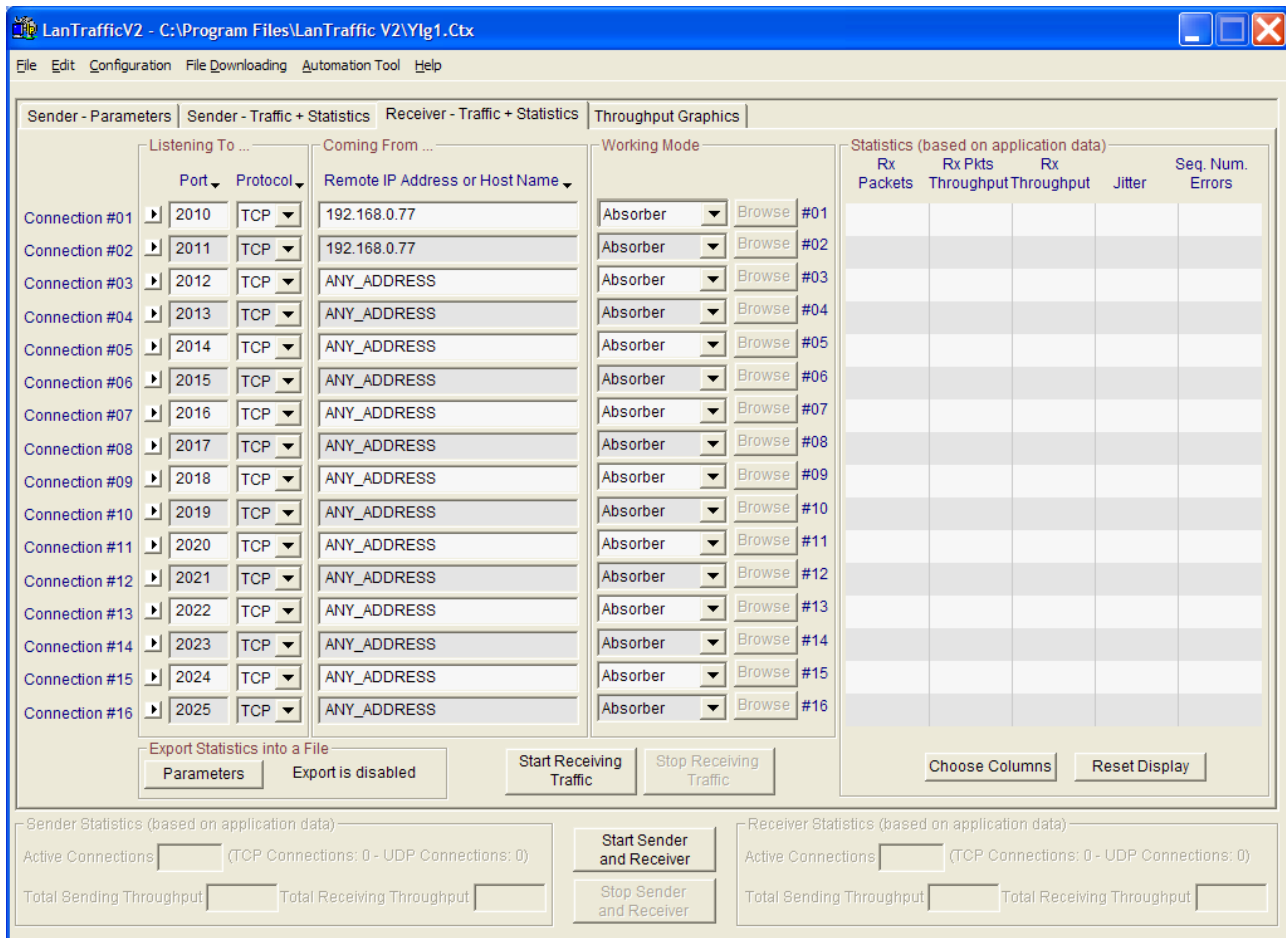
#### 8.1.1 PC #2 parameters

After launching "LanTraffic V2" on PC #2, you select the "Receiver – Traffic + Statistics" tab to enter parameters for connections #01 and #02:

- 2 different values as port numbers: connection #01 get 2010 and connection #02 get 2011.
- Both connections are configured with the TCP protocol.
- You may also enter the PC #1 IP address as source IP address, for each connection but it is not mandatory in that case because the TCP protocol has been selected.
- The Receiver mode is 'Absorber'.



The figure bellow shows the configuration at this point.



To start the Receiver, click on the 'Start Receiving Traffic' button.

### 8.1.2 PC #1 parameters

PC #1 acts as the Sender.

Launch "LanTraffic V2"; the default tab is "Sender – Parameters".

To configure connection #01 and connection #02, proceed as following:

- Enter the PC #2 IP address for connection #01 and connection #02.
- Set the port number of connection #01 to 2010.
- Set the port number of connection #02 to 2011.
- Select TCP as protocol for both connections.
- Click the "Parameters #01" button to choose the traffic mode and to configure it for connection #01. The selection should include:  
Traffic generator type = Packets generator,  
Number of packets = 0 (unlimited),  
Packet size = 1460  
Inter-packet delay = 20 ms,  
TOS = 14 ([see The TOS field](#)).

**LanTrafficV2 - Traffic Generator Parameters - Sender Unitary Testing Mode (connection #01)**

**Step 1: Select the traffic generator type**  
First of all, select the traffic generator which is going to be used on this connection.

☒ Packets generator

**Packets Generator Parameters**

Packets number (0 to 99,999,999)  (0 = infinite value)

**Packet Contents (00 to FF hexa byte)**

☒ Fix

☐ Random  min  max

☐ Alternate  value-1  value-2

☐ Increasing / Decreasing  min  max  step

☐ Mathematical law

**Law : data volume to send**

Uniform law  
Range : [9.77 KB , 2.38 MB]

☐ File to send

**Filename**

Loop counter (1 to 99)  Idle time between each loop (0 to 99 s)

**Step 2: Specify Data size and packets parameters**  
In this step, define Data Size and packets parameters as well as the delay between each sent packet or specify values for some IP Header fields.

**Data Size (1 to 65,535 bytes)**

☒ Fix

☐ Random  min  max

☐ Alternate  size-1  size-2

☐ Increasing / Decreasing  min  max  step

**Inter Packet Delay (0 to 9,999 ms)**

☒ Fix  (See Forewarnings menu please)

☐ Random  min  max

☐ Alternate  value-1  value-2

☐ Increasing / Decreasing  min  max  step

☐ Mathematical law

**RTT Option** ☐ Yes ☒ No

**TOS (1 hexa byte)** Value

**Time To Live (TTL)** Value

**Step 3 (Optional): Enable a throughput limit**  
When one of these two options is selected, "LanTrafficV2" generates the traffic in best effort to respect the throughput chosen.

**Mean Throughput (8 to 999,999 Kb/s)**

☒ Use value  ☐ Data size adjustable

☐ Inter packet delay adjustable

**Mean Throughput (1 to 99,999 Pkts/s)**

☐ Use value (only for UDP connection)

- Same parameters are set for connection #02 but the TOS value is changed to 0.

To start the Sender, select the "Sender – Traffic + Statistics" tab and press 'Start #01' and 'Start #02'.

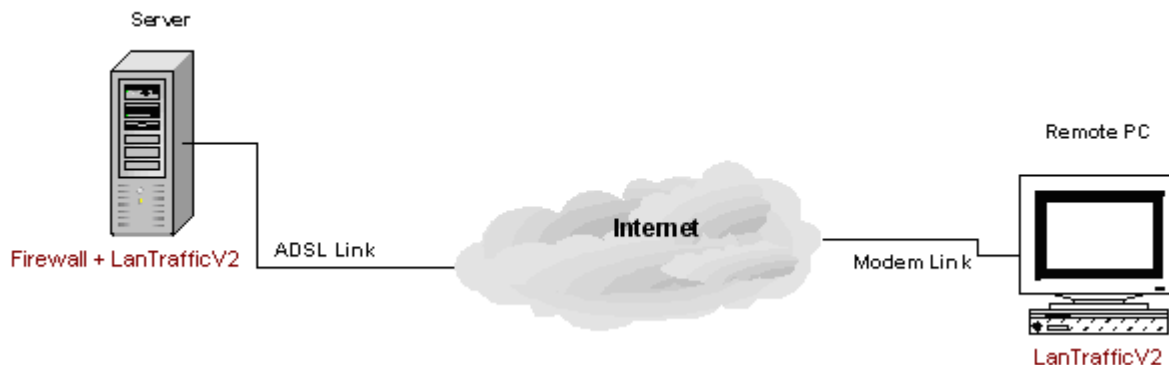
### 8.1.3 What should happened

If your router under test is configured to take into account the TOS field, the connection #01 should be faster than the connection #02 because the connection #01 has requested the maximum throughput to the router via the TOS field.

## 8.2 Checking a firewall configuration

"LanTraffic V2" may be used to check the firewall configuration. The ability for a user to specify the port number connection per connection is used in this test.

Let us assume that a server handles a web site and is linked to Internet via a fixed IP address. This server is also an Internet gateway and it includes a company database. This is why a firewall has been installed. The objective of this test is to check if the firewall access restriction is correct. The remote access will use a modem link as shown in the following figure:



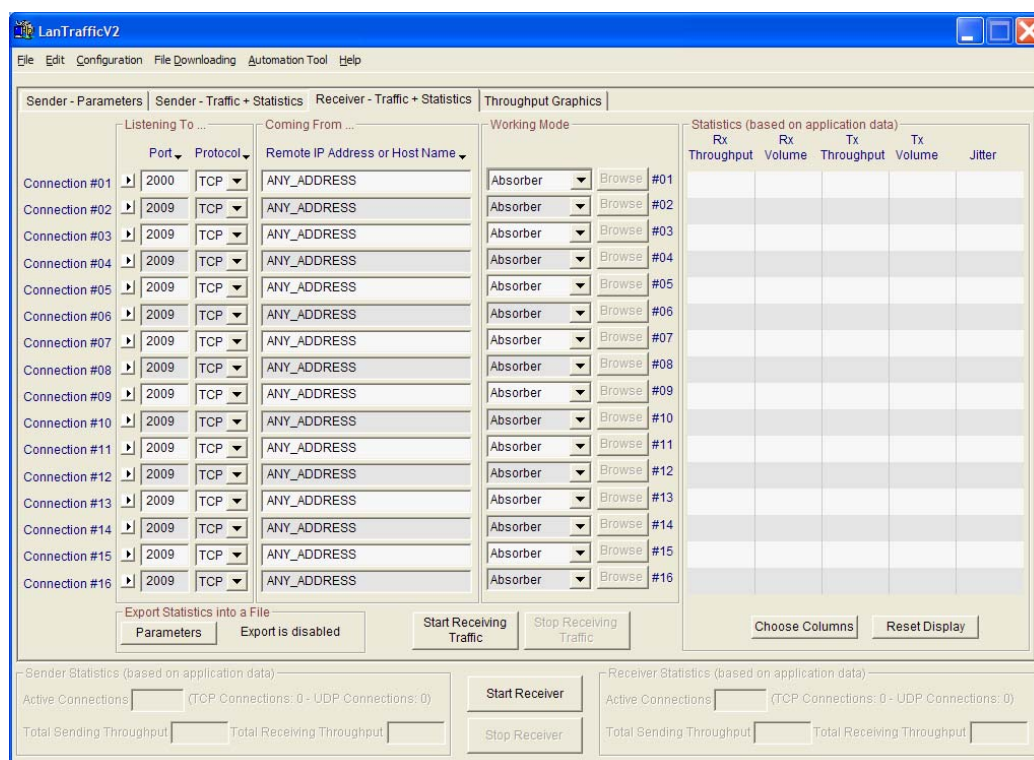
### 8.2.1 LanTraffic V2 parameters on the server

To check that ports are not remotely available on the server, we start "LanTraffic V2" and configure the "Receiver – Traffic + Statistics" tab.

If a connection can be established, the connection has been able to go through the firewall. This is what is NOT expected: the firewall should be reconfigured.

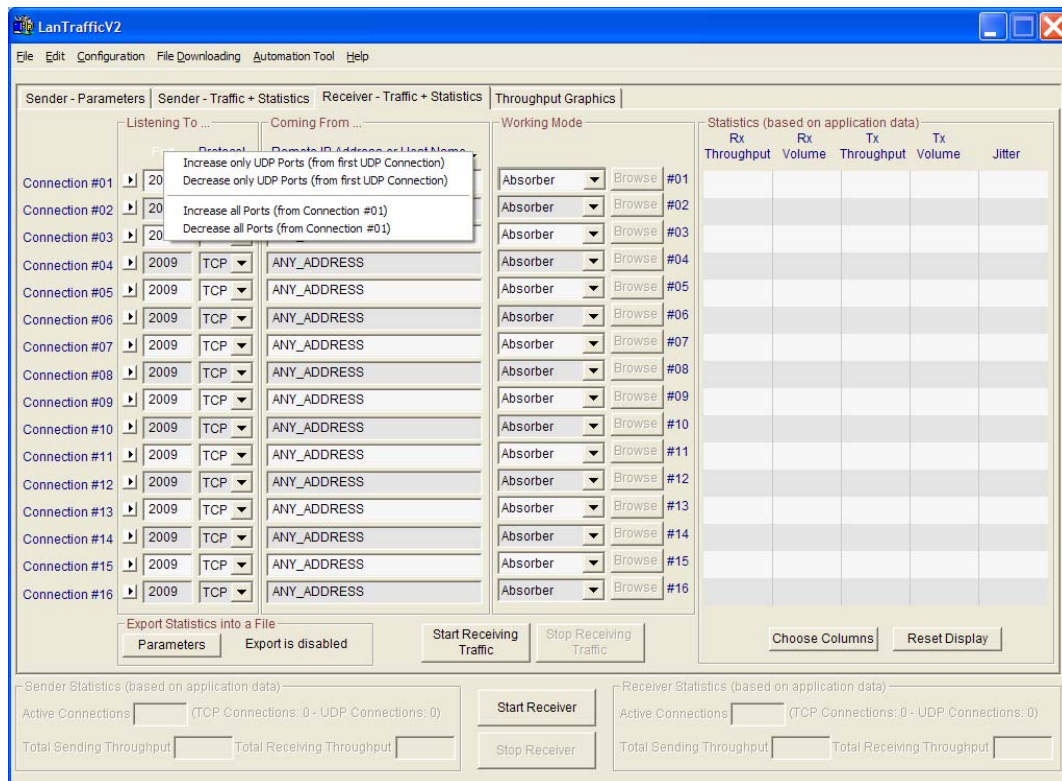
In this example we check TCP connections port 2000 to 2015. You can adapt this range and the protocol to your specific environment.

Let's start with the connection #1.



To access incoming TCP connection from any one, the IP address 'ANY\_ADDRESS' has been selected. Port number is 2000 and protocol is configured with TCP.

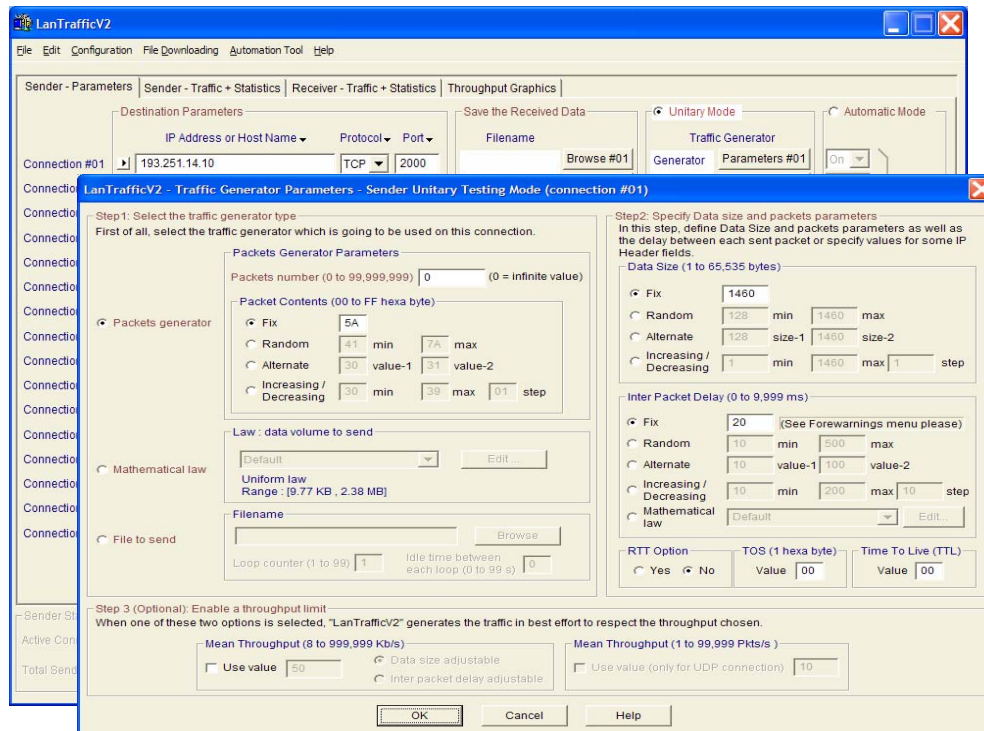
To easily increment the port number for each connection, you can use the 'Port floating menu' as shown:



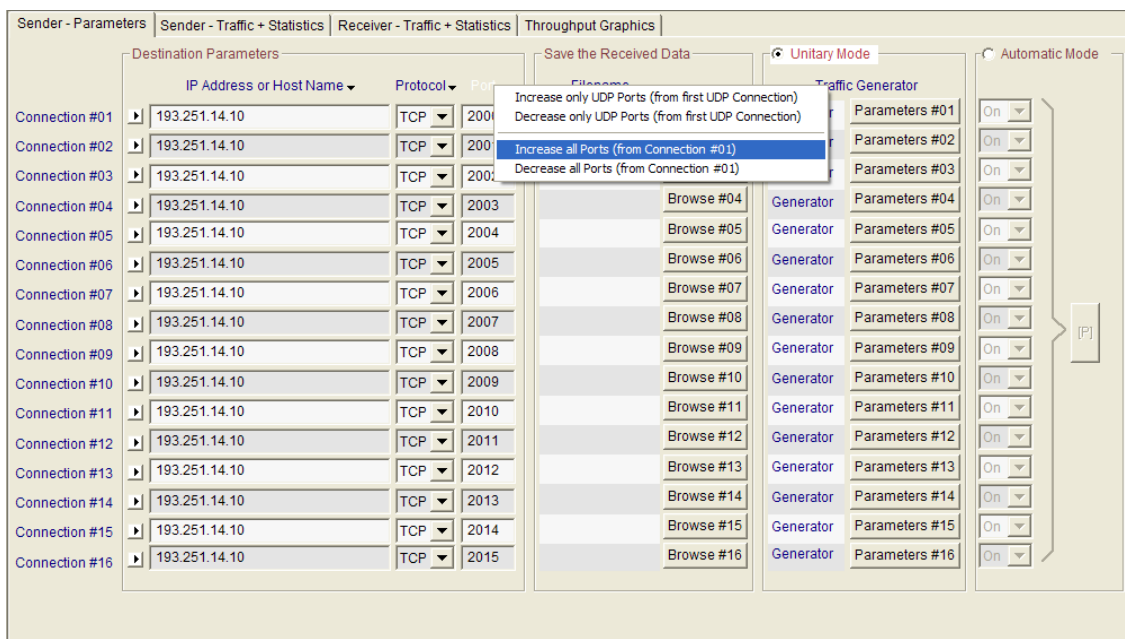
You are ready to start the Server part by pressing the 'Start Receiving Traffic' button.

## 8.2.2 LanTraffic V2 parameters for the Remote PC

To change parameters for the connection #01, select the "Sender-Parameters" tab.



If you assume the server IP address is 193.251.14.10, you enter this IP address, select the TCP protocol and enter 2000 as port number. To change the traffic generator click on the 'Parameters # 01' button. To apply these changes for all connections, you can use the [copy / paste mechanism](#). When the 16 connections are the same, use the 'Port floating menu' to increase the port number as shown in the next figure:



Then select the "Sender – Traffic + Statistics" tab to start connections by clicking the 'Start All Connections' button.



### 8.2.3 What result can you expect

There should be no connection established if the firewall is configured to disable ports 2000-2015 for TCP connections. In that case, an error message is displayed in the Statistics area for each connection: 'Connection failed: no response from the Remote'.

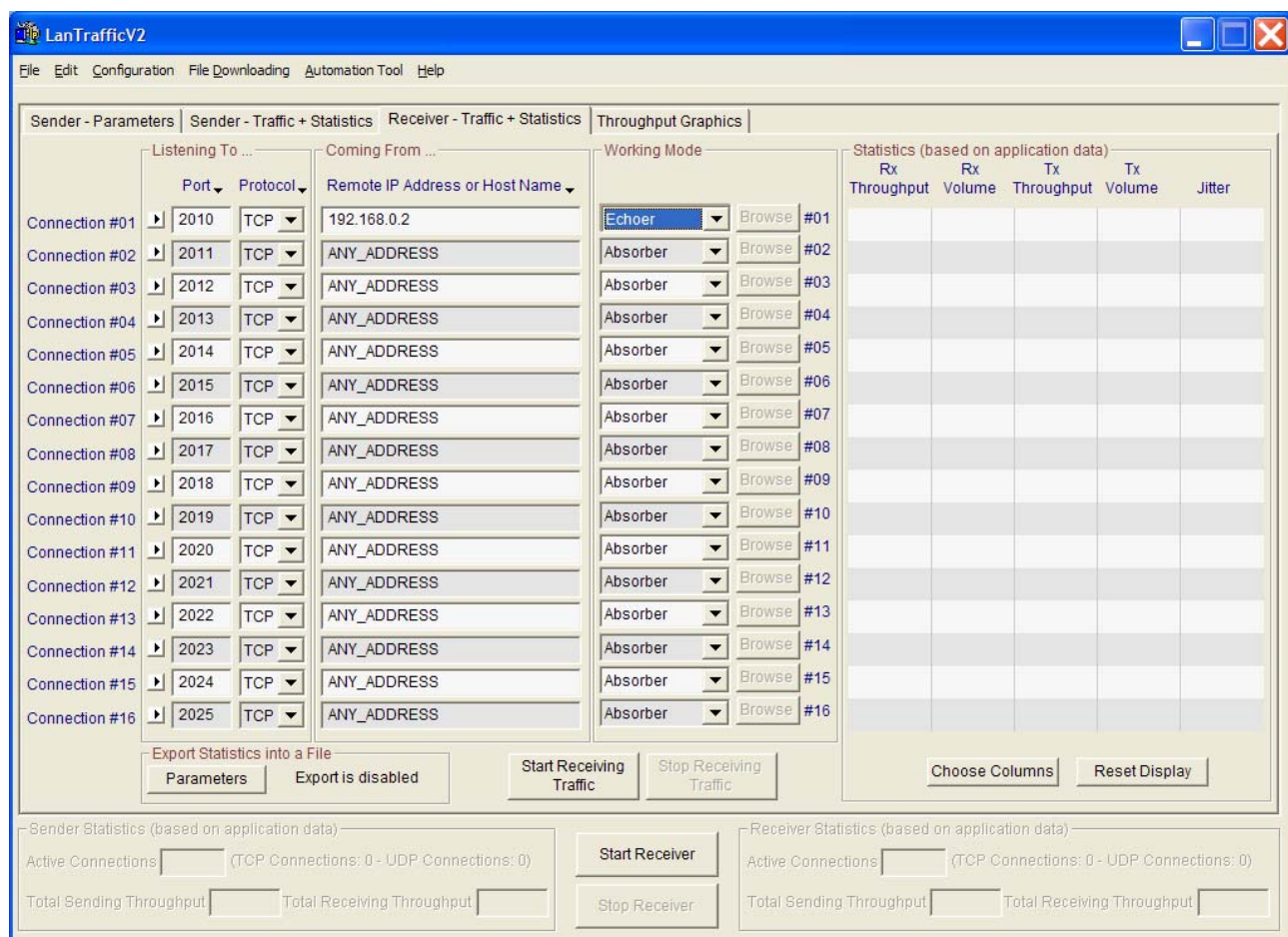
## 8.3 Checking the best throughput

To check the throughput between two PCs, you should use a crossed-cable as shown in the next figure. This test assumes IPv4 usage.



### 8.3.1 PC #2 parameters

Start "LanTraffic V2" on PC #2 and select the "Receiver – Traffic + Statistics" tab.



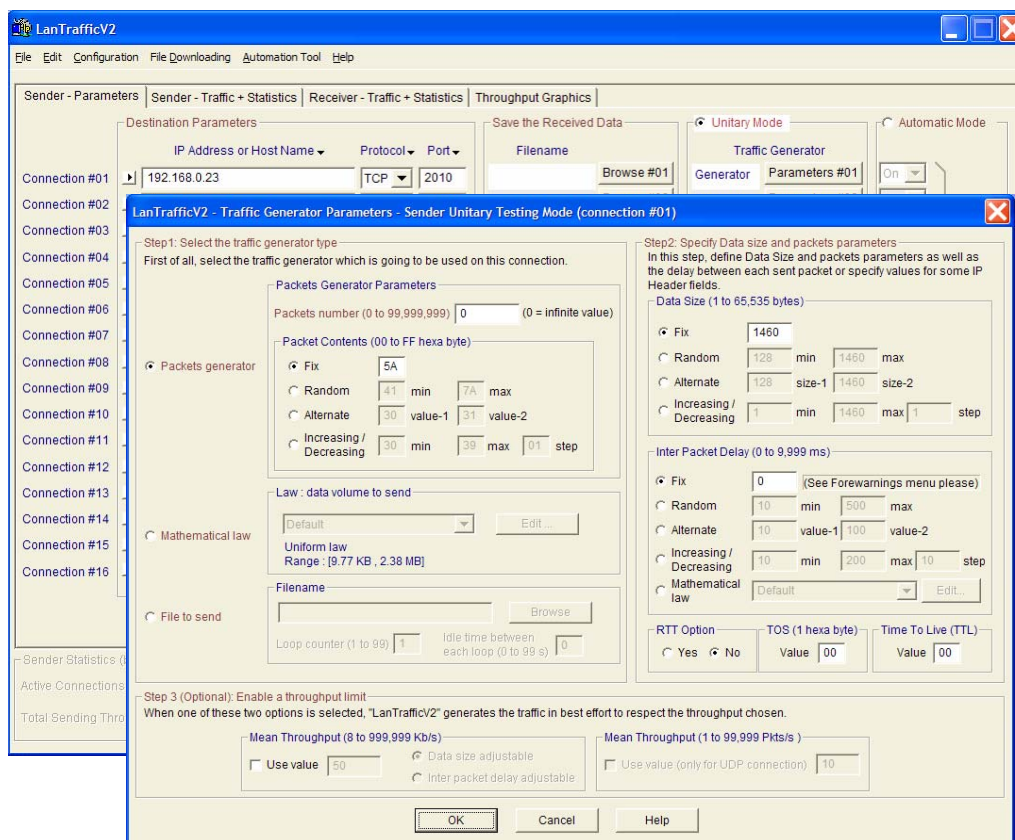
Assuming the connection #01 will be used, enter the IP address of PC #1 (192.168.0.2) or ANY\_ADDRESS, the port number here is arbitrary selected to 2010. Select the TCP protocol and the working mode to 'Echoer'. The echoer mode is useful to check full-duplex speed transfer.

Start the Receiver by pressing the 'Start Receiving Traffic' button.

### 8.3.2 PC #1 parameters

Start "LanTraffic V2" on PC #1 and select the "Sender – Parameters" tab.

The connection #01 will be used in this example. Enter the IP address of PC #2 (192.168.0.23), select the TCP protocol and enter the port number 2010 (same as PC #2). To change the traffic generator click on the 'Parameters #01' button.



Select the unlimited packet number with 0 in the packet number field; the packet size is the best with 1460 bytes long. The inter-packet delay should be 0 for the maximum throughput.

Then select the "Sender – Traffic + Statistics" tab and click on the 'Start #01' button.

Columns 'Throughput' for the PC #2 Sender and PC #1 Receiver will show throughputs. Best throughput depends mainly on the CPU, memory and NIC quality. If PCs used are different, choose the most powerful PC as Receiver.

## 8.4 ADSL connection simulation

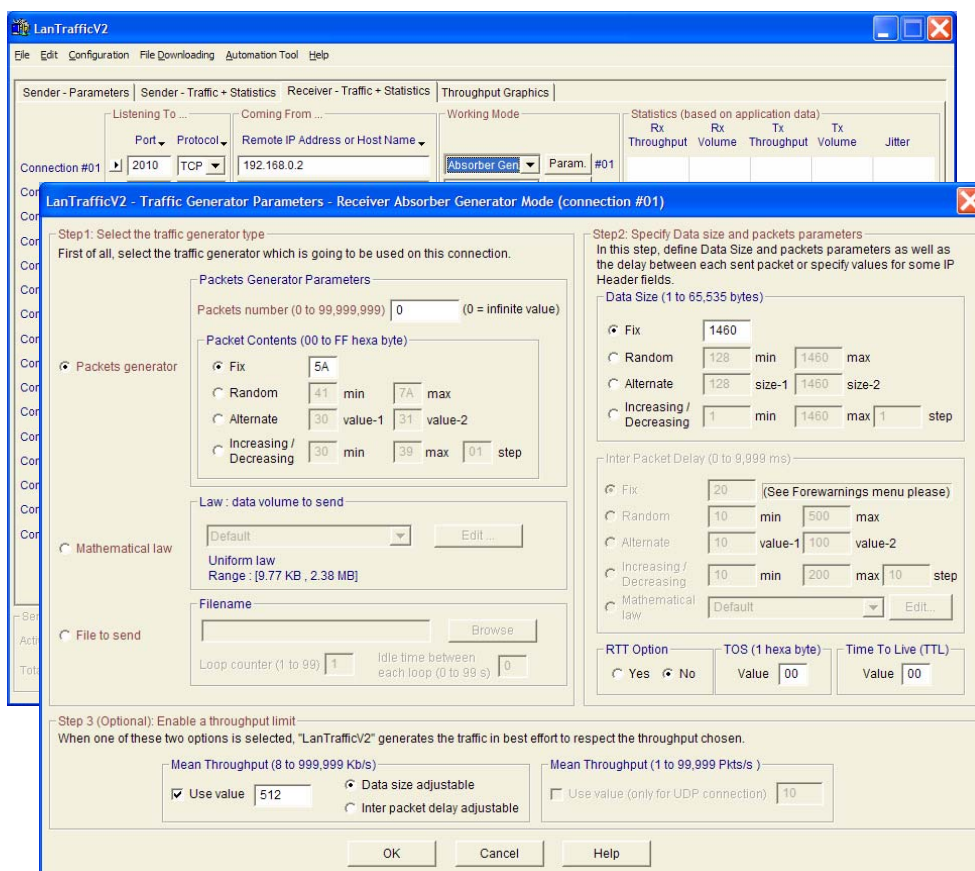
"LanTraffic V2" can be used to simulate an ADSL connection, which is asymmetrical by nature. The next figure is one of those that can be used. Hub or router may also be used to connect the 2 PCs.



Assumption: PC #2 is the user PC and PC #1 is the server. The PC #1 to PC #2 connection link speed is 128 kbps and the reverse link speed is 512 kbps with IPv4.

### 8.4.1 PC #2 parameters

Start "LanTraffic V2" on PC #2 (server) and select the "Receiver – Traffic + Statistics" tab. The connection #01 will be used.





The IP address may be PC #1 (192.168.0.2) or any IP address (ANY\_ADDRESS). Assuming you have selected the port number as 2010 and the TCP protocol, then select the receiving working mode 'Absorber Gen.' (Absorber + Generator).

The button 'Param.' is enabled to change the generator's parameters.

Just select the unlimited number of packets (Packets number = 0) and the packet size to 1460. The throughput is limited to 512kbps: check the 'Use value' box in the 'Mean Throughput' group box and enter 512 in the edit field.

To start the Receiver, push the 'Start Receiving Traffic' button.

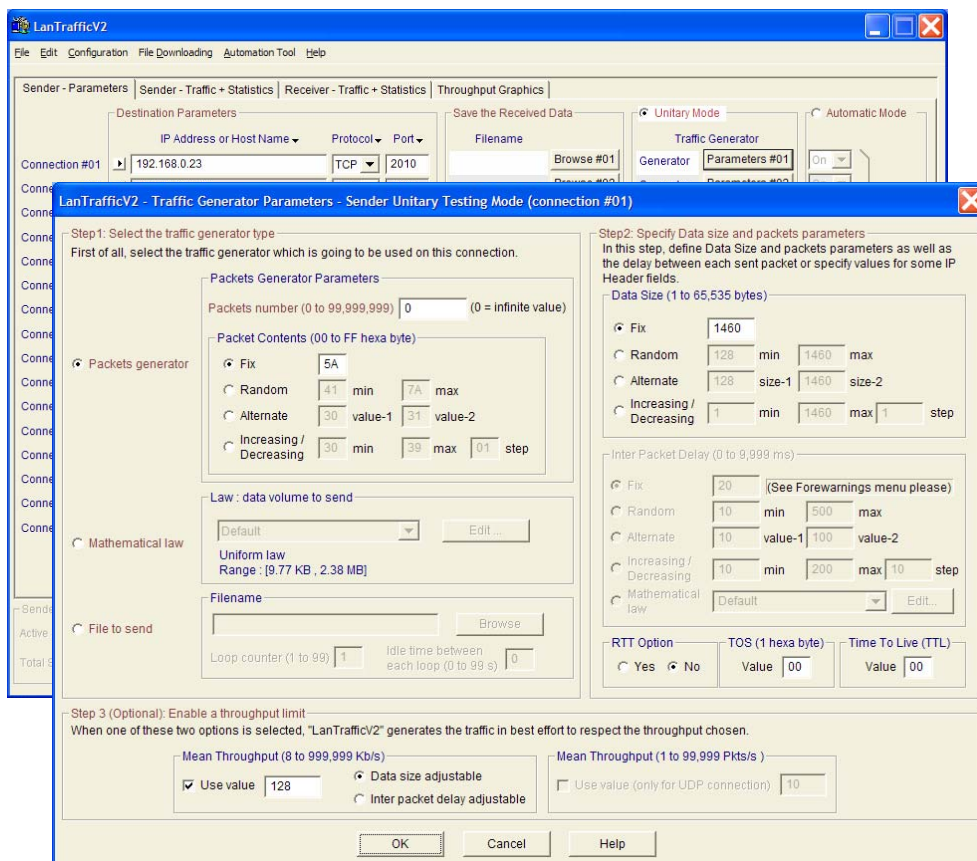
To establish the connection go to the PC #1.



*The traffic will start when the connection will be established with the PC#1. Because the PC #2 is in receiving mode, it can't establish the connection by itself: it should wait for PC #1 to establish the connection before being able to transfer data.*

## 8.4.2 PC #1 parameters

Start "LanTraffic V2" on PC #1 and select the "Sender – Parameters" tab.

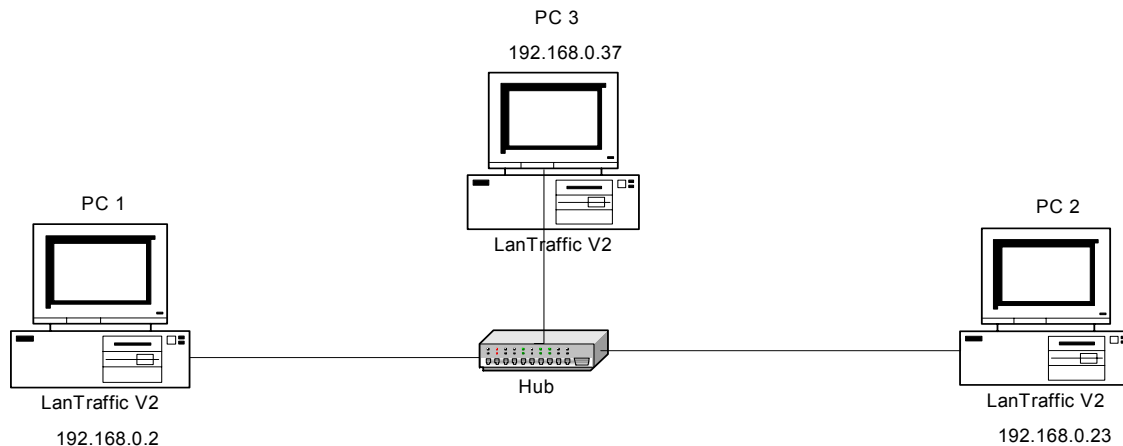


The connection #01 will be used in this example. Enter the IP address of PC #2 (192.168.0.23), select the TCP protocol and enter the port number 2010 (same as PC #2). To change the traffic generator, click on the 'Parameters #01' button. Select the unlimited packet number with 0 in the packet number field; the packet size is 1460 bytes. The throughput is limited to 128 kbps: check the 'Use value' box in the 'Mean Throughput' group box and enter 128 in the edit field.

Then select the "Sender – Traffic + Statistics" tab and click on the 'Start #01' button.

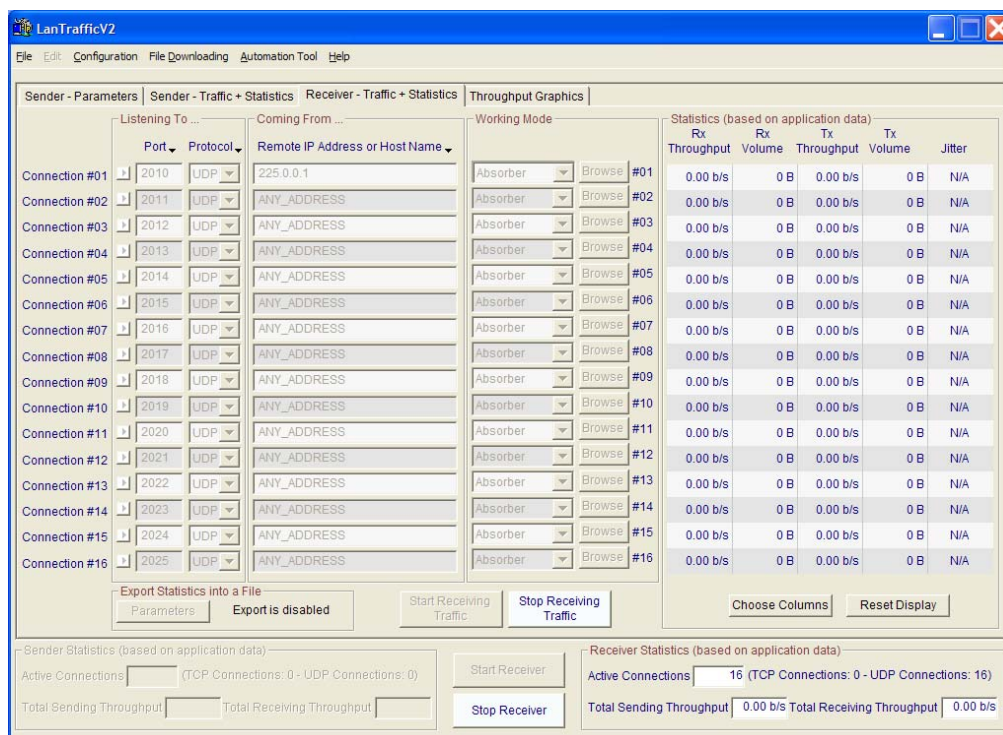
## 8.5 Generating multicast IP traffic

The next figure shows how to generate IPv4 multicast traffic ([see multicast remark](#)). Multicast traffic is based on the UDP protocol. Its characteristic is that multiple receivers can get data from one source – or sender – just indicating from which source they would like to receive data.



### 8.5.1 PC #2 and PC #3 parameters

Let us assume PC #2 and PC #3 are set in the Receiver mode, whereas PC #1 is the Sender (server). Start "LanTraffic V2" on PC #2 and select the "Receiver – Traffic + Statistics" tab.

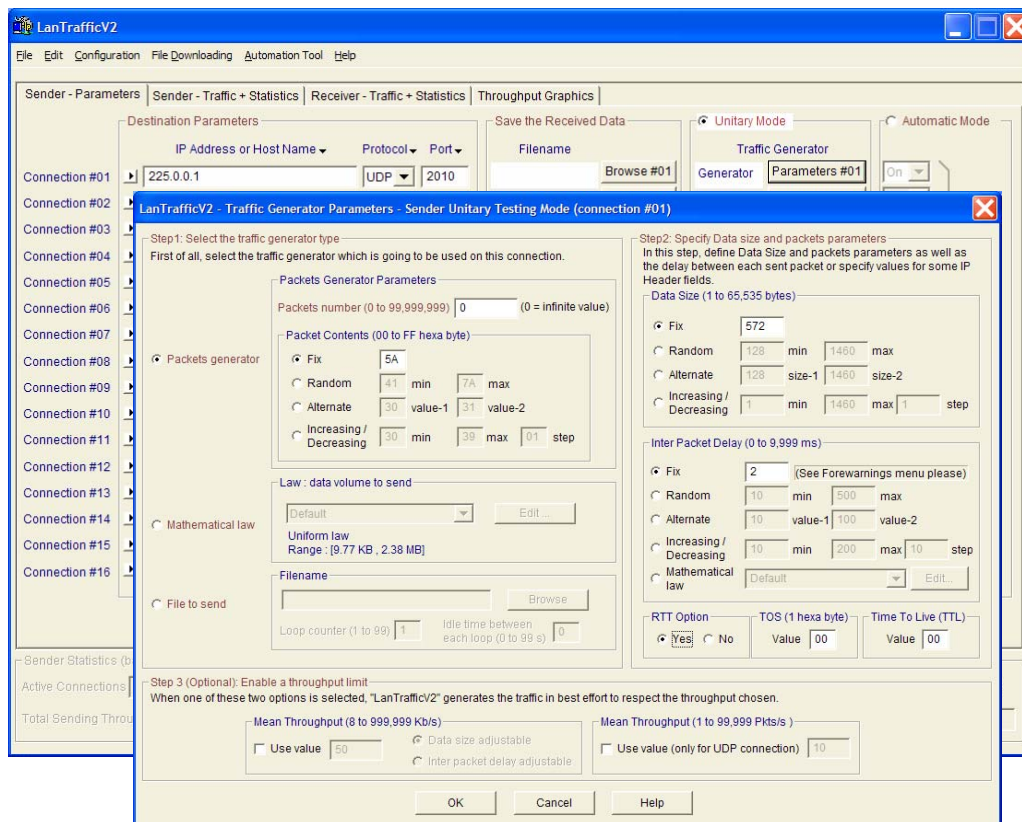


Just select the IP multicast address 225.0.0.1, port number (2010) and UDP as protocol. The Receiver mode should be 'Absorber' because multicast traffic is unidirectional by nature. To start Receivers, click the 'Start Receiving Traffic' button on both PCs.

## 8.5.2 PC #1 parameters

PC #1 is used as the Sender.

Start "LanTraffic V2" and select the "Sender – Parameters" tab.



Assuming the connection #01 is selected and then enter the IP address '225.0.0.1'. Then select the port number as PC #2 and PC #3 (2010) and the UDP protocol. Press the 'Parameters #01' button to set traffic generator parameters. Enter the packet number and the packet size and the inter-packet delay: 2 in this example.

To start the Sender, select the 'Sender – Traffic + Statistics' tab and press the 'Start #01' button.

If the hub does not filter multicast traffic and if your NICs accept the multicast address selection, PC #2 and PC #3 should receive the same number of packets (the number sent by PC #1).

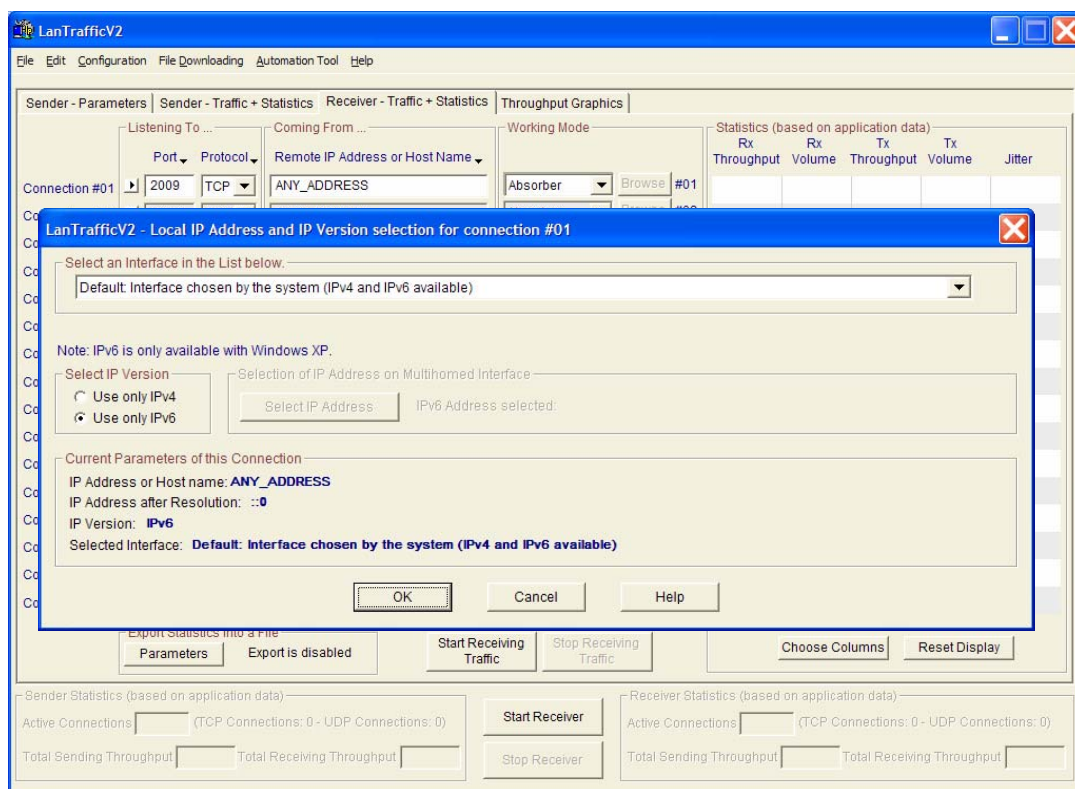
## 8.6 IPV6 connection

To check the IPv6 throughput between two PCs, you may use a crossed-cable as shown in the next figure or a switch.



### 8.6.1 PC #2 parameters

Start "LanTrafficV2" on PC #2 and select the "Receiver - Traffic + Statistics" tab. Click on the black arrow to select IP version 6 for the connection #01.



To select IPv6, you don't need to select an interface from the "Receiver – Traffic + Statistics" tab.

You may check parameters using the black arrow tooltip by moving the mouse over the arrow of the connection #01.



	Listening To ...	Coming From ...	Working
	Port	Protocol	Remote IP Address or Host Name
Connection #01	2009	TCP	ANY_ADDRESS
Connection #02	Click to select the network interface and IP Version to use with the connection #01		
Connection #03	Connection #01		
Connection #04	IP Address or Host Name: ANY_ADDRESS		
Connection #05	IP Address after resolution: ::0		
	IP Version: IPv6		
	Selected Interface: Interface chosen by the system (IPv4 and IPv6 available)		

The screenshot shows the LanTrafficV2 application window. The 'Sender - Parameters' tab is active, displaying a list of 16 connections. Each connection is configured with Port 2009, TCP protocol, and Remote IP Address ANY\_ADDRESS. The 'Working Mode' column shows 'Echoer' for Connection #01 and 'Absorber' for the others. The 'Statistics' section on the right shows a table with columns for Rx Throughput, Rx Volume, Tx Throughput, Tx Volume, and Jitter. The 'Sender Statistics' and 'Receiver Statistics' sections at the bottom show active connections and throughput data.

Sender - Parameters		Receiver - Traffic + Statistics		Throughput Graphics		Statistics (based on application data)				
Listening To ...	Coming From ...	Working Mode				Rx Throughput	Rx Volume	Tx Throughput	Tx Volume	Jitter
Connection #01	2009 TCP ANY_ADDRESS	Echoer	Browse	#01						
Connection #02	2009 TCP ANY_ADDRESS	Absorber	Browse	#02						
Connection #03	2009 TCP ANY_ADDRESS	Absorber	Browse	#03						
Connection #04	2009 TCP ANY_ADDRESS	Absorber	Browse	#04						
Connection #05	2009 TCP ANY_ADDRESS	Absorber	Browse	#05						
Connection #06	2009 TCP ANY_ADDRESS	Absorber	Browse	#06						
Connection #07	2009 TCP ANY_ADDRESS	Absorber	Browse	#07						
Connection #08	2009 TCP ANY_ADDRESS	Absorber	Browse	#08						
Connection #09	2009 TCP ANY_ADDRESS	Absorber	Browse	#09						
Connection #10	2009 TCP ANY_ADDRESS	Absorber	Browse	#10						
Connection #11	2009 TCP ANY_ADDRESS	Absorber	Browse	#11						
Connection #12	2009 TCP ANY_ADDRESS	Absorber	Browse	#12						
Connection #13	2009 TCP ANY_ADDRESS	Absorber	Browse	#13						
Connection #14	2009 TCP ANY_ADDRESS	Absorber	Browse	#14						
Connection #15	2009 TCP ANY_ADDRESS	Absorber	Browse	#15						
Connection #16	2009 TCP ANY_ADDRESS	Absorber	Browse	#16						

Export Statistics into a File: Parameters Export is disabled

Start Receiving Traffic Stop Receiving Traffic

Choose Columns Reset Display

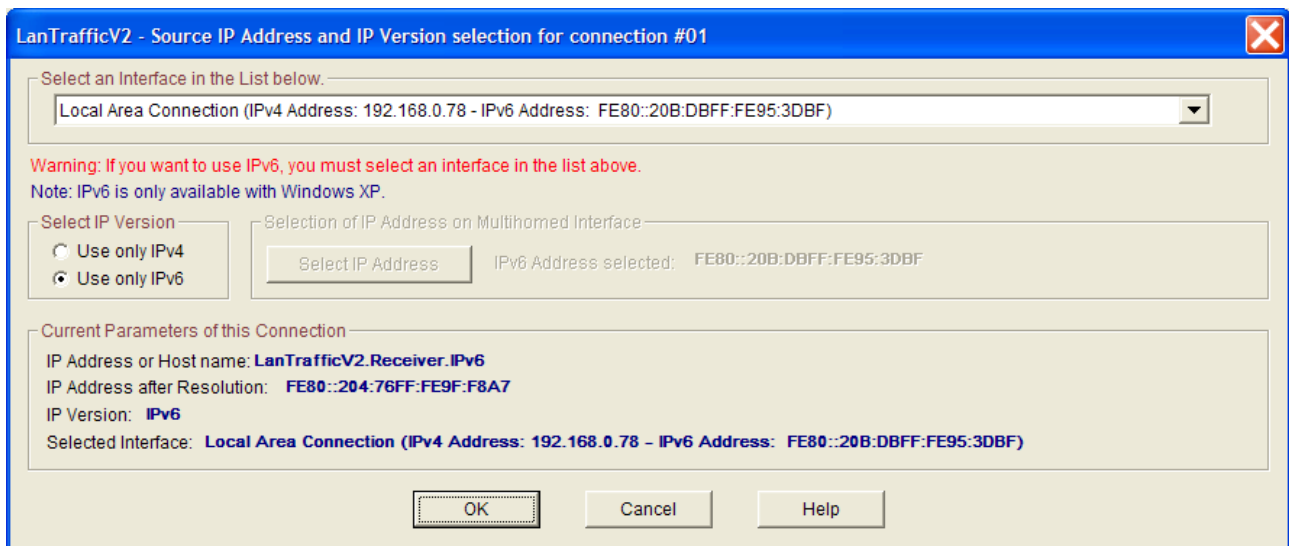
Sender Statistics (based on application data): Active Connections: 0 (TCP Connections: 0 - UDP Connections: 0) Total Sending Throughput: Total Receiving Throughput:

Receiver Statistics (based on application data): Active Connections: 0 (TCP Connections: 0 - UDP Connections: 0) Total Sending Throughput: 0.00 b/s Total Receiving Throughput: 0.00 b/s

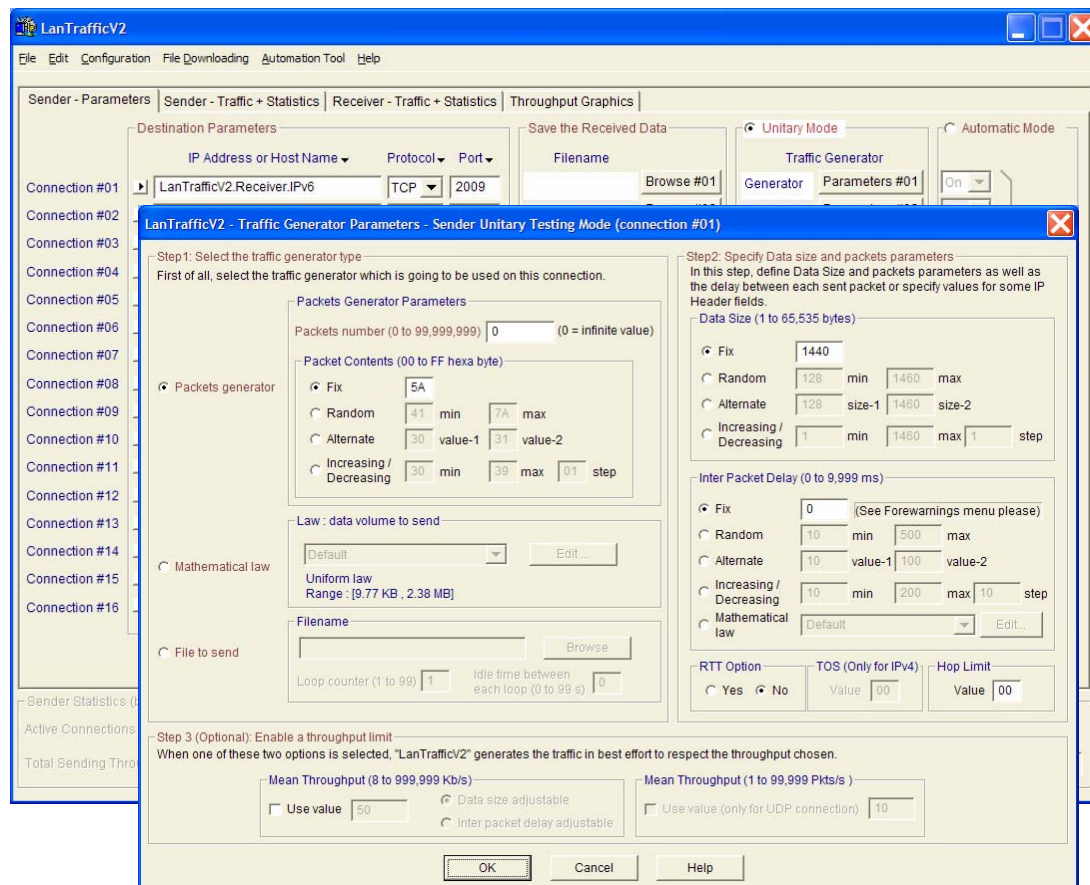
Assuming the connection #01 will be used, enter the IP address ANY\_ADDRESS, the port number here is arbitrary selected to 2009. Select the TCP protocol and the receiving working mode to 'Echoer'. The echoer mode is useful to check full-duplex speed transfer. Start the Receiver by pressing the 'Start Receiving Traffic' button.

### 8.6.2 PC #1 parameters

Start "LanTraffic V2" on PC #1 and select the "Sender – Parameters" tab. The connection #01 will be used in this example. Change the IPv6 by clicking on the black arrow. For the Sender part, it is mandatory to select an Interface to select the IP version 6.

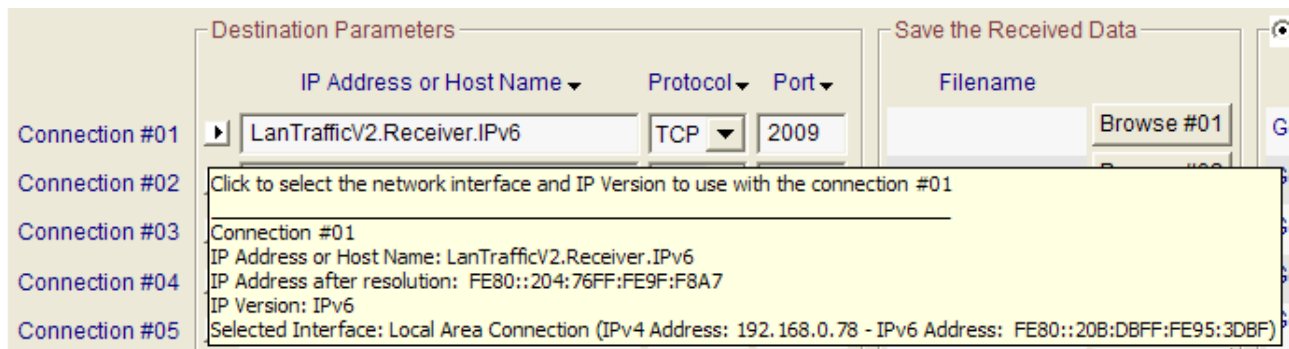


Then, enter a canonical IP address for PC #2, select the TCP protocol and enter the port number 2009 (same as PC #2). To change the traffic generator, click on the 'Parameters #01' button.



Select the unlimited packet number with 0 in the packet number field; the packet size is the best with 1440 bytes long. The inter-packet delay should be 0 for the maximum throughput.

The summary tooltip may be used to check the IP version parameters.



Then select the "Sender – Traffic + Statistics" tab and click on the 'Start #01' button.

The throughput columns for the PC #2 Sender and PC #1 Receiver will show the throughputs. Best throughput depends mainly on the CPU, memory and NIC quality. If PCs used are different, choose the most powerful PC as the Receiver.

## 8.7 Source/Local IP Address and Interface requirements

Some features of “LanTraffic V2” require selecting an Interface, a Source IP address (Sender) or a Local IP address (Receiver).

Interface selection is required in the following cases:

“LanTraffic V2” acting as:	Sender		Receiver	
IP Version	IPv4	IPv6	IPv4	IPv6
<b>Unicast exchange</b>	<i>Interface selection not required</i>	<b>Interface selection required</b>	<i>Interface selection not required</i>	<i>Interface selection not required</i>
<b>Multicast exchange</b>	<i>Interface selection not required</i>	<b>Interface selection required</b>	<i>Interface selection not required</i>	<b>Interface selection required</b>

### Consequences when an Interface is selected

For the **“LanTraffic V2” Sender**, selection of an Interface implies that a source address is fixed with the following consequences:

1. Every packet sent gets the Source IP address selected as source IP address, whatever the destination is.
2. Destination addresses should match the network mask and scope associated to the selected source IP address.
3. When IP address resolution is involved, DNS should be configured for this interface and this/these DNS should be able to resolve the addresses entered.

#### Examples:

- Source IP Address 192.168.0.23 with 255.255.255.0 as network mask and no gateway. Destination IP Addresses matching are: 192.168.0.X with X between 1 and 255.
- Source IP Address 192.168.0.23 with 255.255.255.0 as network mask and no gateway. DNS 192.168.1.1 cannot be reached. IP address resolution is not available: canonical addresses are invalid, except the ones defined in the local HOSTS file. Destination IP Addresses matching are: 192.168.0.X with X between 1 and 255.

For the **“LanTraffic V2” Receiver**, selection of an Interface implies that a local address is fixed with the following consequences:

1. The TCP/IP stack compares every packet received to the local IP address and its network mask, whatever the source is. Packets matching are the only ones sent to the relevant connection of “LanTraffic V2”.
2. When IP address resolution is involved, DNS should be configured for this interface and this/these DNS should be able to resolve the addresses entered.



3. When Echoer or Absorber/Generator modes are selected, the return IP address or Host name should match the network mask and scope associated to the selected source IP address.

Examples:

- Local IP Address 192.168.0.23 with 255.255.255.0 as network mask and no gateway. Packets with Destination IP Addresses matching are: 192.168.0.X with X between 1 and 255.
- Local IP Address 192.168.0.23 with 255.255.255.0 as network mask and no gateway. Packets with source IP address 192.168.1.1 cannot reach this connection. It is no sense to define a source IP address out of the local IP addresses range.
- Local IP Address 192.168.0.23 with 255.255.255.0 as network mask and no gateway. When Echoer or Absorber/Generator modes are selected, packets are sent back only to the Destination IP Addresses matching 192.168.0.X with X between 1 and 255.

## PART 9 Annexes

### 9.1 Mathematical laws used by "LanTraffic V2"

"LanTraffic V2" application is based on the use of laws of random number generation to determine starting time connection and data volume to send. Three mathematical laws are available. Uniform and Exponential laws are used for starting time connection and data volume. Pareto's law is only used for data volume.

The mathematical laws are used:

- ⇒ for the unitary mode when mathematical law data source is selected. In this case, only data volume laws are available.
- ⇒ for the automatic mode: to define the starting time connection generation and data volumes laws.

Hereafter is a detailed presentation of each mathematical law.

#### 9.1.1 Uniform law

- *Presentation*

This law is available for starting time connections generation and data volume to send.

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

With Uniform law, unit used is millisecond for starting time connection generation laws and byte for data volume to send laws.

- *Mathematical function*

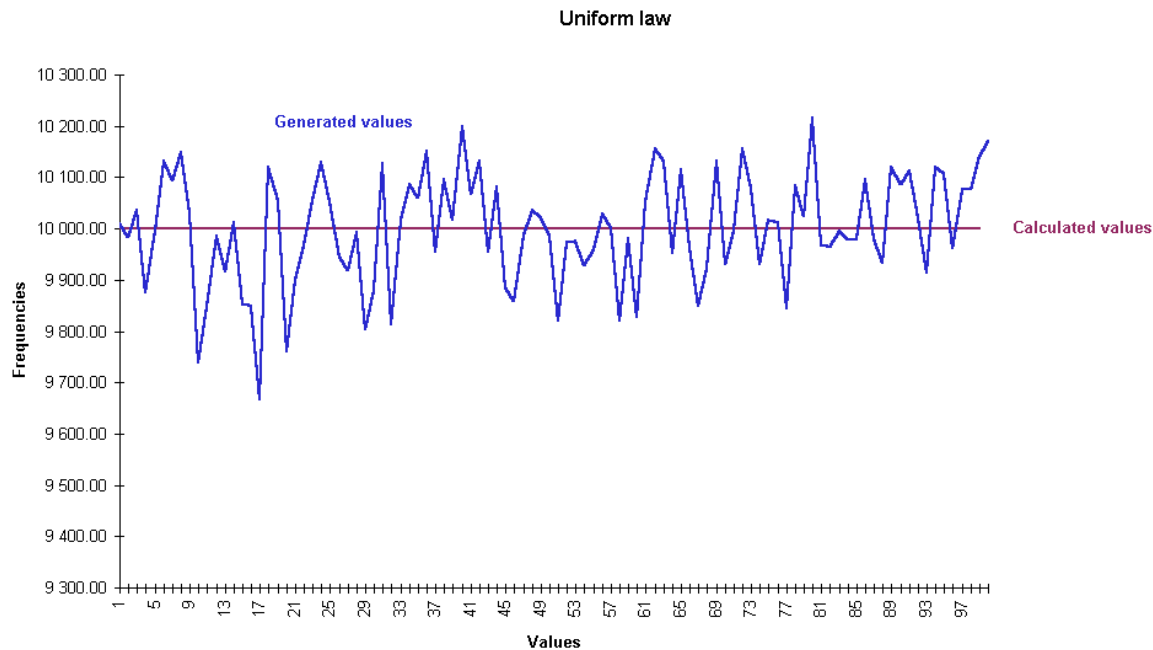
Uniform law on  $(\alpha, \beta)$  range

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

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

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

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



### 9.1.2 Exponential law

- *Presentation*

This law is available for starting time connections generations and data volume to send.

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

Unit is millisecond for starting time connection's generation laws and byte for data volume laws.

- *Mathematical function*

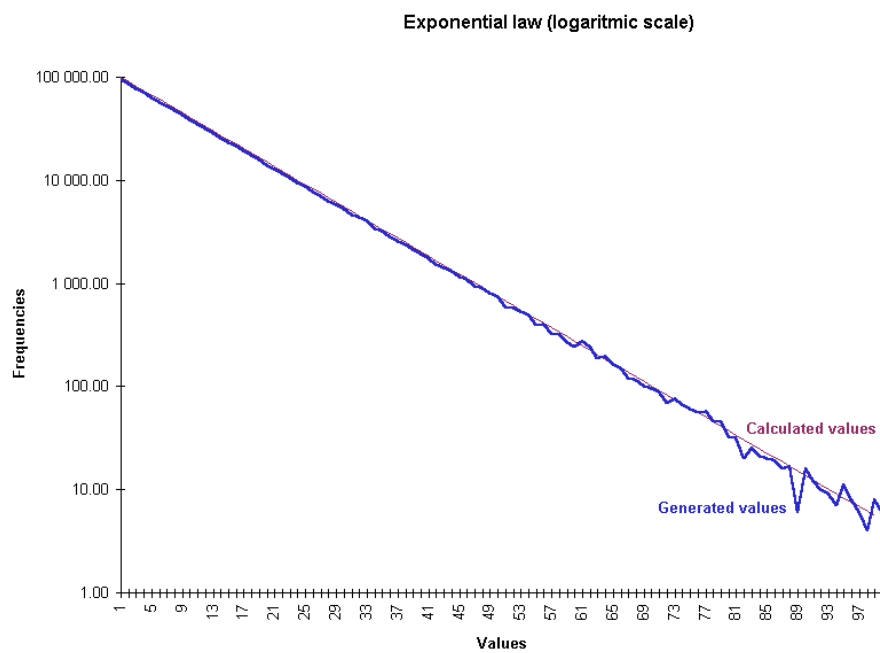
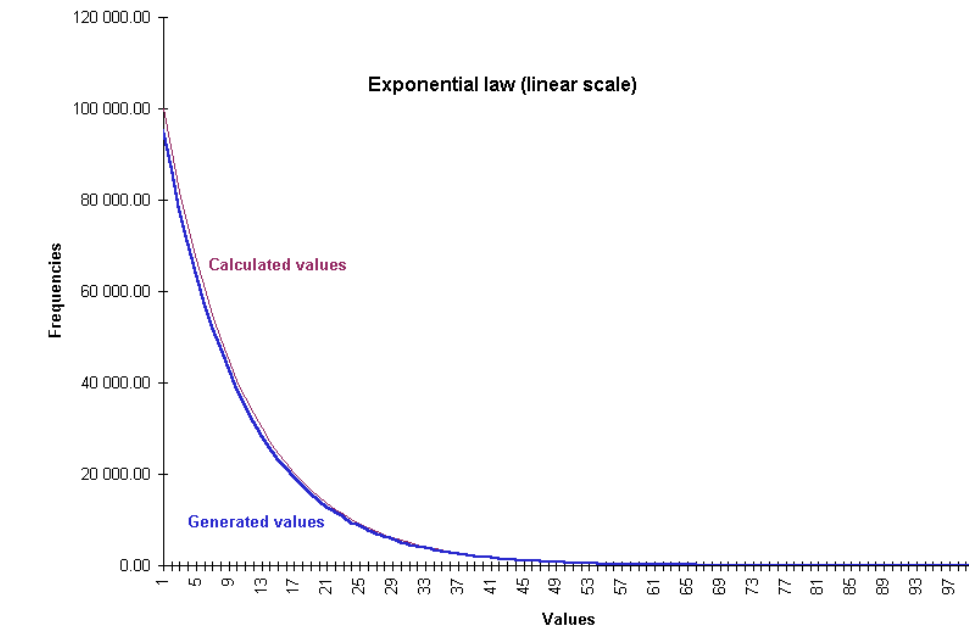
Exponential law ( $\lambda > 0$ )

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

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

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

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



❖ *Exponential law- Table of generated values:*

Values	Starting time laws results	Data volume laws results
$\lambda = 1$	10 ms	10 bytes
$\lambda = 0,1$	100 ms	100 bytes
$\lambda = 0,01$	1 s	1 Kbytes
$\lambda = 0,001$	10 s	10 Kbytes
$\lambda = 0,0001$	1mn 43	100 Kbytes
$\lambda = 0,00001$	17mn 19	1 Mbytes
$\lambda = 0,000001$	2h 53	10 Mbytes
Precision limit for $\lambda$		

### 9.1.3 Pareto Law

- *Presentation*

This mathematical law is available only for data volume generation in unitary and automatic testing mode.

Pareto's law is based on two parameters:  $a$  and  $\beta$ .  $a$  unit is the final unit of the volume.  $\beta$  does not have unit because it represents a coefficient of variation of result around the  $a$  value.

The following values have been noticed:

$\beta = 1000$	Result very near to $a$
$\beta = 100$	Result very near to $a$
$\beta = 15$	Result between the interval $[a, a \times 2]$ (estimation)
$\beta = 1$	Result between the interval $[a, \beta]$ , $\beta$ is very high ( $a \times 1000000$ )
$\beta = 0,1$	Result too high – Calculation bursting.

Pareto's law offers the advantage to generate a result statically very near to  $a$ , but it can generate in some exceptional cases a number very far from  $a$ .

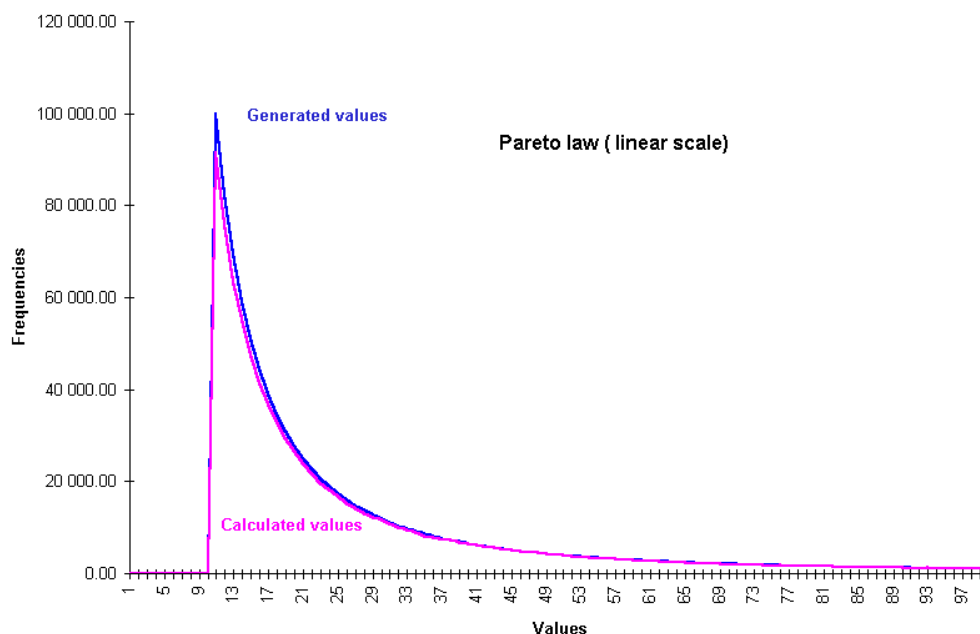
- *Mathematical function*

Pareto law ( $a, \beta \geq 0$ )

$$f(x) = \beta a^\beta x^{-\beta-1} \quad \text{if } x \geq a$$

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

- *Pareto Law - example of generated values for  $1000000\beta a^\beta x^{-\beta-1}$  with:  $a = 10$  and  $\beta = 1$ .*



## 9.1.4 Gauss law

- *Presentation*

The Gauss law has two parameters:  $\mu$  (average) and  $\sigma$  (standard deviation).

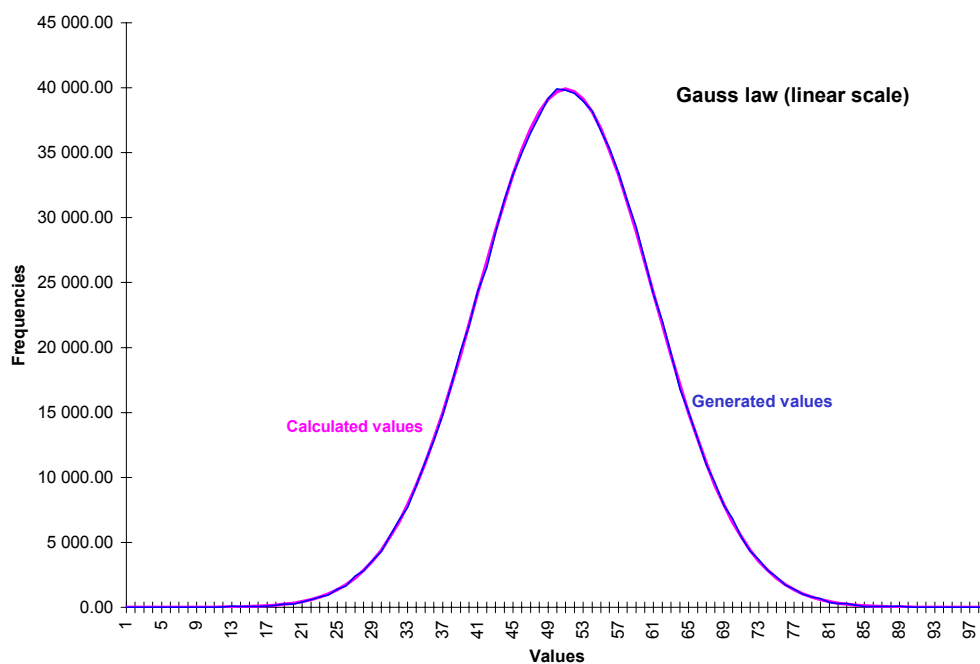
With this law, unit used is millisecond for starting time connection generation laws and byte for data volume to send laws.

- *Mathematical function*

Gauss law on  $(-\infty, +\infty)$  range

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad \text{for } x \in \mathbb{R}, \text{ with average } \mu \text{ and variance } \sigma^2$$

- *Gauss law - example of generated values with:  $\mu = 50$  and  $\sigma = 10$*



## 9.2 “LanTraffic V2” Traces

In case of problem when using “LanTraffic V2”, the trace functionality allows to retrieve in a file or in a debug window, information regarding Winsock exchanges made by “LanTraffic V2”.

Traces activation is done by modifying directly in the registry database of Windows, the value of *DEBUGLEVEL* in the key [\\HKEY\\_LOCAL\\_MACHINE\\SOFTWARE\\LanTrafficV2](#)

*DEBUGFILENAME* parameter defines the name for the file receiving traces.  
You must reset manually content of this file to avoid disk space wasting.

If the *DEBUGFILENAME* parameter is not selected (empty chain), traces are sent to the debug standard output -via OutputDebugString – for use with an external trace tool (e.g. ‘Softlce’ or the Microsoft Development environment).



**“LanTraffic V2” application must be restarted after “DebugLevel” or “DebugFileName” parameter modification.**

## 9.3 “LanTraffic V2” configuration parameters saved in the registry

The based key to access parameters is \\HKEY\_LOCAL\_MACHINE\\SOFTWARE\\LanTrafficV2. Updated information about Registry is available in the file “Version.txt” delivered with the “LanTraffic V2” software.

General parameters may be changed by the user to configure “LanTraffic V2” to the local environment or to specific needs.



**Parameters associated to the help should not be changed without express recommendation from ZTI Support to avoid help unusable.**

### 9.3.1 General configuration parameters

Key name	Type	Default value	Description
<i>AutomatonDebugFilename</i>	REG_SZ	AUT_DEBUG.LOG	User defined.
<i>AutomatonDebugLevel</i>	REG_DWORD	0x0	0x00000001 Errors 0x00000100 Addition of the current time 0x00010000 Put Debug information into the file defined by <i>AutomatonDebugFileName</i>
<i>AutomatonPath</i>	REG_SZ	<i>Installation dependent</i>	Full path name to the location of the automation tool used by “LanTraffic V2”.
<i>DebugFileName</i>	REG_SZ	LTV2_DEBUG.LOG	User defined
<i>DebugLevel</i>	REG_DWORD	0x0	0x00000001 Errors 0x00000002 Important information 0x00000010 Winsock return codes (partial) 0x00000020 Trace Receiver statistics (inter-packet delay in reception & time used to send when echoing) 0x00000100 Addition of the current time 0x00000200 Addition of Statistics 0x00001000 Verbose information 0x00010000 Put Debug information into the file defined by <i>DebugFileName</i>

Key name	Type	Default value	Description
<i>LTV2PATH</i>	REG_SZ	<i>Installation dependent</i>	Full path name to the location of "LanTraffic V2" used by the automation tool.
<i>SendTimeOut</i>	REG_DWORD	10	number of seconds for Winsock2 to send data. <b>Required for the Echoer mode</b>
<i>TCPConnectRetryCounter</i>	REG_DWORD	0x1	Number of retry to establish a TCP connection
<i>TCPInactivity</i>	REG_DWORD	5	TCP Inactivity tempo (seconds). The receiver stops the connection if no data is received during this time.
<i>TCPNoDelay</i>	REG_DWORD	0x0	0x0 : Nagle algorithm enabled Other value: Nagle algorithm disabled
<i>TCPReceiverPacketSize</i>	REG_DWORD	8192	Defines the packet size provided to Winsock2 WSARecv function call in bytes.
<i>UDPInactivity</i>	REG_DWORD	5	UDP Inactivity tempo (seconds). In the Receiver tab, the Generator of the Absorber/Generator connection stops when no data is received during this time.



**"LanTraffic V2" application must be restarted after each modification of these parameters.**

### 9.3.2 Help configuration parameters



**These parameters are for information only.  
They should not be changed without express recommendation from ZTI support.**

Key name	Type	Description
ACROREADINFO	REG_SZ	Reserved
ACROREADTIMER	REG_DWORD	Reserved
HELP-AUTOMATICPARAM	REG_DWORD	Reserved
HELP-EDIT-LAWS-AUTOMATIC-STARTING	REG_DWORD	Reserved
HELP-EDIT-LAWS-AUTOMATIC-VOLUME	REG_DWORD	Reserved
HELP-EDIT-LAWS-UNITARY-VOLUME	REG_DWORD	Reserved
HELP-EXPORTSTATS-SENDER	REG_DWORD	Reserved
HELP-EXPORTSTATS-RECEIVER	REG_DWORD	Reserved
HELP-FILEDOWNLOADING	REG_DWORD	Reserved
HELP-MENU	REG_DWORD	Reserved
HELP-PARAMCNX-SENDER	REG_DWORD	Reserved
HELP-PARAMCNX-RECEIVER	REG_DWORD	Reserved
HELP-THROUGHPUT	REG_DWORD	Reserved
HELP-UNITARYPARAM	REG_DWORD	Reserved



## 9.4 Default values of a context

The default values when opening a new context are:

- Sender - Parameters**

<b>Interface:</b>	Interface chosen by the system		
<b>IP version:</b>	IPv4		
<b>IP address:</b>	NO_ADDRESS		
<b>Port Number:</b>	2009		
<b>Protocol:</b>	TCP		
<b>Testing mode:</b>	Unitary Mode	<b>Data source:</b>	Packet generator (number of packets: infinite, packet contents: fix = 5A)
		<b>Packets size:</b>	Fix = 1460 bytes
		<b>Inter Packet Delay:</b>	Fix = 20 ms
		<b>RTT option:</b>	No
		<b>TOS value:</b>	0
		<b>TTL value:</b>	0

- Sender – Traffic + Statistics**

<b>Columns for the statistics</b>	Tx Throughput Tx Volume Tx Packets Rx Throughput Rx Volume Rx Packets Jitter
<b>Clear on Stop:</b>	Unchecked
<b>Export Statistics into a File:</b>	Export is disabled
<b>Maximum size:</b>	10 MB

- Receiver - Traffic + Statistics**

<b>Interface:</b>	Interface chosen by the system
<b>IP version:</b>	IPv4
<b>IP address:</b>	ANY_ADDRESS
<b>Port number:</b>	2009
<b>Protocol:</b>	TCP
<b>Working Mode:</b>	Absorber
<b>Columns for the statistics</b>	Rx Throughput Rx Volume Tx Throughput Tx Volume Jitter
<b>Export Statistics into a File:</b>	Export is disabled
<b>Maximum size:</b>	10 MB

- Throughput Graphics**

<b>Refresh time for graphic display:</b>	2 sec
<b>Physical Link Throughput:</b>	10 Mb/s

- Configuration

<b>General Parameters</b>	
<b>Refresh time:</b>	2 sec
<b>Throughput sampling period:</b>	5 sec
<b>Timeout for TCP packets echoed:</b>	500 ms
<b>Timeout for UDP packets echoed:</b>	700 ms
LanTraffic V2 Buffer size	
<b>Receive buffer size:</b>	8192
<b>Transmit buffer size:</b>	8192

<b>AutoComplete ...</b>	Enable
-------------------------	--------

- File transfer

<b>Port number:</b>	2500
---------------------	------

- Sender and Receiver statistics file

<b>Maximum size:</b>	10 MB
----------------------	-------

- Data volume mathematical laws

<i>Name</i>	<i>Type</i>	<i>Parameters</i>	<i>Range</i>
<b>Default</b>	Uniform	Alpha = 10,000 Beta = 2,500,000	[9.77 KB, 2.38 MB]
<b>Small Volume</b>	Uniform	Alpha = 5,000,000 Beta = 10,000,000	[4.77 KB, 9.54 MB]
<b>High Volume</b>	Uniform	Alpha = 110,000,000 Beta = 1,050,000,000	[105 MB, 0.98 GB]
<b>Variable</b>	Uniform	Alpha = 11,000,000 Beta = 950,000,000,000	[10.5 MB, 885 GB]

- Starting time mathematical laws

<i>Name</i>	<i>Type</i>	<i>Parameters</i>	<i>Range</i>
<b>Default</b>	Uniform	Alpha = 20 Beta = 50	[20 ms, 50 ms]
<b>Close connection law</b>	Uniform	Alpha = 100 Beta = 200	[100 ms, 200 ms]
<b>Far off connection law</b>	Uniform	Alpha = 10,000 Beta = 20,000	[10 s, 20 s]
<b>Variable connection law</b>	Uniform	Alpha = 1 Beta = 100,000	[1 ms, 1 mn 40s]