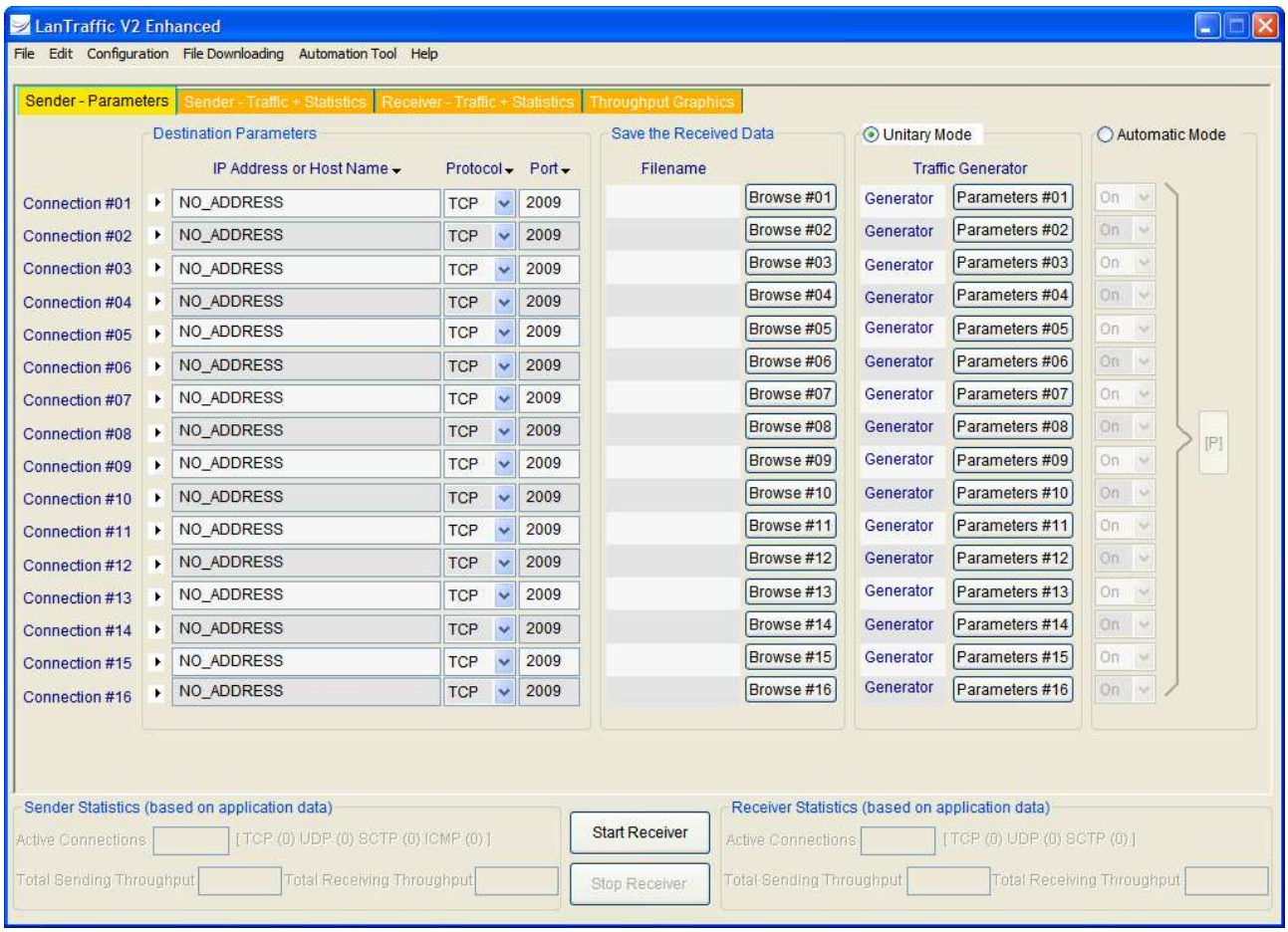
LanTraffic V2 Enhanced

Version 2.7

Traffic Generator for IP Networks (IPv4 & IPv6)

FTTx, LAN, MAN, WAN, WLAN, WWAN, Mobile, Satellite, PLC, etc.

Designed for Windows x64 platforms and 10Gbps Ethernet



User Guide

ZTI / 1 boulevard d'Armor / BP 20254 / 22302 Lannion Cedex / France
Phone: +33 2 9648 4343 / Fax: +33 2 9648 1485
Email: contact@zti-telecom.com / Web: www.zti-telecom.com

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

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

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

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

To contact us:

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

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

Software License Agreement

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

- **COPYRIGHT**

The enclosed Software and documentation (here after called the Products) remains the property of ZTI.
French copyright laws and international treaties protect 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 the hard disk of your system accordingly with the software protection described in the next paragraph.
- Make one backup copy of the software, provided that this copy is not used or install on any computer.
- Use the product properly and on the following 64-bit Windows platforms only: Windows Vista, Windows Server 2003, Seven or Server 2008.

In accordance with copyright and patent laws, the License 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**

LanTraffic V2 Enhanced with its add-ons is licensed on a workstation basis. You will need to purchase a separate license for each machine that you install it on. Each licensed copy of the software installed on a workstation has:

- a unique USB Software Protection Key to be plugged to run the software.

- **LIMITED WARRANTY**

The software is supplied without any express or implied warranty regarding the performances or results obtained by the use of the Products.
ZTI warrants that the software media (i.e. CD-ROM) will be free of material defects for a ninety (90) days period following 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 only remedy is the replacement of the media software. In no event, ZTI will be liable for any kind of direct or indirect damages caused by the Products.

- **COURT OF LAW**

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

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

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

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

Table of Contents

Part 0 Preface 8

0.1 Organization of this guide 8

0.2 Minimum System Requirements 9

0.3 References 9

0.4 Terms used in this document 10

0.5 Technical Support 10

Part 1 Overview 11

1.1 LanTraffic V2 Enhanced Key Features 11

1.2 The Automation Tool for LanTraffic V2 Enhanced 16

Part 2 Install LanTraffic V2 Enhanced 17

2.1 How to install the software downloaded from the Internet 17

2.2 How to install the software from the CD-ROM 17

2.3 During the installation 18

2.3.1 64-bit version required 18

2.3.2 Choose the LanTraffic V2 Enhanced package to install 19

2.3.3 LanTraffic V2 Enhanced packages in a few words 19

2.3.4 Which package should I install? 20

2.3.4.1 I want to evaluate LanTraffic V2 Enhanced 20

2.3.4.2 I already use LanTraffic V2 Enhanced … 20

2.3.4.2.1 … and I want to upgrade and keep my permanent license (installed with a previous 32-bit version) 20

2.3.4.2.2 … and I want to upgrade and use the USB Software Protection Key I bought 20

2.3.4.3 I just bought LanTraffic V2 Enhanced … 20

2.3.4.3.1 … and I received the CDROM & USB Software Protection Key 20

2.3.4.3.2 … and I will receive the CDROM & USB Software Protection Key in a few days. 20

2.4 What has been installed on my computer? 21

2.5 How to reinstall another package? 22

2.6 How to transfer the software to another computer? 22

Part 3 How to handle your license 23

3.1 LanTraffic V2 Enhanced Trial 23

3.1.1 LanTraffic V2 Enhanced License Information window 23

3.1.2 End of the fifteen-day trial period 23

3.2 LanTraffic V2 Enhanced & USB Software Protection Key 24

Part 4 Uninstall LanTraffic V2 Enhanced 25

Part 5 LanTraffic V2 Enhanced Getting Started 26

Part 6 Run LanTraffic V2 Enhanced 30

Part 7 LanTraffic V2 Enhanced and Windows Firewall 31

7.1 How to authorize TCP and UDP connections with Windows Firewall 31

7.2 How to authorize UDP and TCP connections with Windows Firewall 32

7.3 How to authorize ICMPv4 and ICMPv6 traffic with Windows Firewall 33

Part 8 Graphical User Interface 34

8.1 Main Window 34

8.2 Display general rules of the Graphical User Interface 35

8.3 Used units for the information display 36
8.3.1 Volume units 37
8.3.1.1 Volume kB Unit 37
8.3.1.2 Volume KiB Unit 37
8.3.2 Throughput units 37
8.3.2.1 Throughput kb/s Unit 37
8.3.2.2 Throughput Kib/s Unit 37

Part 9 Using LanTraffic V2 Enhanced 39

9.1 Main steps 39

9.2 Menu description 40
9.2.1 File menu 40
9.2.1.1 File/New 40
9.2.1.2 File/Open 40
9.2.1.3 File/Save 40
9.2.1.4 File/Save as … 40
9.2.1.5 File/Recent Contexts … 40
9.2.1.6 File/Exit 41
9.2.2 Edit menu 41
9.2.2.1 Edit/Destination Parameters: IP Address or Host Name (for Sender) 41
9.2.2.2 Edit/Destination Parameters: Protocol (for Sender) 41
9.2.2.3 Edit/Destination Parameters: Port (for Sender) 41
9.2.2.4 Edit/Listening To: Port (for Receiver) 42
9.2.2.5 Edit/Listening To: Protocol (for Receiver) 42
9.2.2.6 Edit/Coming From: Remote IP Address or Host Name (for Receiver) 42
9.2.3 Configuration menu 43
9.2.3.1 Configuration/Stack Parameters 43
9.2.3.2 Configuration/General Parameters 44
9.2.3.3 Configuration/AutoComplete … 46
9.2.4 File Downloading menu 47
9.2.5 Automation Tool menu 50
9.2.5.1 Automation Tool/Automation Tool, what for?… 50
9.2.5.2 Automation Tool/Open… 50
9.2.5.3 Automation Tool/Close 50
9.2.5.4 Automation Tool/Bring to the top 50
9.2.6 Help menu 51
9.2.6.1 Help/Help 51
9.2.6.2 Help/Forewarnings … 51
9.2.6.2.1 Inter packet delay 51
9.2.6.2.2 Echoer modes 51
9.2.6.2.3 UDP connections 51
9.2.6.3 Help/Getting Started (IPv4) 52
9.2.6.4 Help/About LanTraffic V2 Enhanced 52

9.3 Total statistics 53
9.3.1 Sender statistics 53
9.3.2 Receiver statistics 53

9.4 The Sender part 54
9.4.1 Sender - Parameters tab 54
9.4.1.1 Destination parameters 55
9.4.1.1.1 Summary of connection parameters 55
9.4.1.1.2 Select the network interface, IP version and source IP address 56
9.4.1.1.3 IP Address translation mechanism 58
9.4.1.1.4 Duplicate parameters of a connection onto others 58
9.4.1.1.5 IP address floating menu 59
9.4.1.1.6 Protocol floating menu 59
9.4.1.1.7 Port floating menu 60
9.4.1.2 Save the Received Data (except for ICMP connections) 60
9.4.1.3 Configure the Unitary Mode for TCP and/or UDP 61
9.4.1.3.1 Step 1: select the traffic generator type for this connection 62
9.4.1.3.1.1 Packets Generator 62
9.4.1.3.1.2 Mathematical law 63

9.4.1.3.1.3 File to send 68
9.4.1.3.2 Step 2: Specify data size and packets parameters 68
9.4.1.3.2.1 Data Size 68
9.4.1.3.2.2 Inter Packet Delay 69
9.4.1.3.2.3 RTT option 69
9.4.1.3.2.4 The DSCP field (with IPv4 only) 70
9.4.1.3.2.5 The TTL field 71
9.4.1.3.3 Step 3 (optional): Activate a throughput limit 71
9.4.1.4 Configure the Unitary Mode for ICMP connections 72
9.4.1.5 Configure the Automatic Mode 73
9.4.1.5.1 Starting time connections generation laws 74
9.4.1.5.2 Data volume to send laws 78
9.4.1.5.3 Packet Size 79
9.4.2 Sender - Traffic + Statistics tab 80
9.4.2.1 Destination Parameters 80
9.4.2.2 Sender Statistics 81
9.4.2.3 Export Statistics into a File 83
9.4.2.3.1 Sender statistics file format 84
9.4.2.3.2 Export Sender file sample 85
9.4.2.4 Run the Unitary Mode 86
9.4.2.5 Run the Automatic Mode 88

9.5 The Receiver part 89
9.5.1 Duplicate parameters of a connection onto others 89
9.5.2 Listening To … 90
9.5.2.1 Summary of the connection parameters 90
9.5.2.2 Select the network interface, IP version and local IP address 91
9.5.2.3 Port floating menu 93
9.5.2.4 Protocol floating menu 94
9.5.3 Coming From … 94
9.5.3.1 IP address floating menu 94
9.5.3.2 IP Address translation mechanism 95
9.5.4 Working Mode 96
9.5.4.1 Absorber mode 96
9.5.4.2 Absorber File mode 96
9.5.4.3 Echoer mode (with TCP and UDP only) 96
9.5.4.4 Echoer File mode (with TCP and UDP only) 96
9.5.4.5 Generator mode (with TCP and UDP only) 97
9.5.4.6 Disable mode 97
9.5.5 Statistics 98
9.5.6 Export Statistics into a File 101
9.5.6.1 Receiver statistics file format 102
9.5.6.2 Export Receiver file sample 103

9.6 The Throughput Graphics tab 105
9.6.1 The Graphical Display object 106
9.6.2 The Display Configuration object 108

Part 10 Command Line Parameters 109

10.1 General rule 109

10.2 Commands available to start LanTrafficV2 109
10.2.1 Context filename 109
10.2.2 Starting the "LanTraffic V2 Enhanced" Receiver part 109
10.2.3 Starting the "LanTraffic V2 Enhanced" Sender part 109

10.3 Commands available when LanTrafficV2 is started 109
10.3.1 Stopping the "LanTraffic V2 Enhanced" Sender and Receiver parts 109
10.3.2 Unload the "LanTraffic V2 Enhanced" application 110

10.4 Command line samples 110

10.5 Error return code 110

Part 11 Source/Local IP Address and Interface requirements 111

Part 12 Appendix....112

12.1 Mathematical laws used by LanTraffic V2 Enhanced....112
12.1.1 Uniform law....112
12.1.2 Exponential law....113
12.1.3 Pareto Law....121
12.1.4 Laplace-Gauss law....122

12.2 LanTraffic V2 Enhanced Traces....123

12.3 LanTraffic V2 Enhanced configuration parameters saved in the Registry....123
12.3.1 General configuration parameters....123
12.3.2 Help configuration parameters....124
12.3.3 Unit configuration parameter....124

12.4 Default values of a context....125

12.5 LanTraffic V2 Enhanced features versus OS, protocols and IP versions....127

Part 0 Preface

0.1 Organization of this guide

This user guide is made to helping you to discover and use **LanTraffic V2 Enhanced**. It is organized as follows:

- **Part 1: Product Overview**

This part briefly describes the key features of the **LanTraffic V2 Enhanced** and **Automation Tool for LanTraffic V2 Enhanced**.

- **Part 2: Install LanTraffic V2 Enhanced**

Presents the product requirements, how to install the software downloaded from the Internet or from the CD-ROM, provides important information to upgrade from previous versions and explains how to choose the most suitable **LanTraffic V2 Enhanced** package.

- **Part 3: How to handle your license?**

Describes how to proceed for the license transfer

- **Part 4: Uninstall LanTraffic V2 Enhanced**

Explains how to uninstall the software.

- **Part 5: LanTraffic V2 Enhanced Getting Started**

New users can use this help as an introduction to **LanTraffic V2 Enhanced** and generate or receive traffic with the IPv4 protocol in a few clicks.

- **Part 6: Run LanTraffic V2 Enhanced**

Details how to run the software and configure the license if needed.

- **Part 7: LanTraffic V2 Enhanced / Windows Firewall**

Gives details about the way to configure the Windows firewall to authorize the use of **LanTraffic V2 Enhanced**.

- **Part 8: Graphical User Interface**

This part describes the main rules and principles of representation used by **LanTraffic V2 Enhanced** Graphical User Interface.

- **Part 9: Using LanTraffic V2 Enhanced**

How to use **LanTraffic V2 Enhanced**. This part includes menu and functionalities description. It is based on Windows and Tabs description. Each tab is presented separately.

- **Part 10: Command Line Parameters**

How to use a command line with parameters to start **LanTraffic V2 Enhanced**.

- **Part 11: Source/Local IP Address and Interface requirements**

Explains in which cases, the interface selection is mandatory.

- **Part 12: Appendix**

Provides additional information about the mathematical laws used by **LanTraffic V2 Enhanced**, **LanTraffic V2 Enhanced** traces, configuration parameters saved in the Registry database, the default values of a new context and a synthesis showing the availabilities of **LanTraffic V2 Enhanced** features regarding the OS, protocols and IP versions.

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

Warning

Zoom or Advice

Note or Remark

0.2 Minimum System Requirements

To appropriately operate **LanTraffic V2 Enhanced** you need the following minimum system requirements:

- 64-bit version of Windows Server 2003, Windows Server 2008, Windows Vista or Windows Seven
- Pentium processor with 512 MB memory
- 1024 x 768 display and DPI setting = Normal size (96 DPI)
- 20 MB free hard disk space

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

0.3 References

[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"

[RFC1889] "RTP: A Transport Protocol for Real-Time Application" explaining the jitter calculation.

[RFC 4960] "Stream Control Transmission Protocol"

0.4 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 Enhanced** displays the tooltip during 5 seconds.
Automation	Automation is an add-on scripting tool used to pilot automatically **LanTraffic V2 Enhanced**.

0.5 Technical Support

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

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

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

You can contact Technical Support by:

Email:	Send as many details as possible to support@zti-telecom.com or support@zti.fr
Fax:	Send as many details as possible to +33 2 9648 1485
Telephone:	support is available from 09:00 am to 06:00 pm (GMT Time +1 or +2), from Monday to Friday. Call +33 2 9648 4343

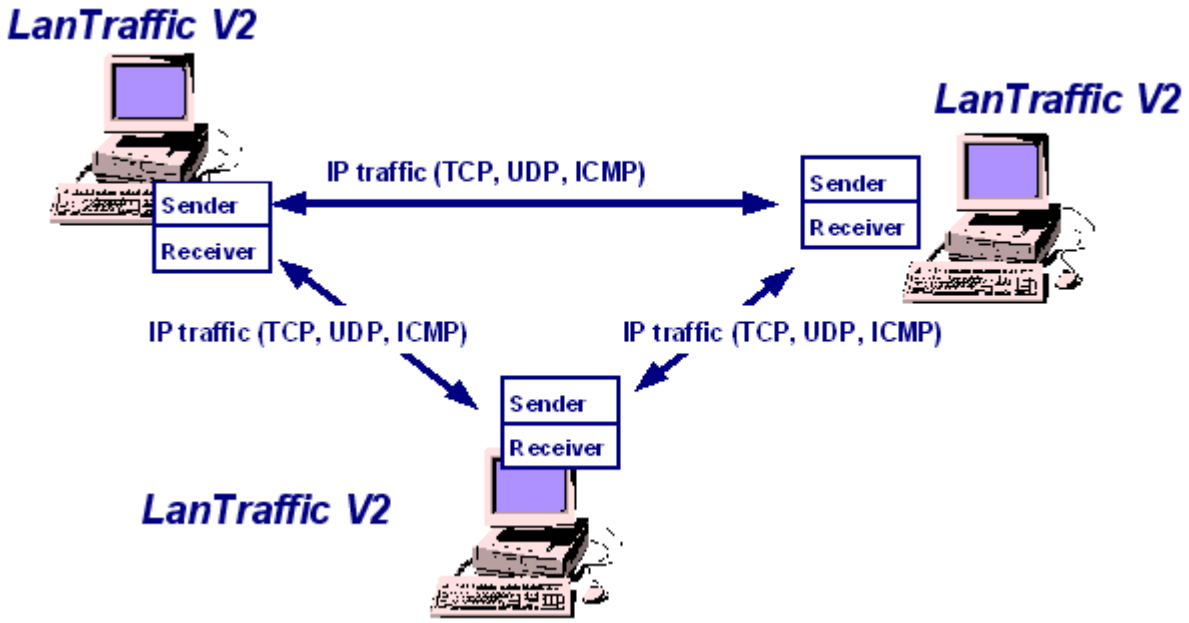
Part 1 Overview

1.1 LanTraffic V2 Enhanced Key Features

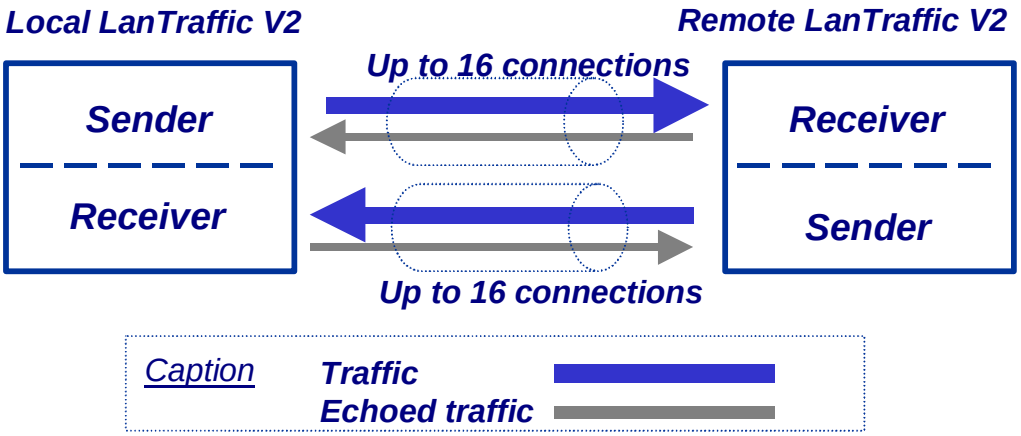
The **LanTraffic V2 Enhanced** software generates traffic for IP networks by using the following protocols: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol).

LanTraffic V2 Enhanced is supported on Windows 64-bit platforms: Windows Vista, Windows Server 2003, Seven or Server 2008. It needs at least one Ethernet connection (LAN or WLAN card i.e. NIC, remote access…).
The minimum screen resolution is 1024 x 768 and the DPI setting should be “Normal size (96 DPI)”.
LanTraffic V2 Enhanced requires Acrobat Reader to display the software's Help file.
The add-on software called **Automation Tool for LanTraffic V2 Enhanced** allows automating operations with **LanTraffic V2 Enhanced**. For instance, you can run test campaigns automatically.

Various testing configurations can be implemented using more than two PCs. **LanTraffic V2 Enhanced** creates TCP or UDP (Unicast, Multicast or Broadcast) connections between PCs through the IP network. **LanTraffic V2 Enhanced** creates also ICMP connections.



The **LanTraffic V2 Enhanced** testing tool is made of a **Sender** part and a **Receiver** part.



- The **Sender** generates up to 16 simultaneous UDP (Unicast, Multicast or Broadcast) and/or TCP connections and/or ICMP connections. The connections can be established in two different testing modes:

  Unitary Mode: you can select the traffic generator data source and configure packets size and inter packet delay for each connection. With the ICMP protocol you can:

  ⇨ ICMP Echo request packet number and content: packet generator (fixed, randomized, alternated and increasing / decreasing).

  ⇨ ICMP Echo Request data size: fixed, randomized, alternated and increasing / decreasing.

  ⇨ ICMP Echo Reply receiving timeout: fixed, randomized, alternated, increasing / decreasing or use of a mathematical law.

  LanTraffic V2 Enhanced 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.

  ⇨ ***Automatic Mode***: select one mathematical law for connections generating (up to 16 connections) and starting time, and then select a second mathematical law for data volume to be sent. This mode is available with UDP and TCP only. With this mode, ICMP connections can not be started.

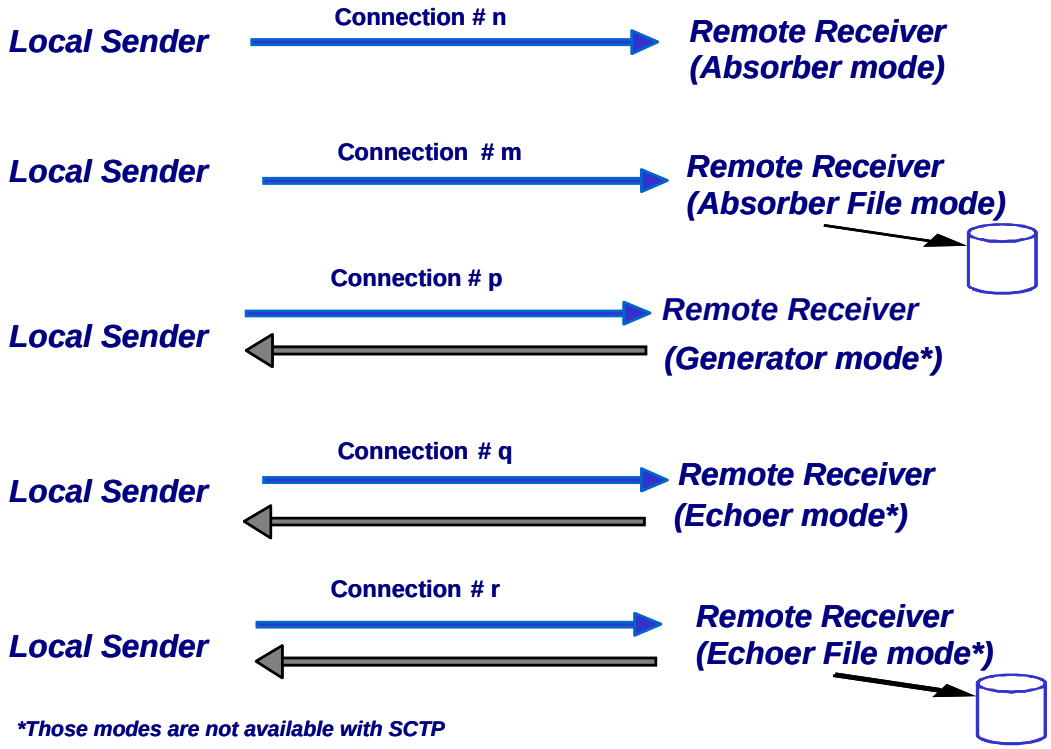
  ⇨ **Statistics**: for each connection the following statistics parameters are displayed by the **Sender** and can be saved in a file:

  - Sent throughput(1)
  - Received throughput(1)
  - Sent packet throughput(1)
  - Received packet throughput(1)
  - Sent data volume(1)
  - Received data volume (volume of data sent by the remote) (1)
  - Sent packets

- Received packets (packets sent by the remote)
- Data volume to send(1)
- Remaining volume (of data to send) (1)
- Sequence numbering errors
- RTT Mean (Round Trip Time)
- Jitter(1)

(1) These statistics are not available with ICMP protocol.

- The **Receiver** receives traffic (up to 16 simultaneous connections) and operates five different working modes: Absorber, Absorber File, Generator, Echoer and Echoer File.
  - Each Receiver connection can be set up according to one of the following five modes:



Note: We consider that the local machine is used for sending traffic and the remote one is used for receiving traffic.

⇨ **Statistics**: for each connection the following statistics parameters are displayed by the **Receiver** part and can be saved in a file:

- Sent throughput
- Received throughput
- Sent packet throughput
- Received packet throughput
- Sent data volume
- Received data volume (volume of data sent by the remote)
- Sent packets
- Received packets (packets sent by the remote)
- Data volume to send
- Remaining volume (of data to send)
- Sequence numbering errors
- Data not echoed
- Jitter

Multicast feature

LanTraffic V2 Enhanced is able to generate and receive Multicast IP traffic (IPv4 and IPv6). The multicast feature is used for the UDP protocol only.

- **Multicast & IPV4**: 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).

- **Multicast & IPv6**: IPv6 multicast addresses are defined in "IP Version 6 Addressing Architecture" [RFC2373].
  This defines fixed and variable scope multicast addresses. IPv6 multicast addresses are distinguished from unicast addresses by the value of the high-order octet of the addresses: a value of 0xFF (binary 11111111) identifies an address as a multicast address; any other value identifies an address as a unicast address (FE80::/10 are Link local addresses, FEC0::/10 are Site Local addresses where FF00::/8 are Multicast addresses).
  Multicast addresses from FF01:: through FF0F:: are reserved.
  The complete list of Reserved IPv6 multicast addresses can be found in “IPv6 Multicast Address Assignments” [RFC 2375].
  The ICMPv6 messages are used to convey IPv6 Multicast addresses resolution.

Broadcast feature (available with IPv4 only)

LanTraffic V2 Enhanced is able to generate and receive Broadcast IP traffic (IPv4 only). The broadcast feature is used for the UDP protocol only.

- **Broadcast & IPV4**: IPv4 addresses as 255.255.255.255 or 192.168.0.255 are BROADCAST IP addresses. These addresses can be used to generate broadcast IP traffic (define the broadcast IP address in the Sender part). To receive broadcast IP traffic, specify the unicast IP address of the Sender in the Receiver part.
- **Broadcast & IPv6:** broadcast does not apply to IPv6.

IP version selection

LanTraffic V2 Enhanced supports IPv6. To use it, please check IPv6 stack is selected on the network interface you want to use.

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

On Ethernet, the maximum size of the IPv6 packet to avoid fragmentation is **1440** bytes whereas it is 1460 bytes in TCP with IPv4.

Interface selection

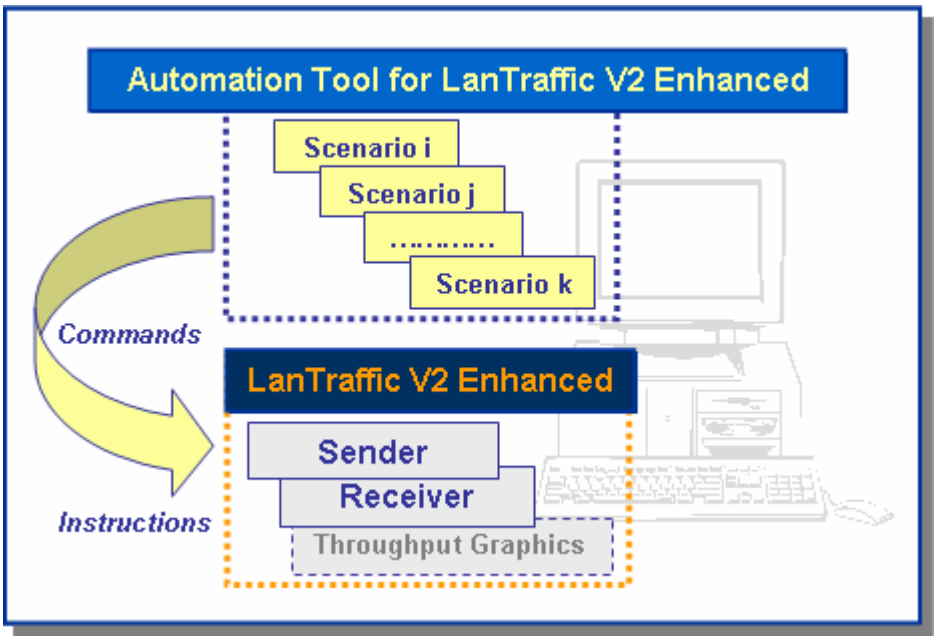
The interface selection of a LAN card (NIC), a virtual NIC such as an IP tunneling protocol or a remote access is useful to control the data traffic hardware route. **LanTraffic V2 Enhanced** is able to generate and receive Unicast and Multicast IP traffic on a selected interface, giving the user a deeper control where data are exchanged and makes multiple routes definition easier.

Statistics values

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

1.2 The Automation Tool for LanTraffic V2 Enhanced

The add-on software **Automation Tool for LanTraffic V2 Enhanced** allows you to edit scenarios, to carry out scenarios, to set the **LanTraffic V2 Enhanced** parameters and to pilot **LanTraffic V2 Enhanced** automatically on the same PC.



A scenario is a succession of commands and instructions.

A command is used to set parameters and/or activate a function of **LanTraffic V2 Enhanced**.
For example the *Set and Start connection(s)* command helps to set parameters for IP connections and to start the traffic on these connections. With such command you specify the IP address, port number, protocol, packet size, inter packet delay, duration, etc. and you start the traffic generation for these connections.

An instruction is used by the Automation Tool to create an internal process. For example, the *Wait Date/Time* instruction suspends the scenario execution up to the specified date and time before to continue.

By using the **Automation Tool for LanTraffic V2 Enhanced** you can:

- Set automatically the parameters of the **LanTraffic V2 Enhanced** software,
- Start and stop IP connections based on timers,
- Execute the scheduled operations in accordance with your own timing,
- Make repetitive tests operations automatically,
- Simplify the tests reproduction,
- And more…

Part 2 Install LanTraffic V2 Enhanced

LanTraffic V2 Enhanced requires less than 15 MB of free disk-space. The default settings folder is C:\Program files\LanTraffic V2 Enhanced. The "**Automation Tool for LanTraffic V2 Enhanced**" add-on software is automatically installed with **LanTraffic V2 Enhanced**.

** To run **LanTraffic V2 Enhanced** your computer screen resolution must be at least 1024 X 768 and the DPI setting should be set up with the "Normal size (96 DPI)" value.*

** To install **LanTraffic V2 Enhanced** you must log on with the administrator rights.*

*We recommend that you shutdown first your anti-virus application before installing **LanTraffic V2 Enhanced**. Please note that you should mask the task bar in a 1024x768 screen resolution, so you get an optimal view of the software interface.*

The installation procedure is a standard installation program for Windows 2000, Windows XP, Windows Server 2003 and Windows Vista.

2.1 How to install the software downloaded from the Internet

*To install **LanTraffic V2 Enhanced,** you must log on with the administrator rights.*

If you have downloaded **LanTraffic V2 Enhanced** trial version from our website, you have downloaded the "LanTrafficV2Enhanced.zip" file including the software and the related documentation. You must first unzip this file in a temporary directory. Then run Setup_LanTrafficV2_Enhanced.exe from this temporary directory to launch the setup procedure.

2.2 How to install the software from the CD-ROM

The installation procedure is a standard installation program.

*To install **LanTraffic V2 Enhanced,** you must log on with the administrator rights.*

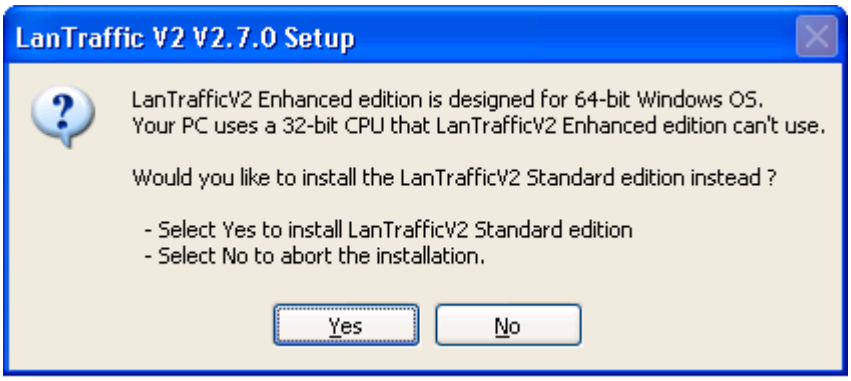
- First, insert the **LanTraffic V2 Enhanced** CD-ROM in your CD-ROM drive.
- Click on "Start", "Execute" and type "CD unit>: \Setup_LanTrafficV2_Enhanced.exe". Follow the **LanTraffic V2 Enhanced** setup instructions to proceed with the installation.

2.3 During the installation

2.3.1 64-bit version required

LanTraffic V2 Enhanced requires a 64-bit version of Windows.

When you start the setup on 32-bit version of your OS, the Setup proposes you to install the **LanTraffic V2 Standard** edition instead of **LanTraffic V2 Enhanced**.



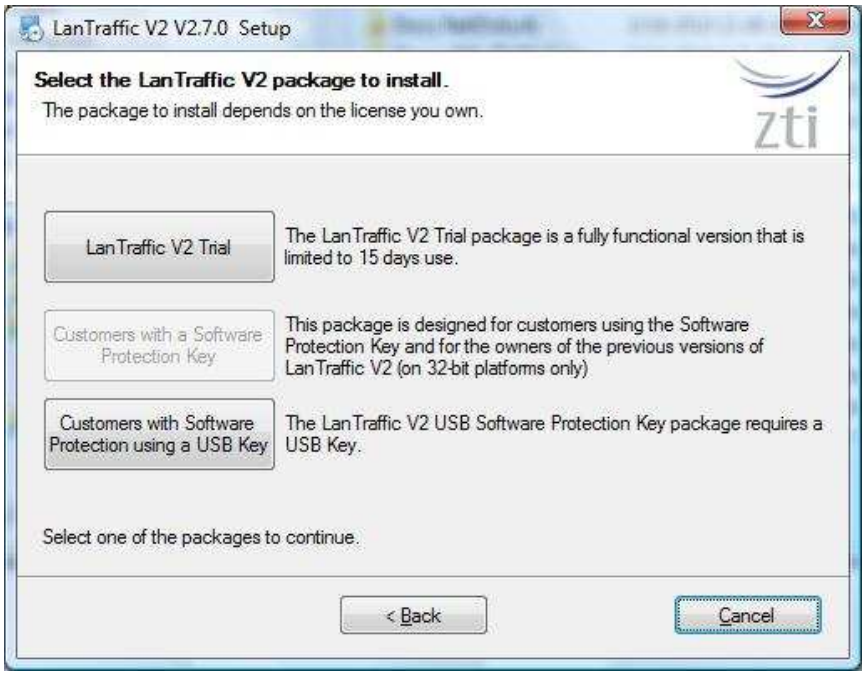
You select **Yes** to install **LanTraffic V2 Standard** or **No** to stop the setup.

To install the LanTraffic V2 Standard edition, please refer to the LanTraffic V2 Standard documentation (Read Me First or User Guide).

The next paragraphs refer only to LanTraffic V2 Enhanced

2.3.2 Choose the LanTraffic V2 Enhanced package to install

Follow the instructions until reaching the **LanTraffic V2 Enhanced** package selection window.



The "Customer with a Software Protection Key" package is available with the 32-bit version of the software only.

2.3.3 LanTraffic V2 Enhanced packages in a few words

To use the **LanTraffic V2 Enhanced** software, there are 2 license schemes:

- The **LanTraffic V2 Enhanced** **Trial package** allows you to use **LanTraffic V2 Enhanced** during 15 days after the first run. When the trial period has expired, the license should be purchased.

- For new users, the **LanTraffic V2 Enhanced** **USB Software Protection Key package** requires a USB key with the **LanTraffic V2 Enhanced** license. The **USB key** is provided with **LanTraffic V2 Enhanced** from version 2.6. This package allows the installation of **LanTraffic V2 Enhanced** on several PCs but the only PC able to run **LanTraffic V2 Enhanced** is the one having the USB key plugged in.

This software is licensed on a per workstation basis. This means that you will need to get a separate license for each machine you will run it on. The license may be a software key (for previous users) or the USB key. Each licensed copy of the software gets a USB Software Protection key that can be moved from one installation to the other.

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

2.3.4 Which package should I install?

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

2.3.4.1 I want to evaluate LanTraffic V2 Enhanced

In that case, choose the *"LanTraffic V2 Enhanced Trial"* package. You will be able to use **LanTraffic V2 Enhanced** during 15 days only.

2.3.4.2 I already use LanTraffic V2 Enhanced …

This paragraph is dedicated to the users owning a previous version of **LanTraffic V2 Enhanced.**

2.3.4.2.1 … and I want to upgrade and keep my permanent license (installed with a previous 32-bit version)

In that case, please contact the ZTI Customer sales or your reseller to upgrade from the *"Customers with a Software Protection Key"* package to the *"Customers with Software Protection using a USB Key"* package.

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

In that case, choose the package *"Customers with Software Protection using a USB Key"*. Plug the USB Software Protection Key before launching **LanTraffic V2 Enhanced.**

2.3.4.3 I just bought LanTraffic V2 Enhanced …

This paragraph is related to the users purchasing **LanTraffic V2 Enhanced version 2.7.**

2.3.4.3.1 … and I received the CDROM & USB Software Protection Key

In that case, choose the package *"Customers with Software Protection using a USB Key"*. Plug the USB Software Protection Key before running **LanTraffic V2 Enhanced.**

2.3.4.3.2 … and I will receive the CDROM & USB Software Protection Key in a few days.

In that case, choose the package *"LanTraffic V2 Enhanced Trial"*. You will get a fully functional but time-limited **LanTraffic V2 Enhanced**.

2.4 What has been installed on my computer?

The default settings install **LanTraffic V2 Enhanced** in the following directory: C:\Program Files\LanTraffic V2 Enhanced.

The **LanTraffic V2 Enhanced** installation procedure installs the main following files on your hard disk:

- LanTrafficV2.exe: program file
- LanTraffic V2 Enhanced User Guide: PDF file.
- Read Me First: PDF file
- Aut_LTV2.exe: program file (Automation tool)
- Automation Tool for LanTraffic V2 Enhanced User Guide: PDF file
- Automation scenario samples and other files required by the software
- Viewer.exe: program file installed with the USB Software Protection package
- ElevateLanTrafficV2.exe: allows running **LanTraffic V2 Enhanced** as Administrator
- Version.txt: text file containing information about the versions.

Start Menu shortcuts created:

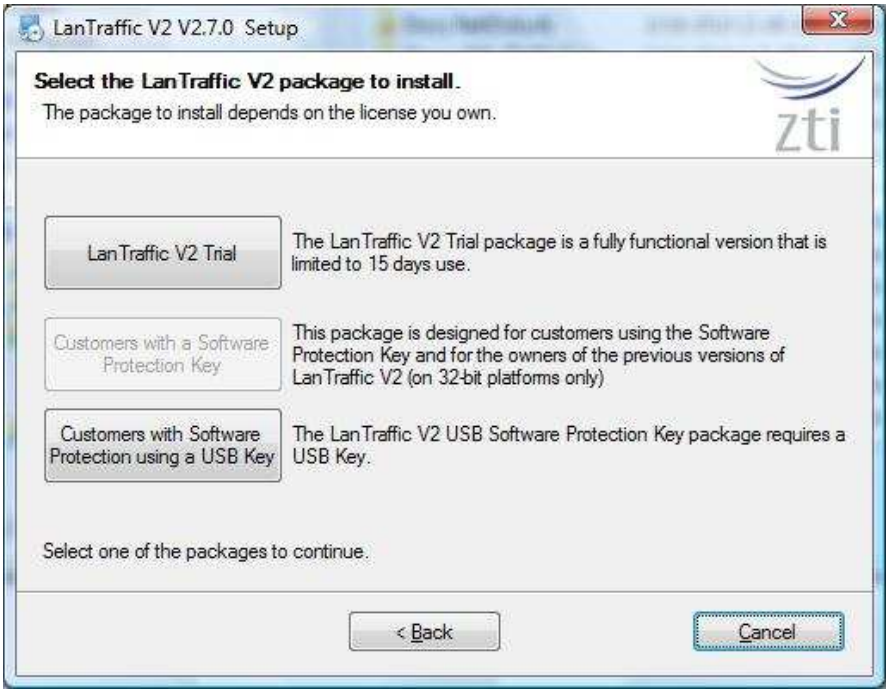
Start > Programs > **LanTraffic V2 Enhanced**

- ⇨ **Automation Tool for LanTrafficV2 Enhanced** (click to run the software)
- ⇨ **Automation Tool for LanTrafficV2 Enhanced** User Guide (PDF file)
- ⇨ **LanTraffic V2 Enhanced** (click to run the software)
- ⇨ **LanTraffic V2 Enhanced** User Guide (PDF file)
- ⇨ Read Me First (PDF file)

*If the RPC mechanism is disabled, a message will ask automatically for the system reboot at the end of the installation. This is mandatory to allow the dialog between the Automation Tool and **LanTraffic V2 Enhanced**.*

2.5 How to reinstall another package?

If you already have installed one of the **LanTraffic V2 Enhanced** V2.7 packages, click Setup_LanTrafficV2_Enhanced.exe and select, in the window below, the new package you want to install.



⚠ *Don't forget that the "Customer with a Software Protection Key" package is available with the 32-bit version of the software only – it can't be used with* ***LanTraffic V2 Enhanced***

2.6 How to transfer the software to another computer?

Install the software on the target computer. You don't need to do any particular operation with the *"Customers with Software Protection using a USB Key"* and *"LanTraffic V2 Enhanced Trial"* packages.

With **LanTraffic V2 Enhanced** & USB Software Protection Key, you do need to plug the USB key before running the software on the target computer.

Part 3 How to handle your license

3.1 LanTraffic V2 Enhanced Trial

You don't require any license to install the **LanTraffic V2 Enhanced Trial package**. After the first run of **LanTraffic V2 Enhanced,** the **LanTraffic V2 Enhanced Trial package** can be used during 15 days.

3.1.1 LanTraffic V2 Enhanced License Information window

When you run **LanTraffic V2 Enhanced,** the information about your trial license is displayed, as shown below.

You are now able to use **LanTraffic V2 Enhanced** during the next 15 days.

3.1.2 End of the fifteen-day trial period

Once the trial period is finished, you are not allowed to use **LanTraffic V2 Enhanced** anymore, as shown below:

When you press the **OK** button, **LanTraffic V2 Enhanced** will stop running. To continue to use **LanTraffic V2 Enhanced please contact you local distributor or ZTI** to get a license.

3.2 LanTraffic V2 Enhanced & USB Software Protection Key

The USB Software Protection Key is the most flexible way to transfer your license to any other PC. Plug it in the computer you want to use **LanTraffic V2 Enhanced** on.

If you are a user of a previous version of **LanTraffic V2 Enhanced** (version 2.5 and under) change for more flexibility to a **USB Software Protection Key** by contacting the Sales Offices (sales@zti-telecom.com) and get some information about how to exchange your Site Key to a **USB Software Protection key**.

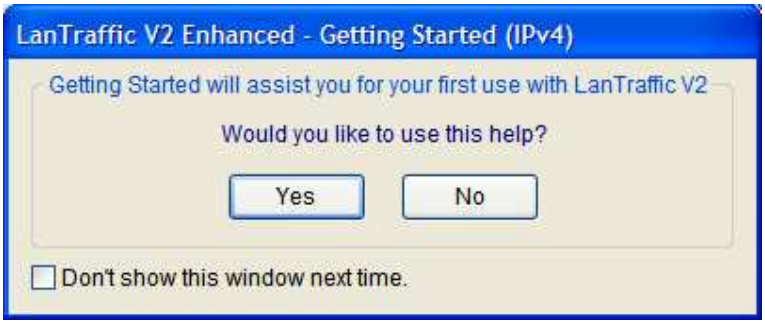
Part 4 Uninstall LanTraffic V2 Enhanced

The uninstall procedure is a standard uninstall program. To uninstall **LanTraffic V2 Enhanced** select “Uninstall LanTraffic V2 Enhanced” in the “Start > Programs > LanTraffic V2 Enhanced” menu.

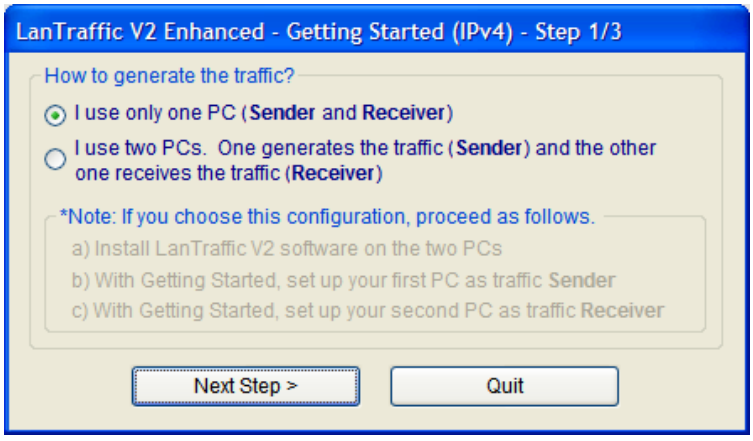
Part 5 LanTraffic V2 Enhanced Getting Started

*Anti-virus or firewall applications may disrupt **LanTraffic V2 Enhanced** when sending or receiving data. Please set up your security software before using **LanTraffic V2 Enhanced** (see Part 6 and Part 7).*

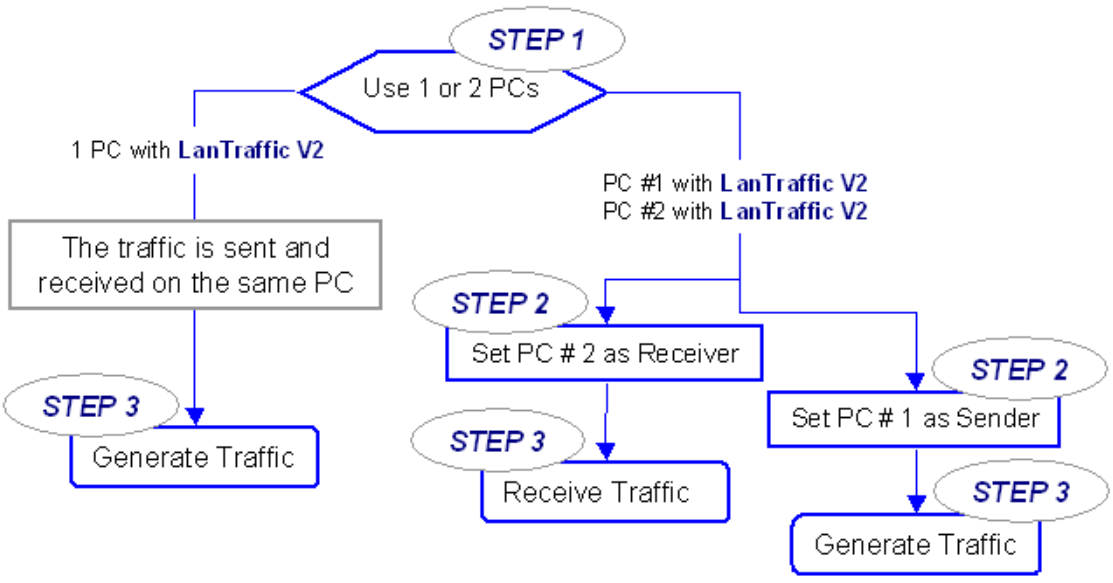
New users can use this help as an introduction to **LanTraffic V2 Enhanced** and generate or receive TCP and UDP data with the IPv4 protocol in a few clicks. Just after launching **LanTraffic V2 Enhanced**, the Getting Started Window is displayed:



Press **No** if you don't want to use this help.
Press **Yes**, the next window will ask you if you want to use 1 or 2 PCs:

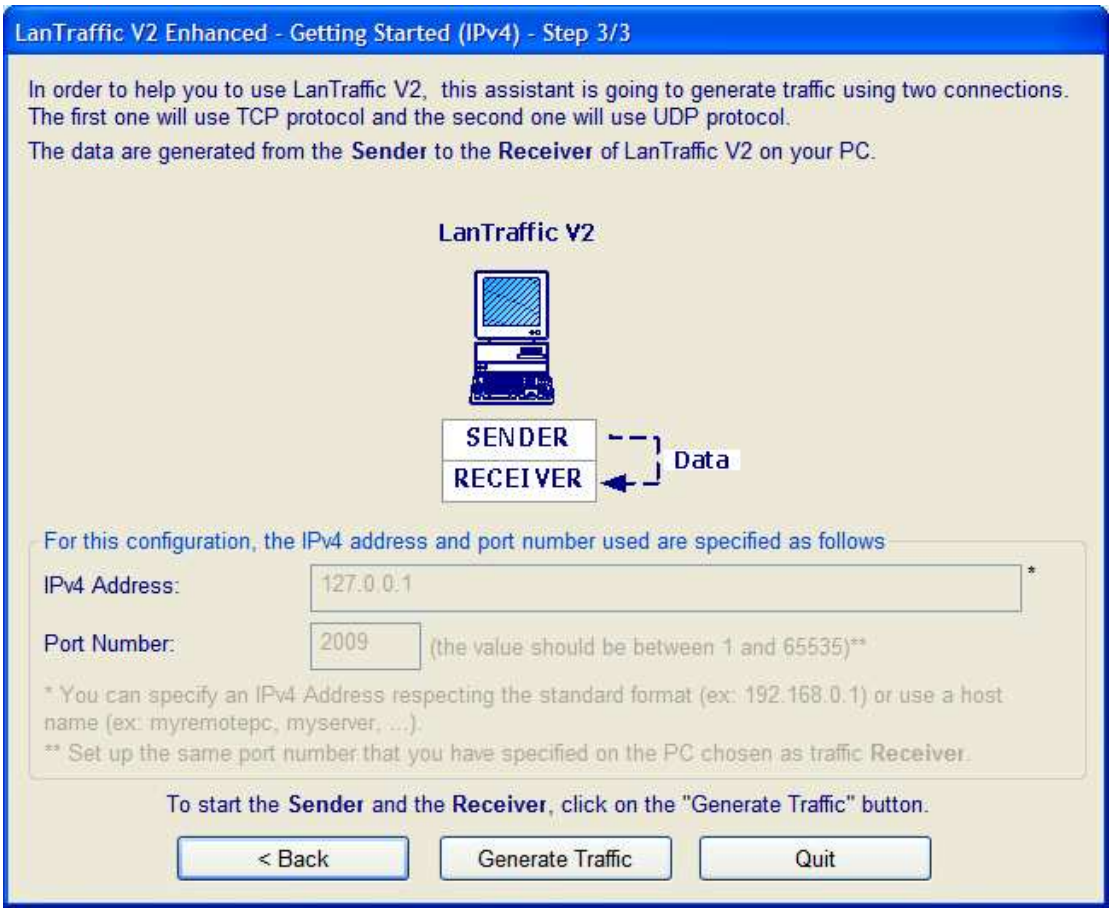


Depending on your choice to use 1 or 2 PCs, the plan below shows the steps:

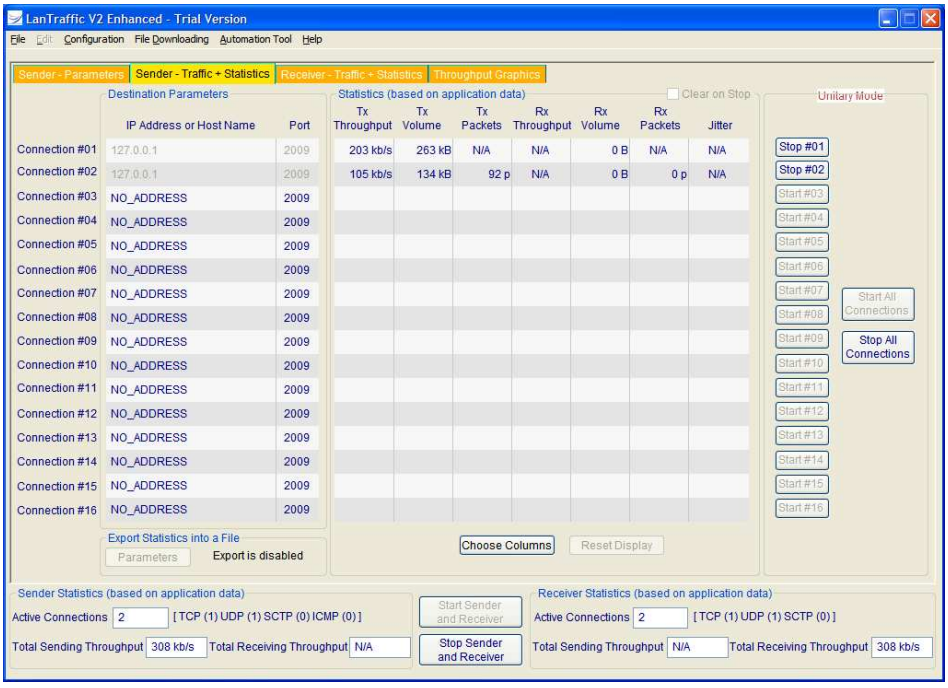


For the use of 1 PC

The following window is displayed.

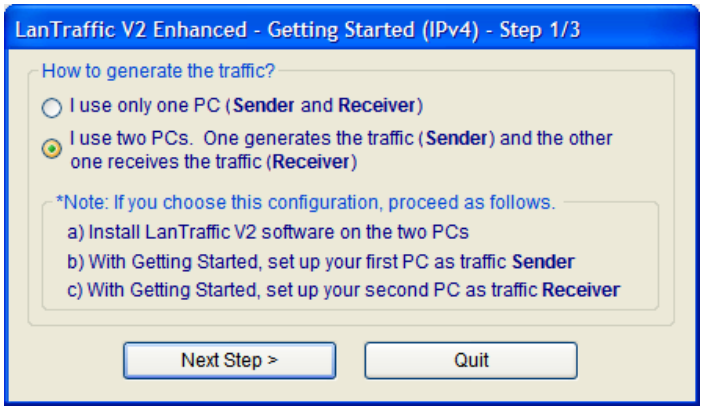


Then press the "Generate traffic" button to continue. The "Sender – Traffic + Statistics" tab of LanTraffic V2 Enhanced will display the two first active connections as shown on the following window:

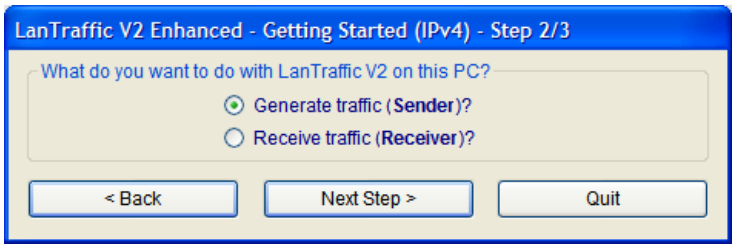


For the use of 2 PCs

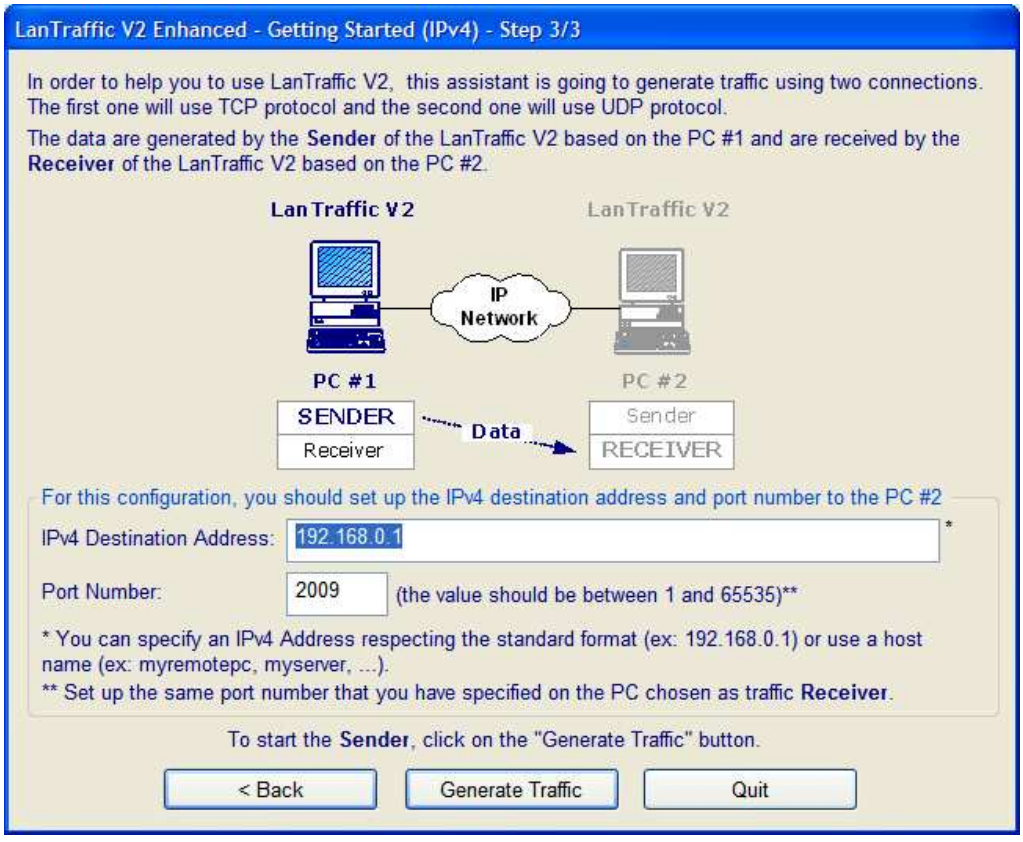
If you select the option: **I use two PCs**, read the following instructions. **LanTraffic V2 Enhanced** must be installed on the two PCs.



Press "Next Step >" to continue.

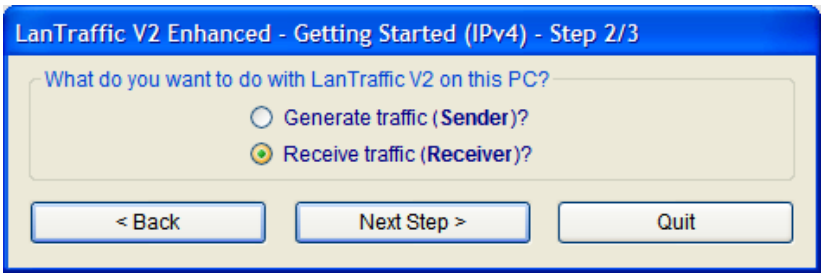


Then choose if you want to generate or receive the traffic on this PC. If you select "Generate traffic" the following window will appear:

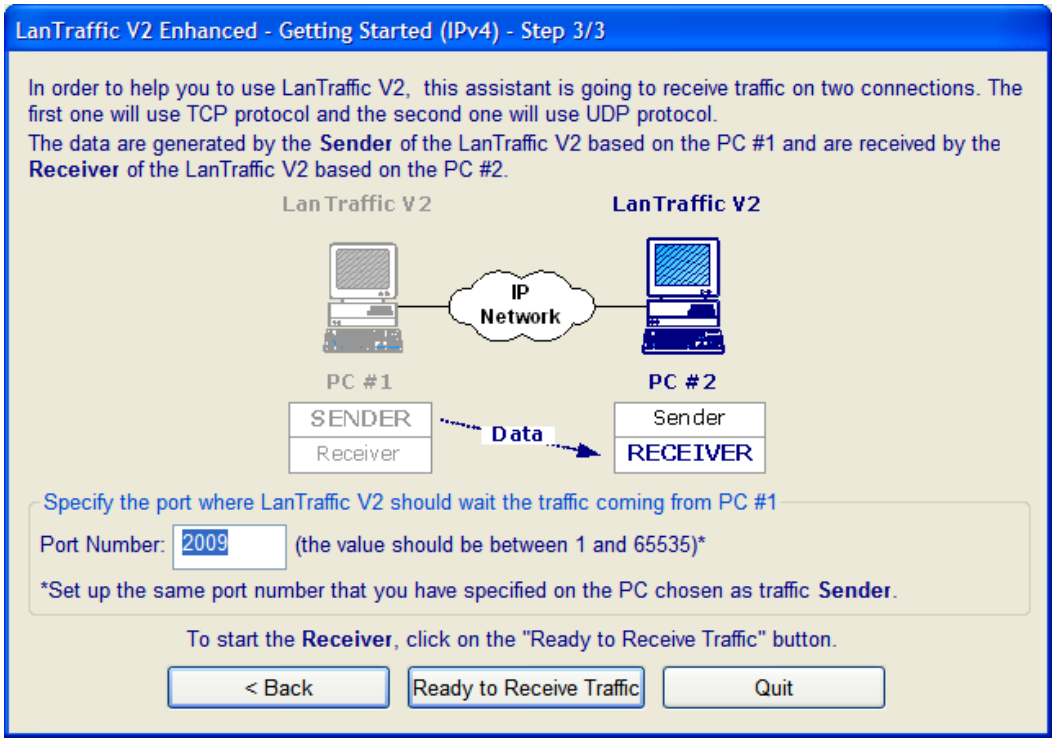


Define the IPv4 address and port number to use. Then press the "Generate traffic" button and a warning dialog is displayed:

Before generating traffic towards PC # 2, the PC # 2 must be configured as Receiver.



Press "Next Step >" to continue on PC # 2.

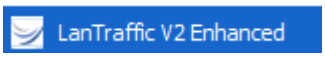


After pressing the "Ready to Receive Traffic" button, a warning message will appear:

Press "OK" and the "Receiver – Traffic + Statistics" tab of **LanTraffic V2 Enhanced** is displayed on PC # 2.
Then go to PC # 1 and start the **LanTraffic V2 Enhanced** Sender. The "Sender – Traffic + Statistics" tab of **LanTraffic V2 Enhanced** displays now the two first active connections. You have now 2 connections generating traffic from PC #1 to PC # 2.

Part 6 Run LanTraffic V2 Enhanced

Use the Windows start menu:

Start ► All Programs ► LanTraffic V2 Enhanced ► 

Click here.

You must have the administrator rights to be able to use the DSCP field. To launch LanTraffic V2 Enhanced with the administrator rights, right-click on the LanTraffic V2 Enhanced shortcut and choose "Run as administrator".

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

15 days trial version	***USB Software Protection Key version***
	***If you use a USB Software Protection Key, there is no window!***

The Windows Firewall window below may appear. This window allows configuring the Windows Firewall settings for **LanTraffic V2 Enhanced**. Click on the "Unblock" button to add **LanTraffic V2 Enhanced** into the authorized programs list.

Part 7 LanTraffic V2 Enhanced and Windows Firewall

*Anti-virus or firewall applications may disrupt **LanTraffic V2 Enhanced** from sending or receiving data. Please set up your security software before using **LanTraffic V2 Enhanced**.*

*Windows Firewall may also disrupt the **LanTraffic V2 Enhanced** performances. To get best performances, you should disable Windows Firewall.*

Some anti-virus configurations can stop **LanTraffic V2 Enhanced** working because of their security settings. For commercial anti-virus, please refer to the related documentation to authorize **LanTraffic V2 Enhanced** to work.

7.1 How to authorize TCP and UDP connections with Windows Firewall

Windows Firewall blocks incoming network connections except for the authorized programs. To allow **LanTraffic V2 Enhanced** receiving incoming TCP or UDP connections, you must add it in the exceptions list of Windows Firewall by proceeding as follows:

Step1: Open a command prompt window. You should be logged on an account giving the administrator rights to be able to modify the firewall configuration.

Step 2: type the command line below and press "Enter".

%> netsh firewall add allowedprogram program="C:\Program Files\LanTraffic V2 Enhanced\LanTrafficV2.exe" name="LanTraffic V2 Enhanced" mode=ENABLE scope=ALL profile=ALL

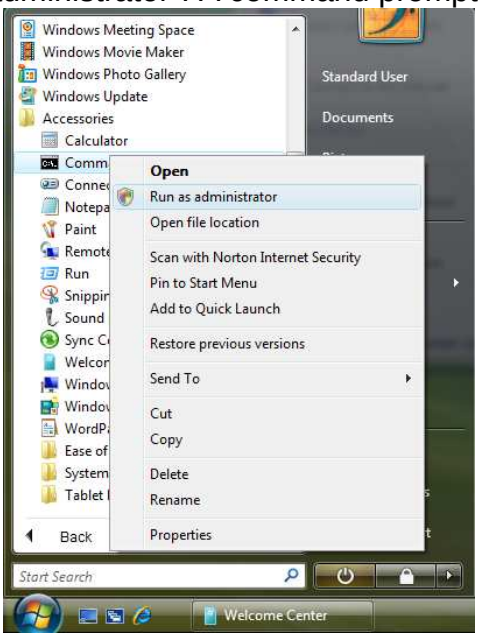
Make sure that "C:\Program Files\LanTraffic V2 Enhanced\" is the installation directory of LanTraffic V2 Enhanced. A message of confirmation is returned by *netsh* if the command is succeeded. If the path you have specified is invalid, *netsh* returns an error message close to the following message: *The system cannot find the file specified.* In that case, please renew Step 2.

Unlike under Windows Vista, the firewall allows the incoming echo replies. You don't need to add a rule to be able to receive ICMPv4/ICMPv6 "echo reply" messages.

7.2 How to authorize UDP and TCP connections with Windows Firewall

Windows Firewall blocks incoming and outgoing network connections except for the authorized programs. By default, all outgoing connections are allowed. But to authorize **LanTraffic V2 Enhanced** receiving incoming connections, you must add it in the exceptions list of Windows Firewall by proceeding as follows:

Step1: Open a command prompt window with the administrator rights. The administrator rights are mandatory to set up the firewall configuration. Open the "All Programs / Accessories" folder and right-click on the "Command Prompt" icon as shown on the figure below and choose "Run as administrator". A command prompt window is opened.



Step 2: type the command line below and press "Enter".

%> netsh firewall add allowedprogram program="C:\Program Files\LanTraffic V2 Enhanced\LanTrafficV2.exe" name="LanTraffic V2 Enhanced" mode=ENABLE scope=ALL profile=ALL

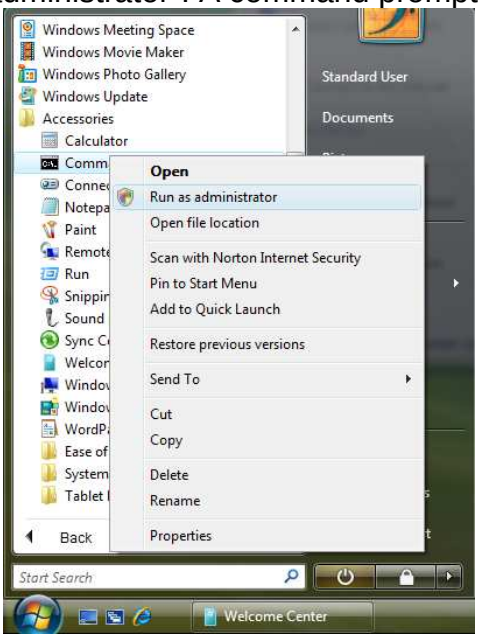
Make sure that "C:\Program Files\LanTraffic V2 Enhanced\" is the installation directory of LanTraffic V2 Enhanced. A message of confirmation is returned by *netsh* if the command is succeeded. If the path you have specified is invalid, *netsh* returns an error message close to the following message: *The system cannot find the file specified.* In that case, please renew Step 2.

The Windows firewall blocks the incoming echo replies traffic. You must add a rule to be able to receive ICMPv4/ICMPv6 "echo reply" messages. Please refer to the paragraphs here after.

7.3 How to authorize ICMPv4 and ICMPv6 traffic with Windows Firewall

Windows Firewall blocks incoming ICMPv4 and ICMPv6 "echo reply" messages. To be able to receive these messages, you must add two new rules by proceeding as follows:

Step1: Open a command prompt window with the administrator rights. The administrator rights are mandatory to do the firewall configuration. Open the "All Programs / Accessories" folder and right-click on the "Command Prompt" icon as shown on the figure below and choose "Run as administrator". A command prompt window is opened.



Step 2: To create the rule for ICMPv4 echo reply messages, type the command line below and press "Enter".

%> netsh advfirewall firewall add rule name="Echo Reply ICMPv4 (used by LanTraffic V2 Enhanced)" dir=in action=allow profile=any localip=any remoteip=any protocol=icmpv4:0,0 interfacetype=any

A message of confirmation is returned by *netsh* if the command is succeeded.

Step 3: To create the rule for ICMPv6 echo reply messages, type the command line below and press "Enter".

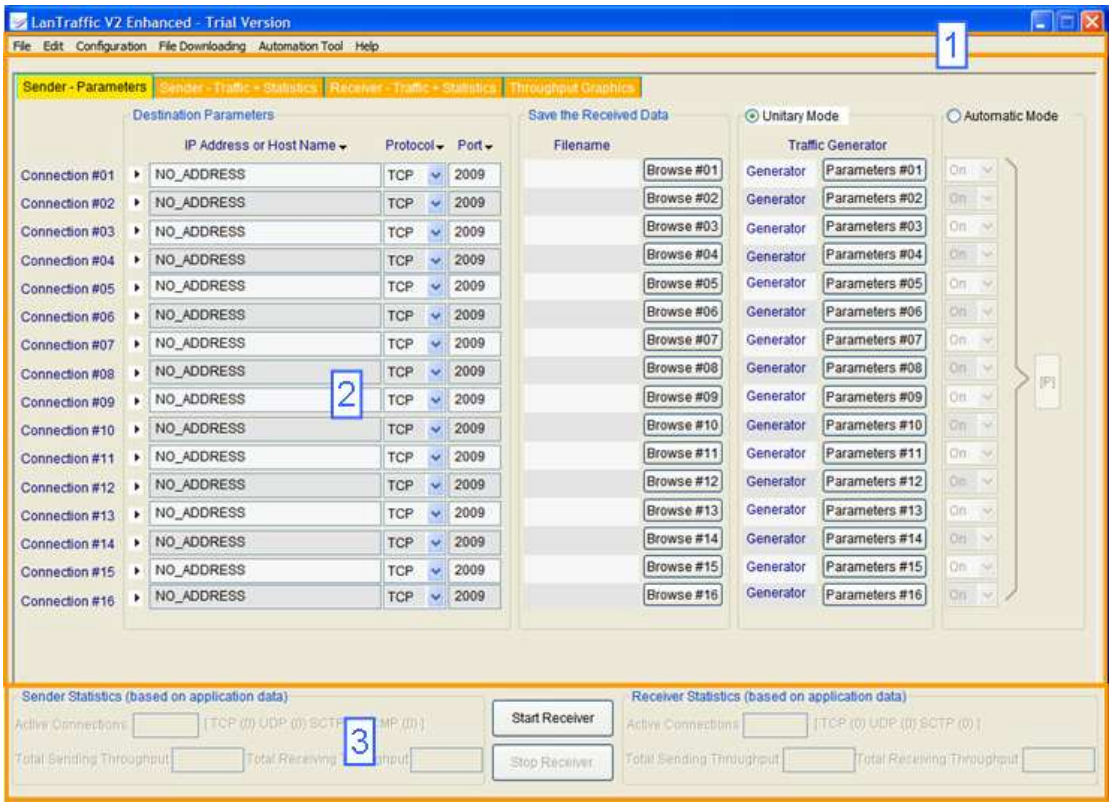
%> netsh advfirewall firewall add rule name="Echo Reply ICMPv6 (used by LanTraffic V2 Enhanced)" dir=in action=allow profile=any localip=any remoteip=any protocol=icmpv6:129,0 interfacetype=any

A message of confirmation is returned by *netsh* if the command is succeeded.

Part 8 Graphical User Interface

8.1 Main Window

When **LanTraffic V2 Enhanced** is launched, the following main window is displayed:



LanTraffic V2 Enhanced *main window*

The **LanTraffic V2 Enhanced** main window is made of three areas:

- ⇨ **Area 1: Menu bar**
- ⇨ **Area 2:** this main area displays the **four tabs** of **LanTraffic V2 Enhanced**. To see a tab, click on the tab title you want to display.
- ⇨ **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 Enhanced GUI is composed of four tabs:

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.

8.2 Display general rules of the Graphical User Interface

LanTraffic V2 Enhanced 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. 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. 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/A” for Not Applicable 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 Enhanced** 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

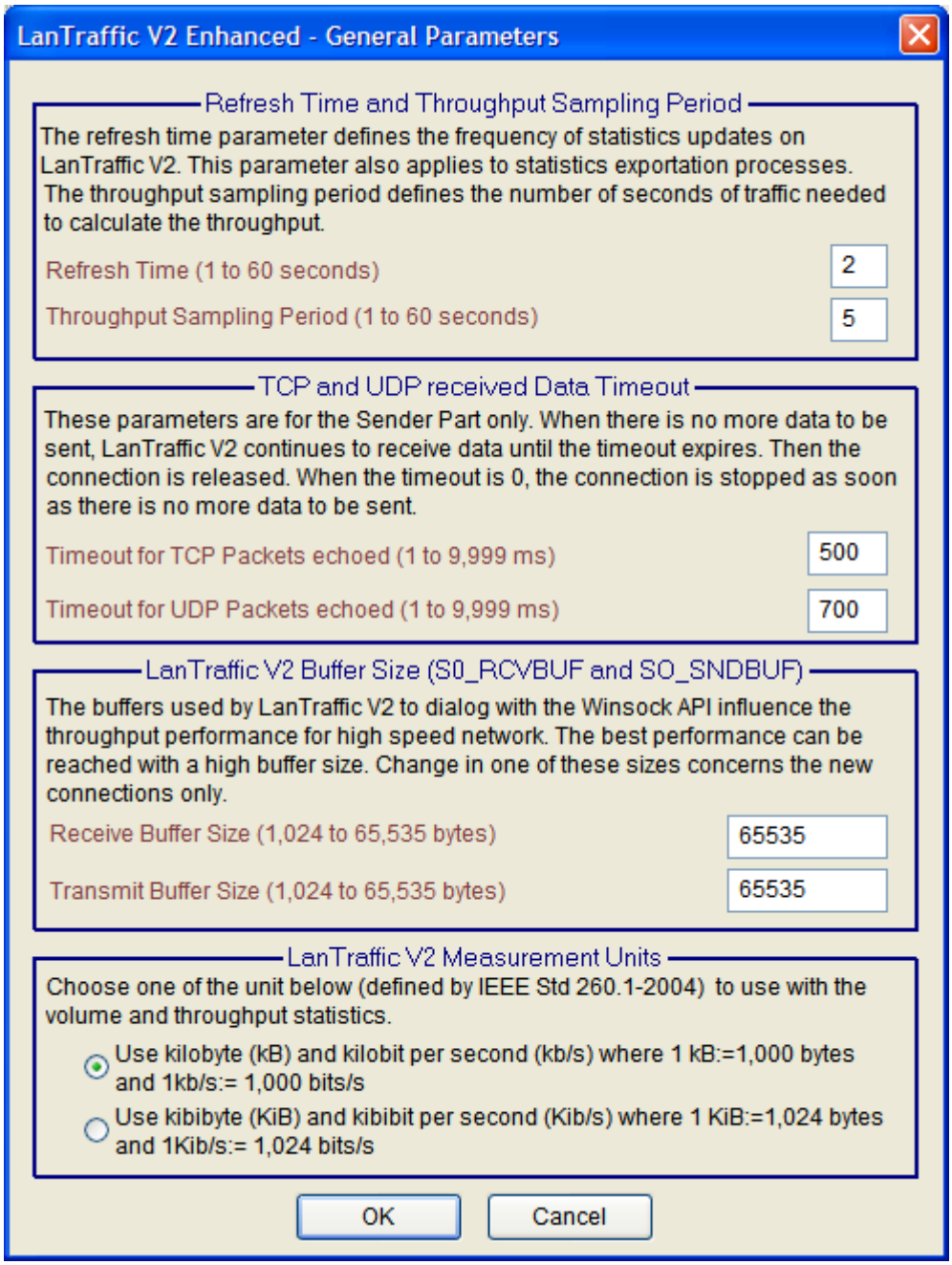
User actions and parameters selection may turn some **LanTraffic V2 Enhanced** GUI fields and action buttons out of reach. Usually all the out of reach fields are grayed.

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 parameters of the connection.
- When a testing mode (unitary or automatic) is selected, it is impossible to change parameters of the unselected testing mode.
- If you enter a non-valid value in a field, the connection could be disabled or actions button in configuration windows could become out of reach.

8.3 Used units for the information display

All information used by **LanTraffic V2 Enhanced** is displayed with its unit and unit is changing in order to limit figure size. In accordance with IEEE Std 260.1 2004, the user can select one of the 2 units to use, using the menu 'Configuration/General Parameters'.



The **LanTraffic V2 Enhanced** unit measurement is saved in the registry, not in the context, because **Automation for LanTrafficV2 Enhanced** uses the selected unit with some *Commands*.

8.3.1 Volume units

8.3.1.1 Volume kB Unit

Display	Meaning
10 B	10 Bytes
1 kB	1 Kilo Bytes (1,000 Bytes)
1 MB	1 Mega Bytes (1,000,000 Bytes)
1 GB	1 Giga Bytes (1,000,000,000 Bytes)
1 TB	1 Tera Bytes (1,000,000,000,000 Bytes)
1.23^65	1.23 x 10^65 Bytes

8.3.1.2 Volume KiB Unit

Display	Meaning
10 B	10 Bytes
1 KiB	1 Kibibytes (1,024 Bytes)
1 MiB	1 Mibibytes (1,048,576 Bytes)
1 GiB	1 Gibibytes (1,073,741,824 Bytes)
1 TiB	1 Tibibytes (1,099,511,627,776 Bytes)
1.23^65	1.23 x 10^65 Bytes

8.3.2 Throughput units

8.3.2.1 Throughput kb/s Unit

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

8.3.2.2 Throughput Kib/s Unit

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

Throughput computing

*The **LanTraffic V2 Enhanced** displayed throughputs correspond to payload data on the sampling period (defined in the **LanTraffic V2 Enhanced** 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.*

Units changing

*To change, a volume value in KiB to a volume value in MiB, **LanTraffic V2 Enhanced** divides the first value per 1024. Ex: 1000 KiB = 0.98 MiB.*
*The same rule is applied with throughput values. In order to have a throughput in Mib/s coming from a throughput in Kib/s, **LanTraffic V2 Enhanced** divides the first value per 1024. Ex: 2048 Kib/s = 2.00 Mib/s.*

*To change, a volume value in kB to a volume value in MB, **LanTraffic V2 Enhanced** divides the first value per 1000. Ex: 1000 kB = 1 MB.*
*The same rule is applied with throughput values. In order to have a throughput in Mb/s coming from a throughput in kb/s, **LanTraffic V2 Enhanced** divides the first value per 1000. Ex: 2000 kb/s = 2.00 Mb/s.*

Part 9 Using LanTraffic V2 Enhanced

9.1 Main steps

The main steps to use **LanTraffic V2 Enhanced** are:

⇨ To send data:

1. *In Tab 1 "Sender – parameters":*
   Configure Sender parameters i.e. IP address, port number, and protocol. You can select the interface and the IP protocol optionally. Then select and configure the 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 select the interface and the IP protocol optionally.

2. *In Tab 3 "Receiver - Traffic + Statistics":*
   Start receiving connections,

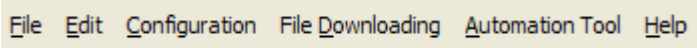
3. Result: exploit statistics and throughput graphs.

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 Enhanced** parameters can be saved into 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.

9.2 Menu description

The menu bar is made of 6 items:



The options for each item are described in this chapter.

9.2.1 File menu

9.2.1.1 File/New

This command opens a new default context in **LanTraffic V2 Enhanced**. Before opening a new default context, running connections must be stopped. The default values of a new context are presented in the Appendix.

9.2.1.2 File/Open

The “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, 2.1, 2.2, 2.3, 2.4, 2.5 or 2.6 is silently read by **LanTraffic V2 Enhanced** version 2.7. 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.

9.2.1.3 File/Save

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

*If **LanTraffic V2** versions 2.0.12, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6 contexts were opened, the context file saved get the new format used by **LanTraffic V2 Enhanced** version 2.7: it will not be available to use with an older version of **LanTraffic V2**.*

9.2.1.4 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 Enhanced** version 2.7 can’t be read by **LanTraffic V2** versions 2.7 and older.

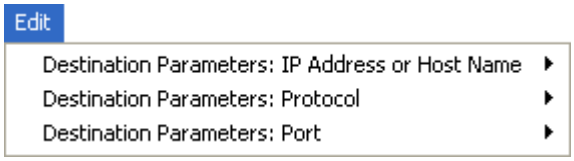
9.2.1.5 File/Recent Contexts …

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

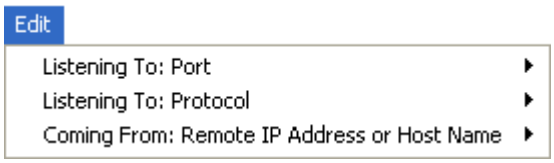
9.2.1.6 File/Exit

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

9.2.2 Edit menu



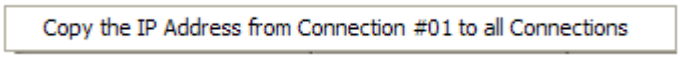
Active tab: "Sender – Parameters"



Active tab: "Receiver – Parameters + Statistics"

9.2.2.1 Edit/Destination Parameters: IP Address or Host Name (for Sender)

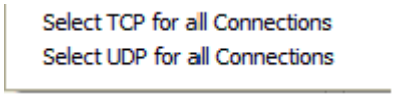
One option is available:



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

9.2.2.2 Edit/Destination Parameters: Protocol (for Sender)

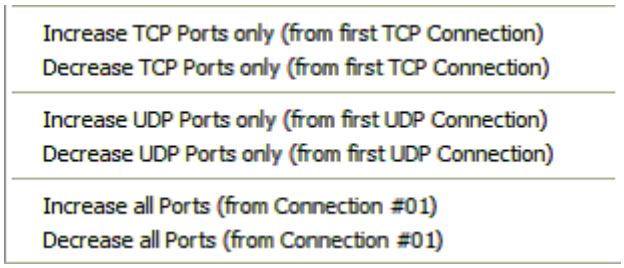
Three options are available:



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

9.2.2.3 Edit/Destination Parameters: Port (for Sender)

Four options are available:

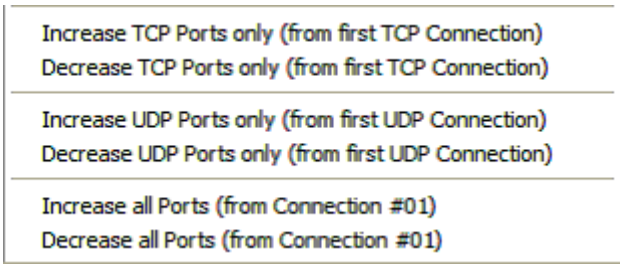


With this menu, you can:

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

9.2.2.4 Edit/Listening To: Port (for Receiver)

Four options are available:

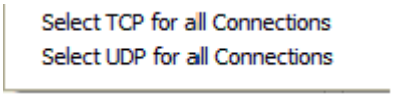


With this menu, you can:

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

9.2.2.5 Edit/Listening To: Protocol (for Receiver)

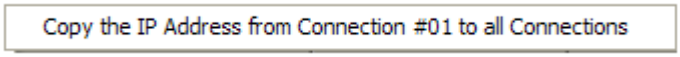
Three options are available:



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

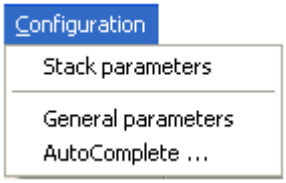
9.2.2.6 Edit/Coming From: Remote IP Address or Host Name (for Receiver)

One option is available:



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

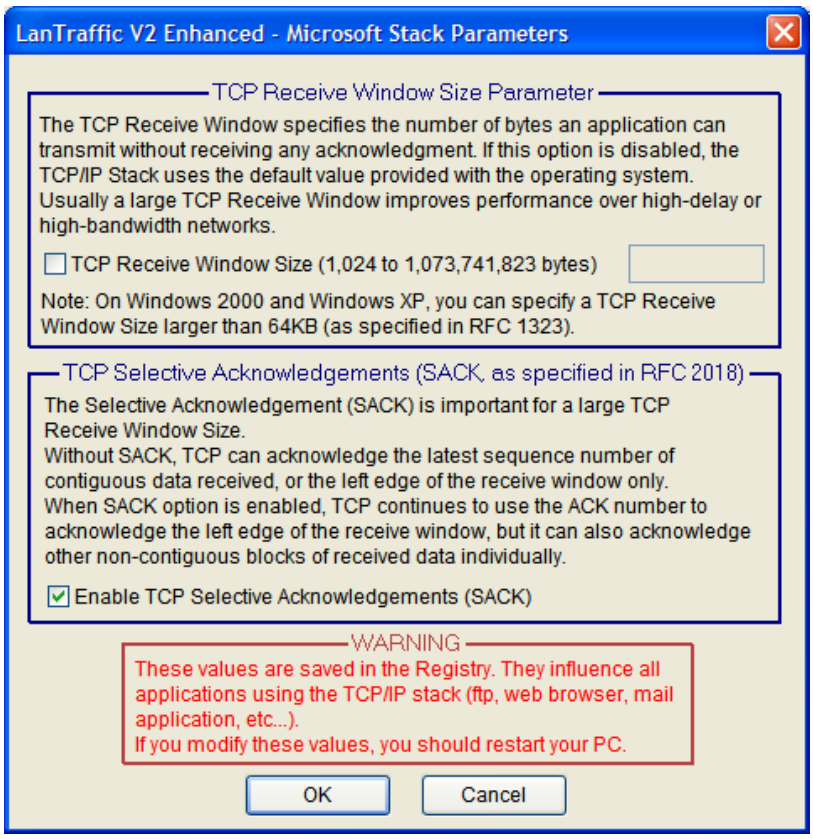
9.2.3 Configuration menu



9.2.3.1 Configuration/Stack Parameters

The "Stack Parameters" window is not available with Windows Vista and later (Seven, 2008 Server). The TCP Window Size and the selective acknowledge are automatically handled by the operating system.

LanTraffic V2 Enhanced 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 Enhanced** enables modifying the TCP Receive Window size and enables the TCP Selective Acknowledgements. When the Stack Parameters command is selected, the following window is displayed:



Stack Parameters window

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

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

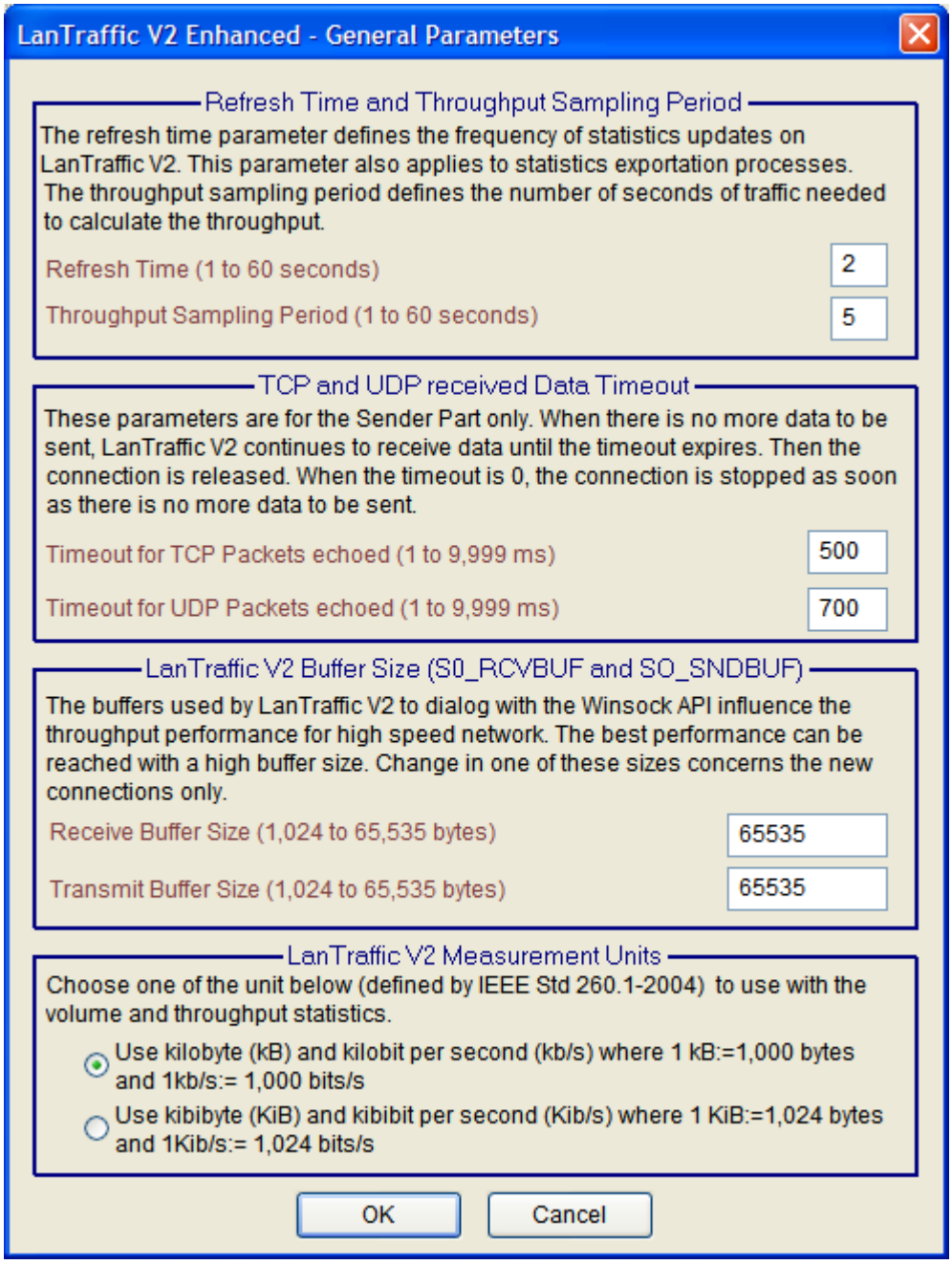
Important: these values influence all applications using the TCP/IP stack

These parameters are stored in the Registry in the keys:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\TCPIP\Parameters
      Name: TcpWindowSize & Tcp1323Opts & SackOpts.
```

9.2.3.2 Configuration/General Parameters

This command allows configuring parameters applied to graphical display, timeouts for echoed connections and the size of buffers used by **LanTraffic V2 Enhanced**.
When selected, the following window is displayed:



General Parameters window

Parameters applying to the GUI display

- **Refresh time:** value entered in this field configures display refresh time for all statistics displayed in **LanTraffic V2 Enhanced**.

- **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 Enhanced** continues TCP data acquisition during a time defined by this timeout. If this value equals zero, **LanTraffic V2 Enhanced** doesn'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 Enhanced** continues UDP data acquisition during a time defined by this timeout. If this value equals zero, **LanTraffic V2 Enhanced** doesn'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**.**

Parameters applying to measurement units

- **Use kilobyte and kilobit:** in this case a kilobyte is equal to 1000 bytes and a kilobit/s is equal to 1000 bits/s.

- **Use kibibyte and kibibit:** in this case a kilobyte is equal to 1024 bytes and a kilobit/s is equal to 1024 bits/s.

More information are available in paragraph **8.3 Used units for the information display**

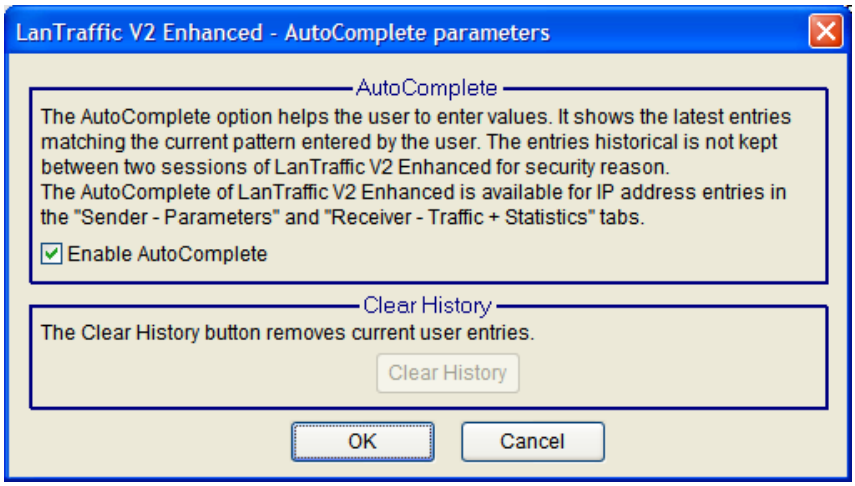
9.2.3.3 Configuration/AutoComplete …

The AutoComplete option is a help feature to input values for the user. It lists possible entries that match user entries typed before. The AutoComplete device with **LanTraffic V2 Enhanced** 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 31st entry is typed, the 1st 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.

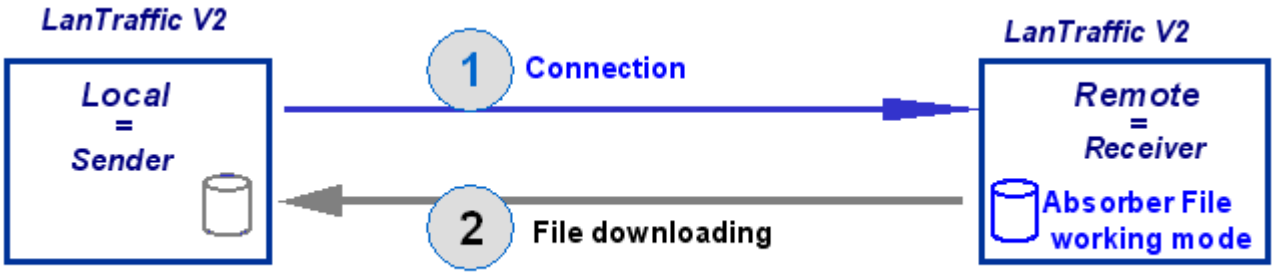
When AutoComplete is disabled, the historical record doesn’t continue to be filled. User entries before AutoComplete deactivation will be available when AutoComplete is activated again.

The historical record is associated to the “LanTraffic V2 Enhanced” session.

*For security reason, the historical record is not kept between sessions and is lost at the end of the **LanTraffic V2 Enhanced** session.*

9.2.4 File Downloading menu

This command allows downloading a file from one **LanTraffic V2 Enhanced** 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).

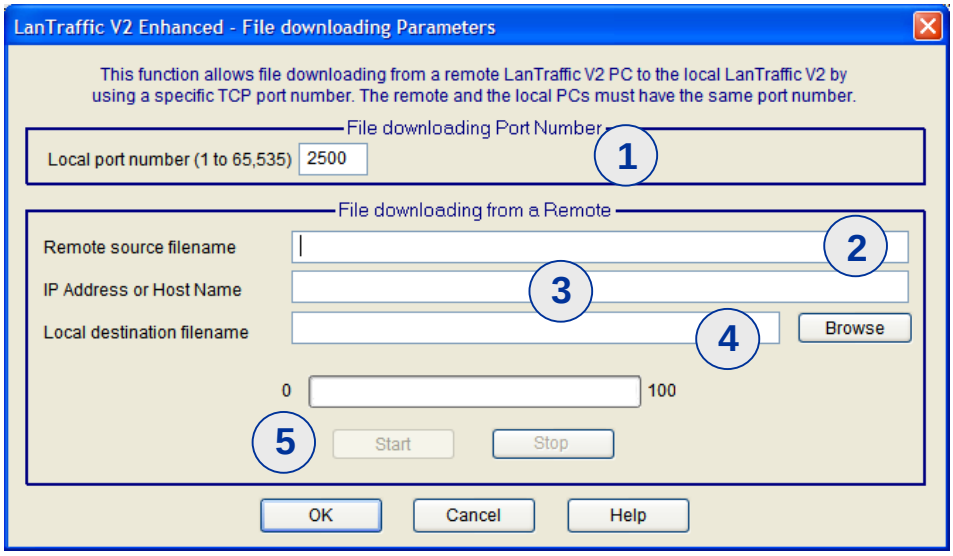
2: The user of the Local Sender machine can get the file back by using the File downloading function.

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 appears:



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. IPv4 or IPv6 address can be set up here.

(4) Give the local name of the destination file

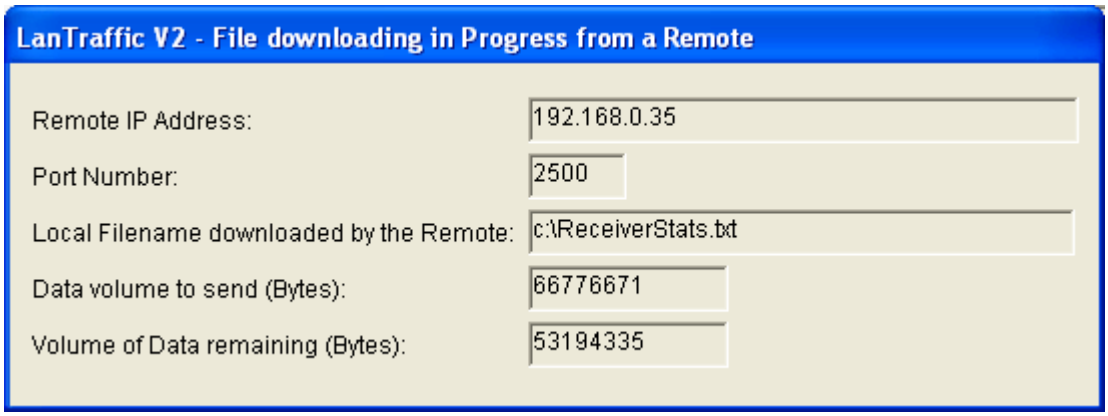
(5) Press “Start” button to begin the file downloading from the remote machine

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

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

*If you use a canonical name, the IP Address Translation mechanism (see § 9.4.1.1.3 IP Address translation mechanism) resolves it. In case of the resolution returns an IPv4 and an IPv6 addresses, **LanTraffic V2 Enhanced** selects the IPv4 address only.*

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



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

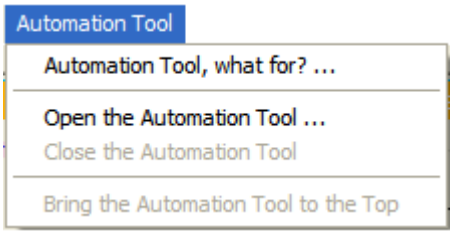
- Remote IP address is the IP address of the machine where the file to download is. This address is never in canonical format. This address can be an IPv4 or an IPv6 address.
- Port number is the port number chosen for file downloading (it must be the same for the remote and local machines).
- Local 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:

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

9.2.5 Automation Tool menu



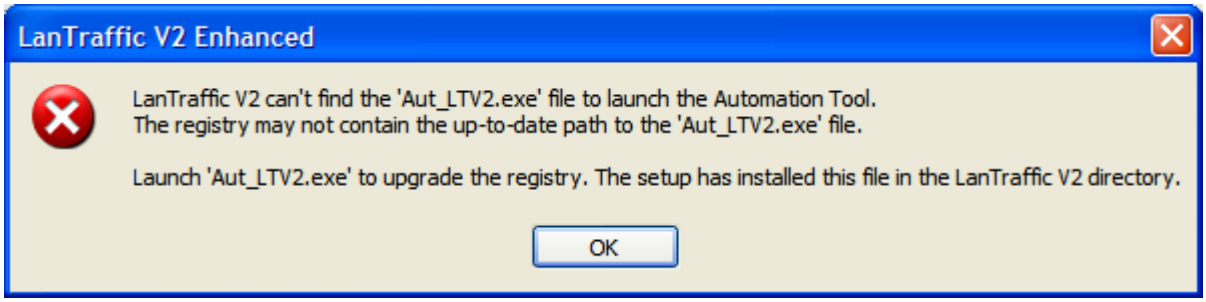
9.2.5.1 Automation Tool/Automation Tool, what for?…

This command opens a window showing a short presentation of the Automation Tool for LanTraffic V2 Enhanced.

9.2.5.2 Automation Tool/Open…

This command starts the "**Automation tool for LanTraffic V2 Enhanced**".
The "Open…" command is grayed when the "Automation tool for LanTraffic V2 Enhanced" is already started because only one instance can be active.

If the Aut_LTV2.exe file is not located in the same directory than **LanTraffic V2 Enhanced**, an error message is displayed:



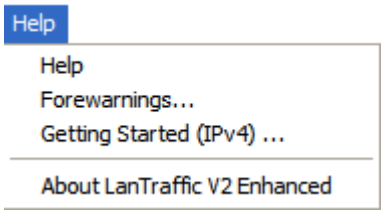
9.2.5.3 Automation Tool/Close

This command stops the **Automation tool for LanTraffic V2 Enhanced**.

9.2.5.4 Automation Tool/Bring to the top

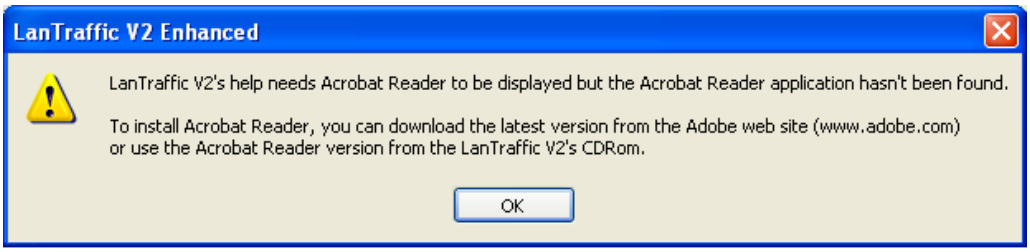
This command displays the **Automation tool for LanTraffic V2 Enhanced** window at the top of the other opened applications, except applications that can't be masked e.g. task manager when this option is selected.

9.2.6 Help menu



9.2.6.1 Help/Help

Help command displays help on **LanTraffic V2 Enhanced**. Pressing the **F1** key can also activate help. To display the **LanTraffic V2 Enhanced**'s 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 Enhanced**'s CD ROM and install Acrobat Reader.

LanTraffic V2 Enhanced doesn't support other PDF readers than Acrobat Reader.

9.2.6.2 Help/Forewarnings …

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

9.2.6.2.1 Inter packet delay

When defining the inter packet delay, you must consider that the minimum resolution handled by **LanTraffic V2 Enhanced** 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 Enhanced" is operating.
The best timer resolution that "LanTraffic V2 Enhanced" can provide is one millisecond.
LanTraffic V2 Enhanced operates in the best effort mode to provide the inter packet delay requested by the user.

9.2.6.2.2 Echoer modes

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

9.2.6.2.3 UDP connections

When several UDP connections are running and according to the traffic level and to the system load, **LanTraffic V2 Enhanced** can have strange behaviors due to the TCP/IP stack limits and working modes.

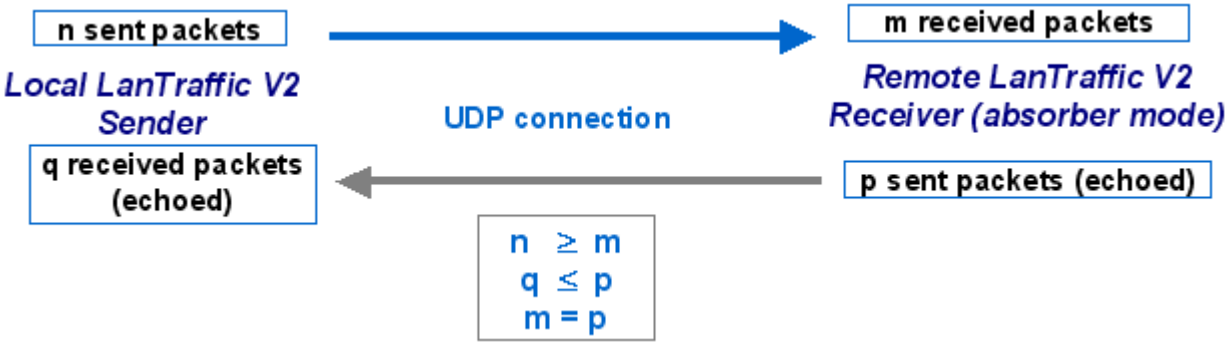
The current release of the Winsock2 API doesn't provide any system limit information to applications such as **LanTraffic V2 Enhanced**, so the following situations may occur.

- **Packets Loss**

The Winsock2 interface doesn't transmit all received packets to the **LanTraffic V2 Enhanced** 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, the 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 echoed connections.
Throughput of connections for the Receiver working in absorber mode may decrease to zero for a variable time.

- **UDP total throughput**

The total sending throughput can 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" (with Windows Server 2003 only) menu or to tune the Microsoft TCP/IP stack.

9.2.6.3 Help/Getting Started (IPv4)

The "Getting Started (IPv4)" command displays the Getting Started procedure.

9.2.6.4 Help/About LanTraffic V2 Enhanced

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

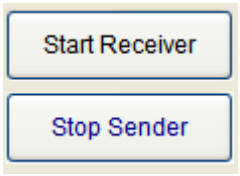
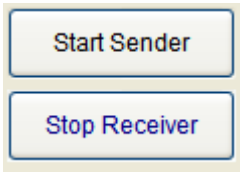
9.3 Total statistics

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

The statistics display refresh time and the sampling period to compute the throughputs are configured in the “Configuration / General Parameters” menu, as described in 9.2.3.2.

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 title of these buttons vary according to the activity state of each entity:

Sender *inactive* ***Receiver*** *inactive*	***Sender*** *active* ***Receiver*** *active*	***Sender*** *active* ***Receiver*** *inactive*	***Sender*** *inactive* ***Receiver*** *active*
			

9.3.1 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, UDP, and ICMP 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 Generator working mode on the Remote Receiver part.

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

9.4 The Sender part

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

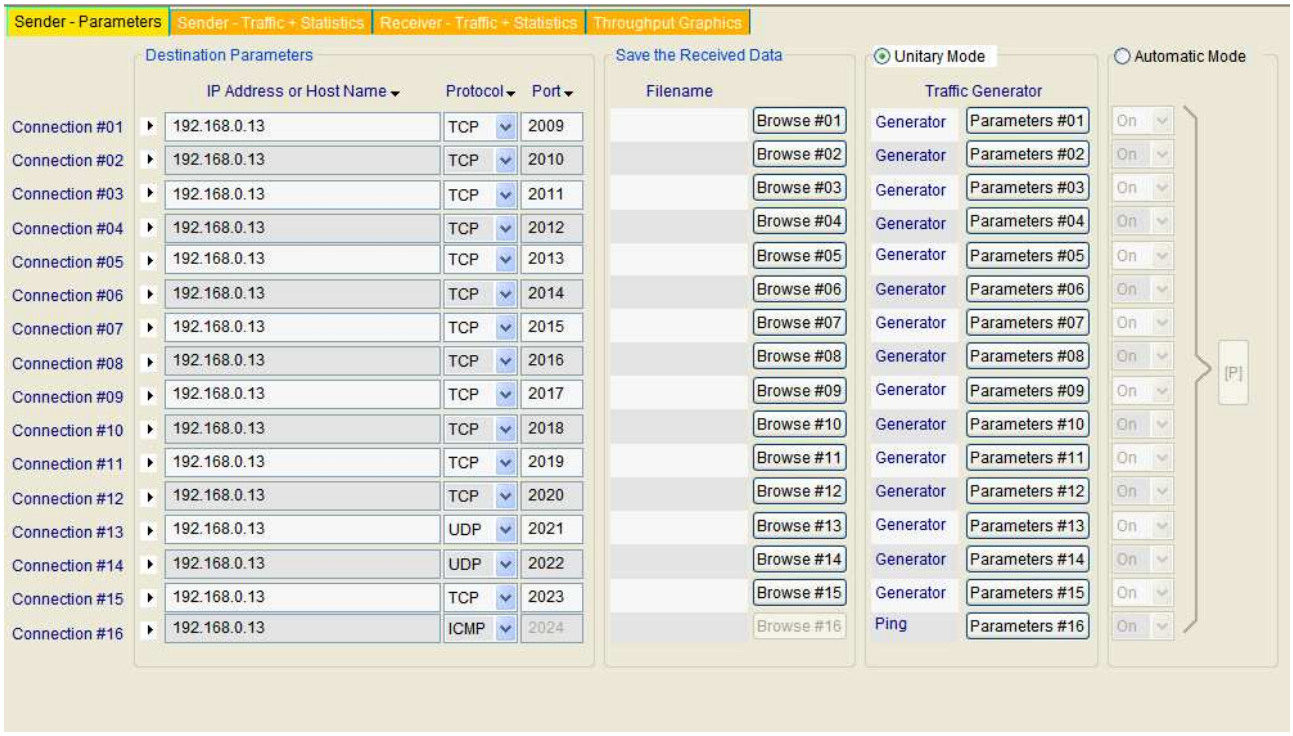
Sender part is represented in two tabs. The first one “Sender-Parameters” is used to configure connections and testing mode. The second one “Sender-Traffic + Statistics” is used to command the traffic generation and visualize the traffic statistics.

9.4.1 Sender - Parameters tab

The first tab of **LanTraffic V2 Enhanced** allows:

- Selecting the interface and the IP version (when IPv6 is installed) for each connection, by clicking the black arrow  .
- Entering the destination parameters (IP address, protocol and port number) for each connection.
- Selecting the files to save received data when connections are working in Echoer mode or 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.



Tab 1: "Sender – Parameters"

9.4.1.1 Destination parameters

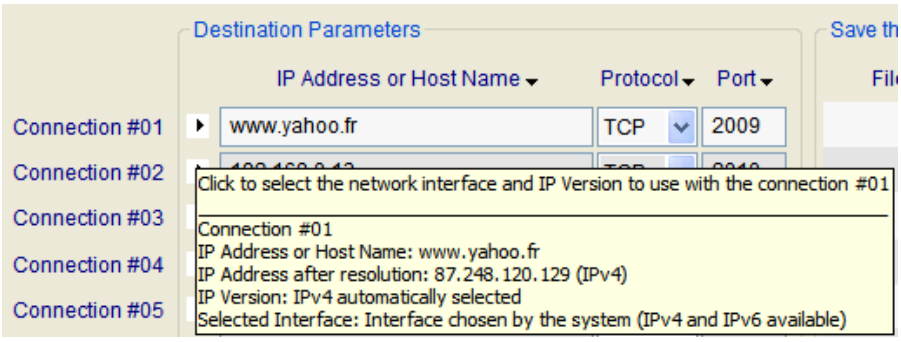
Located at the left part of the tab, this area allows configuring the destination parameters of each sending connection. You can enter the following information:

Network interface selection and IP version 	The black arrow has two purposes: • *To display a summary of the connection parameters.* • *To select the network interface, the IP version or the IP source address for a connection.*
IP address or Host Name	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). The default IP address is NO_ADDRESS (0.0.0.0 for IPv4). Once the value entered, verification is made and the field becomes red if the value is invalid.
Protocol	TCP, UDP or ICMP protocol (default = TCP protocol).
Port**	The port number is limited to 65,535. By default, the entered port number is 2009. In case of invalid value, the value is red colored.

*** Not available with ICMP connections*

9.4.1.1.1 Summary of connection parameters

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



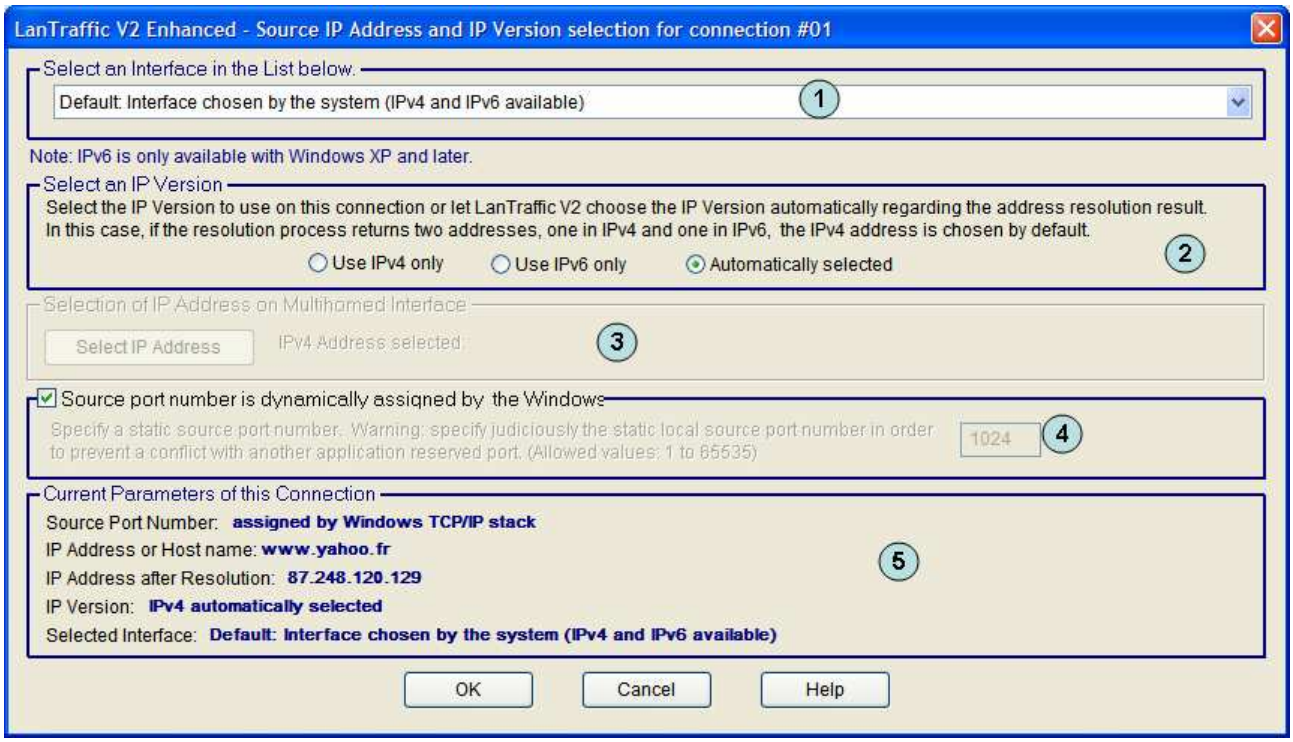
Sender connection tooltip

The tooltip for the Sender connection includes 5 items:

- The first item is the connection number the tooltip refers to.
- The next item is the IP address or Host Name defined by the user.
- The 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).
- The next item is the IP version currently selected.
- The 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").

9.4.1.1.2 Select the network interface, IP version and source IP address

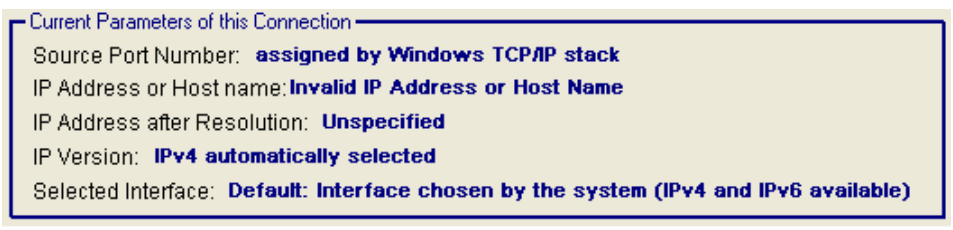
When you click on the black arrow, a window is displayed:



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

(1) The **network interface** selection is optional with IPv4. It is used to select the IPv6 or to force connections to be established using a specific interface.

- By default:
  - The IP version is automatically selected by **LanTraffic V2 Enhanced** regarding the destination address or host name specified on the “Sender - Parameters” tab (see below).
  - 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 the interface order, the IP address and the network address mask.
- You can select one interface from the list of the connected interfaces. **LanTraffic V2 Enhanced** will only use the selected interface to translate IP address and to make a connection. You must select the interface compatible with the remote IP address you want to reach. When the IP address translation failed, the current connection parameters area is updated as follows:



- Interface types are restricted: only Ethernet and PPP are listed. A PPP interface should be in a 'connected' state to belong to the interface list.

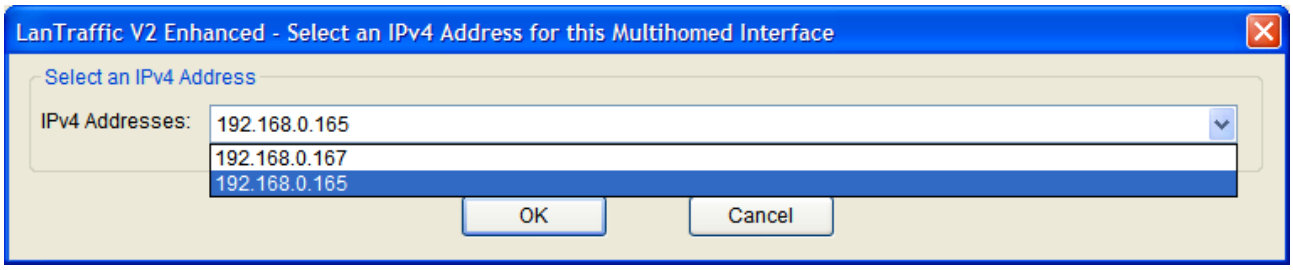
(2) The **IP version** selection is available:

- with all 64-bit Windows; please check if the IPv6 features is checked on your target interface.
- You can allow **LanTraffic V2 Enhanced** to choose automatically the good IP version regarding the address or host name resolution result. If a canonical name corresponds at the same time to an IPv4 and IPv6 address, **LanTraffic V2 Enhanced** chooses the IPv4 address. To use the IPv6 address, you should leave the automatic selection mode and specify the use of IPv6.

If you have selected an IP version, the IP address translation (see 9.4.1.1.3) uses the current selected 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. The selection of a Source IP address is generally not required: **LanTraffic V2 Enhanced** uses the default IP address of the interface to establish connections. It may be useful when routing priority or policy is defined.

Example of an 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) **Specification of the local source port number** is disabled by default. In this case, the system automatically chooses the source port number for any connection generating traffic. In order to respect the rules of a firewall for example, the source port number can be user defined.

(5) **'Current parameters of this connection'** area is an abstract for the connection. It summarizes the IP address, the numerical IP address format, the IP version and the interface selection.

- The source port used is dynamically updated with the user selection.
- IP addresses are static. The IP address translation will process when you click on OK only.
- 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.

9.4.1.1.3 IP Address translation mechanism

LanTraffic V2 Enhanced 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, or to another tab, when the Enter key is pressed or when the Interface parameters change, all of these actions start the IP address translation function.

Because the IP address translation mechanism is time consuming, you should be careful when using IP canonical addresses. The time 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 Enhanced** to restart the translation mechanism for this connection.

When the IP address translation failed, the IP address is written in red on a white background. 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:*

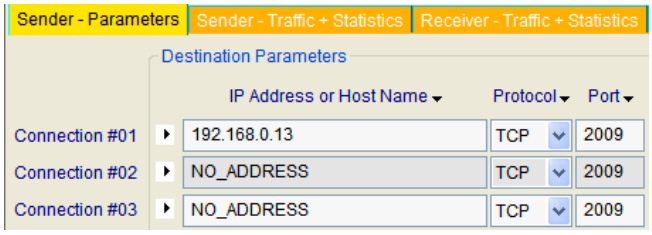
- *the focus leaves the ' IP Address or Host Name' field,*
- *another tab is selected,*
- *you duplicate parameters from one connection to another,*
- *you change the Interface parameters,*
- *a context file is loaded.*

If no IP version has been selected, the IP address translation mechanism chooses the good IP version regarding the IP version returned by the resolution process. If for example, a canonical name represents at the same time an IPv4 and an IPv6 addresses, the IP Address Translation mechanism chooses the IPv4 address. If you want to use the IPv6 address, you should select IPv6 version (see above).

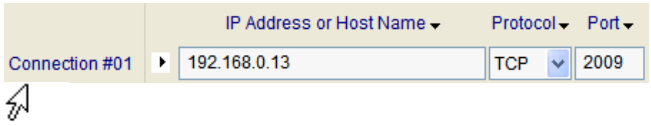
9.4.1.1.4 Duplicate parameters of a connection onto others

In order to facilitate the 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 into numerical format.
Duplication of connection parameters doesn't copy the interface information. When you copy a connection to another one, the IP address translation mechanism is started.

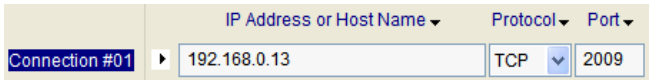
Step 1: first input parameters for a connection (by example, connection #01)



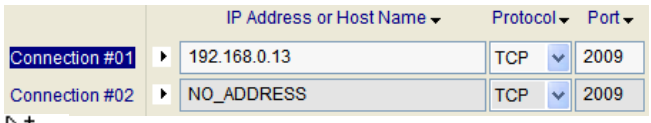
Step 2: move the mouse cursor on the 'Connection #1' label (source). The mouse cursor appears as shown beside.



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

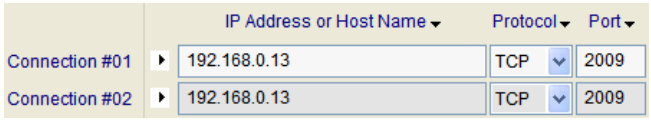


Step 4: when you move the mouse cursor on one another, 'Connection #02' label for example, the mouse cursor changes.



(Copy mode)

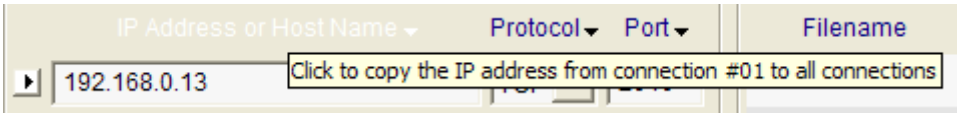
Step 5: then you can paste all parameters of connection #01 to the desired connection (#02 for example as target). Put the mouse cursor on the 'Connection #02' label and then use the left mouse button.



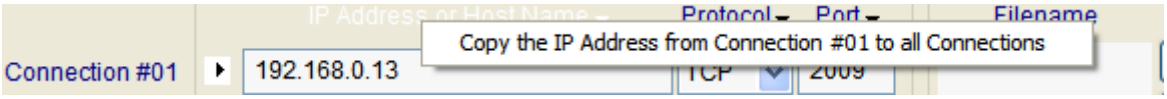
Note: this copy/paste function allows copying parameters from one connection (source) to another one (target). Repeat this process for other connections if needed.

9.4.1.1.5 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:



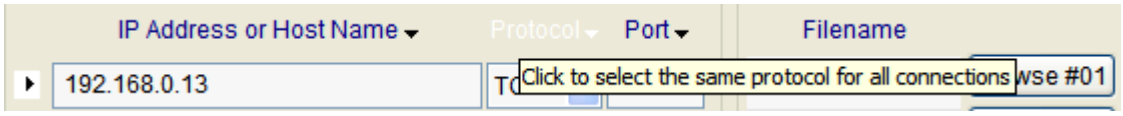
Click on the left mouse button to display the short menu as below:



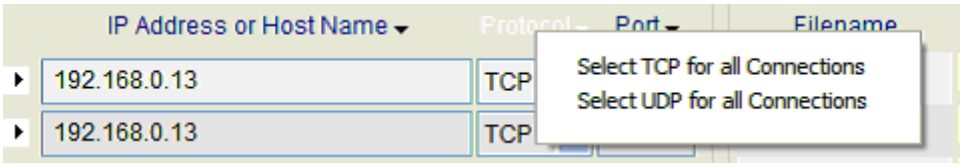
With this function the IP Address field from connection #01 is copied out on all connections from #02 to #16.

9.4.1.1.6 Protocol floating menu

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



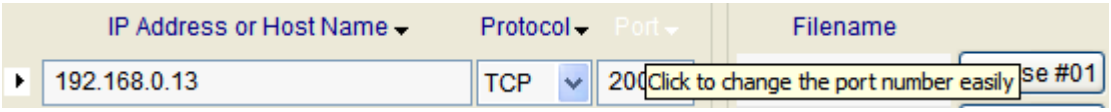
Click on the left mouse button to display the short menu as below:



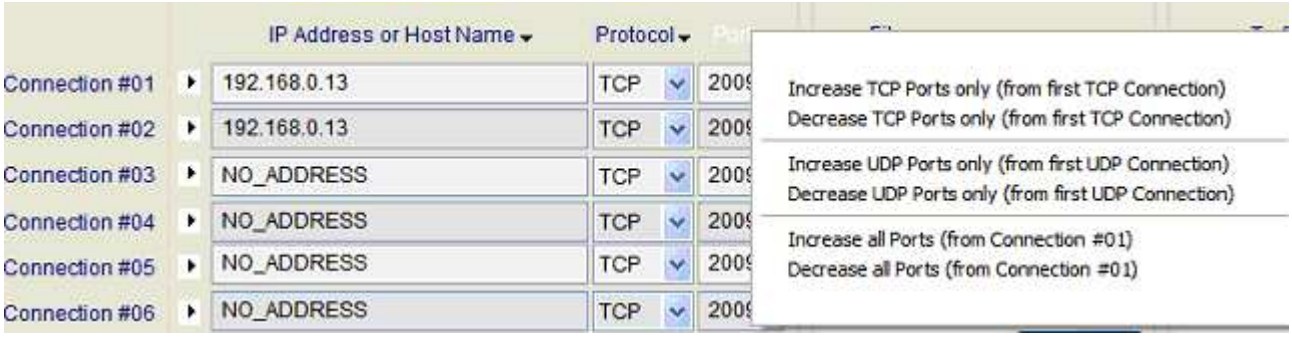
This menu helps to set the same protocol for all connections.

9.4.1.1.7 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 TCP connections, based on the port number of the first TCP connection,
- 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.

9.4.1.2 Save the Received Data (except for ICMP connections)

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 an easy file selection.

9.4.1.3 Configure the Unitary Mode for TCP and/or UDP

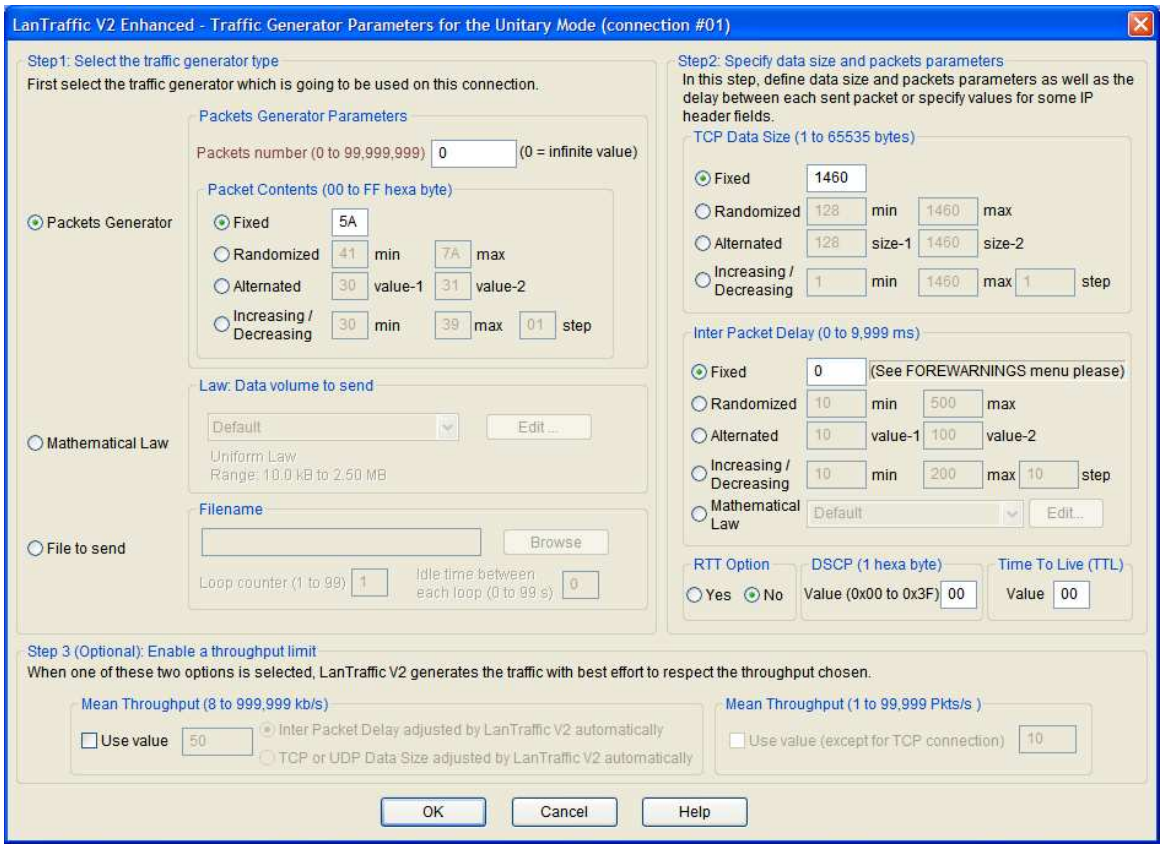
Unitary mode is one of the two testing mode offered by the **LanTraffic V2 Enhanced** Sender part. Notice that each testing mode is exclusive, i.e. it is impossible to mix connections in unitary testing and automatic testing modes.

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), DSCP value – 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” then the Parameters window is displayed.
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.



Unitary testing parameters window (IPv4)

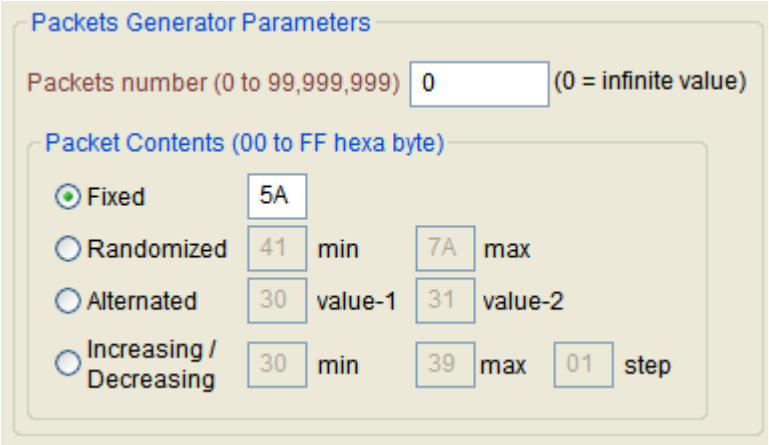
9.4.1.3.1 Step 1: select the traffic generator type for this connection

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)

9.4.1.3.1.1 Packets Generator

When the Packet Generator data source is selected, **LanTraffic V2 Enhanced** will generate an user-defined packets content for this connection.



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.

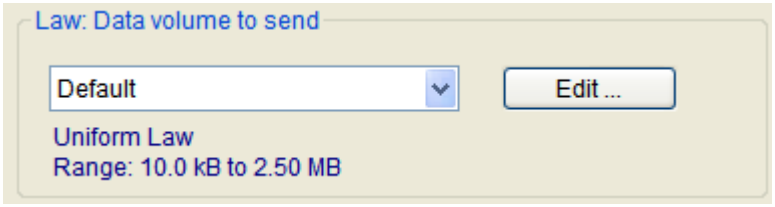
The packet contents can be configured as follows:

- **Fixed:** each packet has the same content.
- **Randomized: LanTraffic V2 Enhanced** computes random packet content included in a user-defined range (min to max).
- **Alternated: LanTraffic V2 Enhanced** 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 calculated. In statistics fields of the "Sender - Traffic + statistics" tab, "N/A" will be displayed.

9.4.1.3.1.2 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.



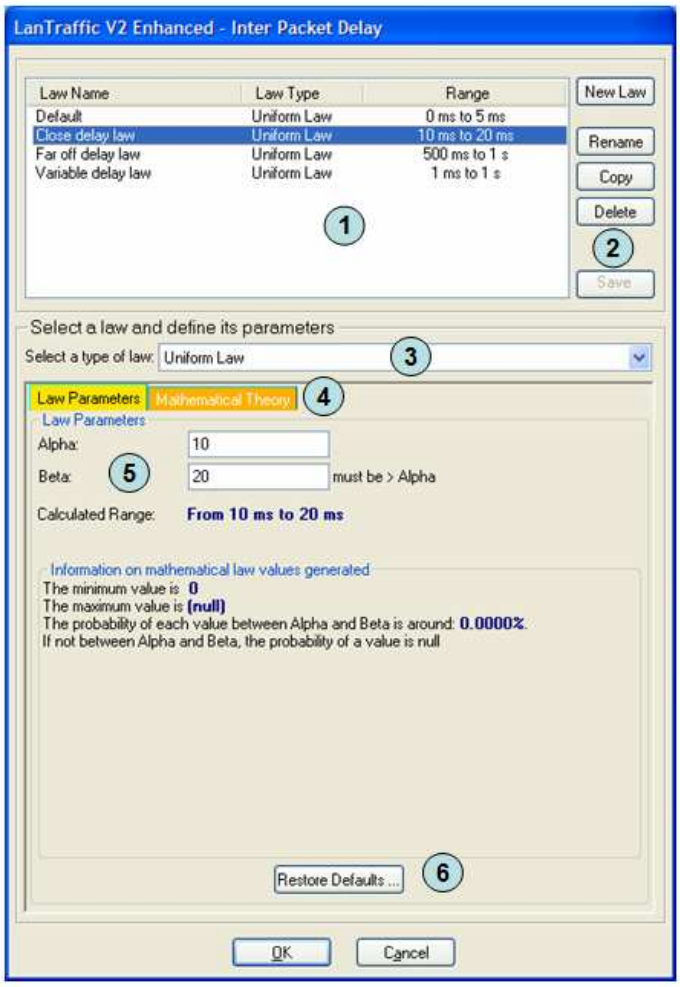
LanTraffic V2 Enhanced unitary testing mode offers four mathematical laws related to the data volume:

- Uniform law
- Exponential law
- Pareto law
- Gauss law

These laws are presented in details in the Appendix.

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 displayed:



Edit data volume to send law

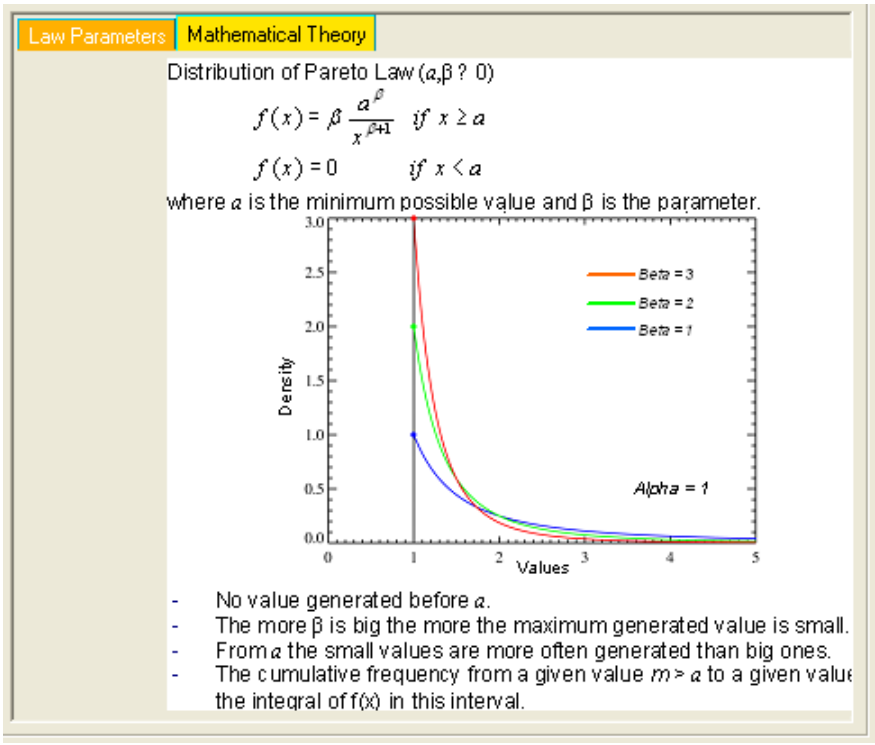
(1) The **'Law List'** area displays the list a existing law identified by the Law Name, the Law Type (one of the 4 mathematical laws) and the range of values. The Law Name is an editable area used to change the name of the law. To change the Law Name, you click in the list on the name you want to change or you use the **Rename** button.

(2) There are 5 buttons to modify the list of laws :

- **New Law:** This button should be used to create a new law (see below for more details).
- **Rename:** This button is used to change the law name like when you click on the law name.
- **Copy:** This button increases the way to create a law from an existing one.
- **Delete:** This button should be used to delete an existing law. You should confirm the deletion.
- **Save:** This button should be used to save any modification in the law list.

(3) The **'Type of Law'** area displays the 4 mathematical laws. It should be used to select the law type of the Law. When the Law Type changes, the law parameters may be checked against an unexpected range of values.

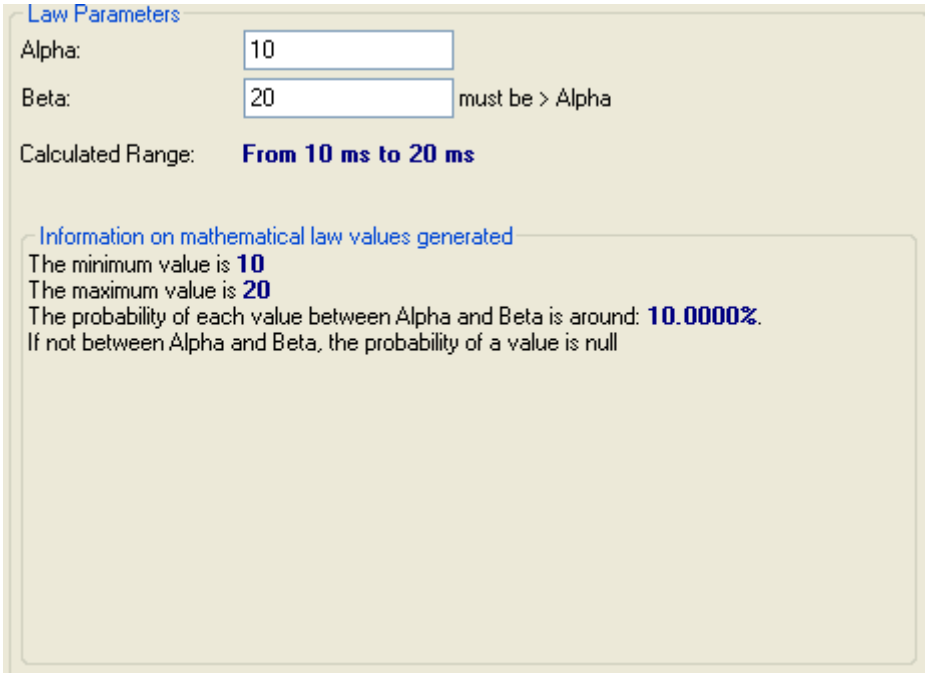
(4) The **'Law Parameters' or 'Mathematical Theory'** tabs display either the parameters of the law or the related Mathematical Theory of the current selected law. The number of parameters and the Mathematical Theory depend on the selected type of law. The next figure illustrate the Pareto law Mathematical Theory:



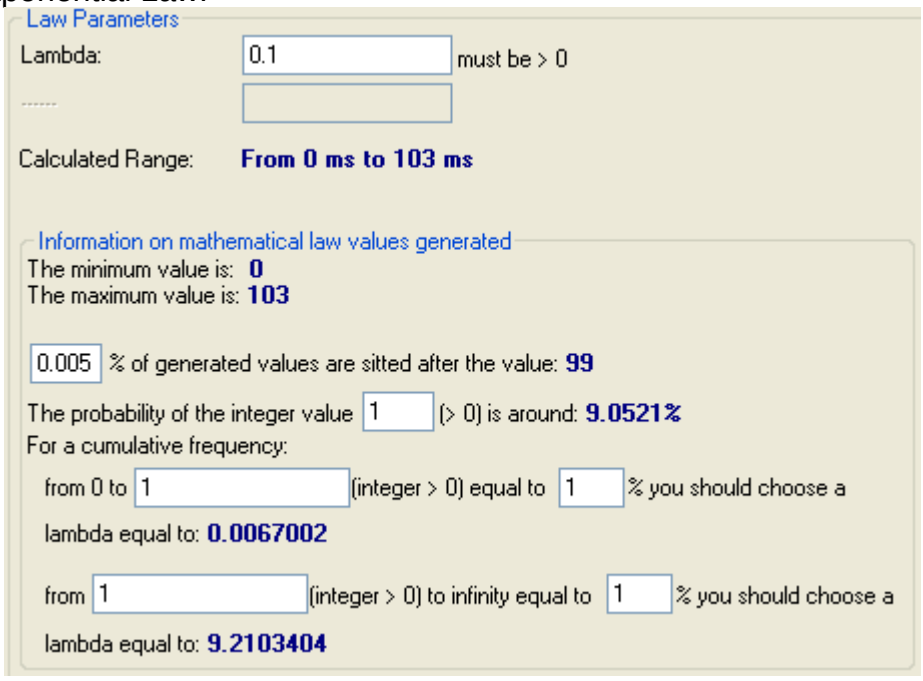
(See Appendix 12.1 Mathematical laws used by LanTraffic V2 Enhanced for more details about Mathematical laws).

(5) The **'Law Parameters'** area allows entering values of the law. Depending on the law, the parameters and the user help regarding specific statistical values change, as shown below:

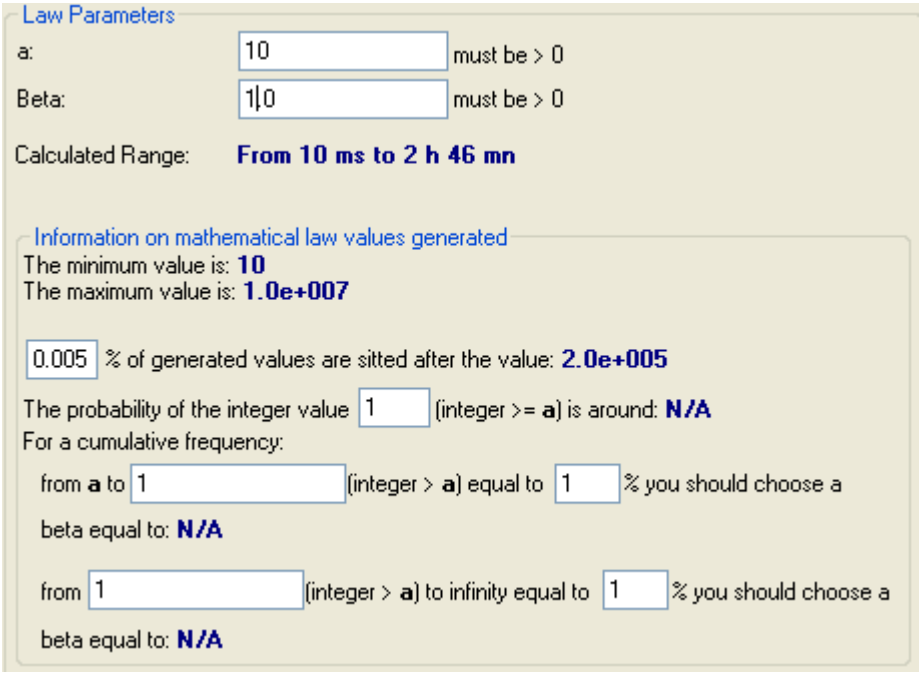
- Uniform Law:



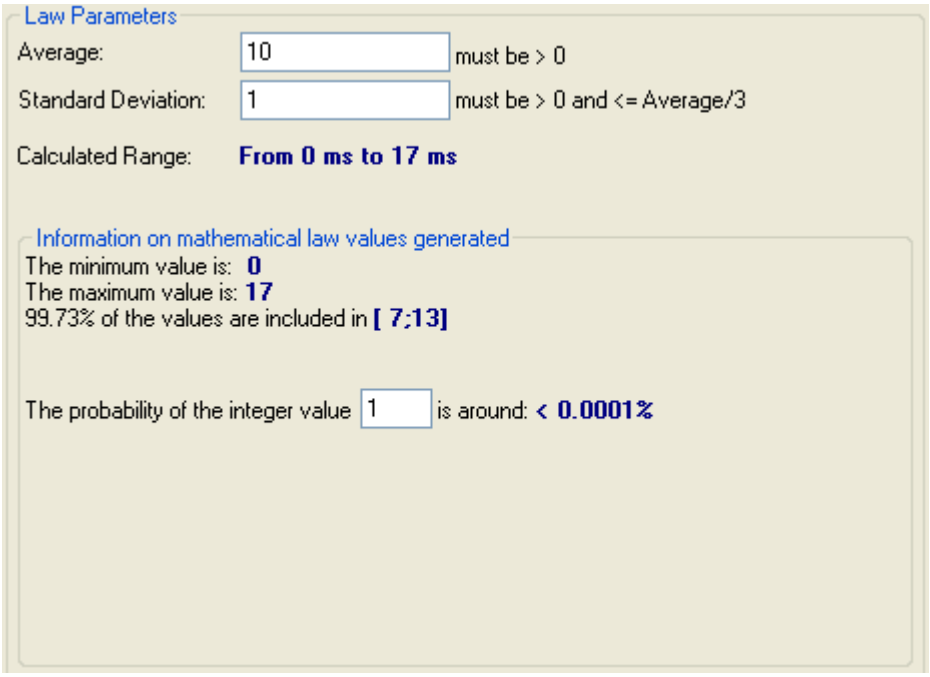
- Exponential Law:



- Pareto Law:



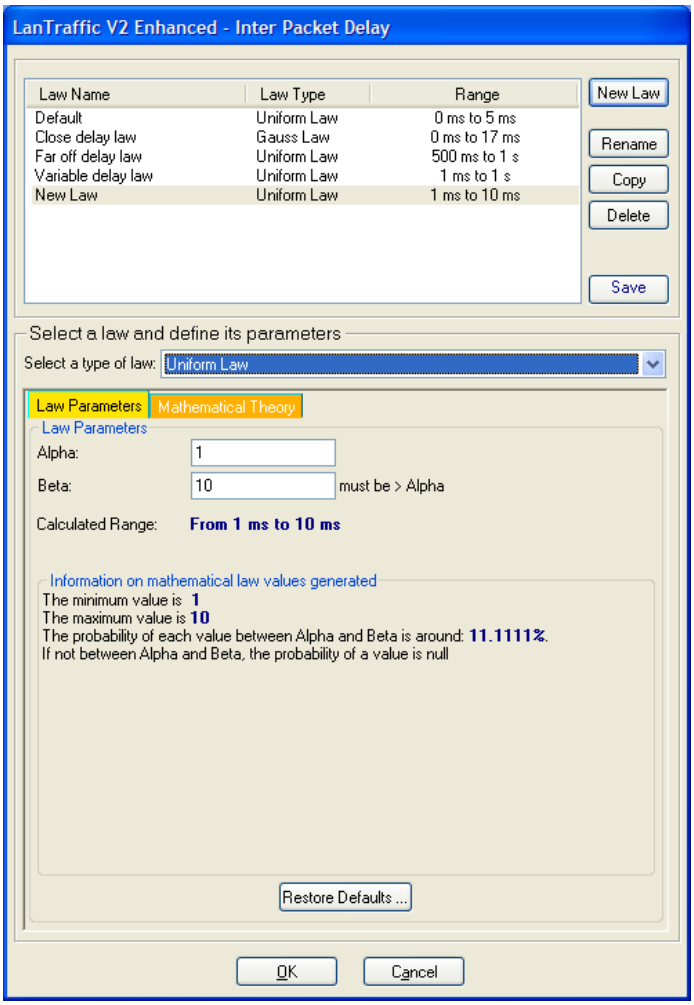
- Gauss Law



(6) The **'Restore Defaults'** button change the values of the two parameters respectively to 10 and 1 (when the second parameter applies).

To add a new data volume to send law:

1. Press the “New Law” button, then a new Law List Entry is created, with the ‘Uniform Law’ as default Law Type :



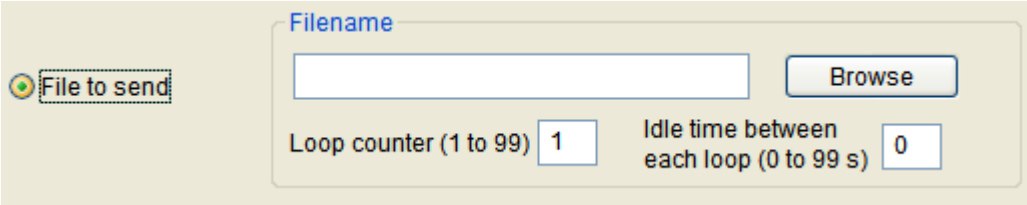
2. Rename the Law by using the Rename button or by editing the Law Name
3. Select the requested mathematical Law Type: Exponential, Uniform, Pareto or Gauss.
4. Enter parameters value for the selected mathematical law (1 or 2 parameters are required depending on the selected law),
5. Repeat operation 1 to 4 to create other laws.
6. Press the ‘Save’ button to register changes. Your last law is selected in the parent window when you press the OK button.

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.

9.4.1.3.1.3 File to send

With this selection **LanTraffic V2 Enhanced** sends the file defined in the 'Filename' sub-area.
The 'Browse' button is made to ease the “file to send” selection.



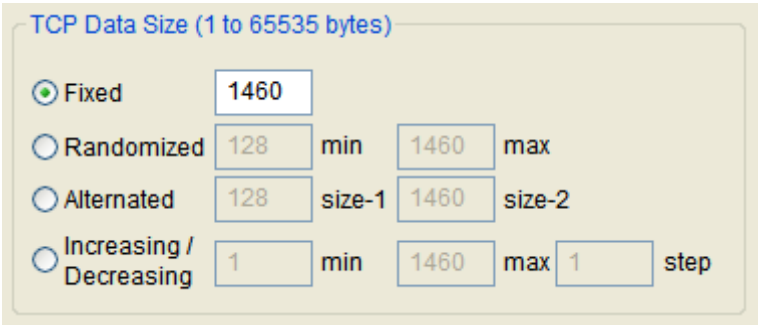
The **Loop counter** should be greater than 0. Each time the file is sent, the loop counter decreases and when the 0 value is reached, the traffic generator stops.

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 the TCP protocol is used (default TCPTimeout value is 5 seconds) because the remote disconnects when the timeout is reached.

9.4.1.3.2 Step 2: Specify data size and packets parameters

9.4.1.3.2.1 Data Size

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



The maximum accepted value depends on the protocol:

- For TCP, the maximum Data Size is **65,535.**
- For UDP, the maximum Data Size is **65,507.**

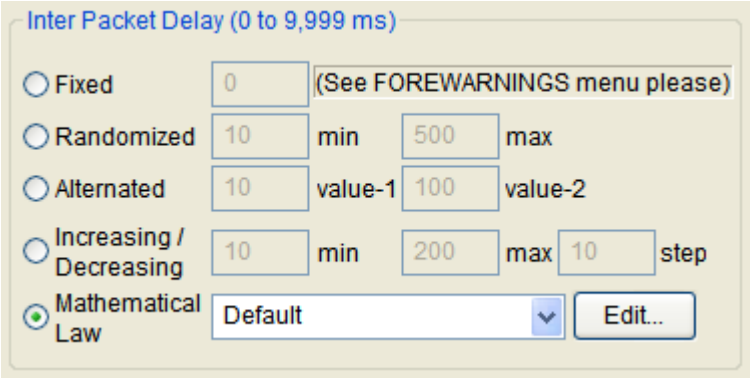
0 (null) is not a valid value. By default, the entered value is 1,460. This value is the default payload for TCP with IPv4. When IPv6 is selected, the payload should be shorter. Packet size can be configured as follows:

- **Fixed**: 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.
- **Randomized: LanTraffic V2 Enhanced** computes a random packet size included in a range specified by the user for each packet to send.
- **Alternated:** two values must be defined. **LanTraffic V2 Enhanced** 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 Enhanced** 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 9.4.1.3.2.3 about the RTT option).*

9.4.1.3.2.2 Inter Packet Delay

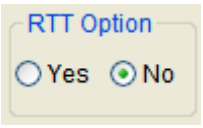
This parameter allows defining the time interval between two packets. Values are limited to 9,999 milliseconds i.e. 10 seconds. A value of zero means no inter-packet delay.



The inter-packet delay can be configured as follows:

- **Fixed**: inter-packet delay is the same for all transmitted packets.
- **Randomized**: **LanTraffic V2 Enhanced** computes a random inter-packet delay included in a range specified by the user for each packet to send.
- **Alternated**: two values must be defined. **LanTraffic V2 Enhanced** 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).

9.4.1.3.2.3 RTT option



When 'Yes' is selected, **LanTraffic V2 Enhanced** adds RTT (Round Trip Time) header information into packets without changing the data size defined.

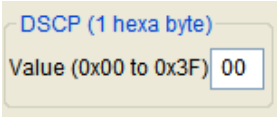
The RTT header format is:

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

This information is 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 paragraph 9.4.1.2). At the Remote Receive side, RTT information is checked to update 'sequencing errors' and jitter statistics.

9.4.1.3.2.4 The DSCP field (with IPv4 only)

This field is available only if IPv4 is selected for the corresponding connection. Under Windows Vista and later, the DSCP field is not available for ICMP connections.



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

The Differentiated Services Code Point is a selector for router's per-hop behaviors. Because it is a selector, there is no implication that a numerically greater DSCP implies a better network service. The RFC 2474 redefined the Type of Service Byte to be:

7	6	5	4	3	2	1	0
Differentiated Services Code Point						ECT	CE

The ECT and CE fields don't refer to the DiffServ quality of service. They are spare bits in the IP Header used by the Explicit Congestion Notification (see RFC 3168 for more details).

This leads the notion of "class", each class being a group of the DSCPs with the same *Precedence* value. Values within a class offer similar network services but with slight differences (different levels of service such as "gold", "silver" and "bronze").
From the initial definition of the RFC 2474, RFC 2697 added the "assured forwarding" service and RFC 2598 defined the "expedited forwarding" service.

The DSCP values are defined as following:

DSCP (Hexa value)	Service	IP header TOS field value in hexadecimal *(if ECT = 0 and CE = 0)*
0 (0x00)	**Best effort**	**0x00**
8 (0x08)	**Class 1**	**0x20**
10 (0x0A)	Class 1, gold (AF11)	0x28
12 (0x0C)	Class 1, silver (AF12)	0x30
14 (0x0E)	Class 1, bronze (AF13)	0x38
16 (0x10)	**Class 2**	**0x40**
18 (0x12)	Class 2, gold (AF21)	0x48
20 (0x14)	Class 2, silver (AF22)	0x50
22 (0x16)	Class 2, bronze (AF23)	0x58
24 (0x18)	**Class 3**	**0x60**
26 (0x1A)	Class 3, gold (AF31)	0x68
28 (0x1C)	Class 3, silver (AF32)	0x70
30 (0X1E)	Class 3, bronze (AF33)	0x78
32 (0x20)	**Class 4**	**0x80**
34 (0x22)	Class 4, gold (AF41)	0x88
36 (0x24)	Class 4, silver (AF42)	0x90
38 (0x26)	Class 4, bronze (AF43)	0x98
40 (0x28)	**Express forwarding**	**0xA0**
46 (0x2E)	Expedited forwarding (EF)	0xB8
48 (0x30)	**Control**	**0xC0**
56 (0x38)	**Control**	**0xE0**

9.4.1.3.2.4.1 How to allow the use of the DSCP field on Windows 2000, XP and Server 2003

Using Registry Editor inaccurately 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. Note that you should back up the registry before editing it. If you are running Windows 2000 or XP you should also update your Emergency Repair Disk (ERD). 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.

Step1: Start Registry Editor (regedit.exe). Go to the following key on Local Machine:

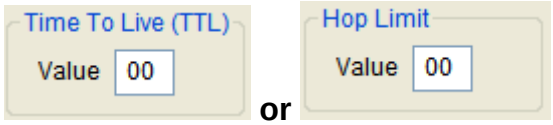
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

Step 2: 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.

9.4.1.3.2.4.2 How to allow the use of the DSCP field on Windows Vista

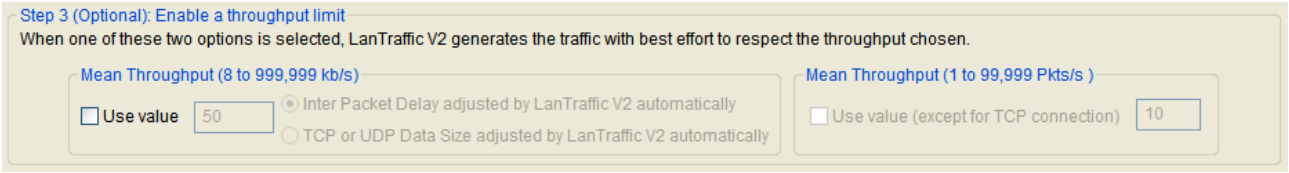
The DSCP field is available for TCP and UDP only. Moreover, to be allowed to use the DSCP field, you must have the administrator rights. You must launch LanTraffic V2 Enhanced using the shortcut **Start > All Programs > LanTraffic V2 Enhanced > LanTraffic V2 Enhanced (Run as administrator).**

9.4.1.3.2.5 The TTL field

 **IPv4** **IPv6**	The user can input the TTL/Hop Limit value (hexadecimal) used for each packet sent on the connection. Default value = 00.

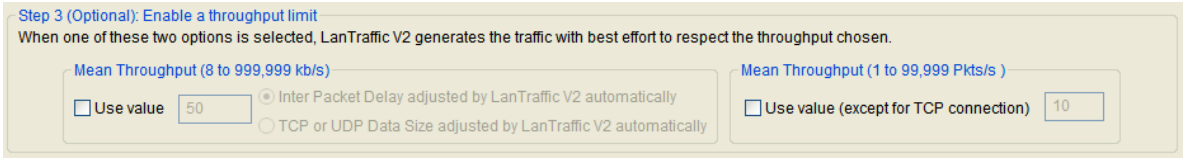
9.4.1.3.3 Step 3 (optional): Activate a throughput limit

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



With this feature, you can define a throughput limit for this connection (in Kilo bits per second) with the 'Use value' check box. You specify the mean throughput in Kbps in the edit box and select one of the two parameters (packet size or inter packet delay). **LanTraffic V2 Enhanced** 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 a UDP connection, the mean throughput is expressed in kb/s or in Kib/s, or it can also be expressed in number of packets per second (Pkts/s):

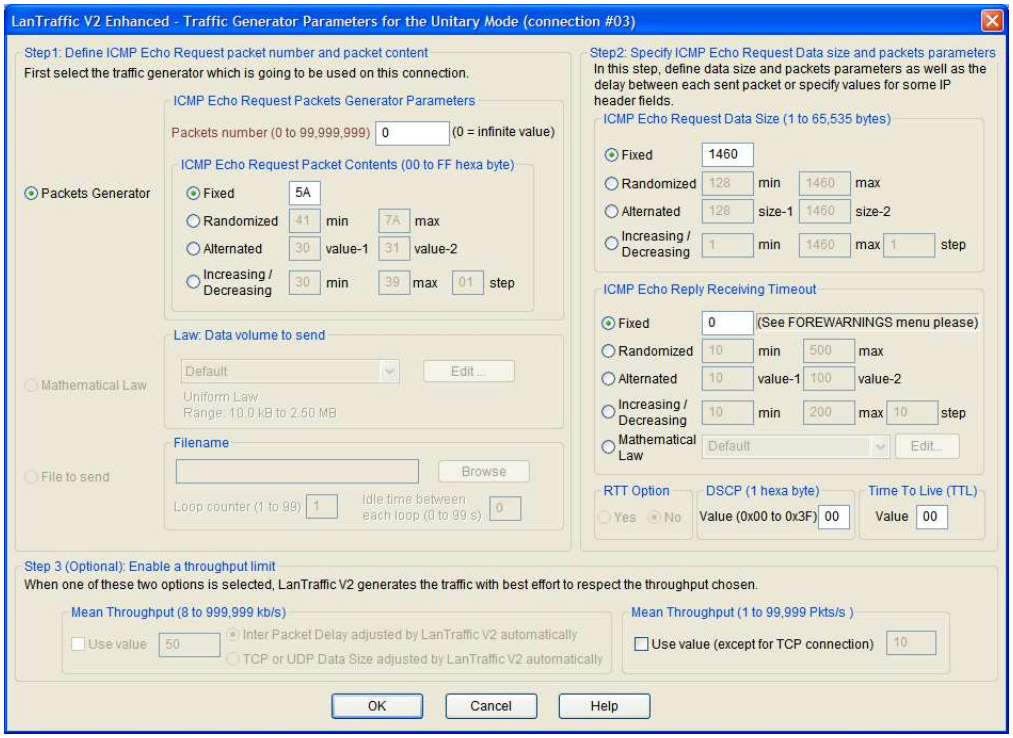


The throughput value must be greater than or equal to 8 Kbps.

9.4.1.4 Configure the Unitary Mode for ICMP connections

LanTraffic V2 Enhanced offers the possibility to generate ICMP Echo Request traffic (the protocol used by Ping), which can use IPv4 or IPv6 IP version.

The ICMP protocol is available with the unitary mode only. You are still allowed to use TCP and/or UDP on other connections. By pressing the “Parameters #n” button, the window below is displayed:



Three areas are proposed to configure the Ping Simulator:

- In the Step 1, the packets number and the packet content can be specified.
- In the upper part of the Step 2, the ICMP Echo Request data size can be defined (up to 65535 bytes).
- The lower part of Step 2 allows the definition of the replies timeout.
- In Step 3 you can define the mean packet throughput.

Note: more information about these three areas is available in paragraph 9.4.1.3

For the “Sender – Traffic + Statistics” tab, four statistics are available when using ICMP Echo Request:

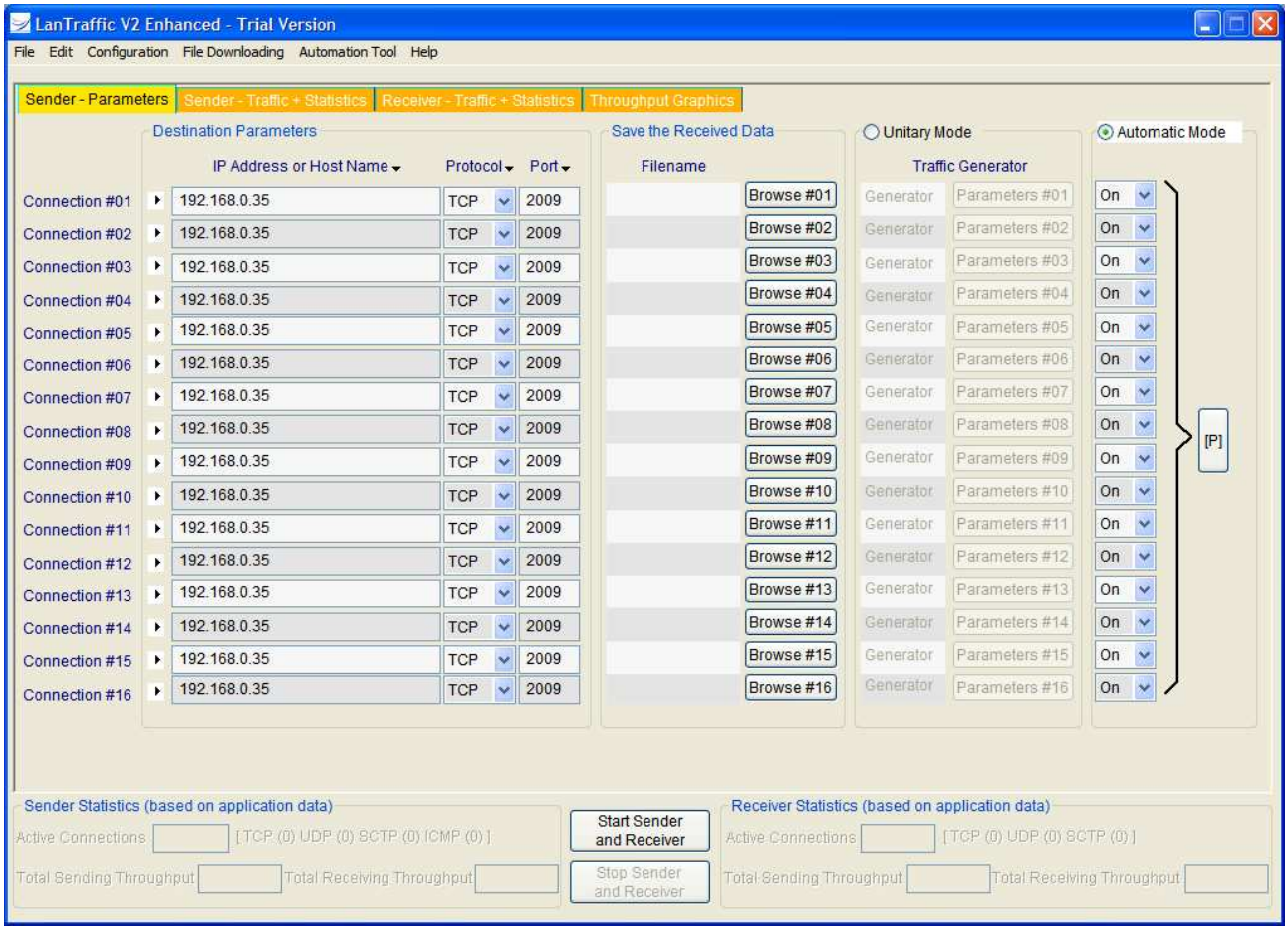
- Tx packets: this value represents the number of ICMP Echo Request packets sent.
- Rx packets: this value is the number of ICMP Echo Reply packets received.
- RTT: this value shows the mean Round Trip Time.
- Seq. Num. Errors (Sequence Numbering Errors): this value represents the number of replies that “LanTraffic V2 Enhanced” does not receive.

9.4.1.5 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.

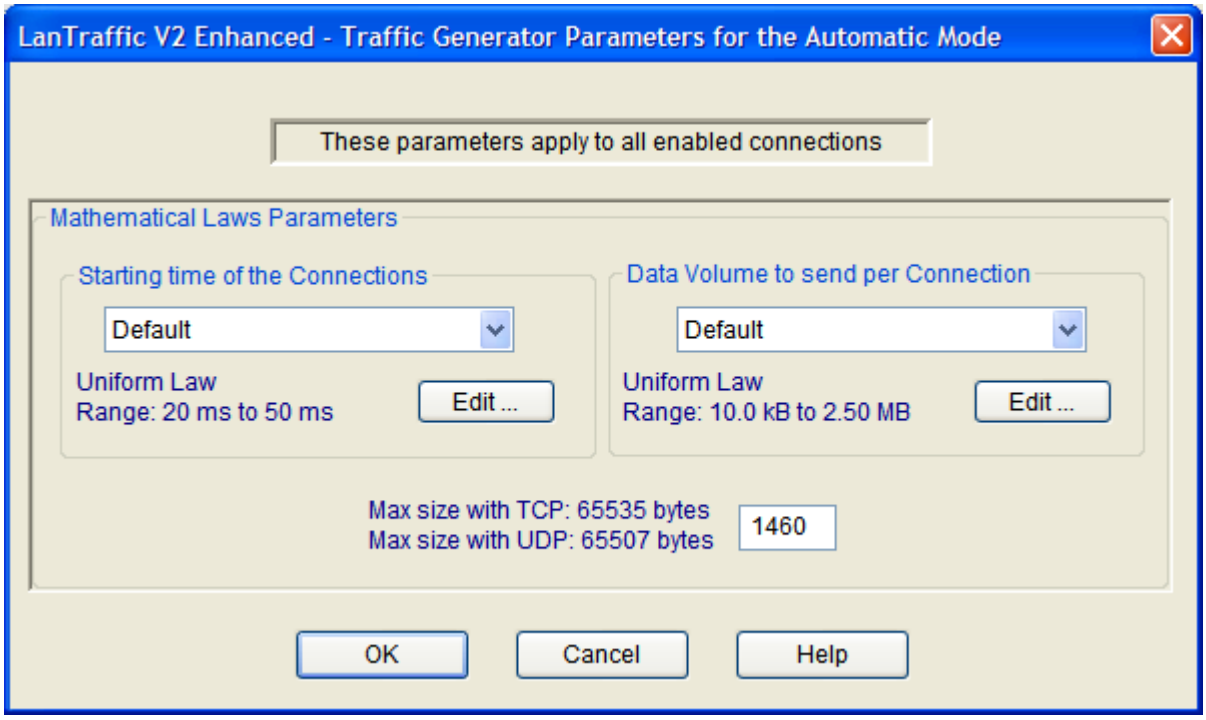
As the unitary testing mode, the automatic testing mode is configured in Tab 1” Sender – Parameters” and run in Tab 2 “Sender Traffic +Statistics”.

Once the 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 displayed allowing to configure the automatic testing mode parameters:

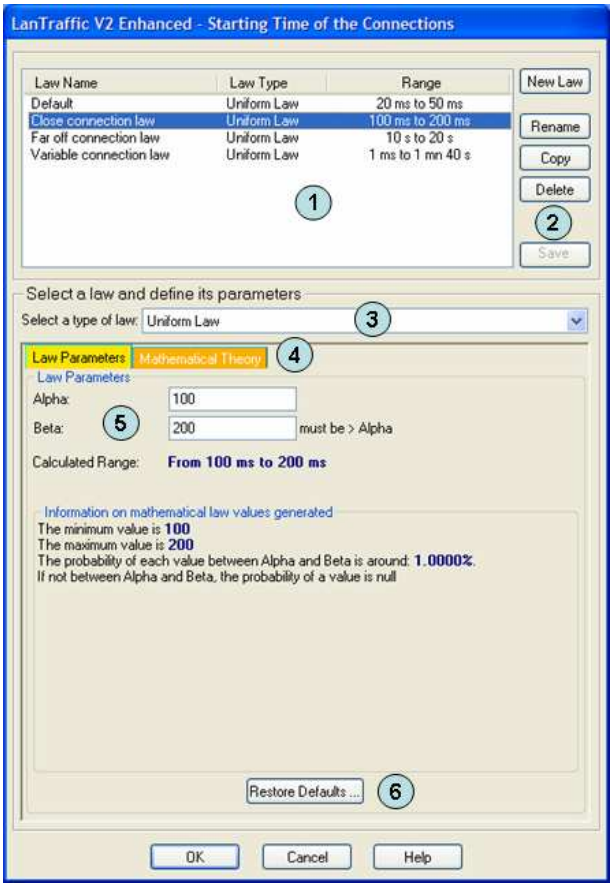
ICMP can't be used with the Automatic Mode. In that case, the ICMP connections are not started.



Automatic testing parameters window

9.4.1.5.1 Starting time connections generation laws

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



Starting time connections generation law window

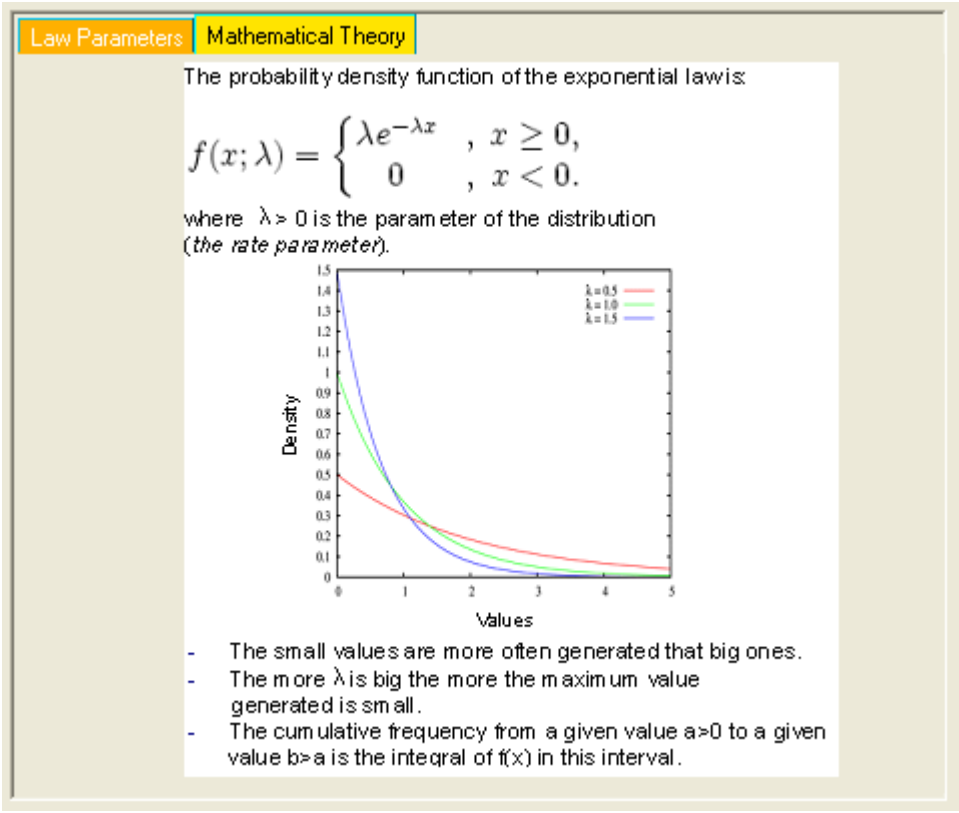
(1) The **'Law List'** area displays the list a existing law identified by the Law Name, the Law Type (one of the 4 mathematical laws) and the range of values. The Law Name is an editable area used to change the name of the law. To change the Law Name, you click in the list on the name you want to change or you use the **Rename** button.

(2) There are 5 buttons to modify the list of laws :

- **New Law:** This button should be used to create a new law (see below for more details).
- **Rename:** This button is used to change the law name like when you click on the law name.
- **Copy:** This button increases the way to create a law from an existing one.
- **Delete:** This button should be used to delete an existing law. You should confirm the deletion.
- **Save:** This button should be used to save any modification in the law list.

(3) The **'Type of Law'** area displays the 4 mathematical laws. It should be used to select the law type of the Law. When the Law Type changes, the law parameters may be checked against an unexpected range of values.

(4) The **'Law Parameters' or 'Mathematical Theory'** tabs display either the parameters of the law or the related Mathematical Theory of the current selected law. The number of parameters and the Mathematical Theory depend on the selected type of law. The next figure illustrate the Pareto law Mathematical Theory:

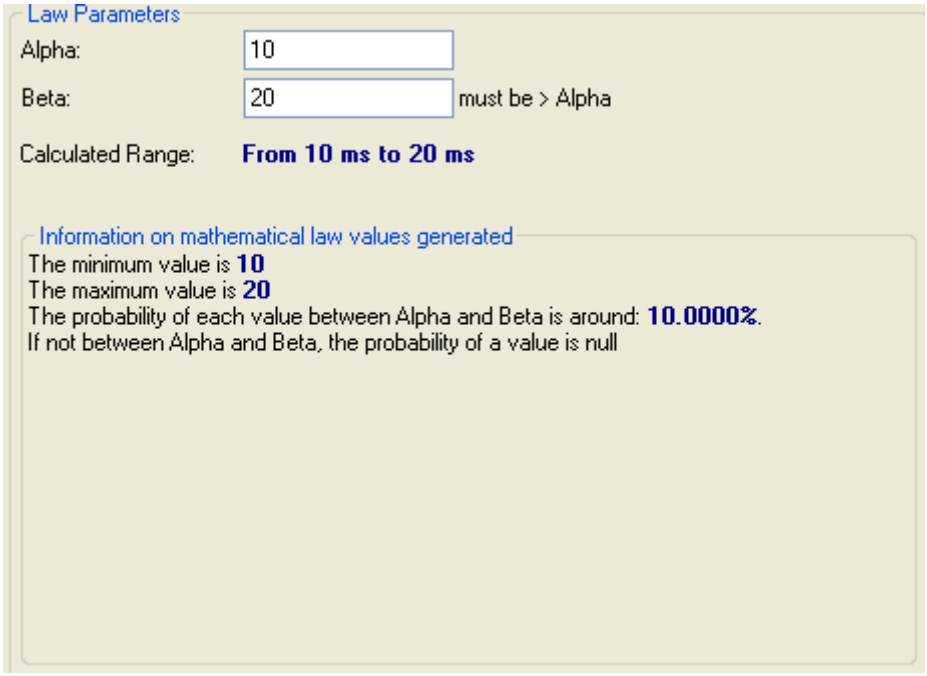


.

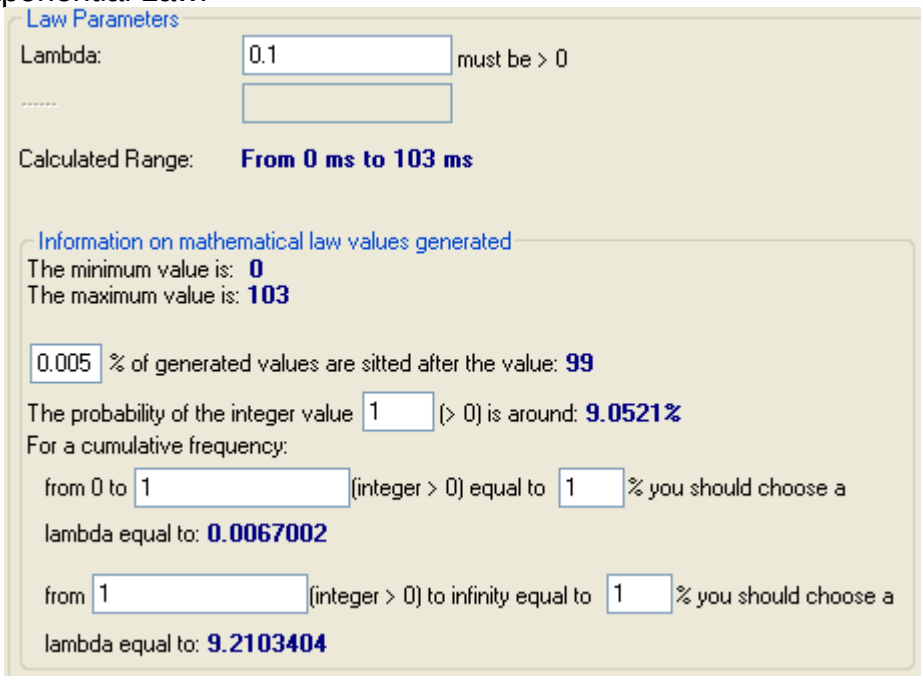
(See Appendix 12.1 Mathematical laws used by LanTraffic V2 Enhanced for more details about Mathematical laws).

(5) The **'Law Parameters'** area allows entering values of the law. Depending on the law, the parameters and the user help regarding specific statistical values change, as shown below:

- Uniform Law:

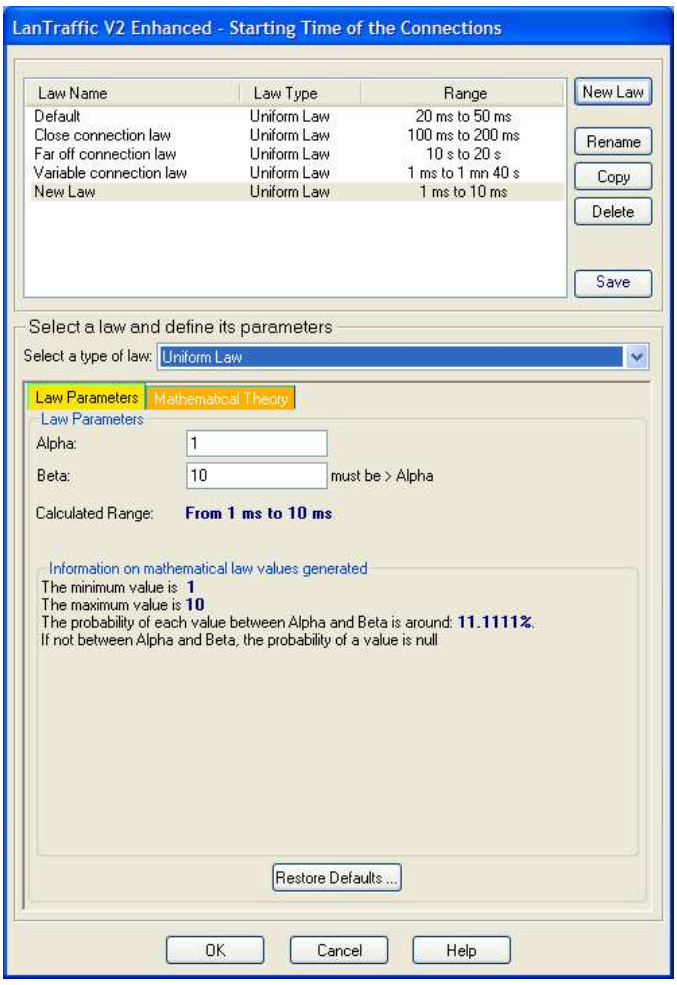


- Exponential Law:



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

1) Press the “New Law” button, then a new Law List Entry is created, with the ‘Uniform Law’ as default Law Type :



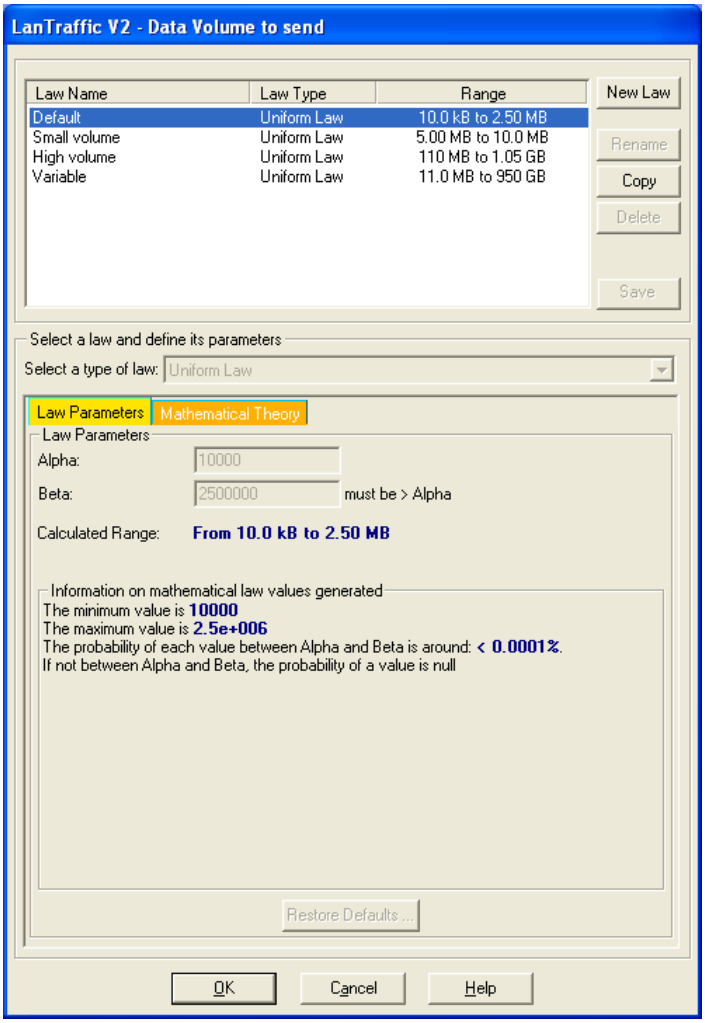
Edit starting time connections generation law window

2) Rename the Law by using the Rename button or by editing the Law Name
3) Select the requested mathematical Law Type: Uniform, Exponential.
4) Enter parameters value for the selected mathematical law (1 or 2 parameters are required depending on the selected law),
5) Repeat operation 1 to 4 to create other laws.
6) Press the ‘Save’ button to register changes. Your last law is selected in the parent window when you press the OK button.

Note that the **Default** law can’t be changed.

9.4.1.5.2 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, Pareto and Gauss laws. (Mathematical laws are presented in details in Appendix paragraph 12.1). You can add, modify, rename or delete a law by pressing the “Edit” button. Then the Data Volume Laws windows appear, as following:

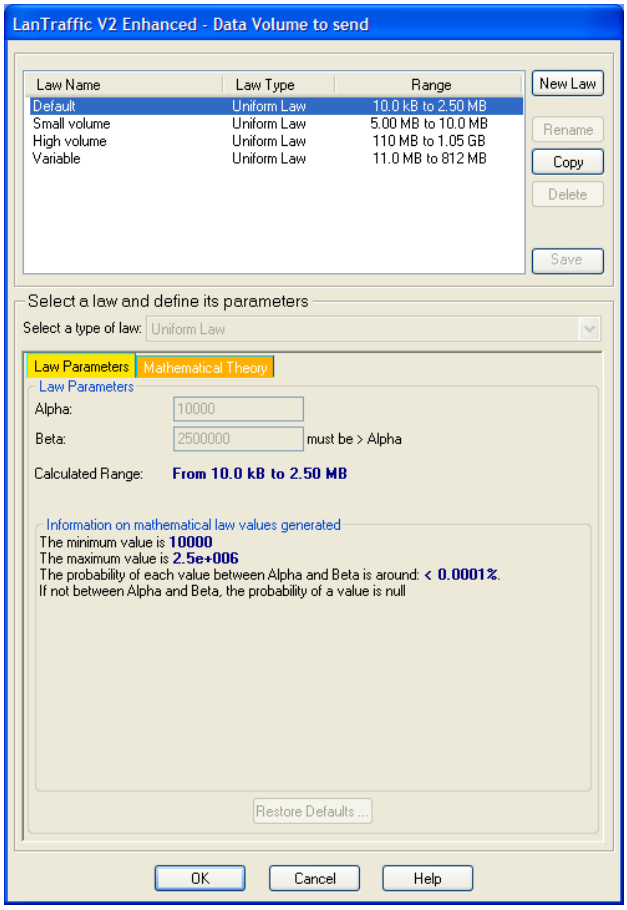


Volume law window

Note that the **Default** law can’t be changed.

To add a new data volume to send law:

1. Press the “New Law” button, then a new Law List Entry is created, with the ‘Uniform Law’ as default Law Type :



Edit data volume law window

2. Rename the Law by using the Rename button or by editing the Law Name
3. Select the requested mathematical Law Type: Exponential, Uniform, Pareto or Gauss.
4. Enter parameters value for the selected mathematical law (1 or 2 parameters are required depending on the selected law),
5. Repeat operation 1 to 4 to create other laws.
6. Press the ‘Save’ button to register changes. Your last law is selected in the parent window when you press the OK button.

According to the operating system used (Windows 2000, XP, Server 2003 or Windows Vista), the WinSock 2 interface could present number-limits of the incoming simultaneous calls. Consequence for LanTraffic V2 Enhanced is the presence of “connection failed”, particularly when the 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 Enhanced”. To reduce these failures, decrease the frequency of connections or increase the data volume.

9.4.1.5.3 Packet 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 for TCP. For UDP, it is limited to 65,507 bytes.

9.4.2 Sender - Traffic + Statistics tab

This second tab related to the Sender allows:

- Displaying destination parameters of each connection,
- Displaying traffic statistics for each connection,
- Starting and stopping each connection if the unitary testing mode is selected.
- Starting and stopping all enabled connections if the automatic testing mode is selected.

⚠ ***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

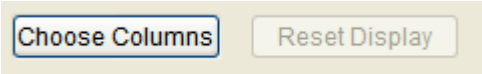
Each area is presented in the following paragraphs.

Tab 2: “Sender - Traffic + Statistics”

9.4.2.1 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.

9.4.2.2 Sender Statistics



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

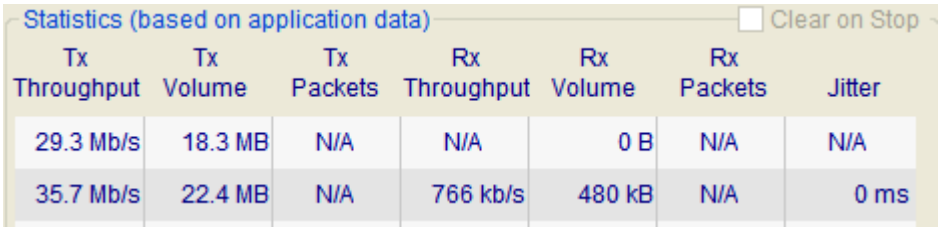
Up to 7 parameters can be simultaneously displayed among 13 parameters described later in this paragraph, and at least one parameter must be selected.

These statistics are calculated 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).

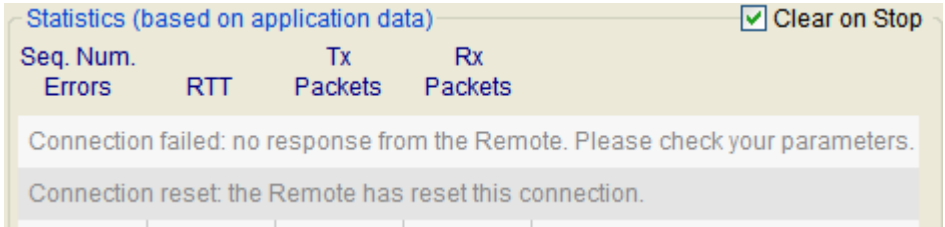
The "**N/A**" (Not Applicable) mention can be displayed instead of a value in the cell of the statistics table if the parameter cannot be calculated.



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.



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

List of the 13 statistic parameters calculated for the Sender

Sending statistics

Tx Packets
Tx Packets (Tx = Transmit) is the number of packets that LanTraffic V2 Enhanced has sent since the connection is started This value isn't available with TCP connections.

Tx Pkts Throughput(1)
Tx Pkts Throughput (Tx = Transmit) is the mean number of packets that LanTraffic V2 Enhanced 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.

Tx Throughput(1)
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.

Tx Volume(1)
Tx Volume (Tx = Transmit) is the number of bytes that **LanTraffic V2 Enhanced** has sent since the connection is started.

Receiving statistics

Rx Packets
Rx Packets (Rx = Receive) is the number of packets that **LanTraffic V2 Enhanced** has received since the connection is started. This value is only available with UDP connections

Rx Pkts Throughput(1)
Rx Pkts Throughput (Rx = Receive) is the mean number of packets that **LanTraffic V2 Enhanced** 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.

Rx Throughput(1)
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.

Rx Volume(1)
Rx Volume (Rx = Receive) is the number of bytes that **LanTraffic V2 Enhanced** has received since the connection is started.

Other statistics

Jitter(1)
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 one-way variation mean (remote Receiver = Generator mode) or the two-ways variation mean (remote Receiver = Echoer mode).

Remaining Volume(1)
'Remaining Volume' is the number of bytes that **LanTraffic V2 Enhanced** has still not sent yet. This information is only available for two Traffic Generator types (Mathematical Law and File to Send).

RTT
'RTT' is the Round Trip Time of a packet that was sent by **LanTraffic V2 Enhanced**. 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.

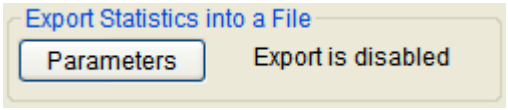
Seq. Numb. Errors
'Seq. Numb. Errors' (Sequence Numbering Errors) is the sum of the Out Of Sequence packets number (OOS) and the number of lost packets. This value is only available if the RTT option is selected (on local Sender: see Traffic Generator Parameters) and if the working mode of the remote Receiver is Generator or Echoer. (Not available with TCP)

Volume To Send(1)
'Volume To Send' is the number of bytes that **LanTraffic V2 Enhanced** should send. This information is available for two Traffic Generator Types only (Mathematical law and File to Send).

(1 These statistics are not available with ICMP

9.4.2.3 Export Statistics into a File

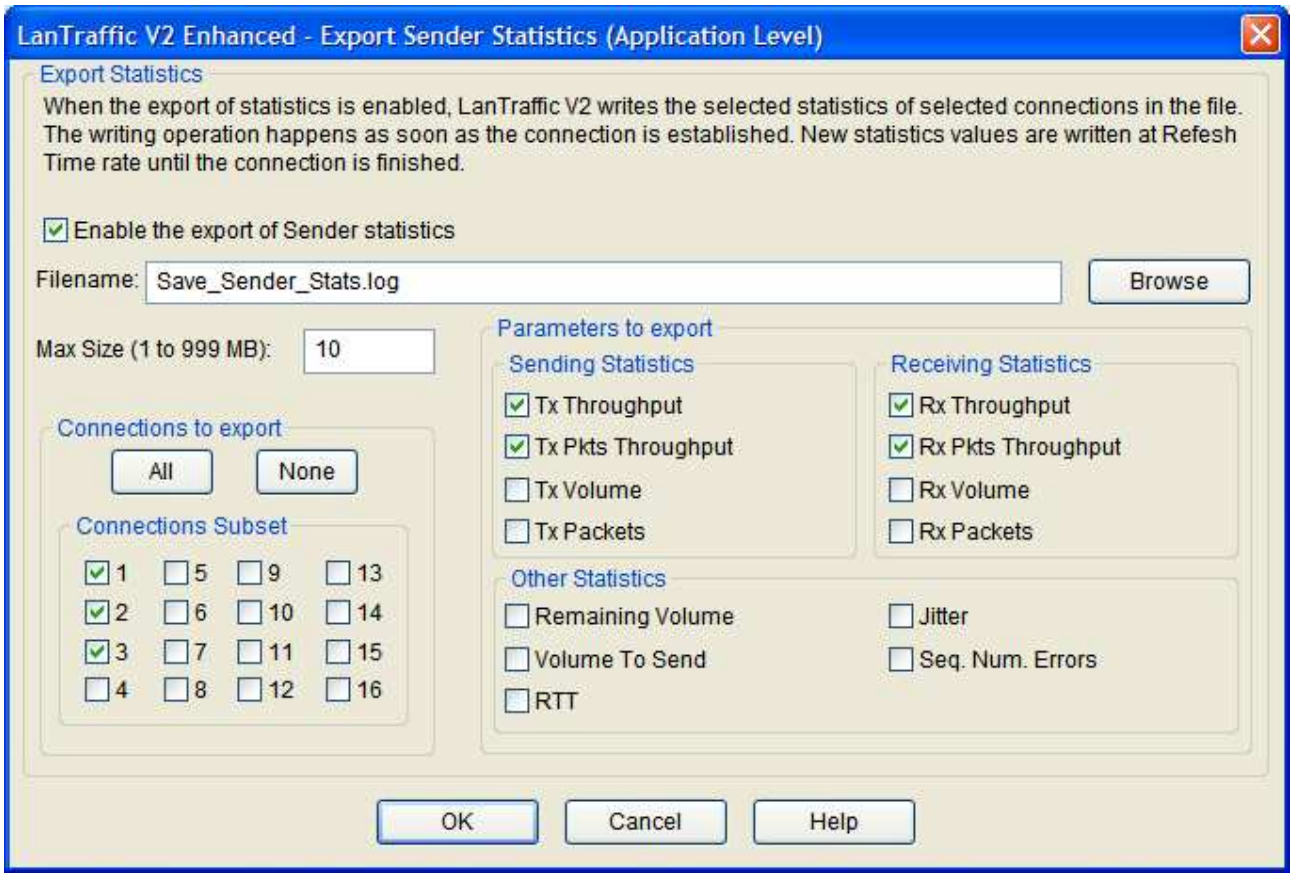
To export all or part of **statistics** into a file, click on the 'Parameters' button when enabled (i.e. if connections of the Sender are not active):



When no parameters are defined, the state is:
Export is disabled

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).

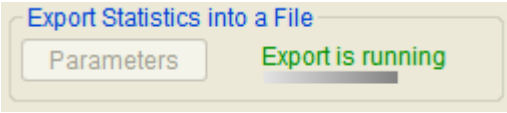


Then press OK to validate, and a new state is displayed:

When parameters have been defined and the export process is enabled, the state is:
Export is enabled

Do not specify the same filename to save statistics for the Sender and the Receiver parts; If you do so, 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, UDP or ICMP 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 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:

9.4.2.3.1 Sender statistics file format

The Sender statistics file is formatted line by line as follows. The data delimiter is the tab.

First line: Starting session MM/DD/YYYY at HH:MM:SS,mmm (**UTC time**)
Second line: LanTrafficV2 Sender
Third line: contains the labels of columns

Connection #nn (Protocol)	Date	Time	Parameter i	Parameter j	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, UDP and ICMP connection events

Connection #nn (TCP or UDP or ICMP) START: 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 Enhanced** for the line.

Connection #nn (TCP or UDP or ICMP) END: This indicates the end of traffic for the connection #nn. Numerical values are latest values computed by **LanTraffic V2 Enhanced** for the line.

Additional mark for TCP, UDP or ICMP disconnection events

Connection Cnx #n (TCP or UDP or ICMP) ERROR: This mark indicates the reason of the disconnection if this one is not produced by the click on the stop button or the scheduled end of the traffic generation (due to the generator parameters, for example: Number packets to send = 1000). When this mark is included in the Sender traces, the numerical values are replaced by the error message returned by **LanTraffic V2 Enhanced**.

Idle connections
When the connection is idle, the numerical values are set to 0 for “Tx Throughput”, “Rx Throughput”, “Tx Volume”, “Rx Volume”, “Tx Packets” and “Rx Packets” columns.

Conventions
“Volume to send” and “Remaining Volume” are filled with the “N/A” symbol when the generator is not configured with “File to send”.
“Seq. Num. Errors”, “Jitter” and “RTT” are filled with the “N/A” symbol until one “RTT” header is found in the received data by the Sender part.
“Tx Packets”, “Rx Packets”, “Tx Pkts Throughput” and “Rx Pkts Throughput” are filled with the “N/A” symbol when the protocol used for the concerned connection is not UDP.
When a connection is using ICMP protocol, all statistics are filled with the “N/A” symbol, except “RTT”, “Seq. Num. Errors”, “Tx Packets” and “Rx Packets”.

9.4.2.3.2 Export Sender file sample

In the following example, 3 connections (#01, #02 and #16) have been selected for the local Sender with 8 parameters exported: Tx (Transmit) Packets, Tx (Transmit) Throughput, Tx (Transmit) Volume, Rx (Receive) Packets, Rx (Receive) Throughput, Rx (Receive) Volume, RTT and Seq. Num. Errors (Sequence Numbering errors):

- Connection #01: Protocol = UDP & Traffic Generator type = Packets generator [Size Packet = 1460, Inter Packet Delay = 20, RTT option = No, Number of packets=10000]
- Connection #02: Protocol = TCP & Traffic Generator type = Packets generator [Size Packet = 1460, Inter Packet Delay = 20, RTT option = Yes, Number of packets=10000]
- Connection #16: Protocol = TCP & Traffic Generator type = Packets generator [Size Packet = 1460, Inter Packet Delay = 20, RTT option = Yes, Number of packets=10000]

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

Parameters set in the General Parameters of the Configuration menu:

- Refresh time = 2 seconds
- Throughput sampling period = 5 seconds
- Unit = kilobytes (kB) & kilobits per second (kb/s)

The 3 connections are started all together; and then the connections #01, #02 and #16 are stopped manually.

Starting session 12/26/2007 at 14:51:11.765 (UTC Time)

LanTrafficV2 Sender

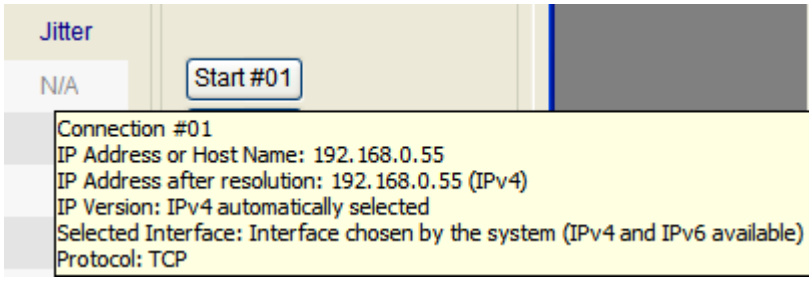
Connection #i (Protocol)	Date	Time	Tx Throughput (kb/s)	Tx Volume (kB)	Tx Packets (Pkts)	Rx Throughput (kb/s)	Rx Volume (kB)	Rx Packets (Pkts)	RTT (ms)	Seq. Num. Errors
Connection #01 (UDP) START	12/26/2007	14:51:11.781	0.00	0.00	0	0.00	0.00	0	N/A	N/A
Connection #02 (TCP) START	12/26/2007	14:51:11.843	0.00	0.00	N/A	0.00	0.00	N/A	0	0
Connection #16 (TCP) START	12/26/2007	14:51:11.843	0.00	0.00	N/A	0.00	0.00	N/A	0	0
Connection #01 (UDP)	12/26/2007	14:51:12.531	66.16	48.48	34	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	12/26/2007	14:51:12.531	63.88	44.20	N/A	0.00	0.00	N/A	0	0
Connection #16 (TCP)	12/26/2007	14:51:12.531	63.88	48.48	N/A	63.88	45.63	N/A	7	0
Connection #01 (UDP)	12/26/2007	14:51:14.546	289.72	186.78	131	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	12/26/2007	14:51:14.546	292.00	186.78	N/A	0.00	0.00	N/A	0	0
Connection #16 (TCP)	12/26/2007	14:51:14.546	292.00	186.78	N/A	292.00	186.78	N/A	5	0
Connection #01 (UDP)	12/26/2007	14:51:16.546	517.84	329.36	231	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	12/26/2007	14:51:16.546	517.84	329.36	N/A	0.00	0.00	N/A	0	0
Connection #16 (TCP)	12/26/2007	14:51:16.546	520.13	329.36	N/A	520.13	329.36	N/A	5	0
Connection #01 (UDP)	12/26/2007	14:51:18.531	568.03	474.79	333	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	12/26/2007	14:51:18.531	568.03	473.36	N/A	0.00	0.00	N/A	0	0
Connection #16 (TCP)	12/26/2007	14:51:18.531	568.03	473.36	N/A	568.03	471.93	N/A	4	0
Connection #01 (UDP)	12/26/2007	14:51:20.531	568.03	614.51	431	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	12/26/2007	14:51:20.531	568.03	620.21	N/A	0.00	0.00	N/A	0	0
Connection #16 (TCP)	12/26/2007	14:51:20.531	568.03	615.94	N/A	568.03	615.94	N/A	5	0
Connection #01 (UDP)	12/26/2007	14:51:22.531	568.03	759.94	533	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	12/26/2007	14:51:22.531	565.75	759.94	N/A	0.00	0.00	N/A	0	0
Connection #16 (TCP)	12/26/2007	14:51:22.531	568.03	759.94	N/A	568.03	759.94	N/A	7	0
Connection #01 (UDP)	12/26/2007	14:51:24.531	570.31	905.37	635	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	12/26/2007	14:51:24.531	570.31	903.95	N/A	0.00	0.00	N/A	0	0
Connection #16 (TCP)	12/26/2007	14:51:24.531	570.31	899.67	N/A	568.03	898.24	N/A	7	0
,,,,	,,,,	,,,,	,,,,	,,,,	,,,,	,,,,	,,,,	,,,,	,,,,	,,,,
,,,,	,,,,	,,,,	,,,,	,,,,	,,,,	,,,,	,,,,	,,,,	,,,,	,,,,
Connection #01 (UDP)	12/26/2007	14:54:26.687	568.03	13864.30	9724	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	12/26/2007	14:54:26.687	570.31	13868.57	N/A	0.00	0.00	N/A	0	0
Connection #16 (TCP)	12/26/2007	14:54:26.687	570.31	13877.13	N/A	568.03	13874.28	N/A	9	0
Connection #01 (UDP)	12/26/2007	14:54:28.687	570.31	14012.58	9828	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	12/26/2007	14:54:28.687	568.03	14016.86	N/A	0.00	0.00	N/A	0	0
Connection #16 (TCP)	12/26/2007	14:54:28.687	570.31	14019.71	N/A	570.31	14016.86	N/A	9	0
Connection #01 (UDP)	12/26/2007	14:54:30.921	568.03	14166.56	9936	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	12/26/2007	14:54:30.921	570.31	14170.84	N/A	0.00	0.00	N/A	0	0
Connection #16 (TCP)	12/26/2007	14:54:30.921	568.03	14175.12	N/A	570.31	14173.69	N/A	9	0
Connection #02 (TCP) END	12/26/2007	14:54:32.078	568.03	14257.81	N/A	0.00	0.00	N/A	0	0
Connection #16 (TCP) END	12/26/2007	14:54:32.531	524.69	14257.81	N/A	526.97	14257.81	N/A	9	0
Connection #01 (UDP)	12/26/2007	14:54:32.906	538.38	14257.81	10000	0.00	0.00	0	N/A	N/A
Connection #01 (UDP) END	12/26/2007	14:54:32.937	538.38	14257.81	10000	0.00	0.00	0	N/A	N/A

9.4.2.4 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 on the left side.
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, then a tooltip is displayed:



Tab 2 "Sender - Traffic + Statistics" – Connection summary

The "Sender – Traffic + Statistics" summary tooltip displays:

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

To carry out the unitary testing session:

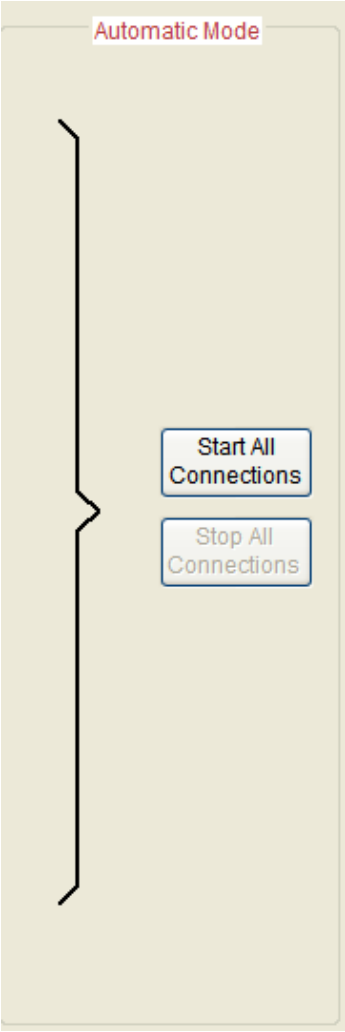
1. *In Tab 2: "Sender Traffic + Statistics"*
   ⇨ If the Sender connections are active, stop all running connections by pressing the "Stop All Connections" button.

2. *In Tab 1: "Sender Parameters"*
   ⇨ Select the Unitary Mode.

3. *In Tab 1: "Sender Parameters"*
   ⇨ If necessary configure the 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.

9.4.2.5 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 on the left.
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 the 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 the 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.

9.5 The Receiver part

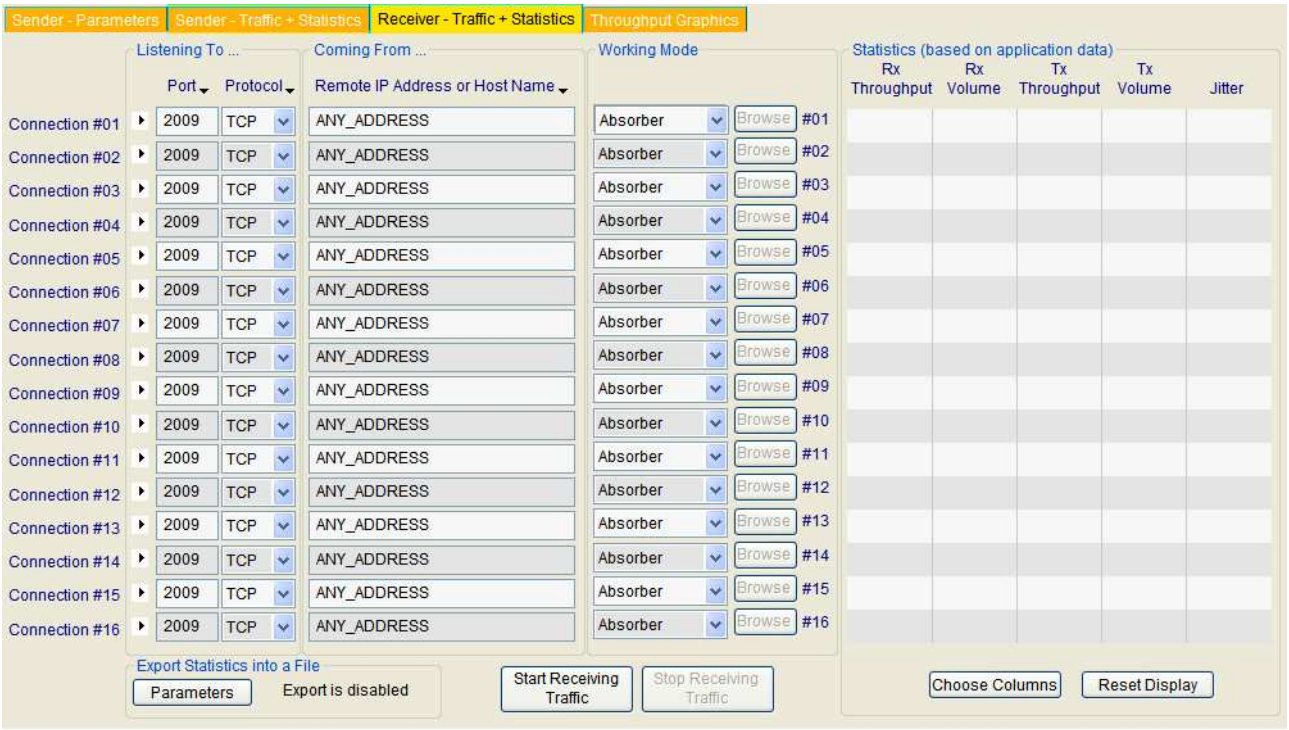
The Receiver part allows receiving UDP, TCP traffic following five different working modes: 'Absorber' or 'Absorber File', 'Echoer' or 'Echoer file', and 'Generator'.

Receiver - Parameter + Statistics tab

By using this tab, you can:

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

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



Tab 3 "Receiver - Traffic + Statistics"

9.5.1 Duplicate parameters of a connection onto others

In order to facilitate input of the parameters for a connection, a *copy/paste function* for all parameters of a connection is available (identical to the *copy/paste function* for the Sender part – see 9.4.1.1.4).

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

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

9.5.2 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 parameters*
- *To select the network interface and the IP version for a connection.*

Port

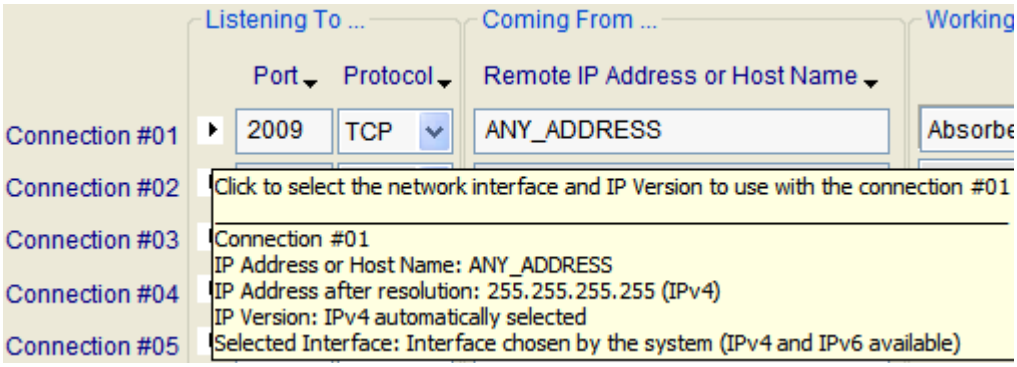
The port number is limited to 65,535.
By default, the entered port number is 2009.
In case of invalid value, the value becomes red.

Protocol

TCP or UDP protocol (default = TCP protocol).

9.5.2.1 Summary of the connection parameters

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



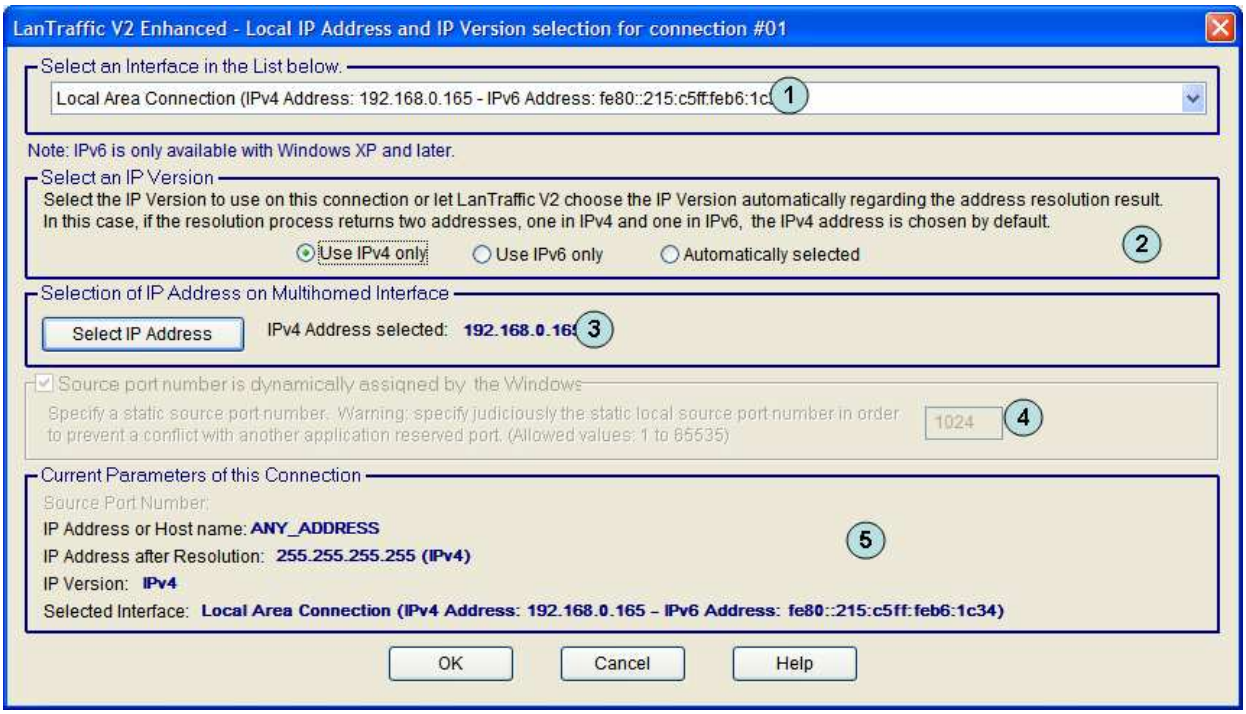
Receiver connection tooltip

The tooltip for the Receiver connection includes 5 items:

- The first item is the connection number the tooltip refers to.
- The next item is the IP address or Host Name defined by the user.
- The 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).
- The next item is the IP version currently selected.
- The 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").

9.5.2.2 Select the network interface, IP version and local IP address

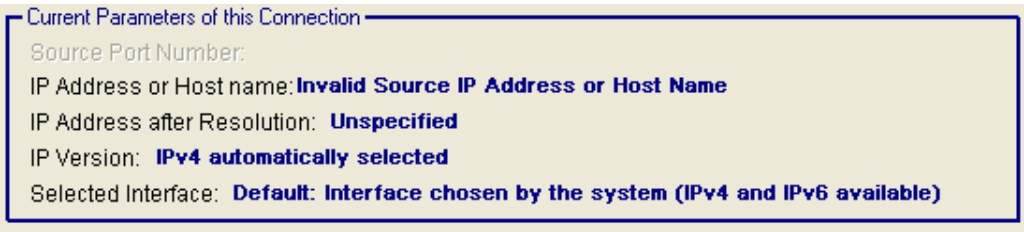
When you click on the black arrow, the following window is displayed:



Network interface, IP version and IP local address for a Receiver 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:
  - The IP version is automatically selected by **LanTraffic V2 Enhanced** regarding the destination address or host name specified on the “Receiver – Traffic + Statistics” tab (see below). By default, NO_ADDRESS is an IPv4 address.
  - 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 the interface order, the IP address and the network address mask.
- You can select one interface from the list of connected interfaces. **LanTraffic V2 Enhanced** will only use the selected interface to translate the IP address and to make a 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:



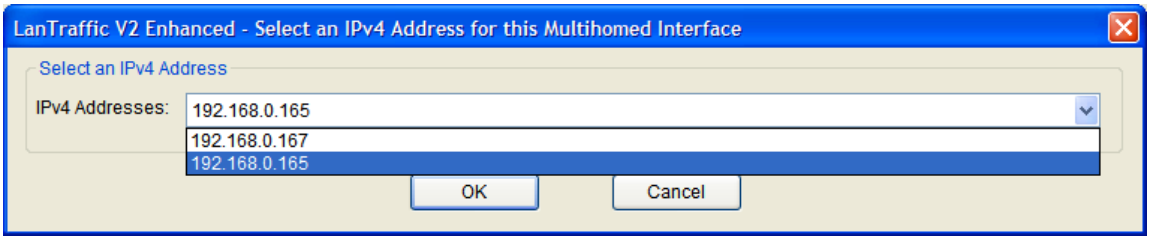
- Interface types are restricted: only Ethernet and PPP are listed. A PPP interface should be in the connected state to belong to the interface list.

(2) The **IP version** selection is available:

- with Windows Server 2003, or Windows Vista and later
- check if IPv6 features is checked on the target interface.
- you can allow **LanTraffic V2 Enhanced** to choose automatically the good IP version regarding the address or host name resolution result. If a canonical name corresponds at the same time to an IPv4 and IPv6 addresses, **LanTraffic V2 Enhanced** chooses the IPv4 address. In this case, to use the IPv6 address, you should select the use of IPv6 only (*Use IPv6 only*).

If you have selected an IP version, the IP address translation (see 9.4.1.1.3) uses the current selected 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. The selection of a Source IP address is generally not required: **LanTraffic V2 Enhanced** uses the default IP address of the interface to establish connections. It may be useful when routing priority or policy is defined. Example of an 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) **Specification of the local source port number** is disabled in the receiver Interface configuration because the source port number and the destination port number are generated by the remote as the originator of the connection.

(5) **Current parameters of this connection** area are an abstract for the connection. It summarizes the IP address, the numerical IP address format, the IP version and the interface selection.

- The source port used is dynamically updated with the user selection.
- The IP addresses are static. The IP address translation will process only when you click on OK.
- The IP version field is dynamically updated with the user selection.
- The current interface is dynamically updated with the user selection.

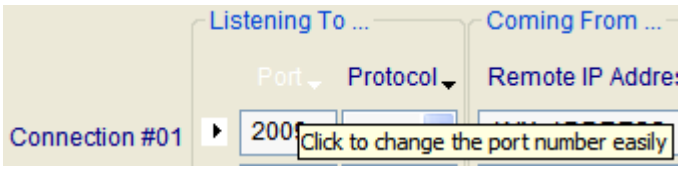
When you click on the OK button, if the interface selected or IP version has changed, the IP address translation is automatically started. It may be time consuming.

So, you can configure various incoming connection criteria:

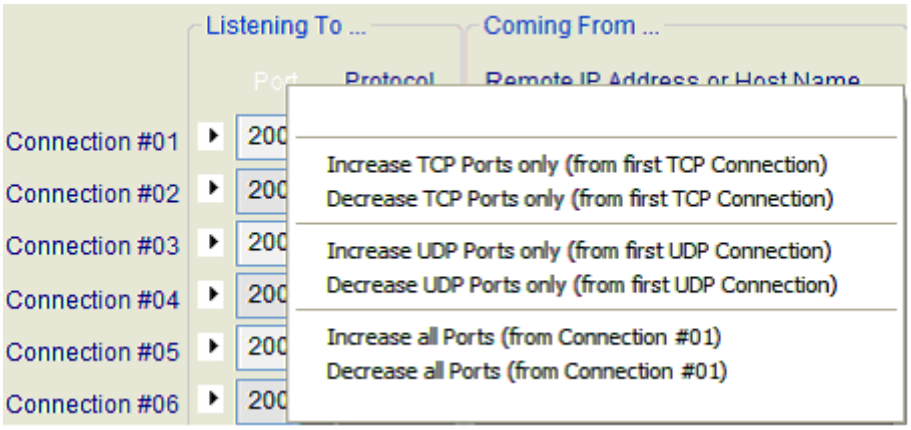
- Interface: you limit a connection to a specific Interface or let the Operating System to return connections from any interfaces.
- IP version: when an Interface offers the two IP versions, you can select the IP version expected or not. By default, the automatic selection is activated.
- When multiple 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.

9.5.2.3 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 the four items menu as following:

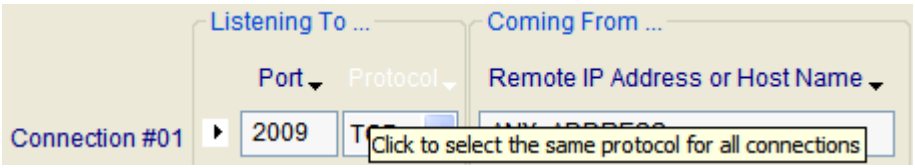


With this menu, you can:

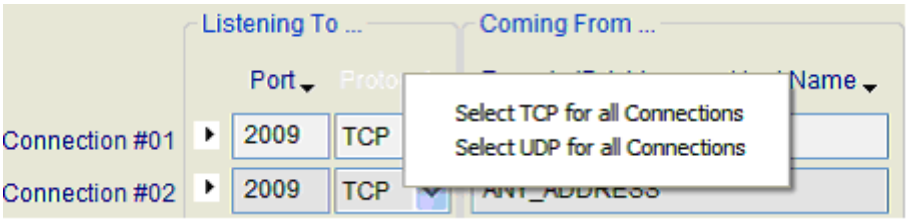
- Set the port number increasingly or decreasingly for all TCP connections, based on the port number of the first TCP connection,
- Set the port number increasingly or decreasingly for all UDP connections, based on the port number of the first UDP connection,
- Set the port number increasingly or decreasingly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

9.5.2.4 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.

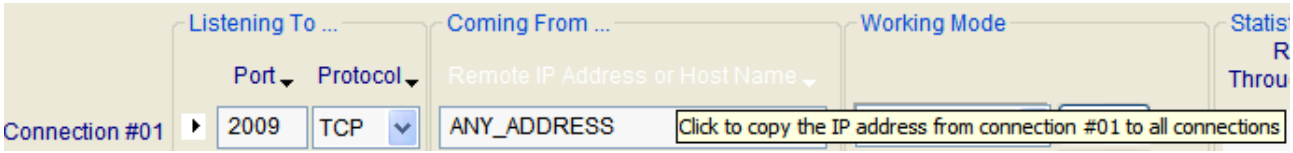
9.5.3 Coming From …

Remote IP address or Host Name: *Enter the IP address (numerical format) or Host Name (canonical format), with the help of AutoComplete when active.*

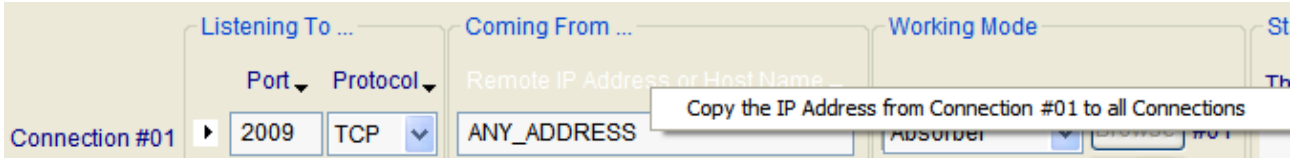
By default, the value is ANY_ADDRESS (This address is a mask to accept connection from any source address. It applies on both IPv4 and IPv6).

9.5.3.1 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 copied out on all connections from #02 to #16.

9.5.3.2 IP Address translation mechanism

LanTraffic V2 Enhanced 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 the Interface parameters change, all of these actions start the IP address translation function.

Because the IP address translation mechanism is CPU consuming, you should be careful 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 the 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 Enhanced** to restart the translation mechanism for this connection.

When the IP address translation failed, the IP address is written in red on a white background. 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,*
- *a context file is loaded.*

9.5.4 Working Mode

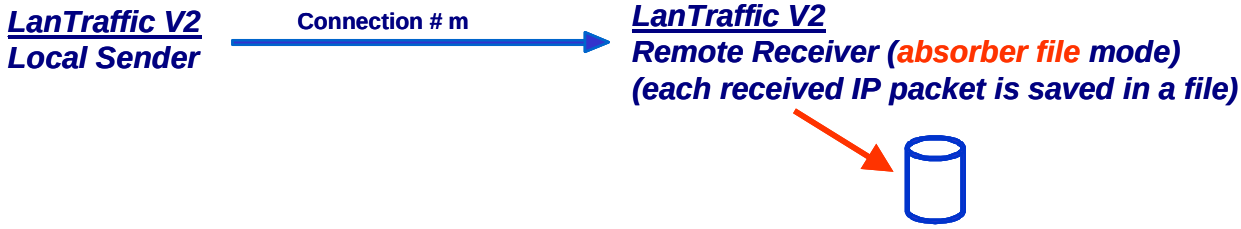
LanTraffic V2 Enhanced offers five different active working modes for the Receiver part: 'Absorber', 'Absorber file', 'Echoer', 'Echoer File', 'Generator'. A 'Disable' (or inactive) mode is also available.

9.5.4.1 Absorber mode

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

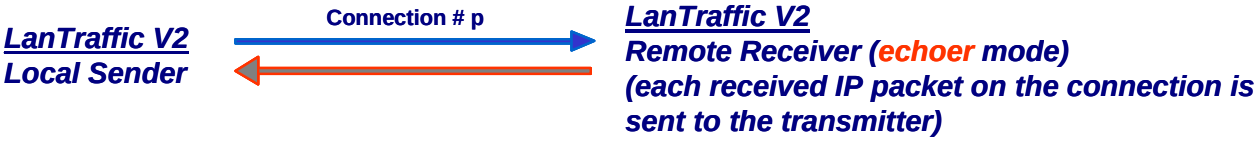
9.5.4.2 Absorber File mode

When a receiving connection is operating in the Absorber File mode, the Receiver will save the 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.



9.5.4.3 Echoer mode (with TCP and UDP only)

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

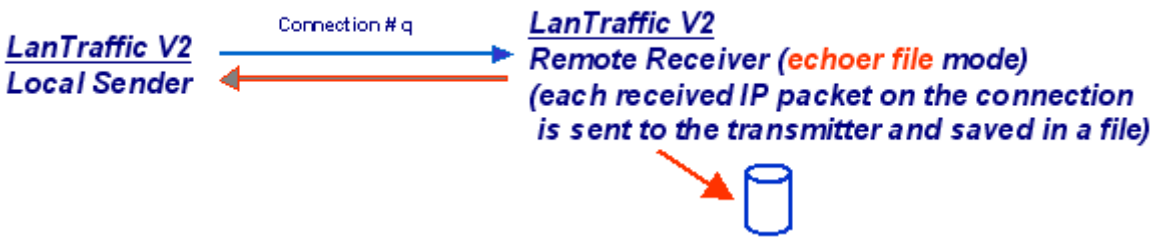


With UDP protocol, echoer mode is available only if a connected sender IP address is specified.

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

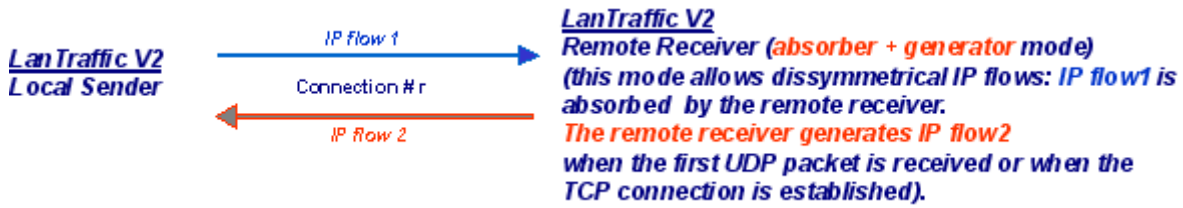
9.5.4.4 Echoer File mode (with TCP and UDP only)

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.

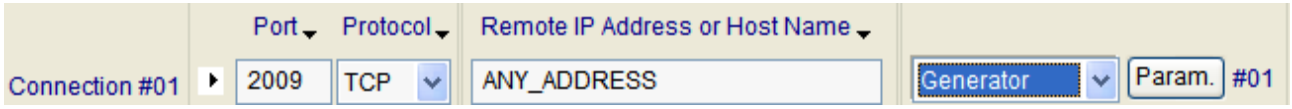


9.5.4.5 Generator mode (with TCP and UDP only)

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



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



When you select the “Generator” mode for a connection (#01 in the example above), a 'Param.' Button is displayed in order to specify the 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 you like for this *IP flow 2* (for example, generate 10,000 packets with a mean throughput of 250 Kbps).

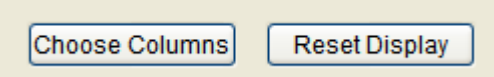
For a TCP connection, *IP flow 2* is generated as soon as the TCP connection will be established between the ‘Local Sender’ and the ‘Remote Receiver’ modules. It stops when ‘Local Sender’ stops the connection or at the end of the ‘Remote Receiver’ Traffic generator.

For a UDP connection, *IP flow 2* is generated as soon as the ‘Remote Receiver’ receives 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.

9.5.4.6 Disable mode

When this mode is selected for a connection, **LanTraffic V2 Enhanced** 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”.

9.5.5 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 Enhanced** 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 Receiver

Sending statistics

Tx Packets
Tx Packets (Tx = Transmit) is the number of packets that **LanTraffic V2 Enhanced** has sent since the connection is started. This value is only available with UDP connections;

Tx Pkts Throughput
Tx Pkts Throughput (Tx = Transmit) is the mean number of packets that **LanTraffic V2 Enhanced** 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.

Tx Throughput
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.

Tx Volume
Tx Volume (Tx = Transmit) is the number of bytes that **LanTraffic V2 Enhanced** has sent since the connection is started.

Receiving statistics

Rx Packets
Rx Packets (Rx = Receive) is the number of packets that **LanTraffic V2 Enhanced** has received since the connection is started. (UDP only)

Rx Pkts Throughput
Rx Pkts Throughput (Rx = Receive) is the mean number of packets that **LanTraffic V2 Enhanced** 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.

Rx Throughput
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.

Rx Volume
Rx Volume (Rx = Receive) is the number of bytes that **LanTraffic V2 Enhanced** has received since the connection is started.

Other statistics

Data Not Echoed
'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.

Jitter
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 one-way variation mean only.

Remaining Volume
'Remaining Volume' is the number of bytes that **LanTraffic V2 Enhanced** has still not sent yet. This information is only available for two Traffic Generator types (Mathematical Law and File to Send).

Seq. Numb. Errors
'Seq. Numb. Errors' (Sequence Numbering 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 Generator or Echoer.

Volume To Send
'Volume To Send' is the number of bytes that "**LanTraffic V2 Enhanced** should send. This information is available for two Traffic Generator Types only (Mathematical law and File to Send).

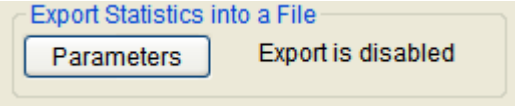
By pressing the 'Start Receiving Traffic' button, all connected sender information and working mode information are grayed,
Disabled connections statistics fields are empty on gray background,
UDP enabled connections statistics fields are filled with “00” value on white background,
TCP connections statistics 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 the Receiver statistics exported into a file***.

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

9.5.6 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):

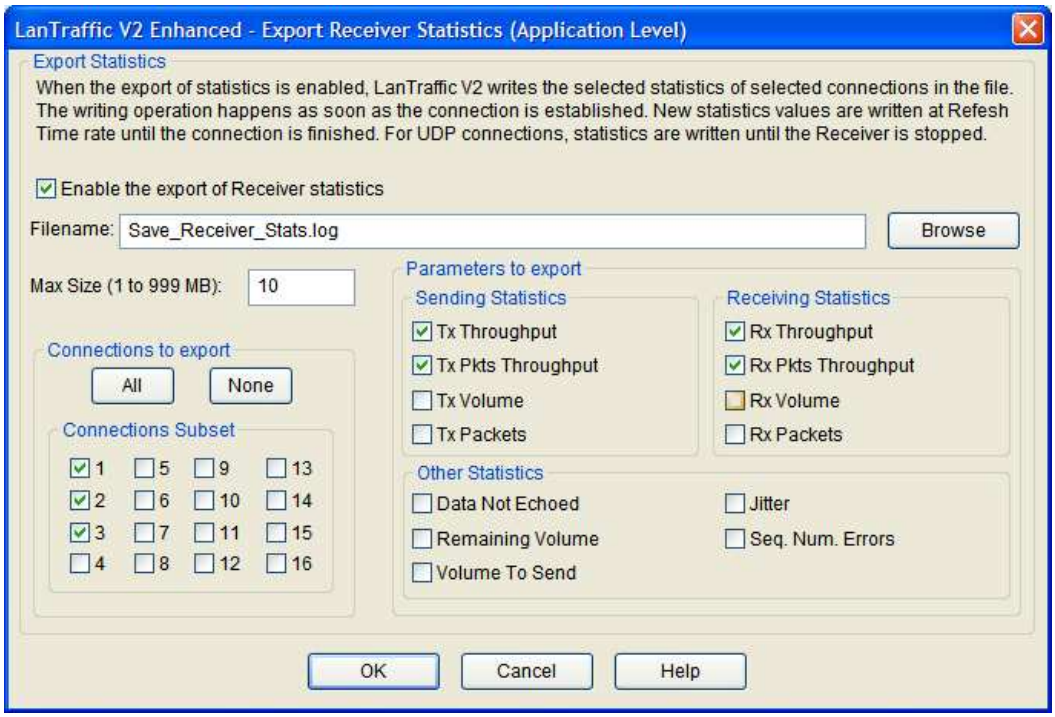


When no parameters are defined, the state is:

Export is disabled

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:

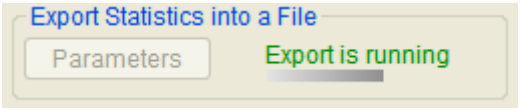
When parameters have been defined and the export process is enabled, the state is:

Export is enabled

Do not specify the same filename to save statistics for the Sender and the Receiver parts; if you do so, 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 or 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:

9.5.6.1 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 j	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) START: 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 Enhanced** 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 Enhanced** for the line.

Additional mark for TCP or UDP disconnection events
Connection #nn (TCP or UDP) ERROR: This mark indicates the reason of the disconnection if this one is not produced by the click on “Stop receiving” button or the normal shutdown of the traffic generation (due to the remote generator parameters, for example: Number packets to send = 1000). When this mark is included in the Receiver

traces, numerical values are replaced by the error message returned by **LanTraffic V2 Enhanced**.

Idle connections

When the connection is idle, numerical values are set to 0 for “Tx Throughput” and “Rx Throughput”.

“Tx Volume”, “Rx Volume” and “Data Not Echoed” columns are zeroes if the selected protocol is TCP. The UDP connection remains active until the Receiver is stopped: latest values remains displayed and exported too.

Conventions

“Volume to send” and “Remaining Volume” are filled with the “N/A” symbol when the generator is not configured with “File to send”. “Seq. Num. Errors” and “Jitter” are filled with the “N/A” symbol until one “RTT” header is found in the received data by the Receiver part.

“Tx Packets”, “Rx Packets”, “Tx Pkts Throughput” and “Rx Pkts Throughput” are filled with the “N/A” symbol when the protocol used for the concerned connection is not UDP.

9.5.6.2 Export Receiver file sample

In the following example, 3 connections (#01, #02 and #03) 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 Numbering errors):

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

The remote Sender has been configured with 3 connections:

- Connection #01: Protocol = UDP & Traffic Generator type = Packets generator [Size Packet = 1460, Inter Packet Delay = 20, RTT option = No, Packets Number = 1000]
- Connection #02: Protocol = TCP & Traffic Generator type = Packets generator [Size Packet = 1460, Inter Packet Delay = 20, RTT option = Yes, Packets Number = 1000]
- Connection #03: Protocol = TCP & Traffic Generator type = Packets generator [Size Packet = 1460, Inter Packet Delay = 20, RTT option = Yes, Packets Number = 1000]

Parameters set in the General Parameters of the Configuration menu:

- Refresh time = 2 seconds
- Throughput sampling period = 5 seconds
- Unit = kilobytes (kB) & kilobits per second (kb/s)

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 stopped manually.

Starting session 12/26/2007 at 16:26:10.500 (UTC Time)

LanTrafficV2 Receiver

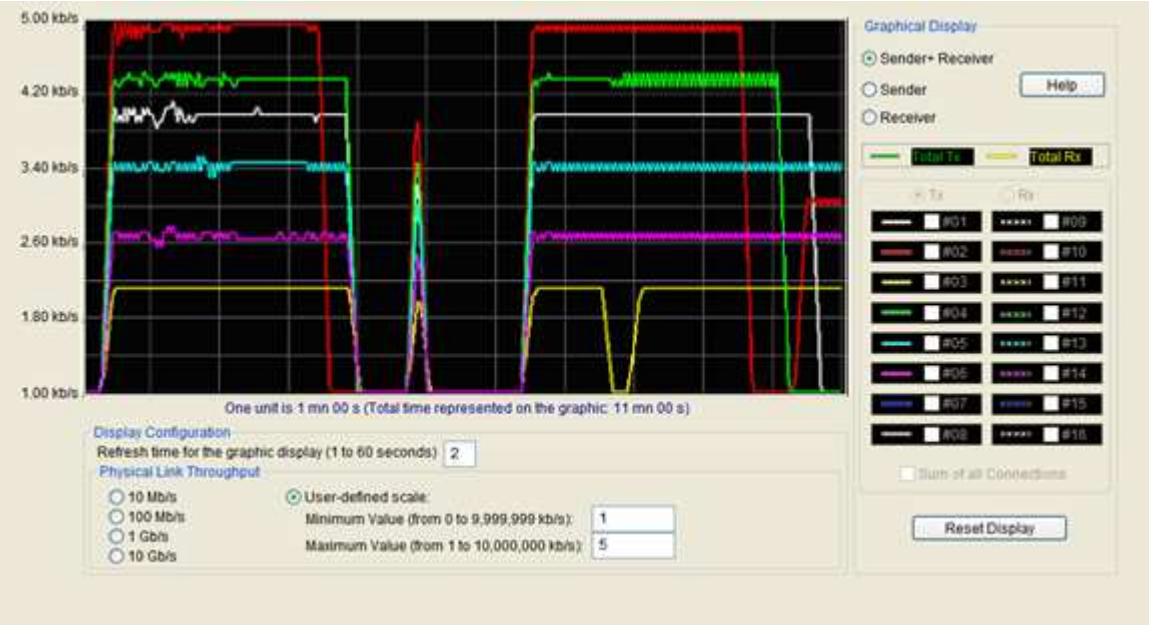
Connection #i (Protocol)	Date	Time	Rx Throughput (kb/s)	Rx Pkts Throughput (Pkts/s)	Rx Packets (Pkts)	Jitter (ms)	Seq. Num. Errors
Connection #03 (UDP) START	12/26/2007	16:26:10.546	0.00	0	0	N/A	N/A
Connection #03 (UDP)	12/26/2007	16:26:10.609	0.00	0	0	N/A	N/A
Connection #03 (UDP)	12/26/2007	16:26:11.437	0.00	0	1	0	N/A
Connection #01 (TCP) START	12/26/2007	16:26:11.484	0.00	N/A	N/A	N/A	N/A
Connection #02 (TCP) START	12/26/2007	16:26:11.484	0.00	N/A	N/A	N/A	N/A
Connection #01 (TCP)	12/26/2007	16:26:13.453	109.50	N/A	N/A	0	N/A
Connection #02 (TCP)	12/26/2007	16:26:13.453	109.50	N/A	N/A	0	N/A
Connection #03 (UDP)	12/26/2007	16:26:13.453	109.50	9	101	0	N/A
Connection #01 (TCP)	12/26/2007	16:26:15.453	337.63	N/A	N/A	0	N/A
Connection #02 (TCP)	12/26/2007	16:26:15.453	337.63	N/A	N/A	0	N/A
Connection #03 (UDP)	12/26/2007	16:26:15.453	337.63	29	201	0	N/A
Connection #01 (TCP)	12/26/2007	16:26:17.453	565.75	N/A	N/A	0	N/A
Connection #02 (TCP)	12/26/2007	16:26:17.453	565.75	N/A	N/A	0	N/A
Connection #03 (UDP)	12/26/2007	16:26:17.453	565.75	49	301	0	N/A
Connection #01 (TCP)	12/26/2007	16:26:19.437	574.88	N/A	N/A	0	N/A
Connection #02 (TCP)	12/26/2007	16:26:19.437	574.88	N/A	N/A	0	N/A
Connection #03 (UDP)	12/26/2007	16:26:19.437	572.59	50	401	0	N/A
Connection #01 (TCP)	12/26/2007	16:26:21.437	574.88	N/A	N/A	1	N/A
Connection #02 (TCP)	12/26/2007	16:26:21.437	570.31	N/A	N/A	0	N/A
Connection #03 (UDP)	12/26/2007	16:26:21.437	570.31	50	500	0	N/A
Connection #01 (TCP)	12/26/2007	16:26:23.437	574.88	N/A	N/A	0	N/A
Connection #02 (TCP)	12/26/2007	16:26:23.437	574.88	N/A	N/A	0	N/A
Connection #03 (UDP)	12/26/2007	16:26:23.437	572.59	50	597	0	N/A
Connection #01 (TCP)	12/26/2007	16:26:25.453	570.31	N/A	N/A	1	N/A
Connection #02 (TCP)	12/26/2007	16:26:25.453	570.31	N/A	N/A	0	N/A
Connection #03 (UDP)	12/26/2007	16:26:25.453	570.31	50	701	0	N/A
Connection #01 (TCP)	12/26/2007	16:26:27.453	574.88	N/A	N/A	1	N/A
Connection #02 (TCP)	12/26/2007	16:26:27.453	574.88	N/A	N/A	1	N/A
Connection #03 (UDP)	12/26/2007	16:26:27.453	572.59	50	801	0	N/A
Connection #01 (TCP)	12/26/2007	16:26:29.437	574.88	N/A	N/A	1	N/A
Connection #02 (TCP)	12/26/2007	16:26:29.437	574.88	N/A	N/A	1	N/A
Connection #03 (UDP)	12/26/2007	16:26:29.437	572.59	50	897	0	N/A
Connection #01 (TCP)	12/26/2007	16:26:31.453	570.31	N/A	N/A	0	N/A
Connection #02 (TCP)	12/26/2007	16:26:31.453	570.31	N/A	N/A	0	N/A
Connection #03 (UDP)	12/26/2007	16:26:31.453	570.31	50	1000	0	N/A
Connection #01 (TCP) END	12/26/2007	16:26:31.984	570.31	N/A	N/A	1	N/A
Connection #02 (TCP) END	12/26/2007	16:26:32.000	568.03	N/A	N/A	0	N/A
,,,,	,,,,	,,,,	,,,,	,,,,	,,,,	,,,,	,,,,
Connection #03 (UDP)	12/26/2007	16:27:45.437	0.00	0	1000	0	N/A
Connection #03 (UDP)	12/26/2007	16:27:47.437	0.00	0	1000	0	N/A

9.6 The Throughput Graphics tab

This fourth tab allows the display of the throughputs for the Receiver and Sender parts, and the configuration of the graphics display,

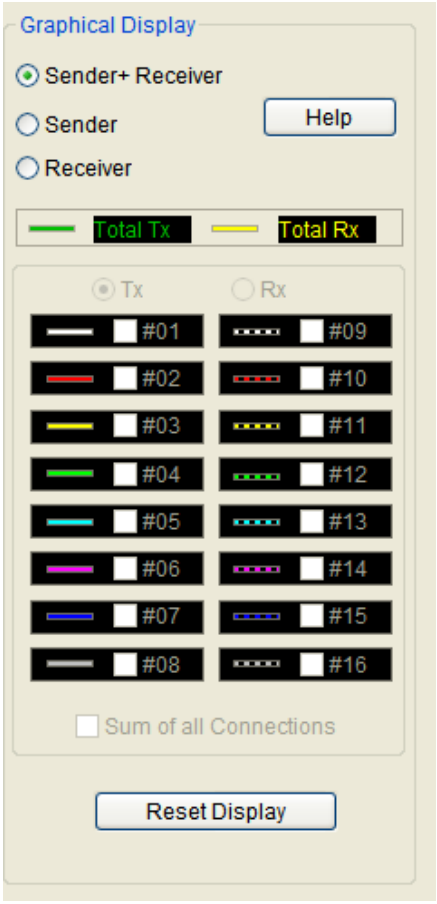
This tab is divided in three areas:

- 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 parameter.



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

9.6.1 The Graphical Display object

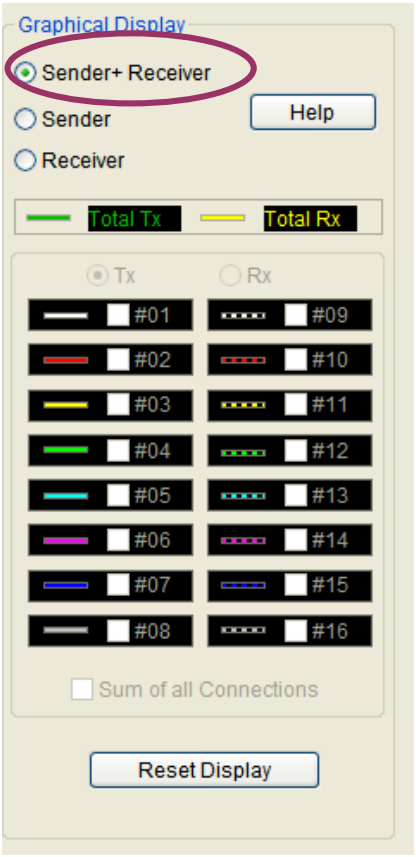


This object allows selecting curves to display with three choices:

- Sender + Receiver: 16 connections for the Sender + 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:

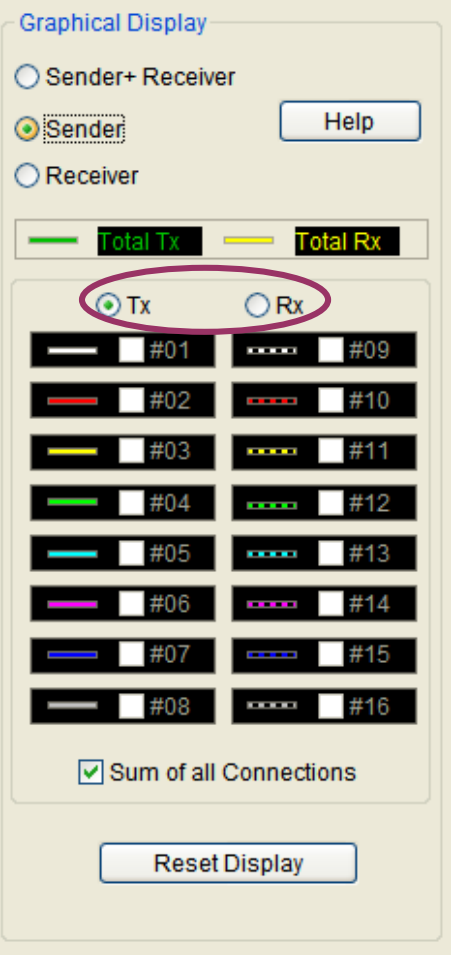


Total Tx (green curve) represents 'Total **LanTraffic V2 Enhanced** sending throughput' = total sending throughput of the Sender + total echoing throughput of the Receiver.

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

If the total **LanTraffic V2 Enhanced** sending throughput and the total **LanTraffic V2 Enhanced** receiving throughput are equal, only the green line is visible. If the throughput is superior to the values represented in the 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.

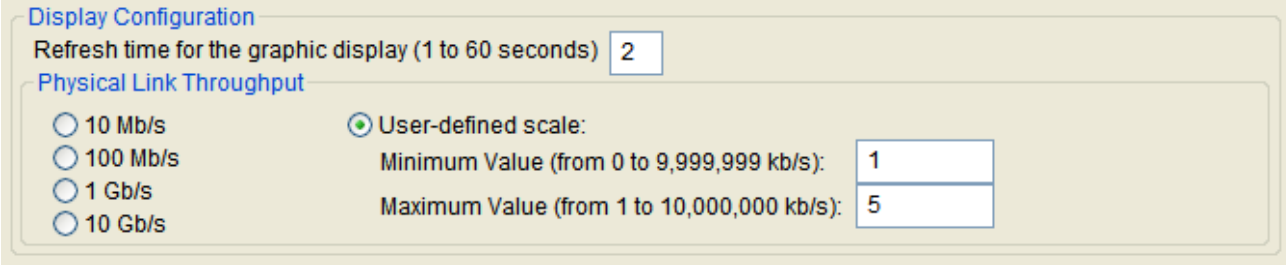
The check box 'Sum of all connections' allows displaying a curve that is the throughput sum of all connections (in the example above, sum of all Transmit throughputs for the sender part).

So, you can see on the 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

9.6.2 The Display Configuration object



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-mn period.
Notice that **LanTraffic V2 Enhanced** offers up to 3 hours historic: set Refresh time for graphic display to 60.

You can configure the **Physical Link Throughput**: used as scale of the throughput graph: 10 Mb/s, 100 Mb/s, 1 Gb/s, 10 Gb/s or any user-defined scale (limited to 10,000,000 kb/s or to 10,485,760 Kib/s).

Part 10Command Line Parameters

LanTraffic V2 Enhanced can be started by using a command line with parameters.

10.1 General rule

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

10.2 Commands available to start LanTrafficV2

The commands below are only available for the first command line i.e. when no LanTrafficV2 instance is running.

10.2.1 Context filename

The context filename is a set of parameters for **LanTraffic V2 Enhanced**. This set can be saved in a file and reloaded later in such a way the user doesn‘t have to re-enter any 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 Enhanced\file.ctx”.
The “ symbol is necessary to use spaces in filenames or directories.

10.2.2 Starting the "LanTraffic V2 Enhanced" Receiver part

There is only one command parameter to start the Receiver part.
Syntax: **-R**

10.2.3 Starting the "LanTraffic V2 Enhanced" 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': -S***Option***
Where ***Option*** may be:

- All: all connections defined are started. To start, a connection should have the IP address defined.
- 01..16: only the connection defined is started.

10.3 Commands available when LanTrafficV2 is started

The commands below are available when a **LanTrafficV2** instance is running.

10.3.1 Stopping the "LanTraffic V2 Enhanced" Sender and Receiver parts

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

Syntax: **-STOP**

10.3.2 Unload the "LanTraffic V2 Enhanced" application

This command parameter allows unloading the **LanTraffic V2 Enhanced** instance.

Syntax: **-UNLOAD**

10.4 Command line samples

- LanTrafficV2 –R

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

- LanTrafficV2 CONTEXT:c:\temp\f20030607.ctx –SAutomatic

This command line launches **LanTraffic V2 Enhanced** and loads the file context "c:\temp\f20030607.ctx."
Then the Sender is started in the 'Automatic testing mode' (for defined connections).

- LanTrafficV2 CONTEXT:c:\temp\f20030607.ctx –SAll

This command line starts **LanTraffic V2 Enhanced** and loads the file context named c:\temp\f20030607.ctx .
Then the Sender is started in the 'Unitary testing mode' for every connection defined.

- LanTrafficV2 CONTEXT:c:\temp\f20030607.ctx –R –S01 –S02 –S04 –S16 –S12

This command line starts **LanTraffic V2 Enhanced** and loads the file context named c:\temp\f20030607.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).

10.5 Error return code

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

Part 11Source/Local IP Address and Interface requirements

With **LanTraffic V2 Enhanced** version 2.7, the interface selection is required to carry out IPv6 unicast exchanges only.

"LanTraffic V2 Enhanced" acting as:	**Sender (UDP, TCP and ICMP)**		**Receiver (UDP and TCP)**	
IP Version	**IPv4**	**IPv6**	**IPv4**	**IPv6**
Unicast exchange	*Interface selection is not required*	*Interface selection is required*	*Interface selection is not required*	*Interface selection is not required*
Multicast exchange	*Interface selection is not required*	*Interface selection is not required*	*Interface selection is not required*	*Interface selection is not required*

Consequences when an Interface is selected

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

1. Every sent packet 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. Be careful: even if the resolution carried out by the operating system on your destination address or host name is right, the connection may not be able to generate data. (Example: bad selected interface, wrong entries into the Host file…)

Examples:

- The source IP Address is 192.168.0.23 with 255.255.255.0 as network mask and no gateway. The matching destination IP Addresses are: 192.168.0.X with X between 1 and 255.

- The source IP Address is 192.168.0.23 with 255.255.255.0 as network mask and no gateway. The DNS 192.168.1.1 cannot be reached. The matching destination IP Addresses are only: 192.168.0.X with X between 1 and 255.

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

1. With UDP protocol, the TCP/IP stack compares every packet received to the local IP address, whatever the source is. Packets matching are the only ones sent to the relevant connection of **LanTraffic V2 Enhanced**.

2. With TCP protocol, **LanTraffic V2 Enhanced** compares the SYN packet received to the local IP address, whatever the source is. If the packet is matching the connection is accepted and a room is reserved for it. Then the packets matching are the only ones sent to this relevant connection.

3. Be careful: even if the resolution is carried out by the operating system on your destination address or host name is right, the connection may not be able to receive data (example: bad selected interface, wrong entries into the Host file…).

Examples:

- The local IP Address is 192.168.0.23. The packets destination IP address matching is: 192.168.0.23.
- The local IP Address is 192.168.0.23. The packets with a destination IP address equal to 192.168.0.30 cannot reach this connection.

Part 12 Appendix

12.1 Mathematical laws used by LanTraffic V2 Enhanced

LanTraffic V2 Enhanced is based on the use of mathematical laws to generate values used:

- In the Unitary Mode for the Traffic Generator:
  - to specify the traffic generator (and data volume to send on the connection) if the option 'Mathematical Law' is selected as data source (four available laws: Uniform, Exponential, Pareto, Gauss)
  - to specify the inter-packet delay if the option 'Mathematical Law' is selected (four available laws: Uniform, Exponential, Pareto, Gauss)
- In the Automatic Mode for the Traffic Generator:
  - to specify the starting time of the connections (two available laws: Uniform, Exponential)
  - to specify the data volume to send for each connection (four available laws: Uniform, Exponential, Pareto, Gauss)

Hereafter is a detailed presentation of each mathematical law.

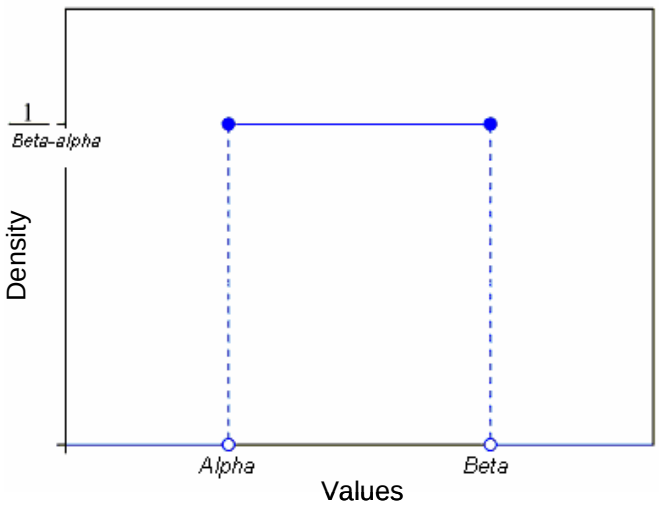
12.1.1 Uniform law

Distribution of Uniform Law is:

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

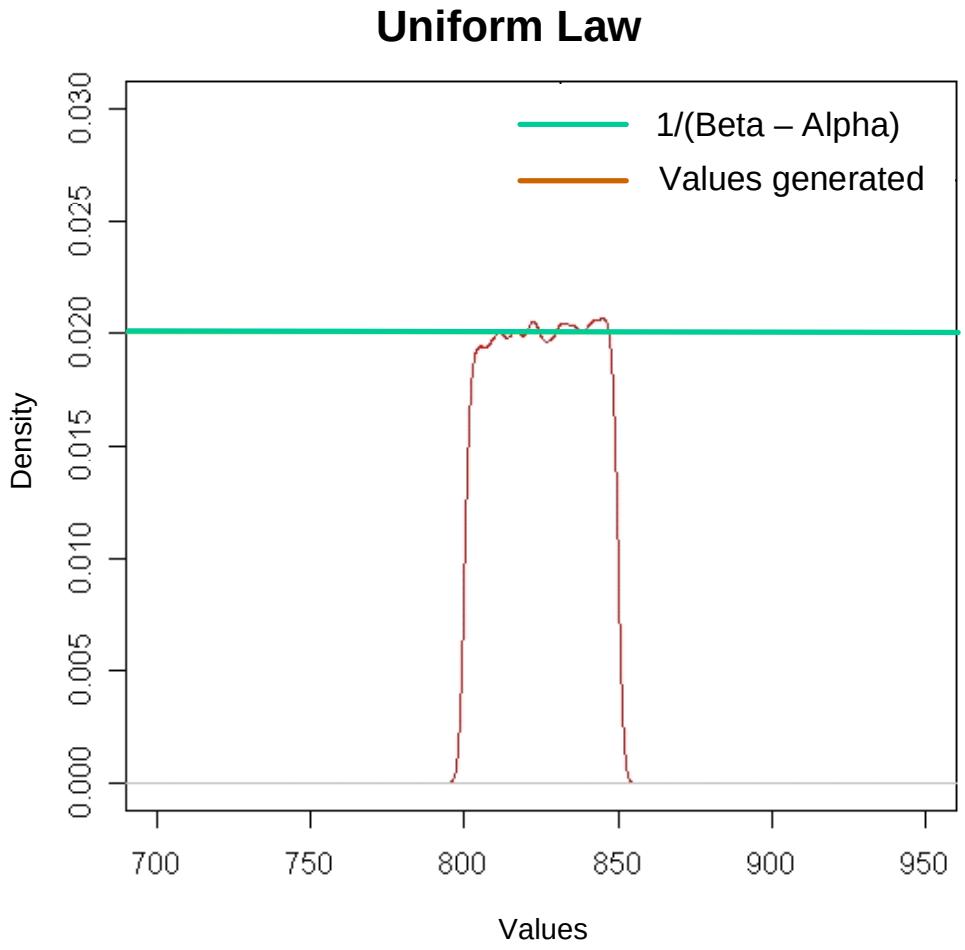
$$f(x) = 0 \qquad for \quad x < Alpha \quad or \quad x > Beta$$

where *Alpha* is the inferior parameter and *Beta* the superior one.



Values between *Alpha* and *Beta* have the same probability to be drawn = 1 / (*Beta* – *Alpha*).
When this law is used, the unit is the millisecond for the starting time of a connection or byte for the data volume to send.

Example of values generated by LanTraffic V2 Enhanced in the interval [800, 850]



Density of probability for the values generated by LanTraffic V2 Enhanced for

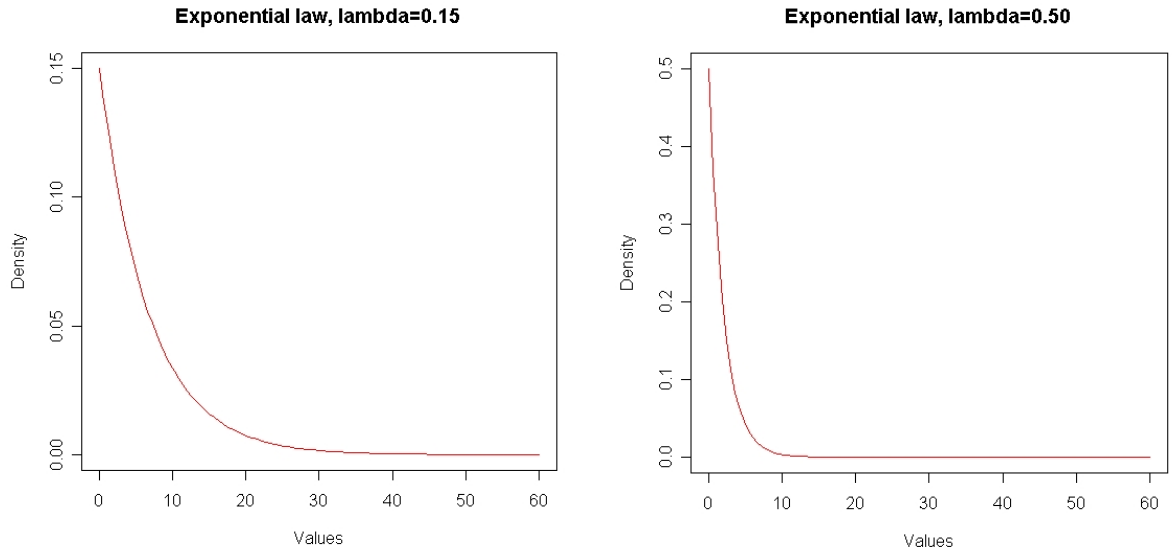
12.1.2 Exponential law

THEORY

The probability density function of the exponential law is:

$$f(x;\lambda) = \begin{cases} \lambda e^{-\lambda x} & , \ x \geq 0, \\ 0 & , \ x < 0. \end{cases}$$

where $\lambda > 0$ is the parameter of the distribution (*the rate parameter*).



The graphs above represent the theoretical density of the exponential distribution with λ=0.15 and λ=0.50.

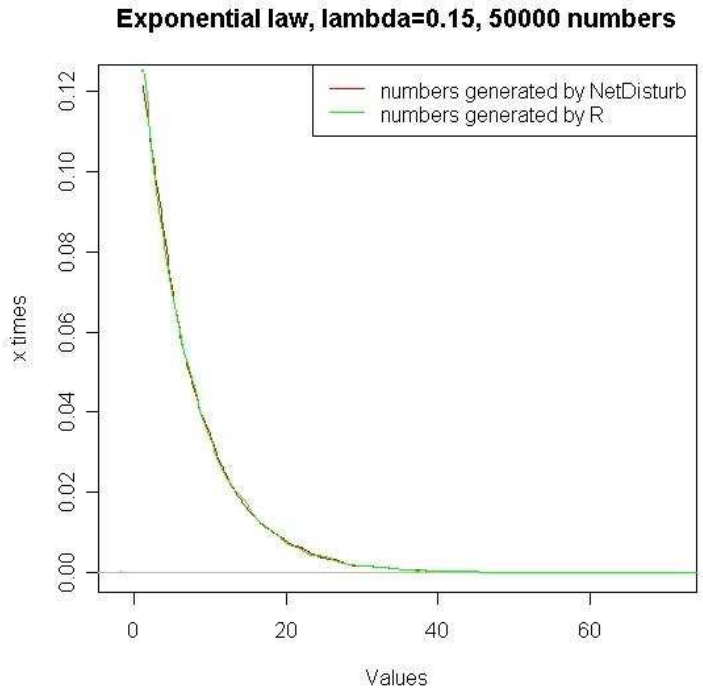
When we use the exponential distribution to draw random numbers, most the drawn values are theoretically small and the probability to draw big numbers is smaller.

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

PRACTICE

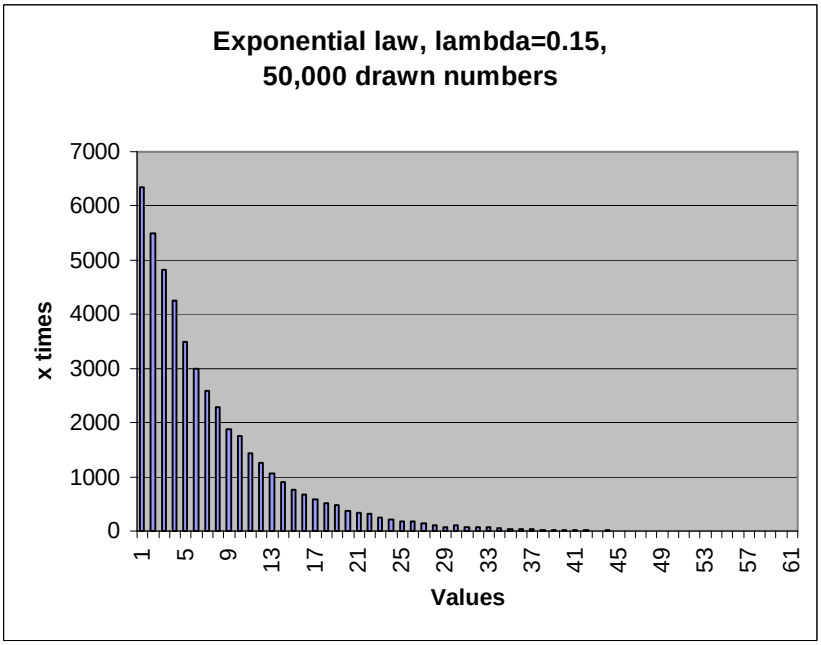
The exponential function is implemented in *LanTraffic V2 Enhanced* to generate numbers following an exponential distribution.
When this law is used, the unit is the millisecond for the starting time of a connection or byte for the data volume to send.

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

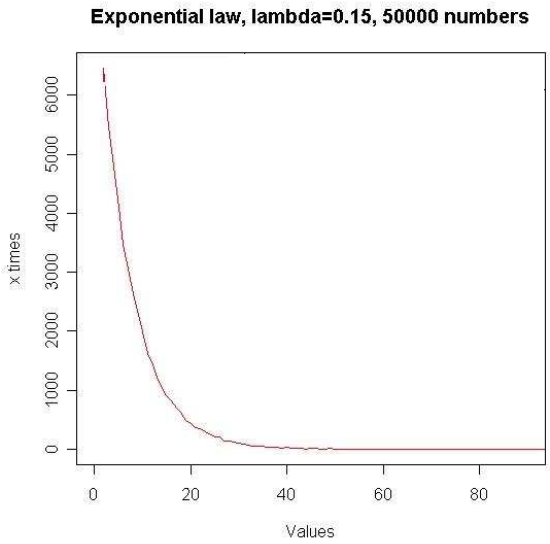


The green curve represents the distribution of random numbers generated by R and the red one represents the distribution of those generated by *LanTraffic V2 Enhanced*. They are very similar.
As shown in the theoretical part, the probability to have small numbers is much bigger than the probability to have big ones.

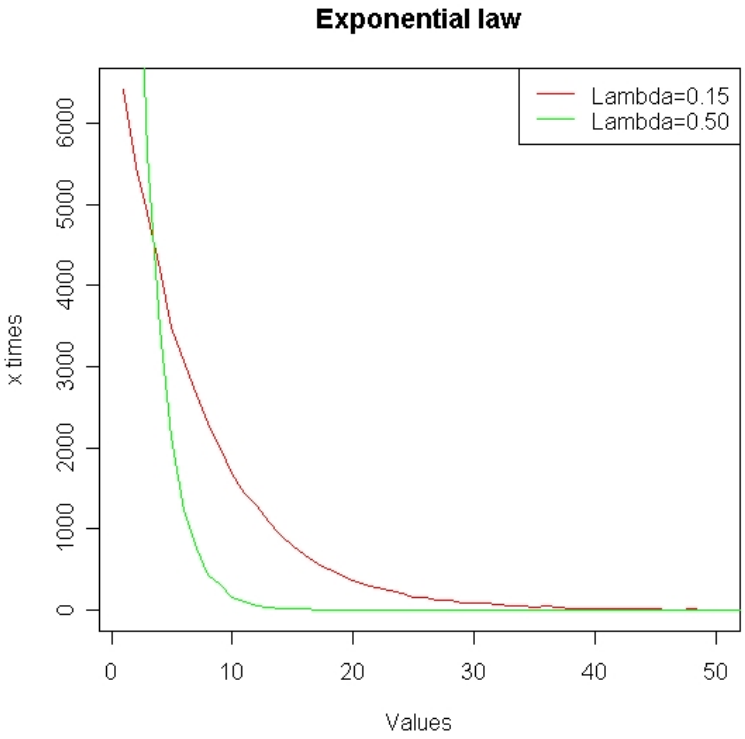
For example, we generate 50000 numbers following the exponential law with λ=0.15. As the numbers generated by the exponential function are of type “double”, we round them up to the nearest integer (e.g. 10.3 rounded up to 10 and 12.8 to 13). The histogram below summarizes the results.



The generated values are on the abscissa axe, and how many times each value is generated on the ordinate axe.
Otherwise, we can represent the same result by a curve.



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



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

We observe that the more the parameter λ is big, the more the maximum number generated is small and the other numbers generated are smaller too.

The table below summarizes the probability (in percent) to draw a value using the exponential function of *LanTraffic V2 Enhanced* with different values for λ in {0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1}.

~ Actually generated values	λ									
	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
0	4.946	9.358	14.126	18.294	22.334	25.850	29.722	33.220	36.050	36.050
1	8.956	16.044	22.426	26.874	30.432	33.538	35.274	36.732	37.956	37.956
2	8.200	13.368	16.178	17.974	18.654	18.488	17.546	16.548	15.364	15.364
3	7.394	10.904	12.478	12.324	11.476	9.908	8.934	7.468	6.308	6.308
4	6.524	9.148	9.048	8.176	6.790	5.580	4.280	3.334	2.574	2.574
5	6.198	7.432	6.468	5.314	4.078	3.028	2.134	1.498	1.056	1.056
6	5.556	6.136	4.848	3.680	2.496	1.642	1.070	0.636	0.408	0.408
7	5.034	4.998	3.718	2.466	1.554	0.868	0.504	0.306	0.166	0.166
8	4.512	4.130	2.766	1.622	0.838	0.502	0.252	0.148	0.058	0.058
9	4.084	3.312	2.074	1.050	0.470	0.272	0.142	0.052	0.042	0.042
10	3.698	2.778	1.484	0.810	0.322	0.174	0.068	0.032	0.008	0.008
11	3.306	2.266	1.146	0.418	0.208	0.054	0.040	0.010	0.004	0.004
12	2.964	1.812	0.822	0.346	0.144	0.034	0.022	0.010	0.006	0.006
13	2.832	1.542	0.600	0.236	0.078	0.036	0.008	0.006	0	0
14	2.584	1.252	0.484	0.124	0.056	0.012	0	0	0	0
15	2.078	0.976	0.330	0.098	0.030	0.004	0.004	0	0	0
16	1.900	0.836	0.242	0.072	0.012	0.004	0	0	0	0
17	1.810	0.658	0.210	0.032	0.014	0.006	0	0	0	0
18	1.646	0.558	0.144	0.030	0.004	0	0	0	0	0
19	1.484	0.420	0.108	0.018	0.008	0	0	0	0	0

20	1.360	0.352	0.112	0.014	0	0	0	0	0	0
21	1.220	0.344	0.048	0.004	0.002	0	0	0	0	0
22	1.088	0.288	0.034	0.008	0	0	0	0	0	0
23	1.004	0.184	0.022	0.004	0	0	0	0	0	0
24	0.976	0.184	0.018	0.010	0	0	0	0	0	0
25	0.780	0.130	0.020	0	0	0	0	0	0	0
26	0.750	0.100	0.018	0.002	0	0	0	0	0	0
27	0.692	0.080	0.008	0	0	0	0	0	0	0
28	0.568	0.064	0.004	0	0	0	0	0	0	0
29	0.552	0.074	0.010	0	0	0	0	0	0	0
30	0.540	0.044	0.002	0	0	0	0	0	0	0
31	0.442	0.032	0	0	0	0	0	0	0	0
32	0.446	0.038	0.004	0	0	0	0	0	0	0
33	0.376	0.026	0	0	0	0	0	0	0	0
34	0.386	0.036	0	0	0	0	0	0	0	0
35	0.280	0.016	0	0	0	0	0	0	0	0
36	0.274	0.012	0	0	0	0	0	0	0	0
37	0.280	0.016	0	0	0	0	0	0	0	0
38	0.212	0.014	0	0	0	0	0	0	0	0
39	0.184	0.006	0	0	0	0	0	0	0	0
40	0.182	0.012	0	0	0	0	0	0	0	0
41	0.166	0	0	0	0	0	0	0	0	0
42	0.142	0.004	0	0	0	0	0	0	0	0
43	0.152	0.004	0	0	0	0	0	0	0	0
44	0.110	0.004	0	0	0	0	0	0	0	0
45	0.110	0.002	0	0	0	0	0	0	0	0
46	0.110	0.004	0	0	0	0	0	0	0	0
47	0.096	0	0	0	0	0	0	0	0	0
48	0.078	0	0	0	0	0	0	0	0	0
49	0.088	0.002	0	0	0	0	0	0	0	0
50	0.072	0	0	0	0	0	0	0	0	0
51	0.060	0	0	0	0	0	0	0	0	0
52	0.060	0	0	0	0	0	0	0	0	0
53	0.048	0	0	0	0	0	0	0	0	0
54	0.034	0	0	0	0	0	0	0	0	0
55	0.036	0	0	0	0	0	0	0	0	0
56	0.022	0	0	0	0	0	0	0	0	0
57	0.044	0	0	0	0	0	0	0	0	0
58	0.018	0	0	0	0	0	0	0	0	0
59	0.018	0	0	0	0	0	0	0	0	0
60	0.030	0	0	0	0	0	0	0	0	0
61	0.016	0	0	0	0	0	0	0	0	0
62	0.008	0	0	0	0	0	0	0	0	0
63	0.016	0	0	0	0	0	0	0	0	0
64	0.018	0	0	0	0	0	0	0	0	0
65	0.010	0	0	0	0	0	0	0	0	0
66	0.014	0	0	0	0	0	0	0	0	0
67	0.014	0	0	0	0	0	0	0	0	0
68	0.014	0	0	0	0	0	0	0	0	0
69	0.018	0	0	0	0	0	0	0	0	0
70	0.014	0	0	0	0	0	0	0	0	0
71	0.010	0	0	0	0	0	0	0	0	0
72	0	0	0	0	0	0	0	0	0	0
73	0.004	0	0	0	0	0	0	0	0	0

74	0.006	0	0	0	0	0	0	0	0	0
75	0.002	0	0	0	0	0	0	0	0	0
76	0.004	0	0	0	0	0	0	0	0	0
77	0	0	0	0	0	0	0	0	0	0
78	0.008	0	0	0	0	0	0	0	0	0
79	0.008	0	0	0	0	0	0	0	0	0
80	0.006	0	0	0	0	0	0	0	0	0
81	0	0	0	0	0	0	0	0	0	0
82	0.002	0	0	0	0	0	0	0	0	0
83	0.004	0	0	0	0	0	0	0	0	0
84	0	0	0	0	0	0	0	0	0	0
85	0.002	0	0	0	0	0	0	0	0	0
86	0	0	0	0	0	0	0	0	0	0
87	0	0	0	0	0	0	0	0	0	0
88	0.002	0	0	0	0	0	0	0	0	0
89	0	0	0	0	0	0	0	0	0	0
90	0.004	0	0	0	0	0	0	0	0	0
91	0	0	0	0	0	0	0	0	0	0
92	0	0	0	0	0	0	0	0	0	0
93	0	0	0	0	0	0	0	0	0	0
94	0	0	0	0	0	0	0	0	0	0
95	0	0	0	0	0	0	0	0	0	0
96	0	0	0	0	0	0	0	0	0	0
97	0.002	0	0	0	0	0	0	0	0	0
98	0	0	0	0	0	0	0	0	0	0
99	0	0	0	0	0	0	0	0	0	0
100	0	0	0	0	0	0	0	0	0	0
101	0	0	0	0	0	0	0	0	0	0
102	0	0	0	0	0	0	0	0	0	0
103	0	0	0	0	0	0	0	0	0	0
104	0.002	0	0	0	0	0	0	0	0	0
105	0	0	0	0	0	0	0	0	0	0

In fact, the generated values are of type double. Here is example of values generated by the exponential law of *LanTraffic V2 Enhanced* with λ =0.1:

0.227489
1.961810
1.217468
13.854097
0.474025
5.870118
2.353334
0.766254
4.868133
0.802894

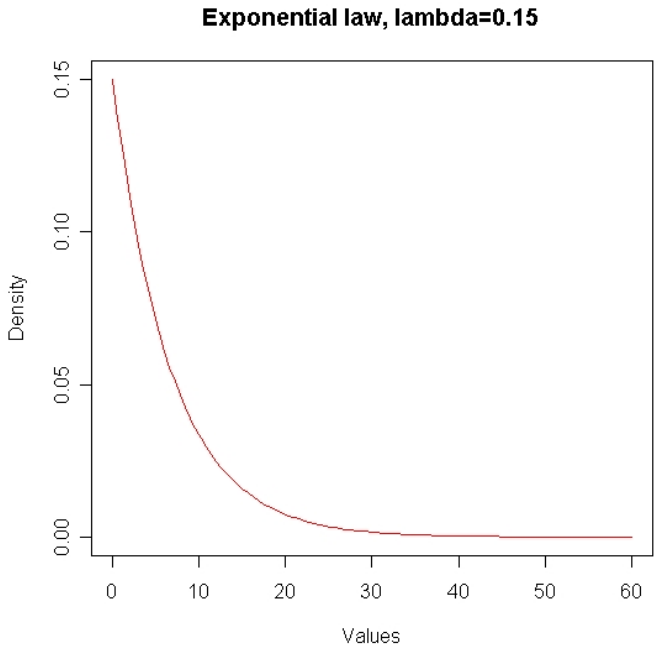
To represent those values in a simple way we round up double to the nearest integer, for example:

real values	represented values
0.227489	0
1.961810	2
1.217468	1
13.854097	14
0.474025	0

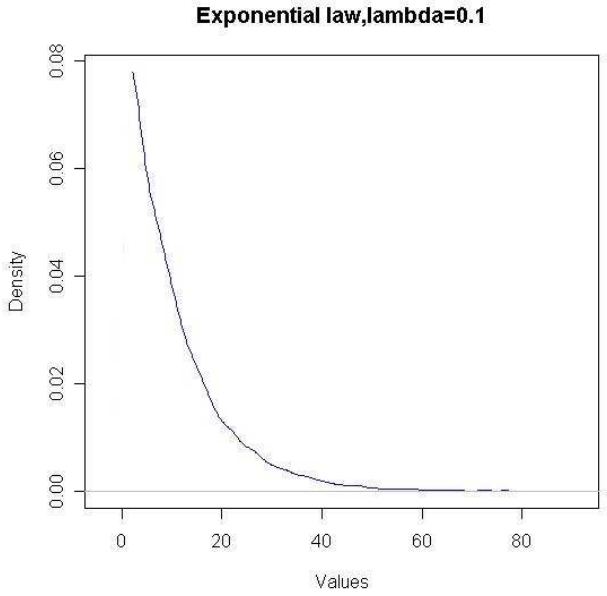
5.870118	6
2.353334	2
0.766254	1
4.868133	9
0.802894	1

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

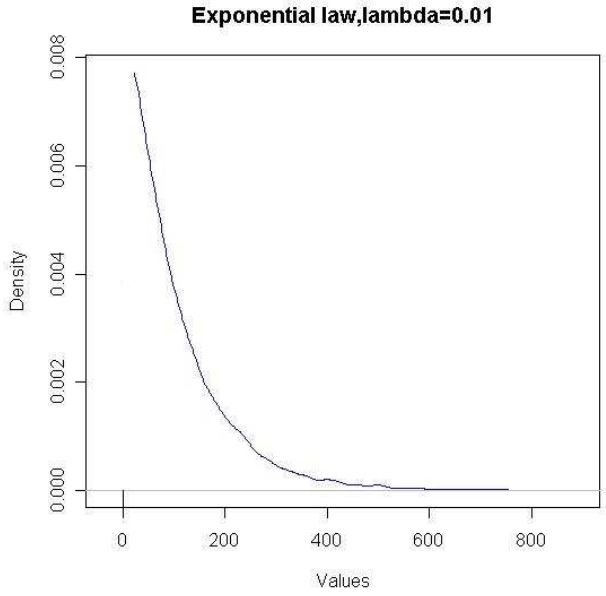
The effect of this approximation is more important when we draw values near "0". Thus the probability in the table to generate "0" is smaller than "1".



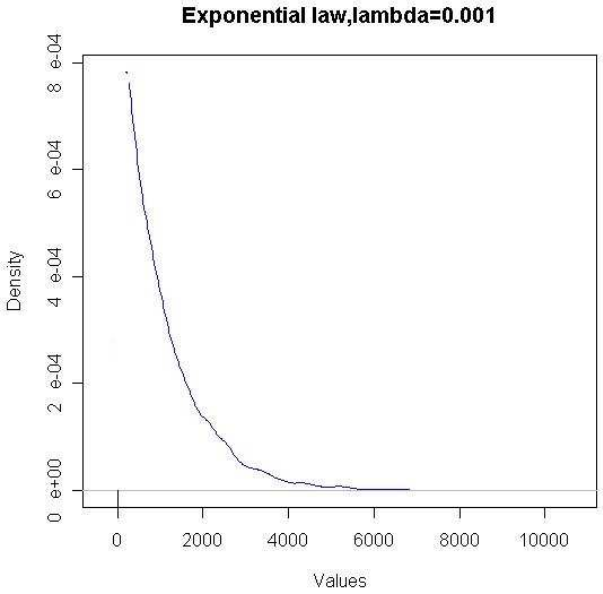
This graph is plotted with real values generated by LanTraffic V2 Enhanced. We observe that the probability for x="0" (=λ) is bigger than for x="1". Here are below graphs plotted with small values for λ.



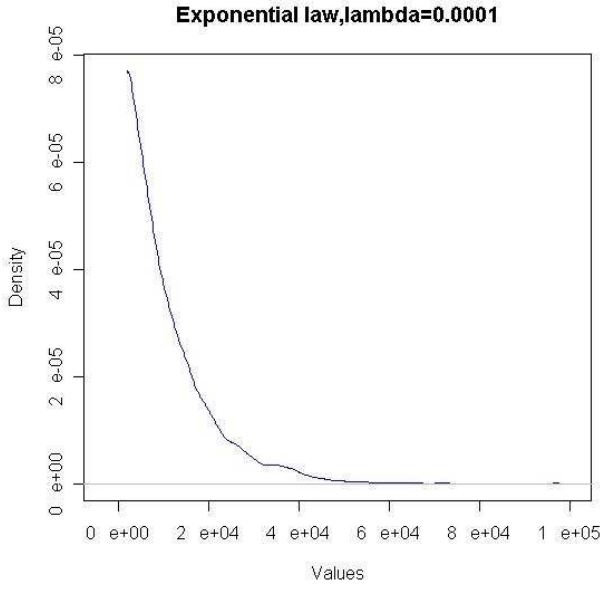
Maximum* drawn value = 221



Maximum* drawn value = 2218



Maximum* drawn value = 22180



Maximum* drawn value = 221807

**Maximum drawn value by the software, theoretically there is no maximum for the exponential law!*

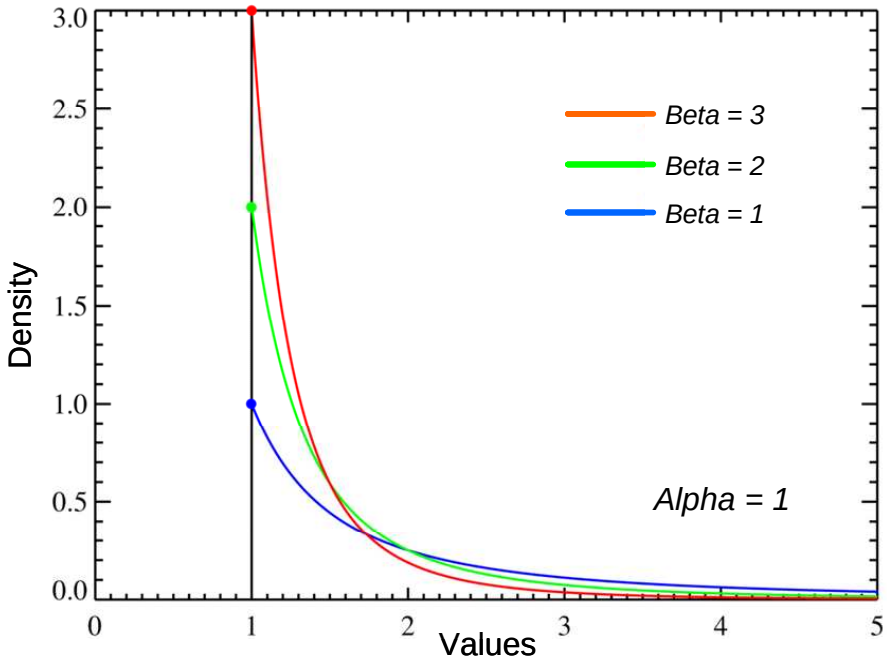
12.1.3 Pareto Law

The probability density function of the Pareto Law (a ,β ≥ 0) is:

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

$$f(x) = 0 \qquad if \ x < a$$

where a is the minimum possible value and β is the parameter.



Pareto probability density functions for various Beta with a = 1

The horizontal axis is the *x* parameter. As *Beta* → ∞ the distribution approaches δ(*x* − a) where δ is the Dirac delta function.

The Pareto distribution is related to the exponential distribution by: $f(x;\beta,a) = Exponential(\ln\frac{x}{a};\beta)$

- No value generated before a .
- The more β is big the more the maximum generated value is small.
- From a the small values are more often generated than big ones.
- The cumulative frequency from a given value *m* > a to a given value *n* > a is the integral of f(x) in this interval.

When this law is used, the unit is the millisecond for the starting time of a connection or byte for the data volume to send.

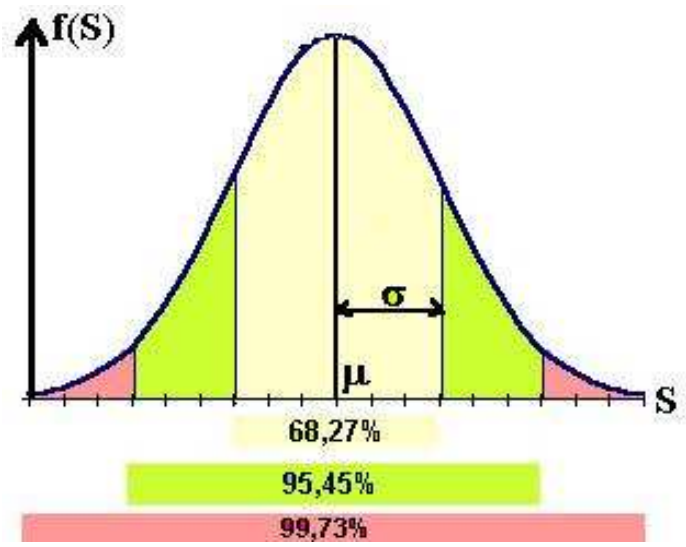
12.1.4 Laplace-Gauss law

When this law is used, the unit is the millisecond for the starting time of a connection or byte for the data volume to send.

The probability density function of the Laplace-Gauss Law is:

$$f(x) = \frac{n}{\sqrt{2\pi}\,\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

where μ is the average and σ is the standard deviation..



- The more σ is small the more drawn values are near μ
- 68.27% of drawn values are in $[\mu - \sigma ; \mu + \sigma]$
- 95.45% of drawn values are in $[\mu - 2\sigma ; \mu + 2\sigma]$
- 99.73% of drawn values are in $[\mu - 3\sigma ; \mu + 3\sigma]$

μ and σ must be defined such as: $\mu > 0$ and $\mu \geq 3\sigma$ with $\sigma > 0$

12.2 LanTraffic V2 Enhanced Traces

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

Traces activation is done by modifying directly in the registry database of Windows, the value of *DEBUGLEVEL* in the key HKEY_CURRENT_USER\SOFTWARE\ZTI\LanTrafficV2Enhanced\Settings

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. DebugView from SysInternals in Microsoft, Inc or DebugMon from OSR, Inc or the Microsoft Development environment).

LanTraffic V2 Enhanced application must be restarted after "DebugLevel" or "DebugFileName" parameter modification.

12.3 LanTraffic V2 Enhanced configuration parameters saved in the Registry

The based key to access parameters is \\HKEY_CURRENT_USER\Software\ZTI\LanTrafficV2Enhnaced\Settings. Updated information about Registry is available in the file "Version.txt" delivered with the **LanTraffic V2 Enhanced** software.
The user may change the General parameters to configure **LanTraffic V2 Enhanced** 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.

12.3.1 General configuration parameters

Key name	Type	Default value	Description
AutomatonDebugFilename	REG_SZ	AUT_DEBUG.LOG	User defined.
AutomatonDebugLevel	REG_DWORD	0x0	0x00000001 Errors 0x00000100 Addition of the current time 0x00010000 Put Debug information into the file defined by *AutomatonDebugFileName*
AutomatonPath	REG_SZ	*Installation dependent*	Full path name to the location of the automation tool used by **LanTraffic V2 Enhanced**.
DebugFileName	REG_SZ	LTV2_DEBUG.LOG	User defined
DebugLevel	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 DebugFileName
LTV2Path	REG_SZ	*Installation dependent*	Full path name to the location of **LanTraffic V2 Enhanced** used by the automation tool.

Key name	Type	Default value	Description
RPCPort	REG_DWORD	1001	Port number used by RPC
SendTimeOut	REG_DWORD	10	number of seconds for Winsock2 to send data. **Required for the Echoer mode**
TCPConnectRetryCounter	REG_DWORD	0x1	Number of retry to establish a TCP connection
TCPInactivity	REG_DWORD	5	TCP Inactivity tempo (seconds). The receiver stops the connection if no data is received during this time.
TCPNoDelay	REG_DWORD	0x0	0x0 : Nagle algorithm enabled Other value: Nagle algorithm disabled
TCPReceiverPacketSize	REG_DWORD	8192	Defines the packet size provided to Winsock2 WSARecv function call in bytes.
UDPInactivity	REG_DWORD	5	UDP Inactivity tempo (seconds). In the Receiver tab, with the Generator working mode, the connection stops when no data is received during this time.

LanTraffic V2 Enhanced must be restarted after each modification of these parameters.

12.3.2 Help configuration parameters

These parameters are for information only. They must not be changed. These information are located in \\HKEY_LOCAL_MACHINE\Software\ZTI\LanTrafficV2Enhanced

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

12.3.3 Unit configuration parameter

LanTraffic V2 Enhanced handles this parameter when a unit change occurs. It must not be changed.

Key name	Type	Description
UsedUnit	REG_DWORD	Reserved
UseLocalTime	REG_DWORD	Reserved

12.4 Default values of a context

The default values when opening a new context are:

- **Sender - Parameters**

Interface	Interface chosen by the system
IP version	Automatically Selected
IP address	NO_ADDRESS
Port Number	2009
Protocol	TCP
Testing mode	Unitary Mode

Data source	Packet generator (number of packets: infinite, packet contents: fix = 5A)
Packets size	Fix = 1460 bytes
Inter Packet Delay	Fix = 0 ms
RTT option	No
DSCP value	0
TTL value	0

- **Sender – Traffic + Statistics**

Columns for the statistics	Tx Throughput Tx Volume Tx Packets Rx Throughput Rx Volume Rx Packets Jitter
Clear on Stop	Unchecked

Export Statistics into a File	Export is disabled
Maximum size	10 MB

- **Receiver - Traffic + Statistics**

Interface	Interface chosen by the system
IP version	Automatically Selected
IP address	ANY_ADDRESS
Port number	2009
Protocol	TCP
Working Mode	Absorber

Columns for the statistics	Rx Throughput Rx Volume Tx Throughput Tx Volume Jitter

Export Statistics into a File	Export is disabled
Maximum size	10 MB

- **Throughput Graphics**

Refresh time for graphic display	2 sec
Physical Link Throughput	10 Mb/s

- **Configuration**

General Parameters	
Refresh time	2 sec
Throughput sampling period	5 sec
Timeout for TCP packets echoed	500 ms
Timeout for UDP packets echoed	700 ms
LanTraffic V2 Enhanced Buffer size	
Receive buffer size	65535
Transmit buffer size	65535

AutoComplete…	Enable

- **File transfer**

Port number	2500

- **Sender and Receiver statistics file**

Maximum size	10 MB

- **Data volume mathematical laws**

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

- **Inter Packet Delay mathematical laws**

Name	*Type*	*Parameters*	*Range*
Default	Uniform	Alpha = 0 Beta = 5	[0 ms, 5 ms]
Close delay law	Uniform	Alpha = 10 Beta = 20	[10 ms, 20 ms]
Far off delay law	Uniform	Alpha = 500 Beta = 1000	[500 ms, 1 s]
Variable delay law	Uniform	Alpha = 1 Beta = 1000	[1 ms, 1 s]

- **Starting time mathematical laws**

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

12.5 LanTraffic V2 Enhanced features versus OS, protocols and IP versions.

The array below shows the **LanTraffic V2 Enhanced** features based on the Windows versions, on the protocols and on the IP versions. The cross in a cell indicates when the feature is available.

Protocol / IP Version	TCP		UDP		ICMP	
	IPv4	*IPv6*	*IPv4*	*IPv6*	*IPv4*	*IPv6*
OS Versions						
Windows Vista	x	x	x	x	x	x
Windows Server 2003	x	x	x	x	x	x
Windows Seven	x	x	x	x	x	x
Windows Server 2008	x	x	x	x	x	x
Sender Part						
Unitary Mode	x	x	x	x	x	x
Automatic Mode	x	x	x	x		
Interface Selection	x	x	x	x	x	x
Receiver Part						
Absorber Mode	x	x	x	x		
Absorber File Mode	x	x	x	x		
Echoer Mode	x	x	x	x		
Echoer File Mode	x	x	x	x		
Absorber Generator	x	x	x	x		
Interface Selection	x	x	x	x		
Traffic Generator Parameters (used by the Unitary Mode and the Absorber Generator Mode)						
Max Data Size (in bytes)	65535	65535	65507	65507	65535	65535
TTL / Hop Limit	x	x	x	x	x	x
DSCP	x		x		x (except on Vista)	
Mean Throughput (Pkts/s)			x	x	x	x
Mean Throughput (kb/s)	x	x	x	x		
RTT	x	x	x	x		