



LanTraffic V2

Version 2.4

Traffic Generator for IP Networks (IPv4 & IPv6)
LAN, MAN, WAN, WLAN, WWAN, Mobile, Satellite, PLC, etc.

LanTraffic V2

File Edit Configuration File Downloading Automation Tool Help

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

Destination Parameters

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

Save the Received Data

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

Unitary Mode | Automatic Mode

Traffic Generator

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

[P]

Sender Statistics (based on application data):

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

Total Sending Throughput: Total Receiving Throughput:

Start Receiver

Stop Receiver

Receiver Statistics (based on application data):

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

Total Sending Throughput: Total Receiving Throughput:

User Guide

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

ZTI could not be liable for any direct or indirect damages caused by the software or User 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 96 48 43 43
Fax: +33 2 96 48 14 85
Web: <http://www.zti-telecom.com> or <http://www.zti.fr>
Email: contact@zti-telecom.com (marketing & sales)
support@zti-telecom.com (technical support)

Copyrights

Copyright ZTI 1997-2005. All rights reserved.
France Telecom licensed product.

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

No part of this manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written consent from ZTI.

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

Software License Agreement

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

- **COPYRIGHT**

The enclosed Software and documentation (here after called the Products) remains 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 Products properly.

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

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

- **SOFTWARE PROTECTION**

LanTraffic V2 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 Site Code, which requires the corresponding unique Site Key to be entered before the tool is operational.

- **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.

- **JURISDICTION**

French laws will govern this agreement.

The court of GUINGAMP (France) shall finally settle all disputes arising out of or in connection with this Agreement.

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

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

Phone: +33 2 96 48 43 43
Fax: +33 2 96 48 14 85
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	<i>Organization of this guide.....</i>	8
0.2	<i>Minimum System Requirements.....</i>	9
0.3	<i>References</i>	9
0.4	<i>Terms used in this document</i>	10
0.5	<i>Technical Support.....</i>	10
PART 1	Product Overview	11
1.1	<i>LanTraffic V2 Key Features.....</i>	11
1.2	<i>The Automation Tool for LanTraffic V2.....</i>	16
PART 2	What's new in LanTraffic V2 Version 2.4	17
2.1	<i>New features and improvements included in the version 2.4</i>	17
2.2	<i>Upgrading from Version 2.2 or 2.3</i>	18
2.3	<i>Upgrading from Versions 2.1 and older.....</i>	18
2.4	<i>Acrobat Reader version compatibility</i>	18
PART 3	Install LanTraffic V2.....	19
3.1	<i>How to install the software downloaded from the Internet.....</i>	19
3.2	<i>How to install the software from the CD-ROM</i>	21
PART 4	Software License Configuration	22
4.1	<i>How to configure the license</i>	22
4.2	<i>License Transfers.....</i>	25
4.2.1	<i>Direct Transfer: move the license from one local directory to another</i>	25
4.2.2	<i>Transfer by media (floppy disk or USB key) from a source PC to a target PC.....</i>	26
4.3	<i>How to kill a license</i>	32
PART 5	Uninstall LanTraffic V2	33
PART 6	LanTraffic V2 Getting Started	34
PART 7	Run LanTraffic V2	40
PART 8	LanTraffic V2 / Windows Firewall	41
8.1	<i>Configuration for UDP, TCP connections and ICMP IPv4.....</i>	41
8.2	<i>Configuration for ICMP IPv6 connections</i>	44
PART 9	Graphical User Interface	45
9.1	<i>Main Window</i>	45
9.2	<i>Display general rules of the Graphical User Interface</i>	46
9.3	<i>Used units for the information display</i>	47
9.3.1	<i>Volume units</i>	47
9.3.2	<i>Throughput units</i>	47
PART 10	Using LanTraffic V2.....	48
10.1	<i>Main steps.....</i>	48
10.2	<i>Menu description.....</i>	49
10.2.1	<i>File menu</i>	49

10.2.1.1	File/New	49
10.2.1.2	File/Open	49
10.2.1.3	File/Save	49
10.2.1.4	File/Save as	49
10.2.1.5	File/Recent Contexts	50
10.2.1.6	File/Exit	50
10.2.2	Edit menu	50
10.2.2.1	Edit/Destination Parameters: IP Address or Host Name	50
10.2.2.2	Edit/Destination Parameters: Protocol	50
10.2.2.3	Edit/Destination Parameters: Port	50
10.2.3	Configuration menu	51
10.2.3.1	Configuration/Stack Parameters	51
10.2.3.2	Configuration/General Parameters	52
10.2.3.3	Configuration/AutoComplete	53
10.2.4	File Downloading menu	55
10.2.5	Automation Tool menu	58
10.2.5.1	Automation Tool/Open	58
10.2.5.2	Automation Tool/Close	58
10.2.5.3	Automation Tool/Bring to the top	58
10.2.6	Help menu	59
10.2.6.1	Help/Help	59
10.2.6.2	Help/Forewarnings	59
10.2.6.2.1	Inter packet delay	59
10.2.6.2.2	Echoer modes	59
10.2.6.2.3	UDP connections	60
10.2.6.3	Help/Getting Started (IPv4)	61
10.2.6.4	Help/About LanTrafficV2	61
10.3	Total statistics	62
10.3.1	Sender statistics	62
10.3.2	Receiver statistics	62
10.4	The Sender part	63
10.4.1	Sender - Parameters tab	63
10.4.1.1	Destination parameters	64
10.4.1.1.1	Summary of connection parameters	64
10.4.1.1.2	Select the network interface, IP version and source IP address	65
10.4.1.1.3	IP Address translation mechanism	67
10.4.1.1.4	Duplicate parameters of a connection onto others	67
10.4.1.1.5	IP address floating menu	68
10.4.1.1.6	Protocol floating menu	69
10.4.1.1.7	Port floating menu	69
10.4.1.2	Save the Received Data	69
10.4.1.3	Configure the Unitary Mode	70
10.4.1.3.1	Step 1: select the traffic generator type for this connection	71
10.4.1.3.1.1	Packets Generator	71
10.4.1.3.1.2	Mathematical law	72
10.4.1.3.1.3	File to send	73
10.4.1.3.2	Step 2: Specify data size and packets parameters	74
10.4.1.3.2.1	Data Size	74
10.4.1.3.2.2	Inter Packet Delay	75
10.4.1.3.2.3	RTT option	75
10.4.1.3.2.4	The TOS field (IPv4 only) / DSCP	76
10.4.1.3.2.5	The TTL field	78
10.4.1.3.3	Step 3 (optional): Activate a throughput limit	78
10.4.1.4	Configure the Automatic Mode	79
10.4.1.4.1	Starting time connections generation laws	80
10.4.1.4.2	Data volume to send laws	81
10.4.1.4.3	Packet Size	82
10.4.2	Sender - Traffic + Statistics tab	83
10.4.2.1	Destination Parameters	83
10.4.2.2	Sender Statistics	84

10.4.2.3	Export Statistics into a File	86
10.4.2.3.1	Sender statistics file format.....	87
10.4.2.3.2	Export Sender file sample.....	88
10.4.2.4	Run the Unitary Mode	90
10.4.2.5	Run the Automatic Mode	91
10.4.3	Using ICMP capacity of the Sender	92
10.5	The Receiver part	93
10.5.1	Duplicate parameters of a connection onto others.....	93
10.5.2	Listening To	94
10.5.2.1	Summary of the connection parameters.....	94
10.5.2.2	Select the network interface, IP version and local IP address.....	95
10.5.2.3	Port floating menu.....	97
10.5.2.4	Protocol floating menu	97
10.5.3	Coming From	98
10.5.3.1	IP address floating menu	98
10.5.3.2	IP Address translation mechanism	98
10.5.4	Working Mode.....	99
10.5.4.1	Absorber mode	99
10.5.4.2	Absorber File mode.....	99
10.5.4.3	Echoer mode.....	99
10.5.4.4	Echoer File mode.....	100
10.5.4.5	Absorber + Generator mode	100
10.5.4.6	Disable mode	101
10.5.5	Statistics	101
10.5.6	Export Statistics into a File	104
10.5.6.1	Receiver statistics file format	105
10.5.6.2	Export Receiver file sample	106
10.6	The Throughput Graphics tab.....	108
10.6.1	The Graphical Display object.....	109
10.6.2	The Display Configuration object.....	111
PART 11	Command Line Parameters	112
PART 12	How To Do	114
12.1	Checking router configuration.....	114
12.1.1	PC #2 parameters	114
12.1.2	PC #1 parameters	115
12.1.3	What should happen?.....	116
12.2	Checking a firewall configuration.....	117
12.2.1	LanTraffic V2 parameters on the server.....	117
12.2.2	LanTraffic V2 parameters for the Remote PC	119
12.2.3	What result can you expect?	120
12.3	Checking the best throughput.....	120
12.3.1	PC #2 parameters	120
12.3.2	PC #1 parameters	121
12.4	ADSL connection simulation	122
12.4.1	PC #2 parameters	122
12.4.2	PC #1 parameters	123
12.5	Generating multicast IP traffic.....	124
12.5.1	PC #2 and PC #3 parameters	124
12.5.2	PC #1 parameters	125
12.6	IPV6 connection	126
12.6.1	PC #2 parameters	126
12.6.2	PC #1 parameters	127
12.7	Source/Local IP Address and Interface requirements	129
PART 13	Annexes	131

13.1	<i>Mathematical laws used by LanTraffic V2</i>	131
13.1.1	<i>Uniform law</i>	131
13.1.2	<i>Exponential law</i>	132
13.1.3	<i>Pareto Law</i>	134
13.1.4	<i>Gauss law</i>	135
13.2	<i>LanTraffic V2 Traces</i>	136
13.3	<i>LanTraffic V2 configuration parameters saved in the Registry</i>	136
13.3.1	<i>General configuration parameters</i>	136
13.3.2	<i>Help configuration parameters</i>	137
13.4	<i>Default values of a context</i>	138

PART 0 Preface

0.1 Organization of this guide

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

- **Part 1: Product Overview**

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

- **Part 2: What's new in LanTraffic V2 version 2.4**

This part is a general overview of new features, main improvements provided with **LanTraffic V2** version 2.4 and important information to upgrade from previous versions.

- **Part 3: Install LanTraffic V2**

Product requirements and how to install the software downloaded from the Internet or from the CD-ROM.

- **Part 4: Software License Configuration**

Describes how to configure the license and how to proceed for the license transfer

- **Part 5: Uninstall LanTraffic V2**

How to uninstall the software.

- **Part 6: LanTraffic V2 Getting Started**

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

- **Part 7: Run LanTraffic V2**

How to run the software and configure the license if needed.

- **Part 8: LanTraffic V2 / Windows Firewall**

How to configure the Windows firewall to authorize the use of **LanTraffic V2**.

- **Part 9: Graphical User Interface**

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

- **Part 10: Using LanTraffic V2**

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

- **Part 11: Command Line Parameters**

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

- **Part 12: How To Do ...**

Some examples about how and where to use **LanTraffic V2**.

- **Part 13: Annexes**

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

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



Warning



Zoom or Advice



Note or Remark

0.2 Minimum System Requirements

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

- Windows 98 (SE recommended), Me, NT4 (SP6 recommended), 2000 or XP
- Pentium processor with 128 MB memory
- 1024 x 768 display and DPI setting = Normal size (96 DPI)
- 15 MB free hard disk space



Windows XP and later is required to use IPv6.



*Acrobat Reader is needed to display the **LanTraffic V2** Help. If Acrobat reader hasn't been installed, a warning message is displayed to inform that **LanTraffic V2** is available without the help 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.msp>
- [RFC2460] "Internet Protocol, Version 6 (IPv6) - Specification"
- [RFC2373] "IP Version 6 Addressing Architecture"

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

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 96 48 14 85
Telephone	Telephone support is available from 09:00 am to 06:00 pm (GMT Time +1 or +2), Monday to Friday. Call +33 2 96 48 43 43

PART 1 Product Overview

1.1 LanTraffic V2 Key Features

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

LanTraffic V2 is supported on the following platforms: Windows XP Home or Professional, Windows 2000 Professional or Server, Windows NT 4 Service Pack 6 Workstation or Server, Windows 98 or Me. It needs at least one Ethernet connection (LAN or WLAN card i.e. NIC, remote access...).

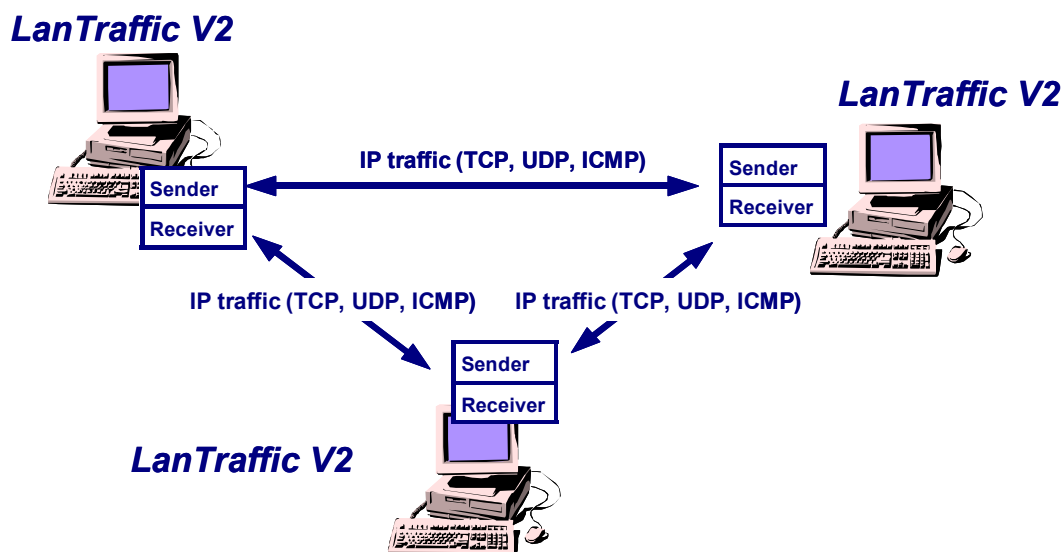
The minimum screen resolution is 1024 x 768 and the DPI setting should be "Normal size (96 DPI)".

LanTraffic V2 requires Acrobat Reader to display the software Help file.

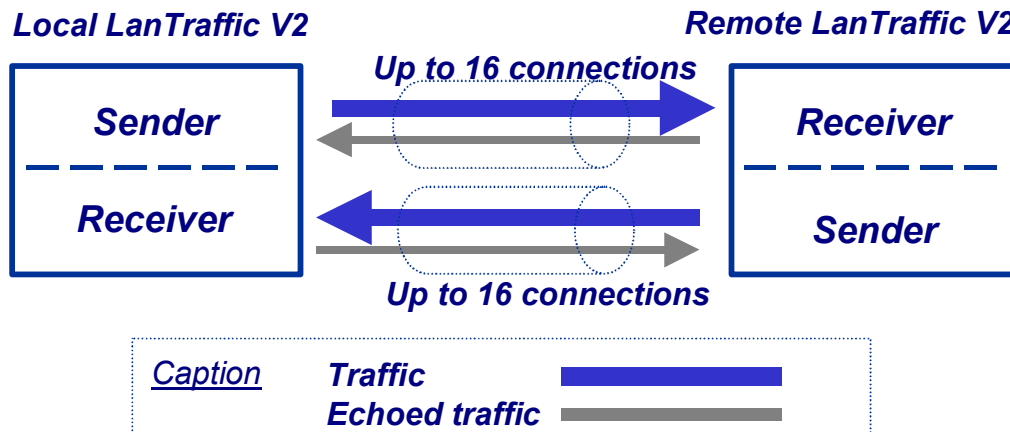
The add-on software called **Automation Tool for LanTraffic V2** allows automating operations with **LanTraffic V2**. For instance, you can run test campaigns automatically.

Various testing configurations can be implemented using more than two PCs.

LanTraffic V2 creates TCP or UDP connections between PCs through the IP network.



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



- The **Sender** generates up to 16 simultaneous UDP and/or TCP connections. 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.

LanTraffic V2 offers three different data sources:

- Automatic data generator by using mathematical laws,
 - Packets generator: many parameters can be defined (number of packets to send, inter packet delay, packet contents, ...)
 - File: selection of a file to send.
- ⇒ **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.
- ⇒ **Statistics**: for each connection the following statistics parameters are displayed by the **Sender** 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
 - RTT Mean (Round Trip Time)
 - Jitter

- The **Sender** can also generate up to 16 simultaneous ICMP connections, but through the unitary testing mode only:

⇒ **Unitary mode:** for each IP connection, you can select the traffic generator data source, specify the ToS byte (Type of Service) and the Time To Live byte (TTL).

Find below the different possibilities available with the ICMP protocol:

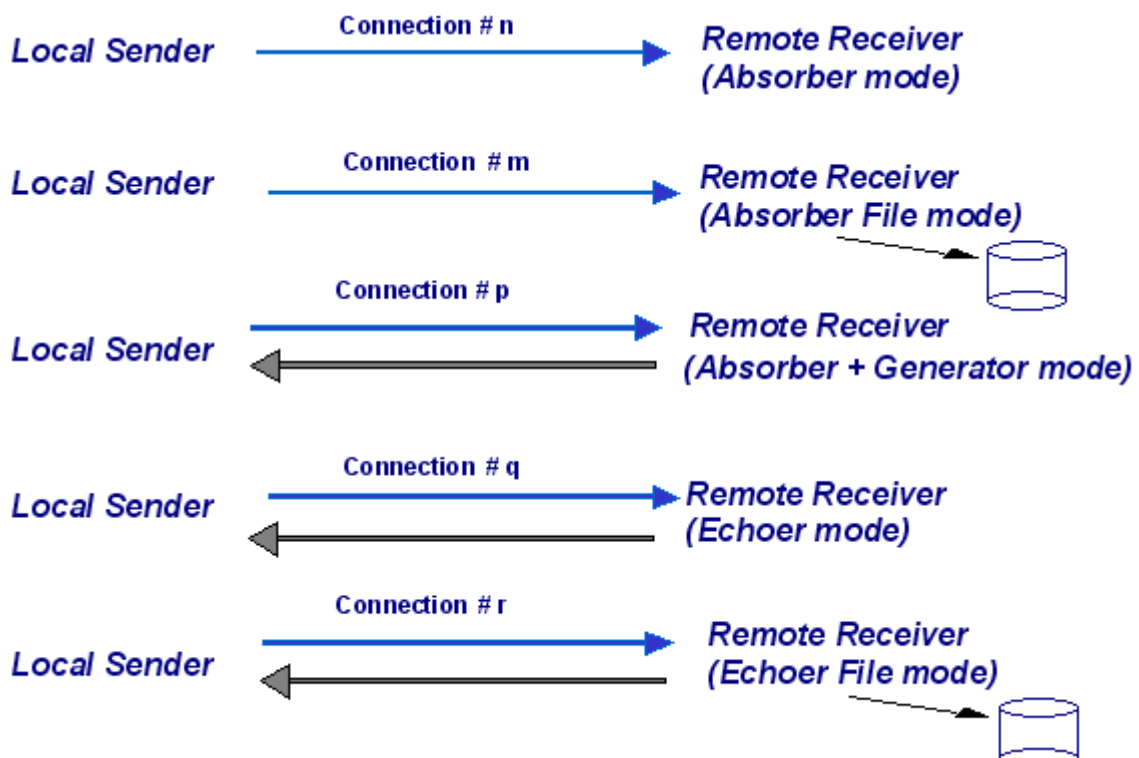
- ICMP Echo request packet number and content: packet generator (fixed, randomized, alternated and increasing / decreasing).
- ICMP Echo Request data size: fixed, randomized, alternated and increasing / decreasing.
- ICMP Echo Reply receiving timeout: fixed, randomized, alternated, increasing / decreasing or use of a mathematical law.

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

- Sent ICMP requests (Tx Packets)
- Received ICMP replies (Rx Packets, responses sent by the target remote)
- Sequence numbering errors
- RTT Mean (Round Trip Time)

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

⇒ Each Receiver connection can be set up according to one of the following five modes:



Note: in this document, we will 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 is able to generate and receive Unicast and 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).
For information: these IPv4 addresses 224.0.0.0 to 224.255.255.255 do not generate IGMP JOIN /LEAVE messages.
- **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.

IP version selection (Windows XP and later)

Please note that **LanTraffic V2** supports IPv6 for Windows XP and later versions (i.e. 2003 Server) but doesn't support IPv6 for Windows 2000.

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

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

With IPv6 the maximum size of the packet is **1440** bytes whereas it is 1460 bytes with IPv4, to avoid IP fragmentation.

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.

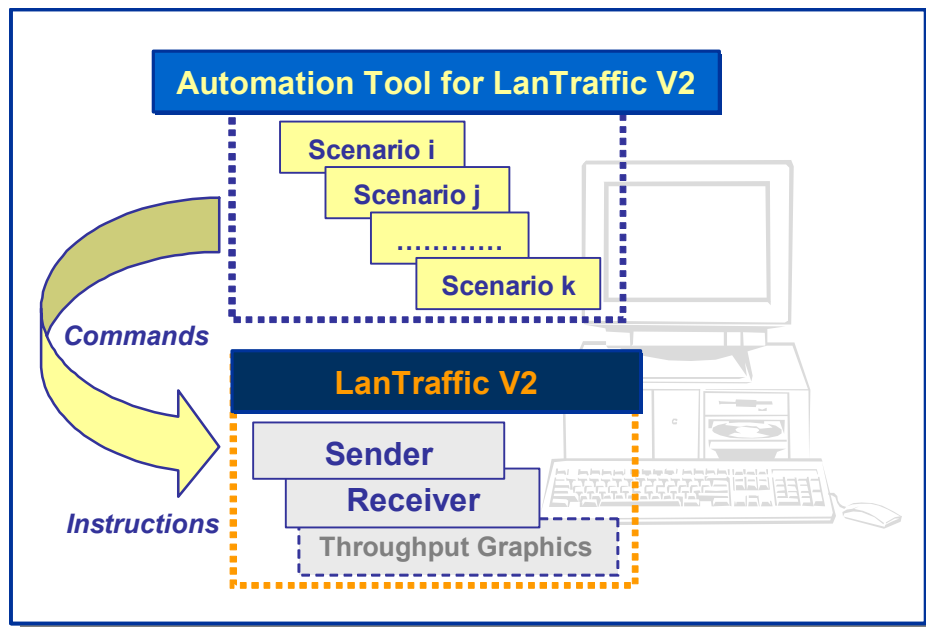
LanTraffic V2 is able to generate and receive Unicast and Multicast IP traffic on a selected interface, giving the user a deeper control where data are exchanged and makes multiple routes definition easier.

Statistics values

Statistics values presented by **LanTraffic V2** 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

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

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** you can:

- Set automatically the parameters of the **LanTraffic V2** 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 What's new in LanTraffic V2 Version 2.4

This part is a general overview of new features and main improvements of **LanTraffic V2** version 2.4. You will find some important information on how to upgrade your software from previous versions.

Details regarding features and corrections included in the different versions of **LanTraffic V2** can be found in the version.txt file located in the installation directory (by default: C:\Program Files\LanTraffic V2).

To upgrade your software from 2.2 or 2.3 to 2.4 version, please refer to paragraph 2.2.
To upgrade your software from 2.1 version and older to 2.4 version, please refer to paragraph 2.3.

2.1 New features and improvements included in the version 2.4

⇒ **LanTraffic V2 (Version 2.4)**

- First time users: Getting Started information
- Automatic choice of the IP Version (IPv4 or IPv6) depending on the specified IP address (IP or Host Name)
- IPv6: File Downloading is now available
- Accuracy increase of the refresh statistics process
- **LanTraffic V2** is now able to do ICMP request generation on the Sender Part
- The source port used to generate data is now user-defined

The contexts created with versions 2.0.12 and higher are reused automatically. When saved, they become the new 2.4 context file format.

⇒ **Automation Tool for LanTraffic V2 (Version 1.3)**

- The Automation Tool is now able to launch an external application for a new scenario command.
- The time reference to interpret date/time (local or UTC) placed in the Automation Tool is now user-defined.
- New feature for the "Wait" command: the time can now be defined without having to enter a date.
- The Automation Tool can be stopped or started to execute a scenario, from the DOS console.

The scenarios created with older versions are reused automatically. When saved, they become the new 1.3 scenario file format.

2.2 Upgrading from Version 2.2 or 2.3

There is no need to uninstall **LanTraffic V2** version 2.3 or 2.2 before upgrading to version 2.4. The installation procedure will detect and update the previous version automatically.

The installation of the **LanTraffic V2** version 2.4 over the **LanTraffic V2** version 2.3 or 2.2 will replace the following application and documentations files:

- LanTrafficV2.exe and Aut_LTV2.exe,
- "Read Me First.pdf", "LanTraffic V2 User Guide.pdf" and "Automation Tool for LanTraffic V2 User Guide.pdf".

The license scheme is maintained during the upgrade process. If an unlimited license is available, **LanTraffic V2** version 2.4 is ready for unlimited use. If you are using a trial version, the number of remaining days remains the same and will continue to decrease up to the final date.

LanTraffic V2 version 2.4 requires Acrobat Reader: see paragraph 2.4 for more details.

2.3 Upgrading from Versions 2.1 and older

There is no need to uninstall **LanTraffic V2** version 2.1 and older before upgrading to version 2.4. The installation procedure will detect and update the previous version automatically.

The license scheme is maintained during the upgrade process. If an unlimited license is available, **LanTraffic V2** version 2.4 is ready for unlimited use. If you are using a trial version, the number of remaining days remains the same and will continue to decrease up to the final date.

LanTraffic V2 version 2.4 requires Acrobat Reader: see paragraph 2.4 for more details.

2.4 Acrobat Reader version compatibility

To access the **LanTraffic V2's** help file, Acrobat Reader is required.

LanTraffic V2 supports Acrobat Reader version from 4.01 to 7.0 that have been tested successfully.

If the Acrobat reader version you are using is too old, you can find the latest version on the **LanTraffic V2's** CD-ROM or download it straight from the Acrobat reader website: www.adobe.com.

PART 3 Install LanTraffic V2

LanTraffic V2 requires less than 15 MB of free disk-space. The default settings folder is C:\Program files\LanTrafficV2.

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



** To run LanTraffic V2 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 for Windows NT, 2000 and XP, you must log on with your administrators rights.*



We recommend that you shutdown first your anti-virus application before installing LanTraffic V2.

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 default settings of **LanTraffic V2** come with a 15-day limited license. When it reaches the deadline, **LanTraffic V2** stops running. Go to PART 3 for more information about the license program.

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

3.1 How to install the software downloaded from the Internet



To install LanTraffic V2 for Windows NT4, 2000 or XP, you must log on with your administrators rights.

If you have downloaded **LanTraffic V2** trial version from our website, you have downloaded the "LanTrafficV2.zip" file including the software and the related documentation.

You must first unzip this file in a temporary directory.

Then run [Setup_LanTrafficV2Bundle.exe](#) from this temporary directory to launch the setup procedure and follow the instructions on the screen.

The default settings install **LanTraffic V2** in the following directory: C:\Program Files\LanTrafficV2.

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

- LanTrafficV2.exe: program file
- LanTraffic V2 User Guide: PDF file (use the free version of Adobe® Acrobat® Reader® software. Available on www.adobe.com).
- Aut_LTV2.exe: program file (Automation tool)
- Automation Tool for LanTraffic V2 User Guide: PDF file
- LanTrafficV2 license help file
- Version.txt: text file which contains information about the versions and the Registry parameters.



All files created by **LanTraffic V2** are saved in the folder where **LanTraffic V2** has been installed.

Start Menu shortcuts created:

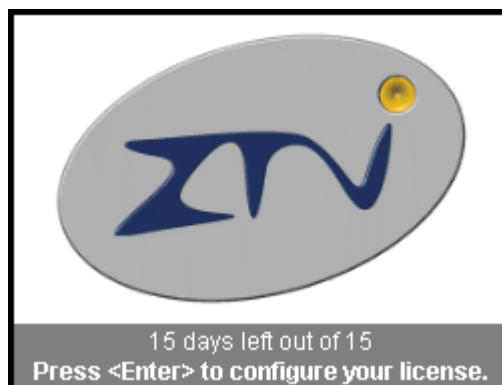
Start > Programs > **LanTraffic V2**

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



You will need to restart your system in order to complete the software installation.

When launching a **LanTraffic V2** trial version for the first time, a message is displayed showing the remaining days of use (for example, 15 days left out of 15 in the following example):



Please refer to PART 4 (Software License Configuration) to configure your unlimited license.

3.2 How to install the software from the CD-ROM

The installation procedure is a standard installation program.



To install LanTraffic V2 for Windows NT4, 2000 or XP, you must log on with your administrators rights.

- First, insert the **LanTraffic V2** CD-ROM in your CD-ROM drive.
- Click on “Start”, “Execute” and type “CD unit>: \Setup_LanTrafficV2Bundle.exe”. Follow the **LanTraffic V2** setup instructions to proceed with the installation. **LanTraffic V2** default settings install files in the following directory: C:\Program Files\LanTrafficV2.

Start Menu shortcuts created:

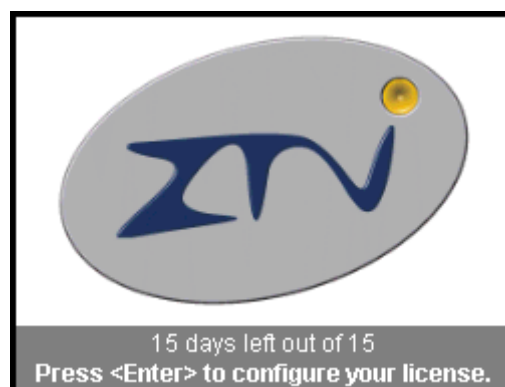
Start > Programs > **LanTraffic V2**

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



You will need to restart your system in order to complete the software installation.

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



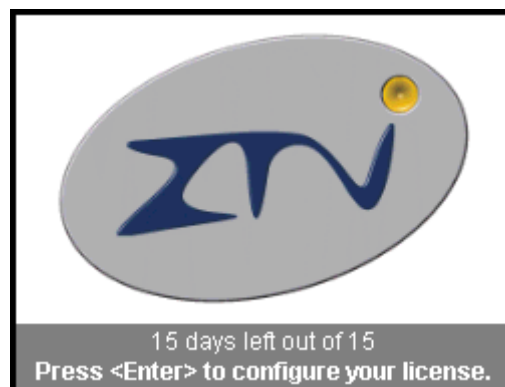
Please refer to PART 4 (Software License Configuration) to configure your unlimited license.

PART 4 Software License Configuration

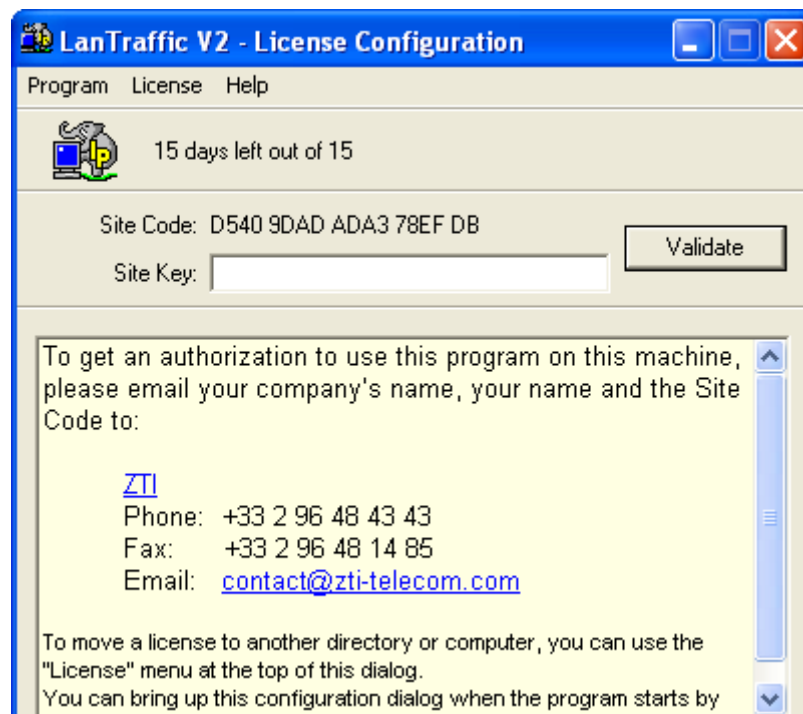
4.1 How to configure the license

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

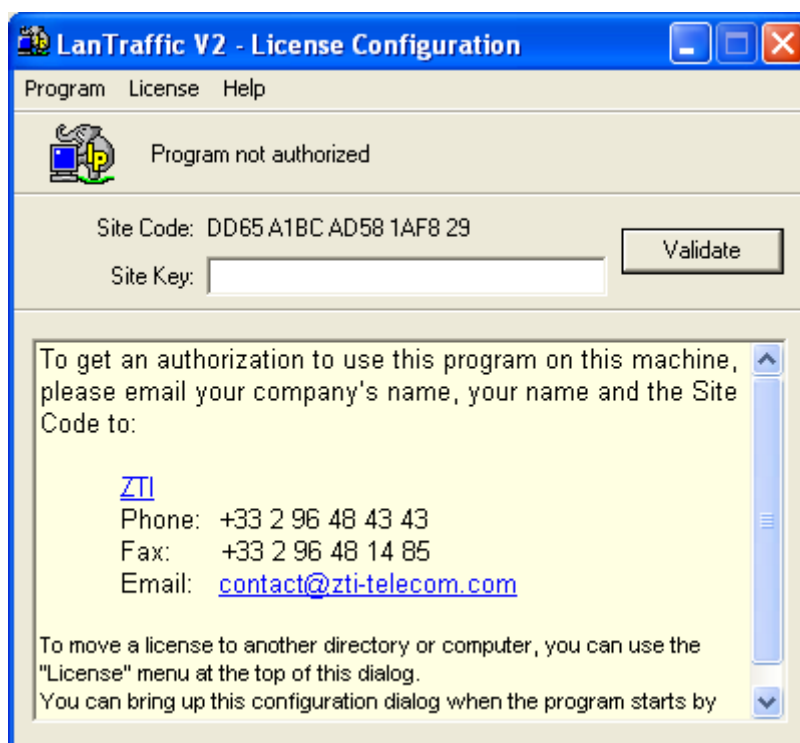
If you wish to configure your license before the trial period ends, press **Enter** just after launching the software when the following message is displayed:



You will then see the following license configuration window:



*At the end of the trial period when you launch **LanTraffic V2**, the same license configuration window appears, but says "Program not authorized" instead of showing the remaining days of use.*



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

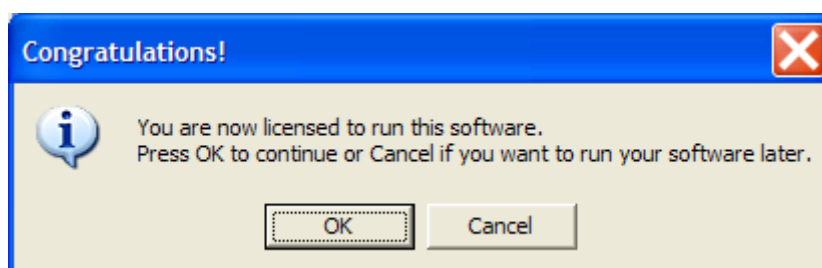
- The **Site Code** (you can copy and paste the Site Code displayed in the license window)
- The name of the software, for example: **LanTraffic V2** or **LanTraffic V2** bundle (including the Automation Tool for LanTraffic V2)
- The OS used
- Your company's name
- Your name and phone number
- The purchase order number and date of purchase

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

After you have received the email with the **Site Key**, open the license configuration window again by pressing the Enter key as explained before.

Copy the Site Key in and then click "Validate".

After validation of the Site Key, you will get the following message:



- ⇒ **Important:** one **Site Code** is associated with one **Site Key**, and only one. A **Site Code** is unique for each PC installed. For security reasons, as soon as you validate a **Site Key** (trial or unlimited), the license program generates a new **Site Code** automatically.
- ⇒ For any question or further information, please contact our technical support:
Email: support@zti-telecom.com or support@zti.fr
Phone: +33 2 96 48 43 43
Fax : +33 2 96 48 14 85



When you launch **LanTraffic V2** with an unlimited license, you will see the following window:



4.2 License Transfers



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

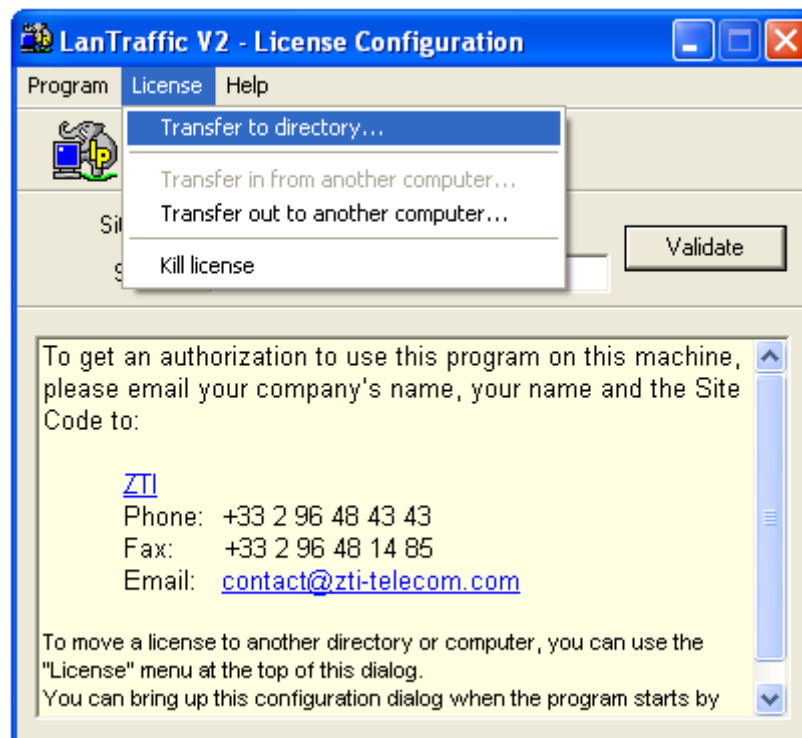
Licenses can be transferred using one of the following methods:

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

4.2.1 **Direct Transfer:** move the license from one local directory to another

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

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



- Provide the path name of the target program (*for example* C:\Program Files\LanTrafficV2\LanTrafficV2.exe).
The license is now transferred to the new directory.

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



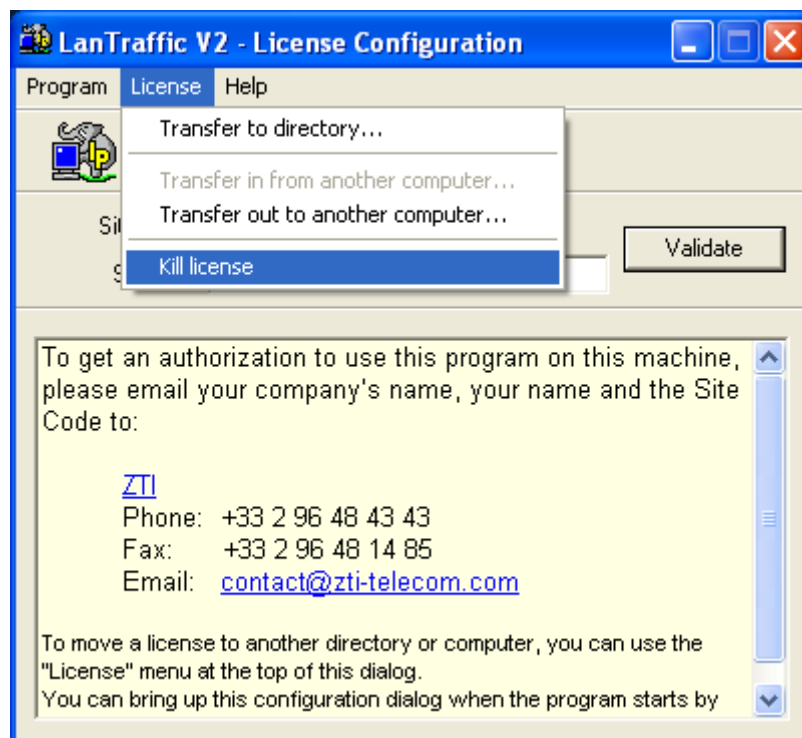
A floppy disk or USB key is needed for this kind of transfer.

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

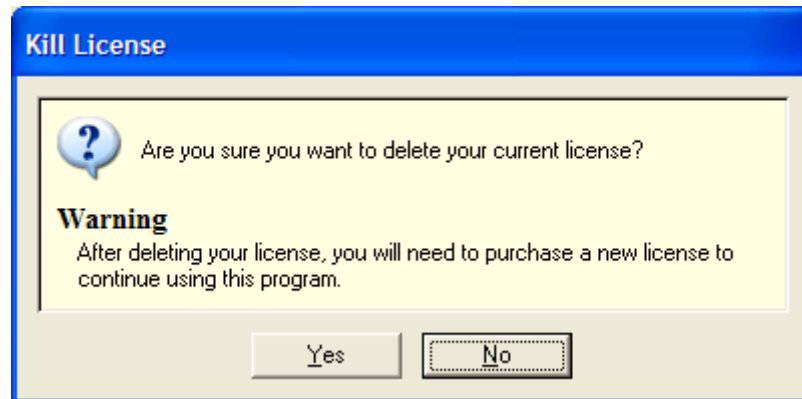
- 1) First install the program on the target PC (PC # 2).
- 2) Run the software on PC # 2 and delete the trial license in order to get an unauthorized license on this PC.
If the "Transfer in from another computer ..." item of the license menu is disabled, you must kill the license.

How to kill a license?

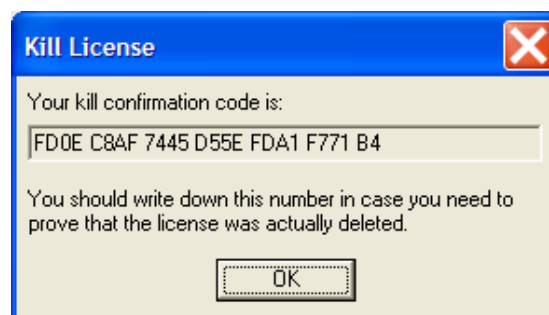
When the license configuration window appears, press **Enter** and select "License > Kill license" in the license menu.



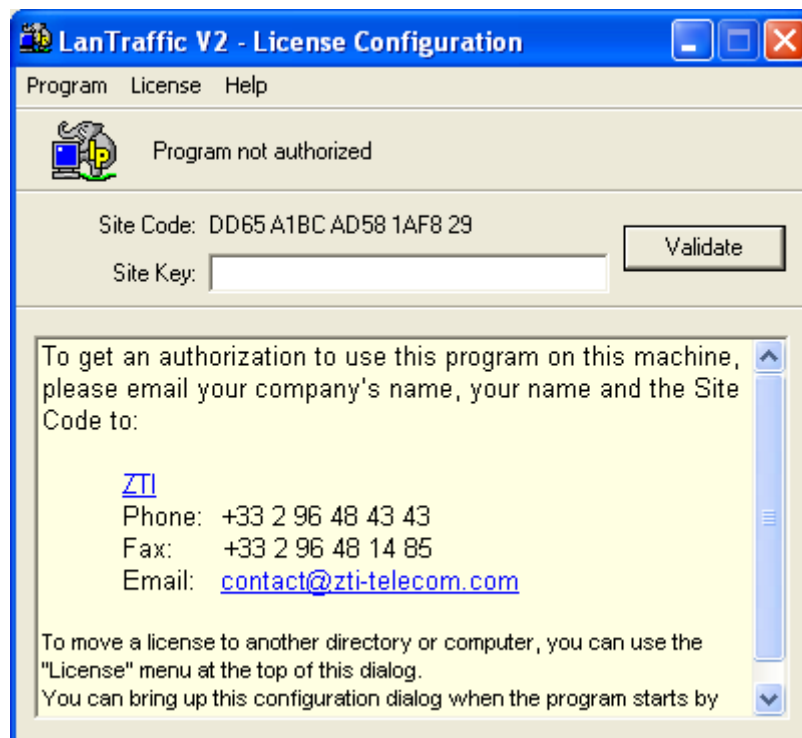
A message box will appear:



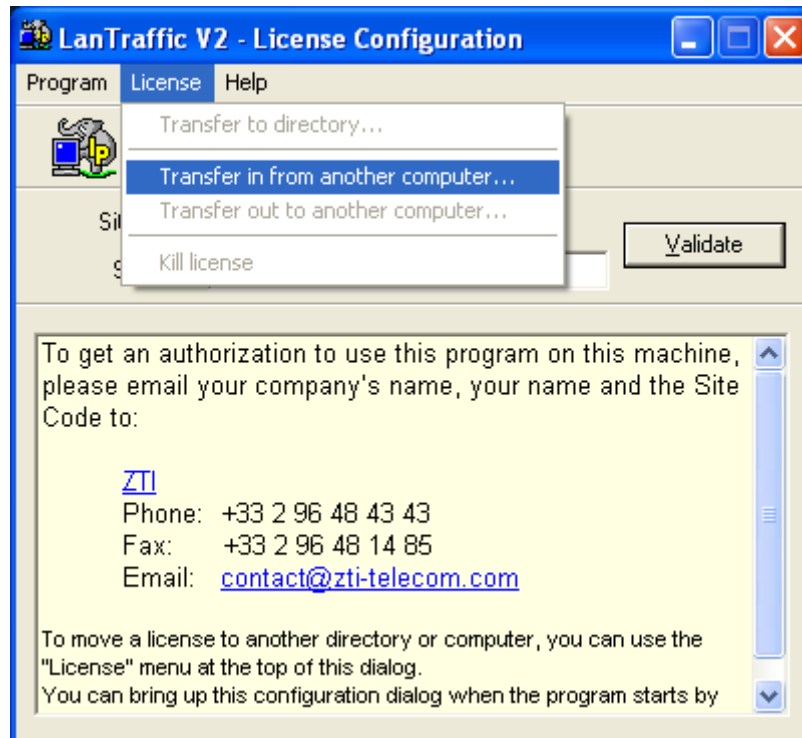
Press 'Yes' to kill the license and a confirmation code is displayed:



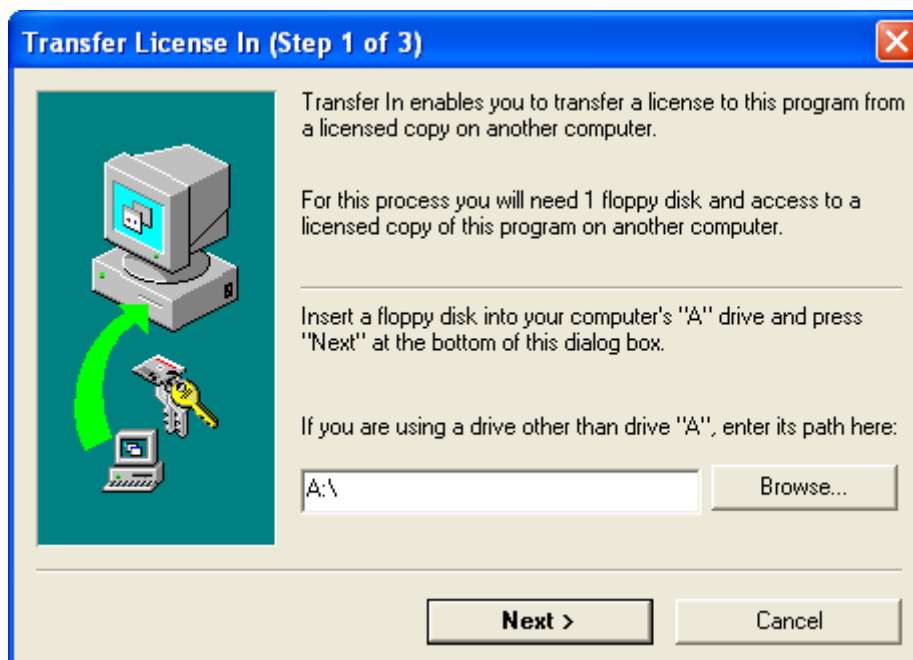
Click 'OK' and the license window displays now "Program not authorized":



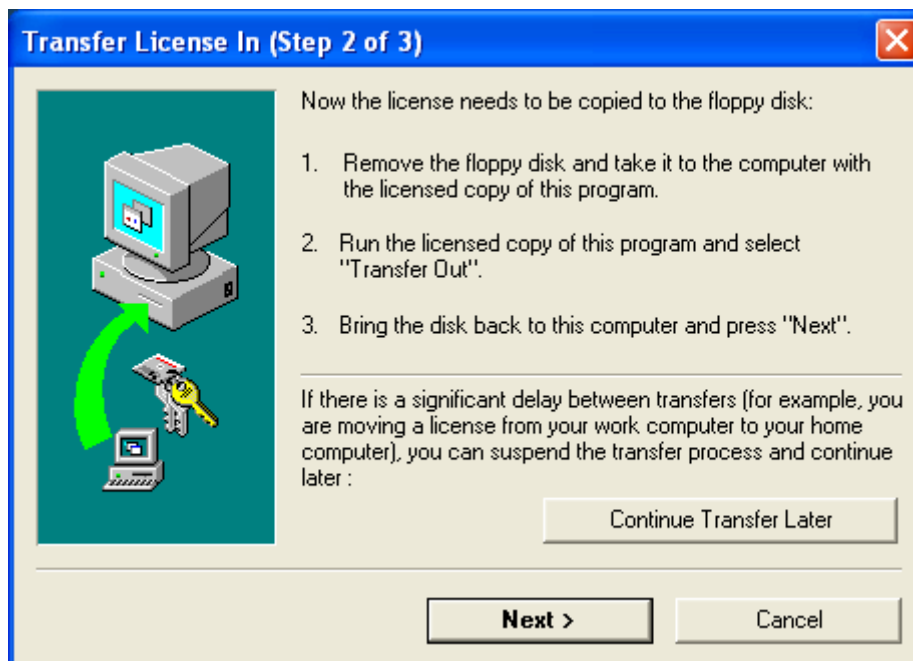
3) Select "License > Transfer in from another computer ..." from the license menu:



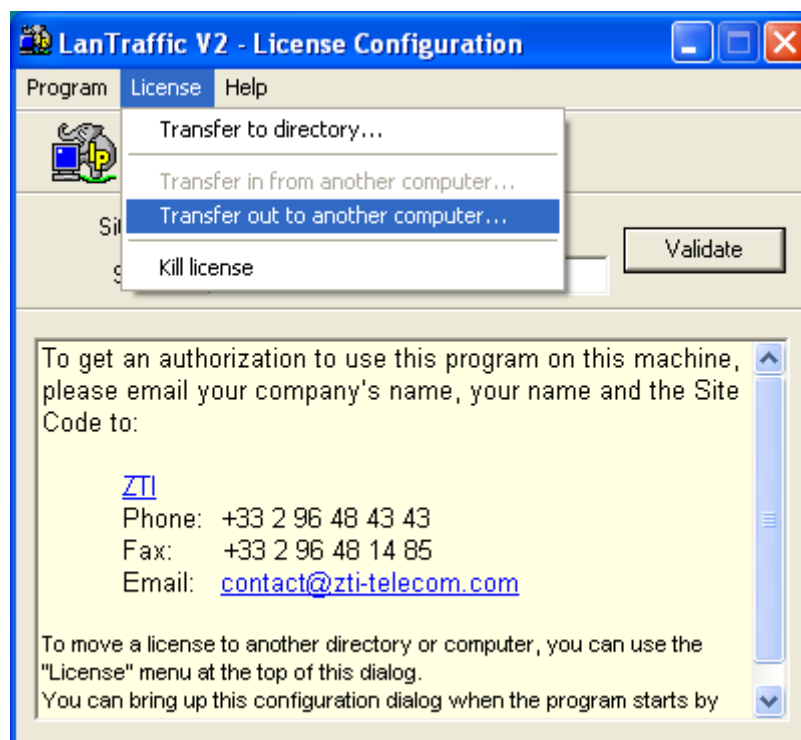
The "Transfer License In (Step 1 of 3)" window is displayed:



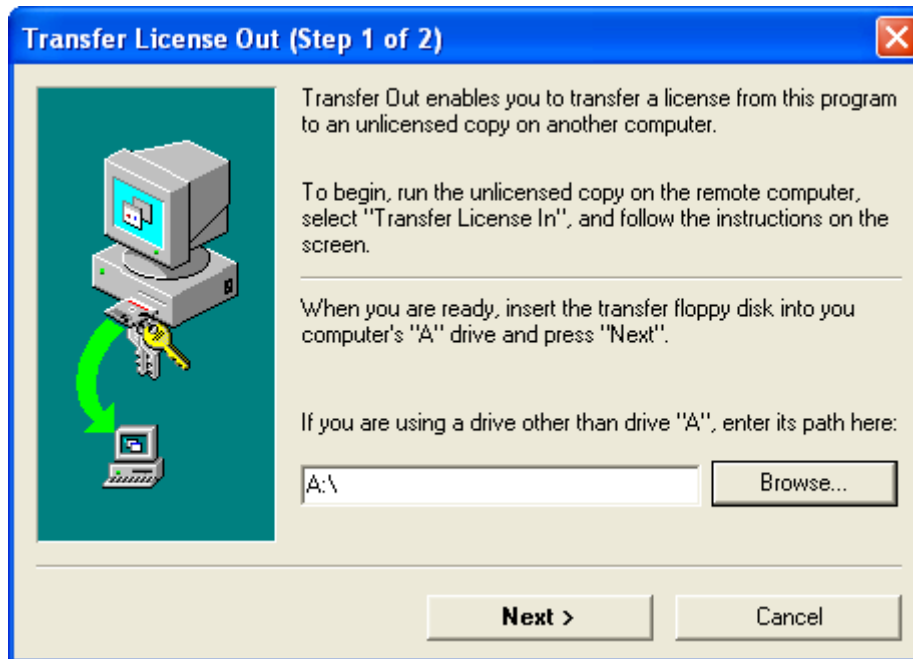
4) Insert a floppy disk or use a USB key as requested in step 1 of 3 and specify the path. Then press "Next >": the "Transfer License In (Step 2 of 3)" window is displayed:



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

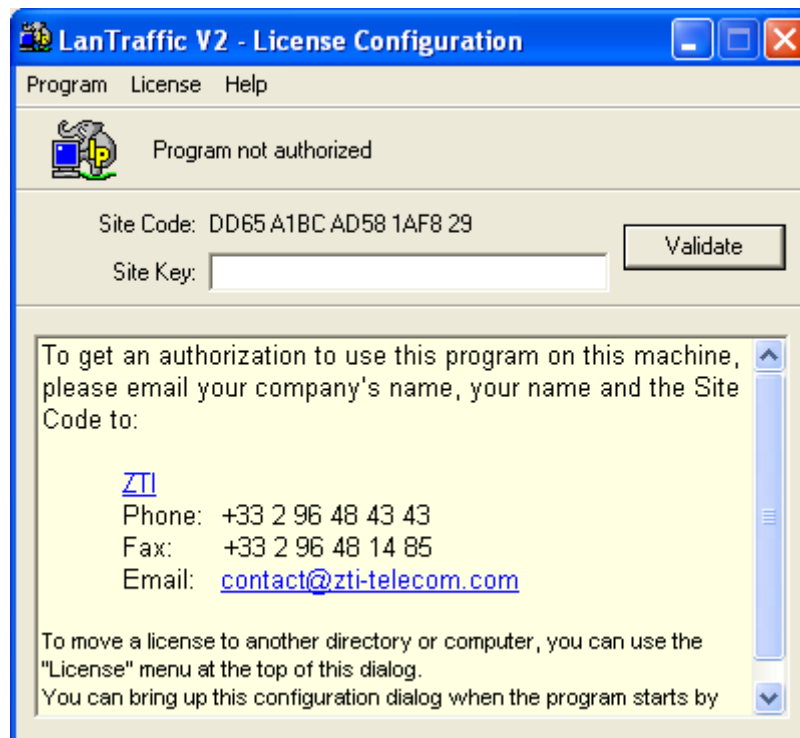


The following window is displayed:



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

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



You can check that the license is not available anymore on the source PC since LanTraffic V2 license is on a workstation basis.

Contact us to get information on site license (contact@zti.fr or contact@zti-telecom.com).

6) Remove the media from PC #1 and return to PC #2.

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

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



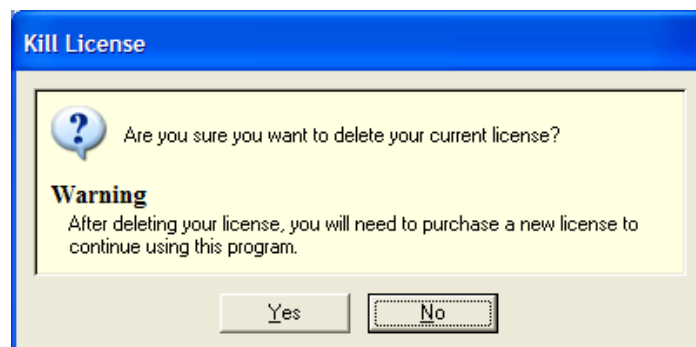
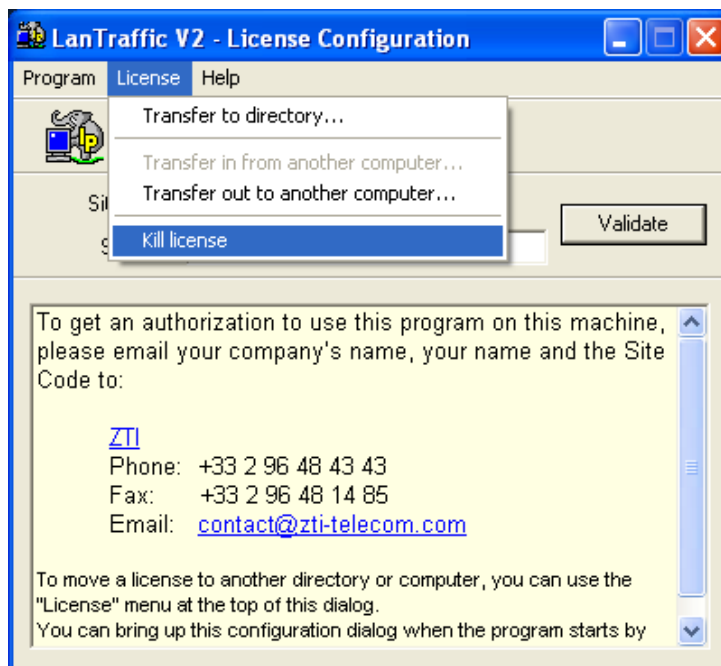
Click Finish to continue.

4.3 How to kill a license

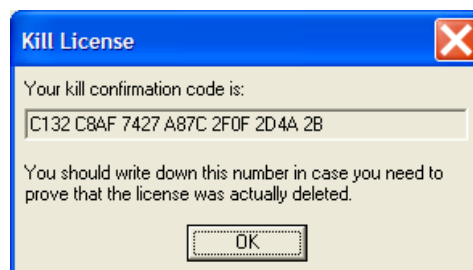
If you would like to transfer an unlimited license key onto a PC where a trial period is still active, you should first delete the active trial period. If you don't delete the active trial period, you will not be able to transfer an unlimited license.

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

- From the license configuration window, select "License > Kill License" in the license menu as shown below:



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



PART 5 Uninstall LanTraffic V2

The uninstall procedure is a standard uninstall program.

To uninstall **LanTraffic V2** select “Uninstall LanTraffic V2” in the “Start > Programs > LanTraffic V2” menu.

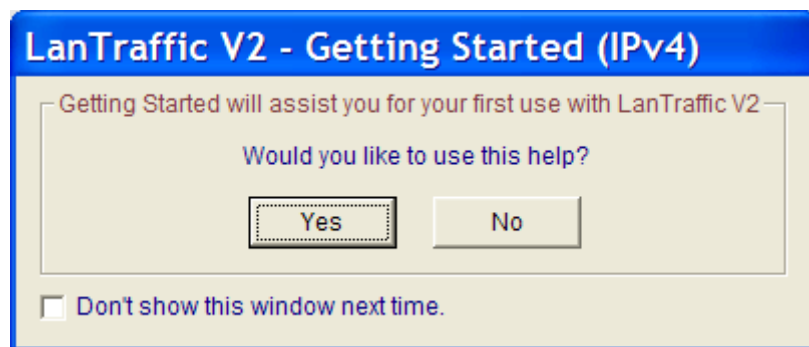
PART 6 LanTraffic V2 Getting Started



Anti-virus or firewall applications may disrupt **LanTraffic V2** when sending or receiving data.
Please set up your security software before using **LanTraffic V2** (see PART 7 and PART 8).

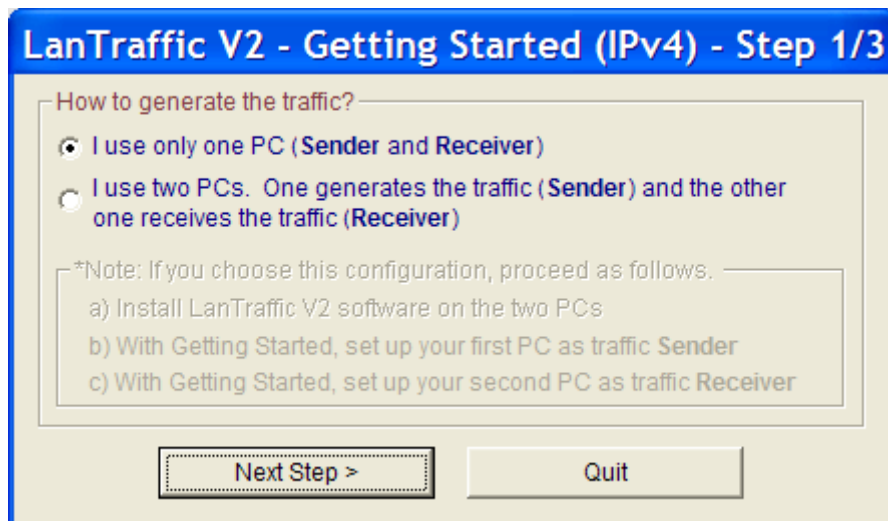
New users can use this help as an introduction to **LanTraffic V2** and generate or receive traffic with the IPv4 protocol in a few clicks.

Just after launching **LanTraffic V2**, the Getting Started Window is displayed:

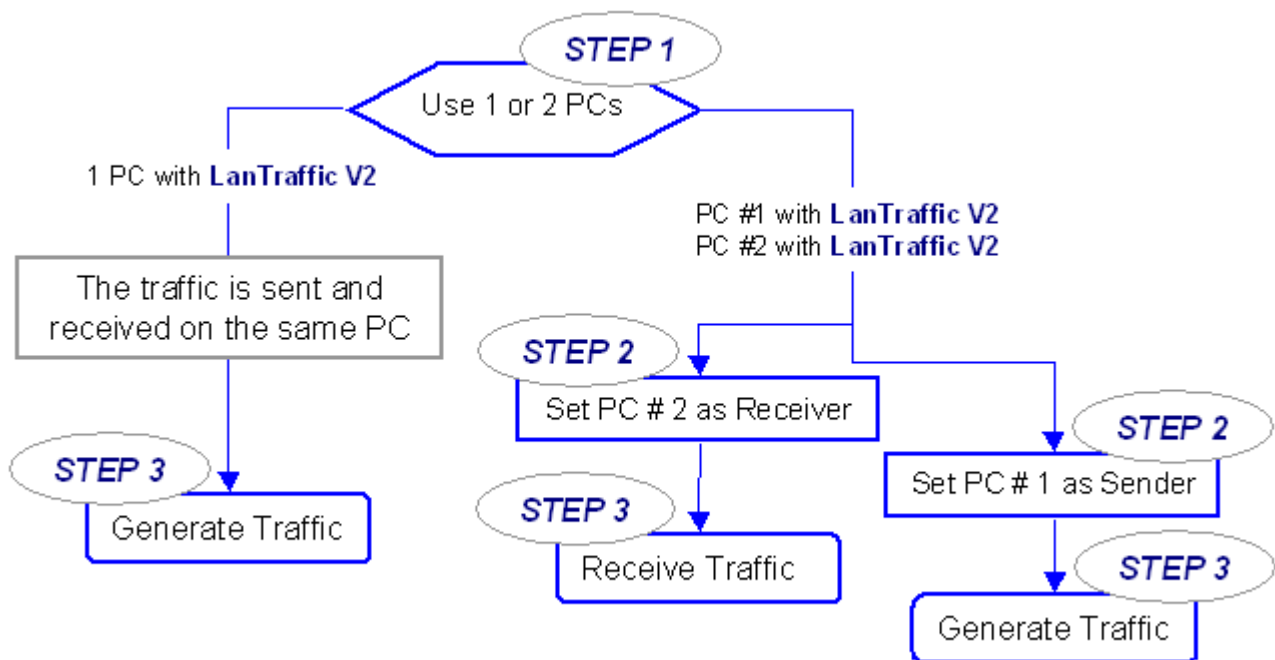


Press **No** if you don't want to use this help.

Press **Yes**, the next window will ask you if you want to use 1 or 2 PCs:

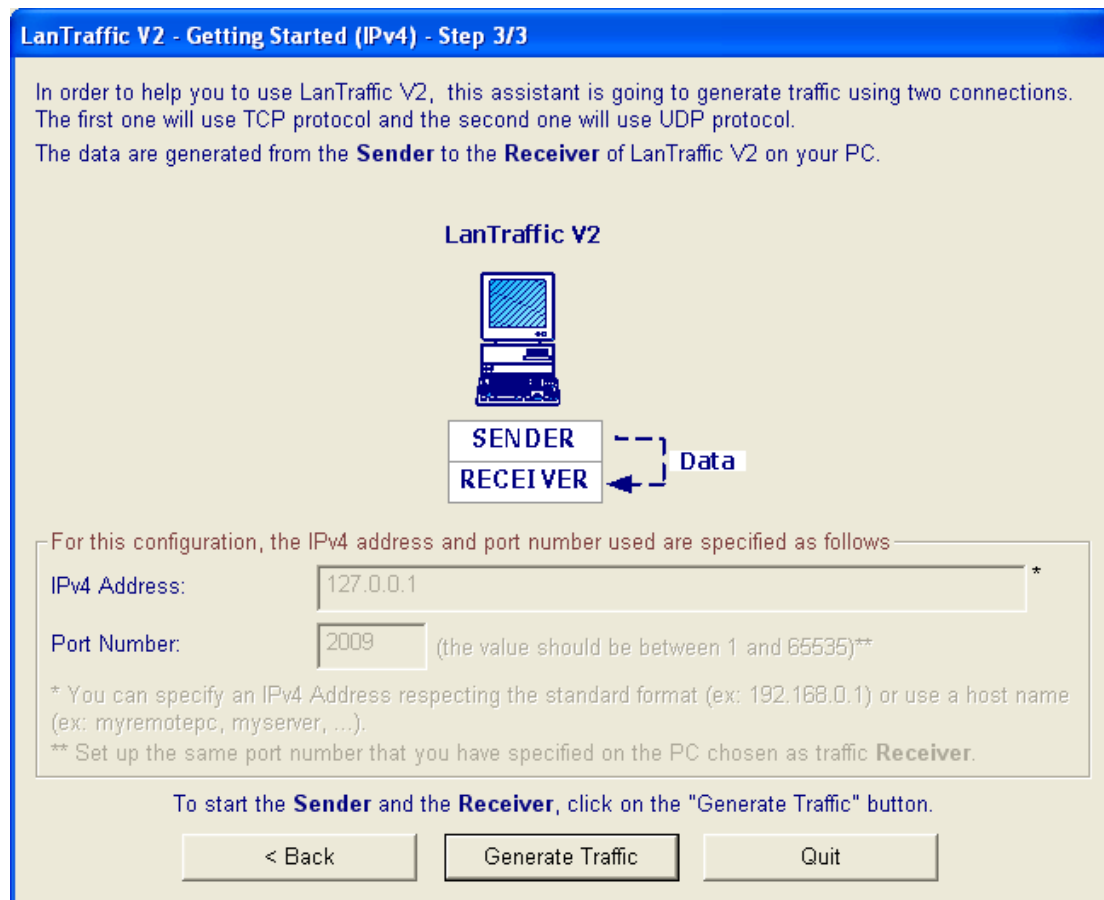


Depending on your choice to use 1 or 2 PCs, the plan below shows the steps:

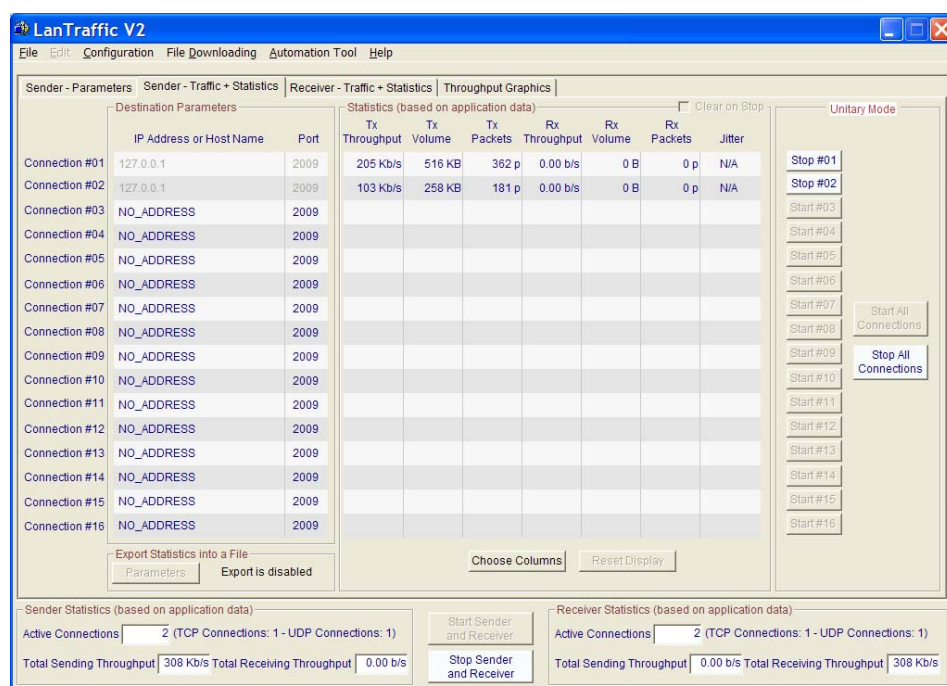


For the use of 1 PC

The following windows are displayed.

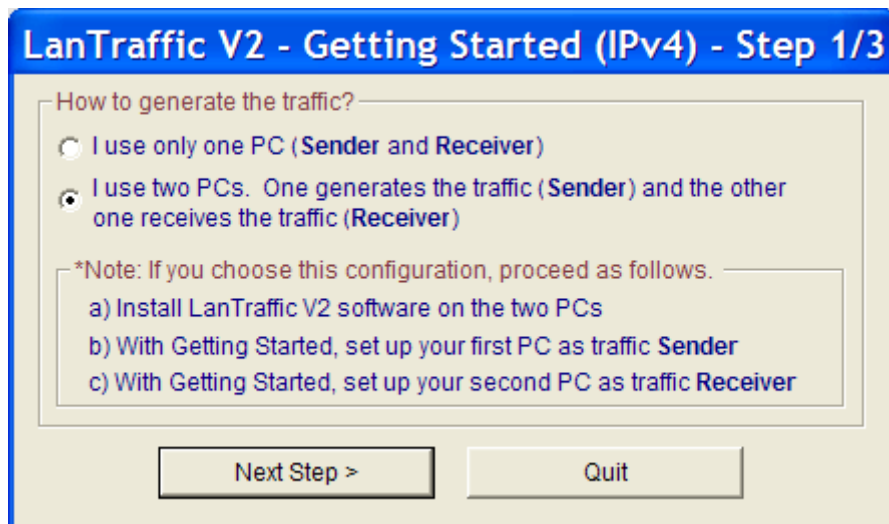


Then press the "Generate traffic" button to continue. The "Sender – Traffic + Statistics" tab of LanTraffic V2 will display the two first active connections as shown on the following window:

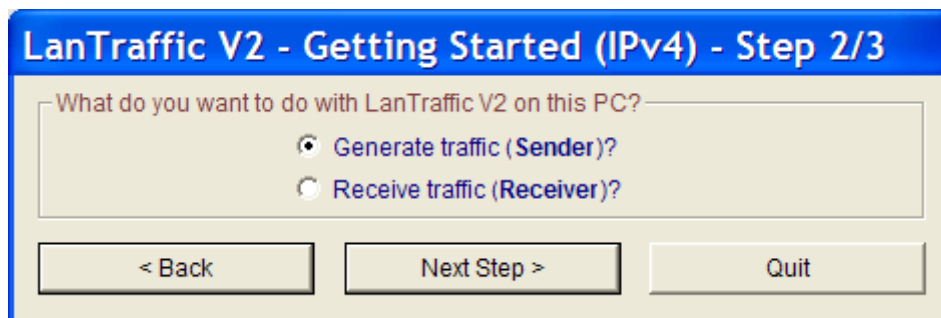


For the use of 2 PCs

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



Press "Next Step >" to continue.

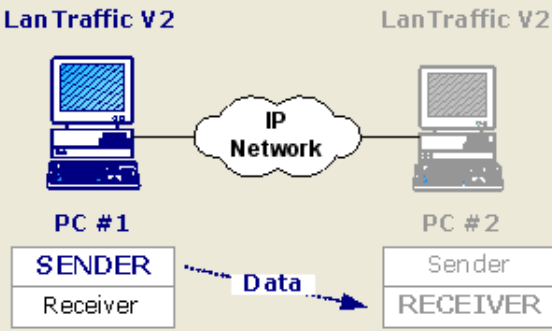


Then choose if you want to generate or receive the traffic on this PC.

If you select "Generate traffic" the following window will appear:

LanTraffic V2 - Getting Started (IPv4) - Step 3/3

In order to help you to use LanTraffic V2, this assistant is going to generate traffic using two connections. The first one will use TCP protocol and the second one will use UDP protocol. The data are generated by the **Sender** of the LanTraffic V2 based on the PC #1 and are received by the **Receiver** of the LanTraffic V2 based on the PC #2.



For this configuration, you should set up the IPv4 destination address and port number to the PC #2

IPv4 Destination Address: *

Port Number: (the value should be between 1 and 65535)**

* You can specify an IPv4 Address respecting the standard format (ex: 192.168.0.1) or use a host name (ex: myremotepc, myserver, ...).

** Set up the same port number that you have specified on the PC chosen as traffic **Receiver**.

To start the **Sender**, click on the "Generate Traffic" button.

< Back Generate Traffic Quit

Define the IPv4 address and port number to use.

Then press the "Generate traffic" button and a warning dialog is displayed:

LanTraffic V2 - Getting Started (IPv4)

Did you set up and start the LanTraffic V2 Receiver on PC #2?

Yes No

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

LanTraffic V2 - Getting Started (IPv4) - Step 2/3

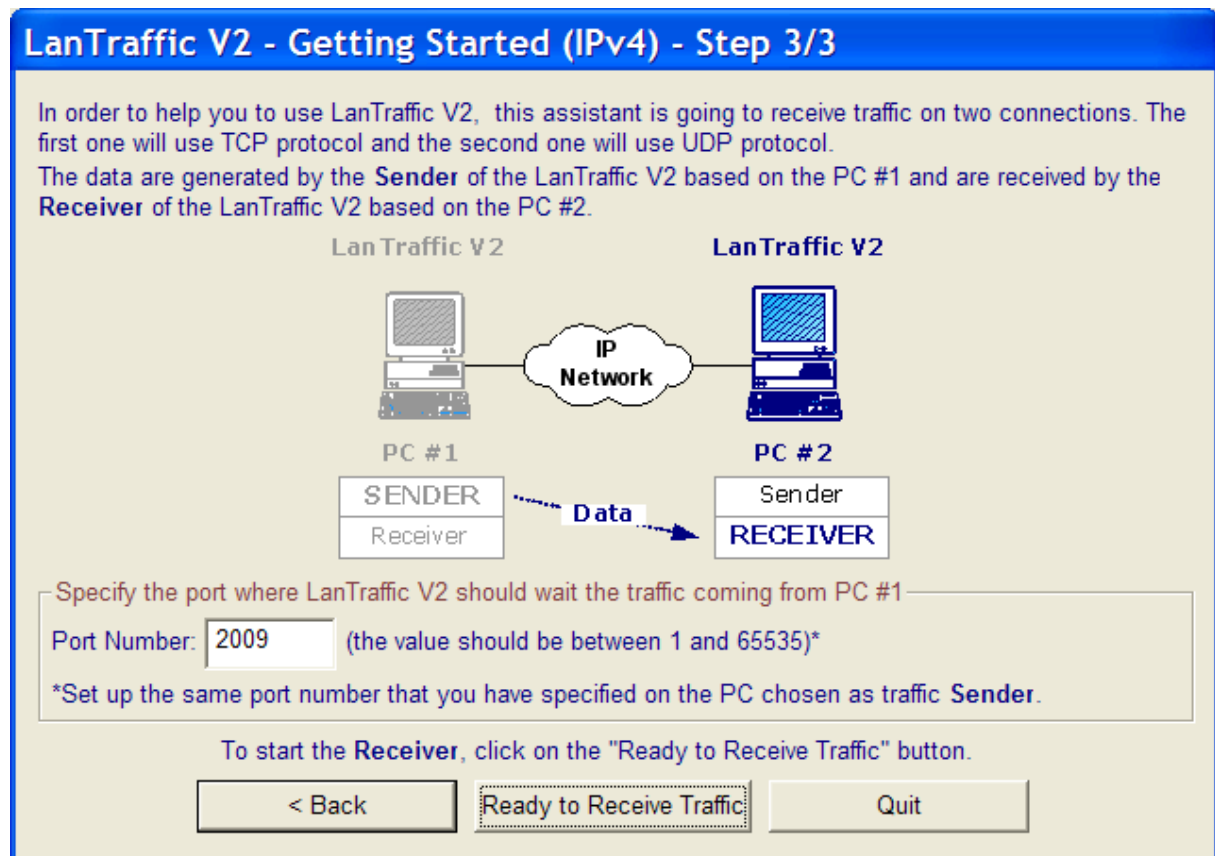
What do you want to do with LanTraffic V2 on this PC?

☐ Generate traffic (Sender)?

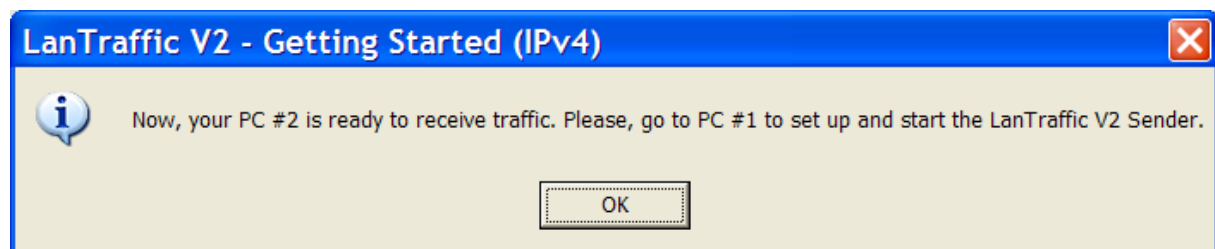
☒ Receive traffic (Receiver)?

< Back Next Step > Quit

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



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



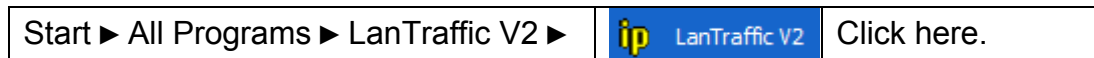
Press "OK" and the "Receiver – Traffic + Statistics" tab of **LanTraffic V2** is displayed on PC # 2.

Then go to PC # 1 and start the **LanTraffic V2** Sender. The "Sender – Traffic + Statistics" tab of **LanTraffic V2** displays now the two first active connections.

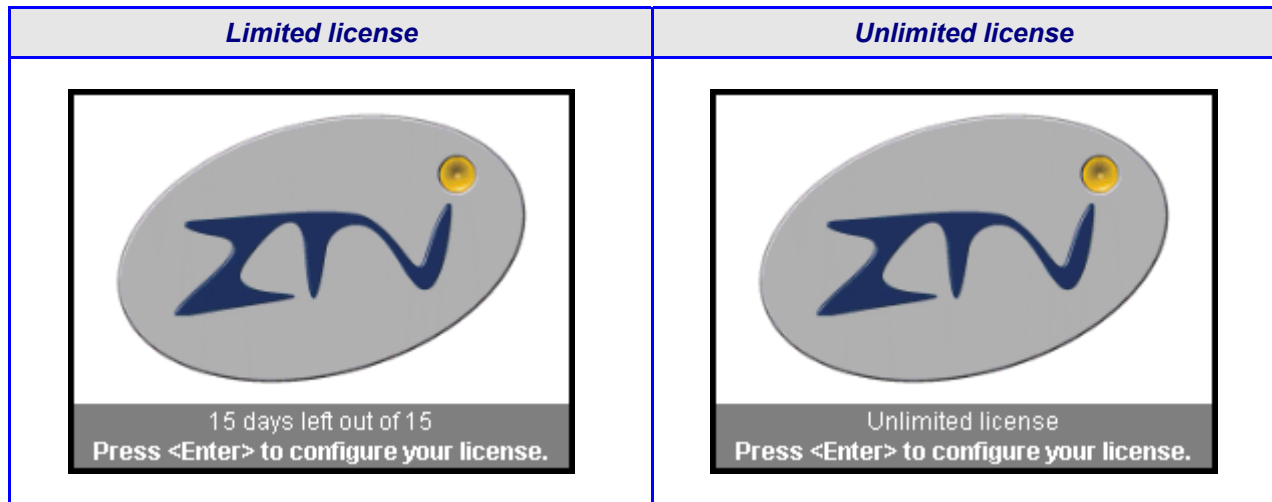
You have now 2 connections generating traffic from PC #1 to PC # 2.

PART 7 Run LanTraffic V2

Use the Windows start menu:



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



Press **Enter** only if you need to configure your license,
If you don't, allow a few seconds for the main window of **LanTraffic V2** to open.

With Windows XP Service Pack 2, the window below may appear.
This window allows configuring the Windows Firewall settings for **LanTraffic V2**.
Click on the “Unblock” button to add **LanTraffic V2** into the authorized programs list.



PART 8 LanTraffic V2 / Windows Firewall



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

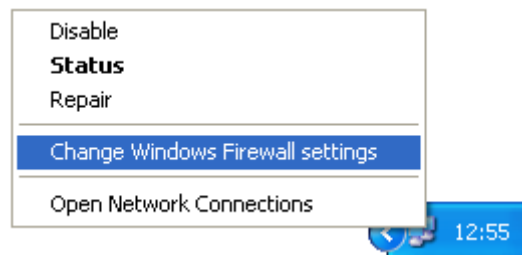
Some anti-virus configurations can stop **LanTraffic V2** working because of their security settings.

For commercial anti-virus, please refer to the related documentation to authorize **LanTraffic V2**.

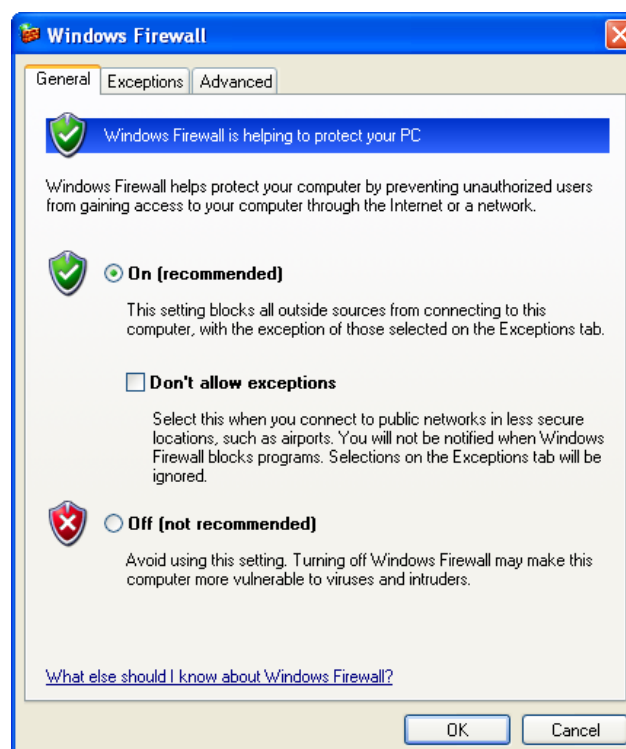
8.1 Configuration for UDP, TCP connections and ICMP IPv4

See below how to configure the Windows Firewall included in Windows XP Service Pack 2 to use UDP & TCP connections for IPV4 and IPv6, and the ICMP (IPv4) connections. ICMP with IPv6 requires a specific configuration (see paragraph 8.2).

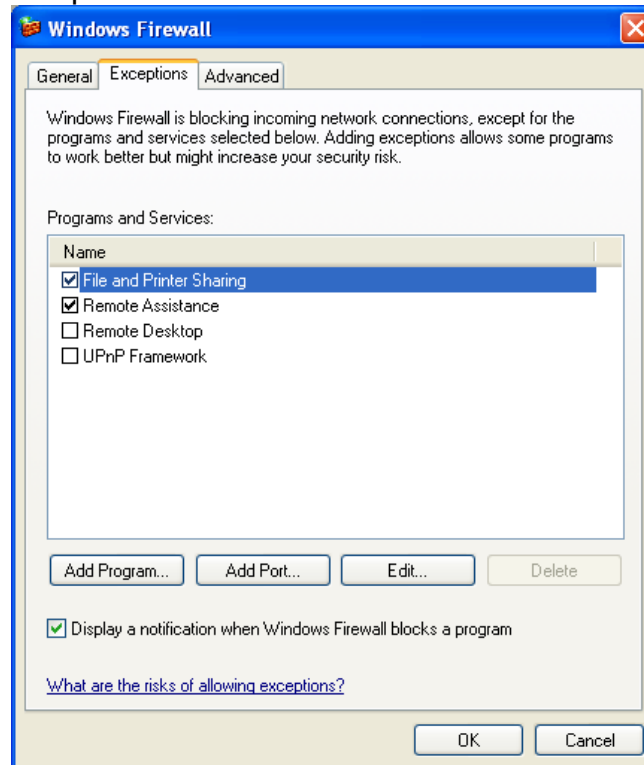
1. Open the Windows Firewall settings window by right clicking on the two computers representing the network interface that **LanTraffic V2** will use.



2. The window below appears. If the Firewall is off, there is no need to change the settings. If the Firewall is active, proceed as described below:

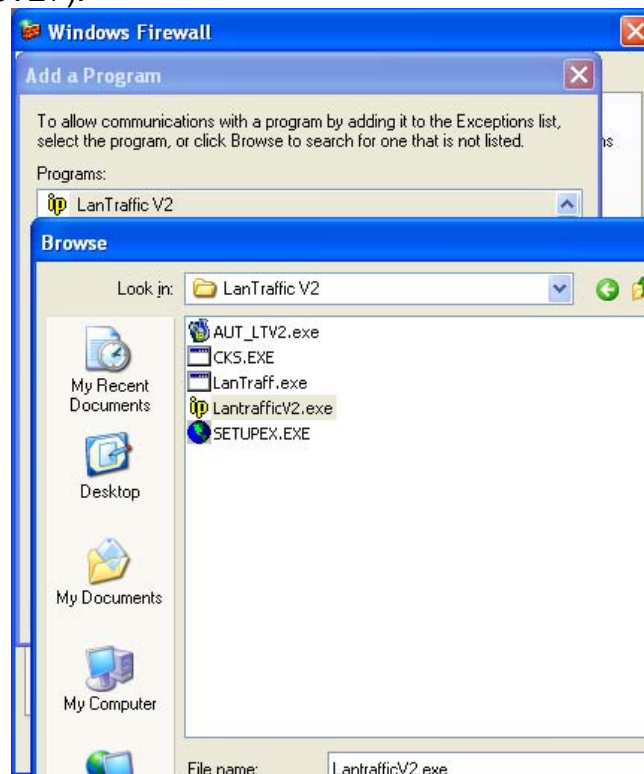


3. Switch on the “Exceptions” tab.

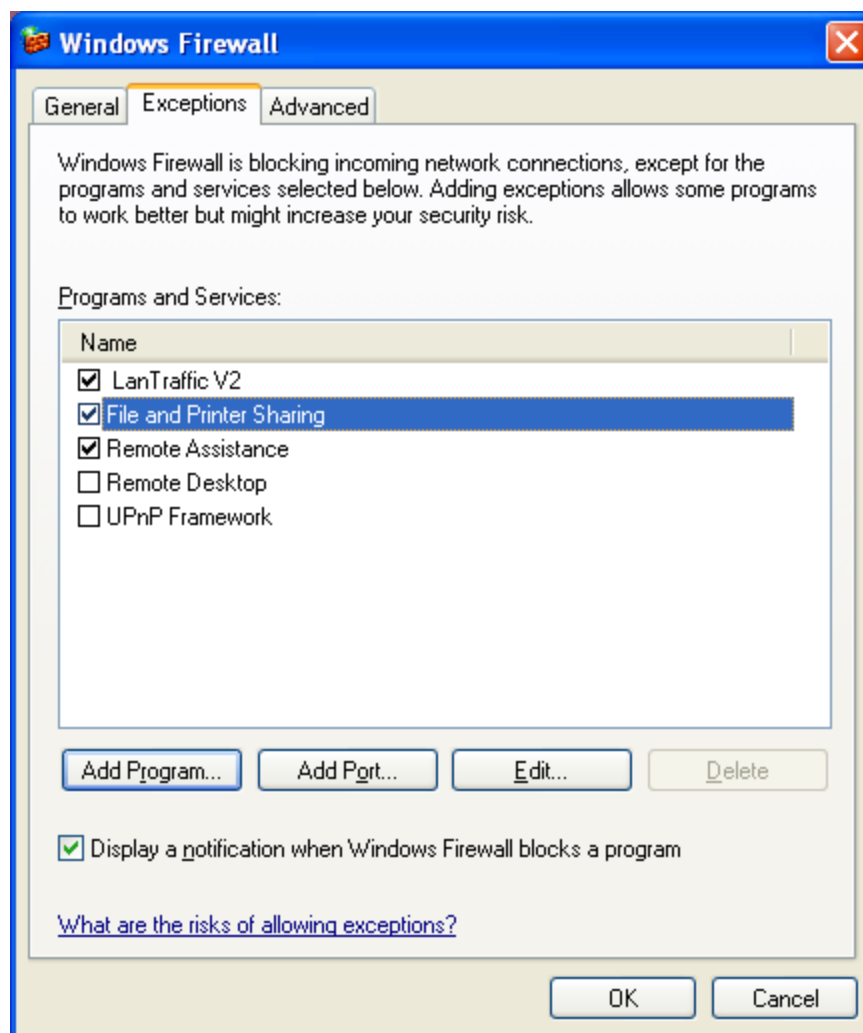


If **LanTraffic V2** is already in the list, just select it by checking the box and press “OK”.

If **LanTraffic V2** is not in the list, click on the “Add Program ...” button. Then click on the “Browse” button and add it by selecting the LanTrafficV2.exe file placed in the installation directory (default settings: “[Drive]:\Program Files\LanTrafficV2”).



4. Then select **LanTraffic V2** into the program list and press “OK”.



Now **LanTraffic V2** is allowed to use ports, to generate and to receive **TCP and UDP** IPv4 and IPv6 traffic, including ICMP (IPv4). Click “OK” to save the new settings.

8.2 Configuration for ICMP IPv6 connections

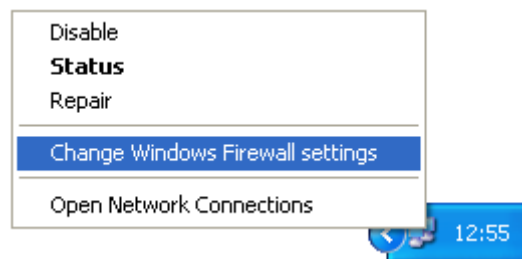


The use of the ICMP IP V6 connection requires disabling the Windows Firewall before using LanTraffic V2.

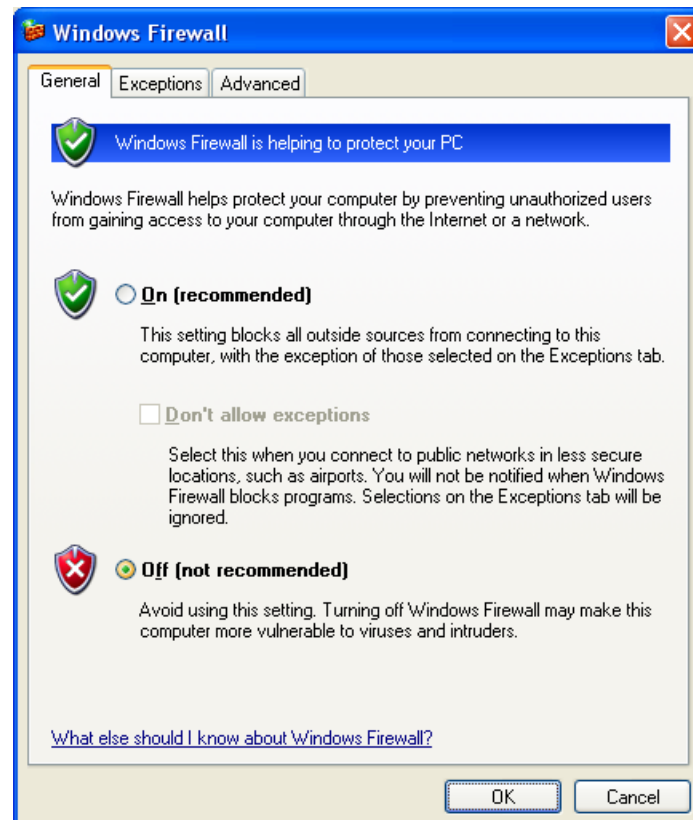
By disabling the Windows Firewall, you enable the TCP, UDP and ICMP (IPv4) connections as described in the paragraph 8.1.

See below how to disable the Windows Firewall included in Windows XP Service Pack 2 to use ICMP IPv6 connections, as well as TCP, UDP and ICMP (IPv4) connections.

1. Open the Windows Firewall settings window by right clicking on the two computers representing the network interface that **LanTraffic V2** will use.



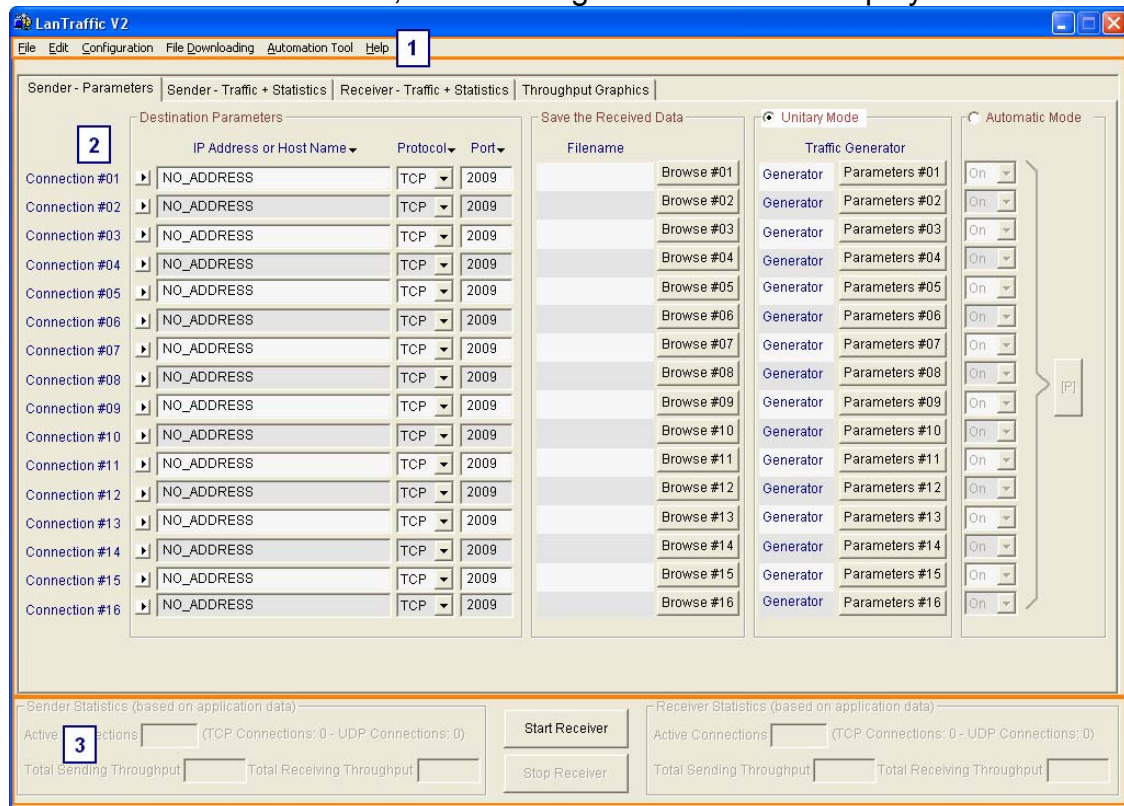
2. The window below appears. If the Firewall is off, there is no need to change the settings. If the Firewall is active, select the **Off** option as shown. Then click OK.



PART 9 Graphical User Interface

9.1 Main Window

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



LanTraffic V2 main window

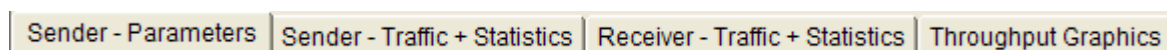
The **LanTraffic V2** main window is made of three areas:

- ⇒ **Area 1: Menu bar**
- ⇒ **Area 2:** this main area displays the **four tabs** of **LanTraffic V2**.
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 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.

9.2 Display general rules of the Graphical User Interface

LanTraffic V2 fields can be filled following four situations:

- Fields in which you can enter values

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

- Statistics fields

Statistics fields are automatically filled. They are identifiable by blue writing on white background color. 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** further to use enter or parameters selection. They are displayed as reminder and will be modified by another user action.

These fields are recognizable by black writing on gray background.

- Fields turned out of reach further to user action

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

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

- As soon as a connection is running, it is impossible to change its parameters. You must stop the connection in order to change the 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.

9.3 Used units for the information display

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

9.3.1 Volume units

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

9.3.2 Throughput units

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



Throughput computing

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

The displayed throughput is an “application” throughput.

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



Unit changing

To change, a volume value in KB to a volume value in MB, **LanTraffic V2** divides the first value per 1024. Ex: 1000 KB = 0.98 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** divides the first value per 1024. Ex: 2048 Kb/s = 2.00 Mb/s.

PART 10 Using LanTraffic V2

10.1 Main steps

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

⇒ **To send data:**

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

10.2 Menu description

The menu bar is made of 6 items:

File Edit Configuration File Downloading Automation Tool Help

The options for each item are described in this chapter.

10.2.1 File menu



10.2.1.1 File/New

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

10.2.1.2 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 or 2.3 is silently read by **LanTraffic V2** version 2.4. 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.

10.2.1.3 File/Save

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



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

10.2.1.4 File/Save as ...

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

The context file saved by the **LanTraffic V2** version 2.4 can't be read by versions 2.3 and older.

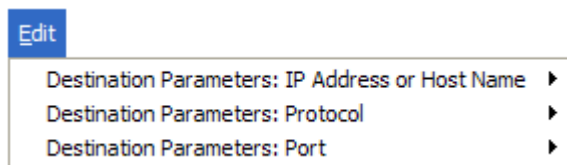
10.2.1.5 File/Recent Contexts ...

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

10.2.1.6 File/Exit

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

10.2.2 Edit menu



10.2.2.1 Edit/Destination Parameters: IP Address or Host Name

1 option is available:

Copy the IP Address from Connection #01 to all Connections

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

10.2.2.2 Edit/Destination Parameters: Protocol

2 options are available:

Select TCP for all Connections
Select UDP for all Connections

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

10.2.2.3 Edit/Destination Parameters: Port

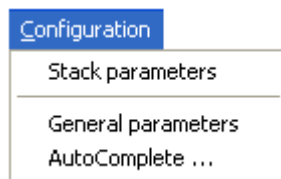
4 options are available:

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

With this menu, you can:

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

10.2.3 Configuration menu

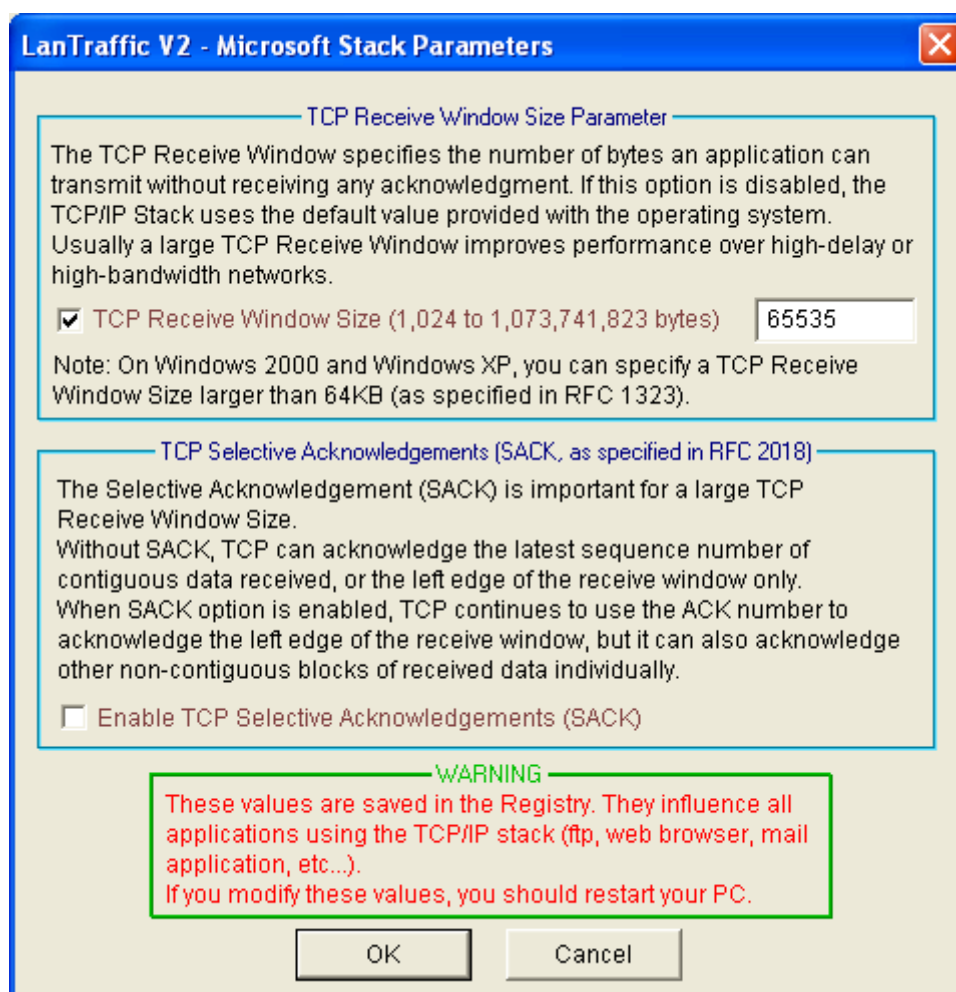


10.2.3.1 Configuration/Stack Parameters

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

LanTraffic V2 enables modifying the TCP Receive Window size and 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 are saved in the Registry and influence all applications using the TCP/IP stack

Paths to these parameters in the Registry depend on the operating system:

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

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



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

10.2.3.2 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**.

When selected, the following window is displayed:

LanTraffic V2 - General Parameters

Refresh Time and Throughput Sampling Period

The refresh time parameter defines the frequency of statistics updates on LanTraffic V2. This parameter also applies to statistics exportation processes. The throughput sampling period defines the number of seconds of traffic needed to calculate the throughput.

Refresh Time (1 to 60 seconds)

Throughput Sampling Period (1 to 60 seconds)

TCP and UDP received Data Timeout

These parameters are for the Sender Part only. When there is no more data to be sent, LanTraffic V2 continues to receive data until the timeout expires. Then the connection is released. When the timeout is 0, the connection is stopped as soon as there is no more data to be sent.

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

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

LanTraffic V2 Buffer Size (SO_RCVBUF and SO_SNDBUF)

The buffers used by LanTraffic V2 to dialog with the Winsock API influence the throughput performance for high speed network. The best performance can be reached with a high buffer size. Change in one of these sizes concerns the new connections only.

Receive Buffer Size (1,024 to 65,535 bytes)

Transmit Buffer Size (1,024 to 65,535 bytes)

General Parameters window

Parameters applying to the GUI display

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

Parameters applying to echoed connections

- **Timeout for TCP packets echoed (ms):** value entered in milliseconds. This field is used for echoed TCP connections. When the connection is stopping, **LanTraffic V2** continues TCP data acquisition during a time defined by this timeout. If this value equals zero, **LanTraffic V2** 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** continues UDP data acquisition during a time defined by this timeout. If this value equals zero, **LanTraffic V2** 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.

10.2.3.3 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** is available for IP address entries in the "Sender – Parameters" and "Receiver – Traffic + Statistics" tabs.

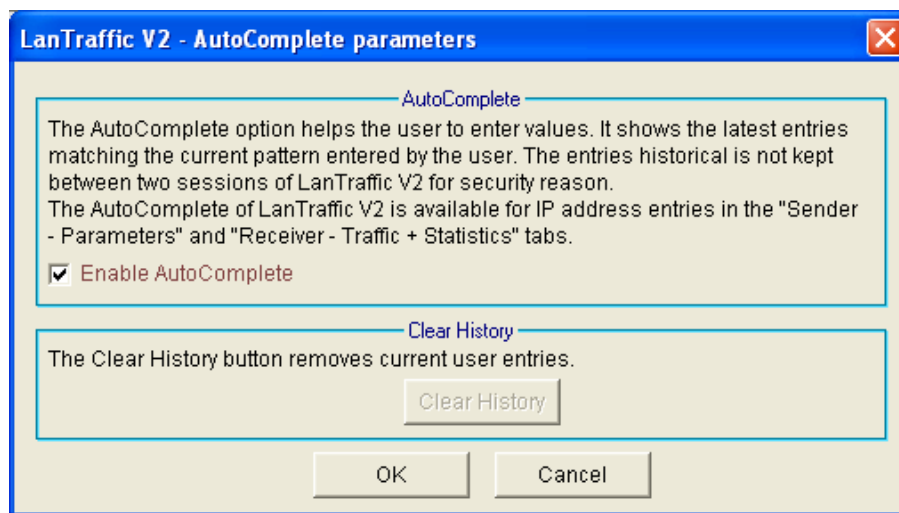


Example of AutoComplete entry in the "Sender – Parameters" tab.

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.

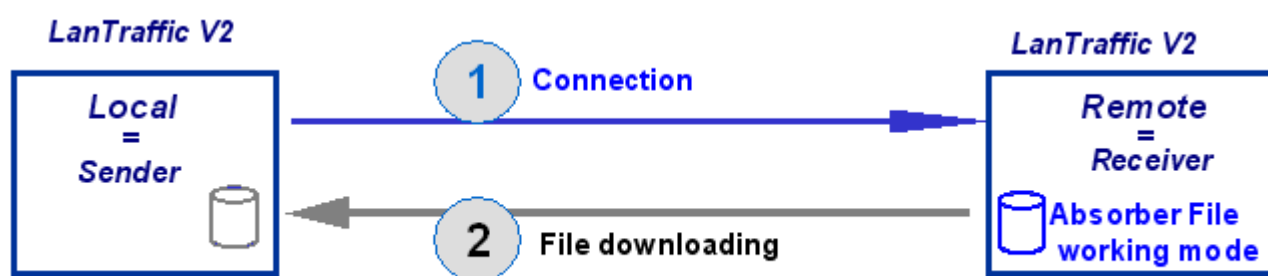
	<p><i>The historical record is associated to the "LanTraffic V2" session.</i></p> <p><i>For security reason, the historical record is not kept between sessions and is lost at the end of the LanTraffic V2 session.</i></p>
---	---

10.2.4 File Downloading menu

File Downloading

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

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



Example of File downloading in File absorber receiving working mode environment

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

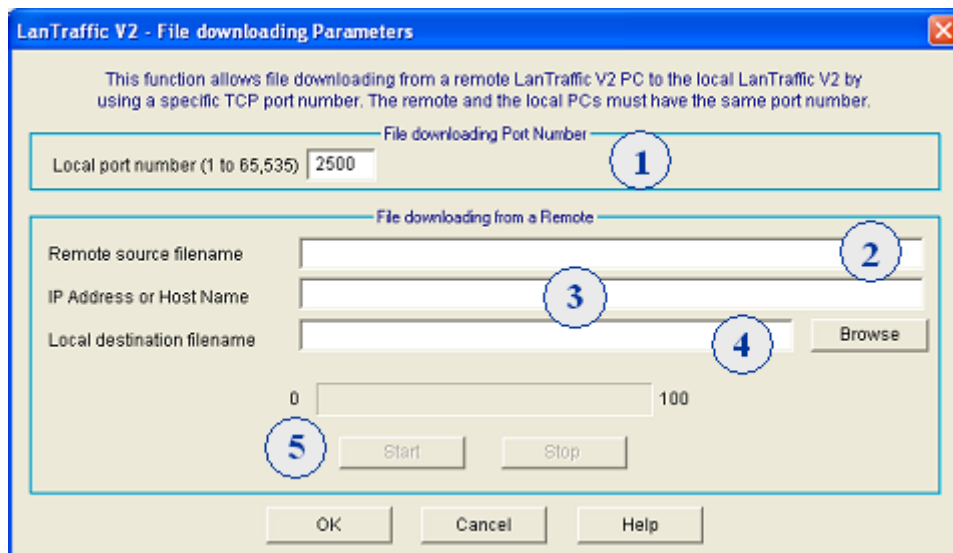
2: The user of the Local Sender machine can get the file back by using the File downloading function.

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.

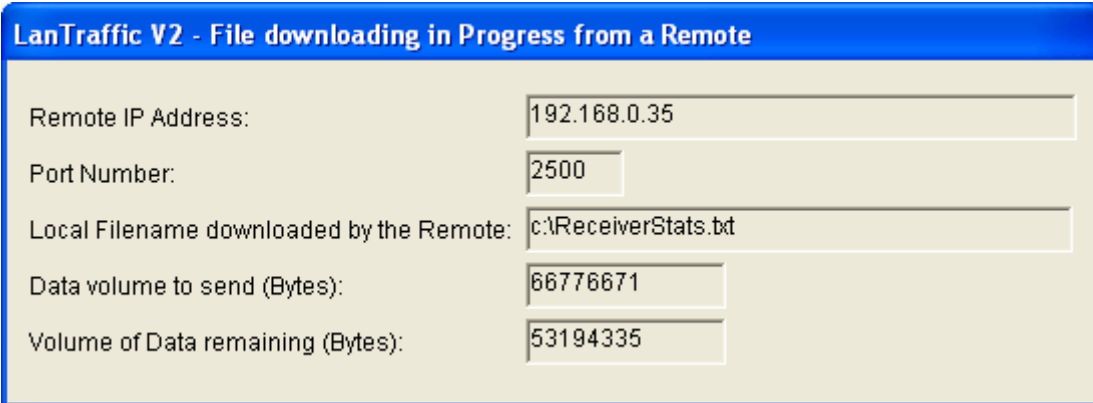


When “Start” button is on, it is impossible to press OK or to close the window. You should abort it by pressing the “Stop” button or wait for the end of file transfer operation.



*If you use a canonical name, the IP Address Translation mechanism (see § 10.4.1.1.3 IP Address translation mechanism) resolves it. In case of the resolution returns an IPv4 and an IPv6 addresses, **LanTraffic V2** selects the IPv4 address only.*

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



LanTraffic V2 - File downloading in Progress from a Remote	
Remote IP Address:	192.168.0.35
Port Number:	2500
Local Filename downloaded by the Remote:	c:\ReceiverStats.txt
Data volume to send (Bytes):	66776671
Volume of Data remaining (Bytes):	53194335

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.

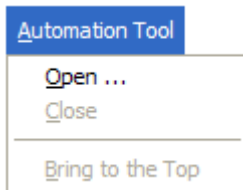


During a file transfer, you will not be allowed to close the application on the Remote machine.

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 an ACK is sent by the Local machine.
- When the Remote machine receives an ACK (or expiration of the Timeout), it disconnects.

10.2.5 Automation Tool menu

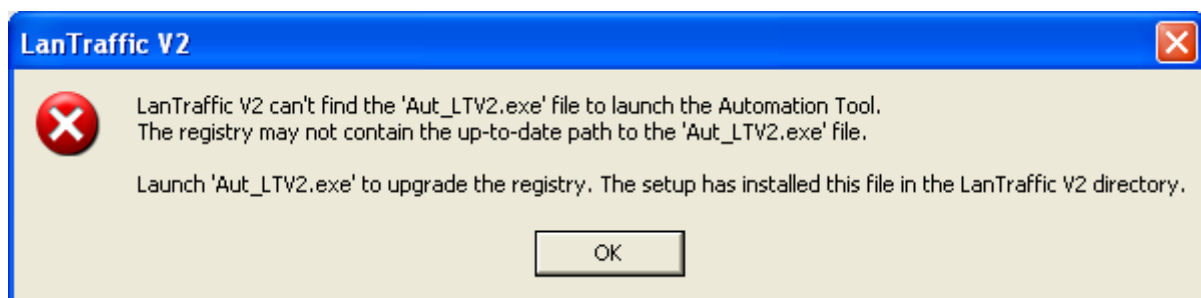


10.2.5.1 Automation Tool/Open...

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

The “Open...” command is grayed when the “Automation tool for LanTraffic V2” is already started because only one instance can be active.

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



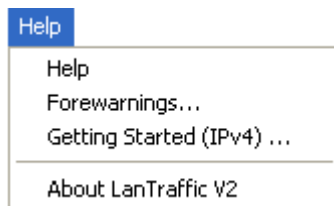
10.2.5.2 Automation Tool/Close

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

10.2.5.3 Automation Tool/Bring to the top

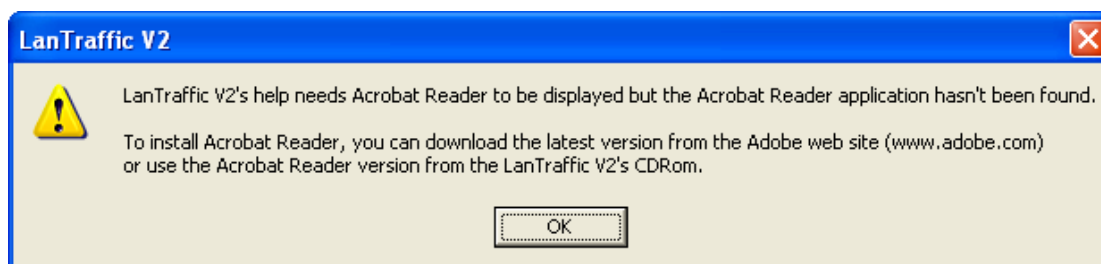
This command displays the **Automation tool for LanTraffic V2** window at the top of the other opened applications, except applications that can't be masked e.g. task manager when this option is selected.

10.2.6 Help menu



10.2.6.1 Help/Help

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



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

10.2.6.2 Help/Forewarnings ...

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

10.2.6.2.1 Inter packet delay

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

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

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

10.2.6.2.2 Echoer modes

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

10.2.6.2.3 UDP connections

When several UDP connections are running and according to the traffic level and to the system load, **LanTraffic V2** 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**, so the following situations may occur.

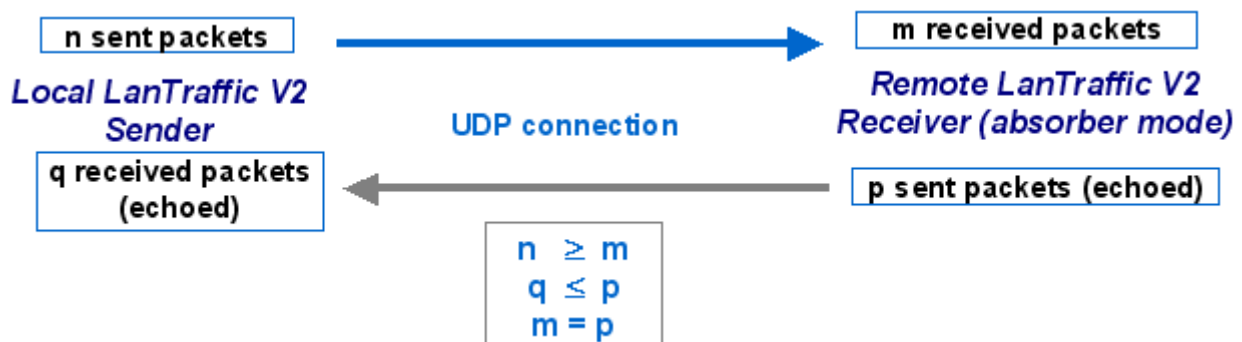
▪ Packets Loss

The Winsock2 interface doesn't transmit all received packets to the **LanTraffic V2** Receiver.

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



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



In this case, 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" menu or to tune the Microsoft TCP/IP stack.

10.2.6.3 Help/Getting Started (IPv4)

The “Getting Started (IPv4)” command displays the Getting Started procedure.

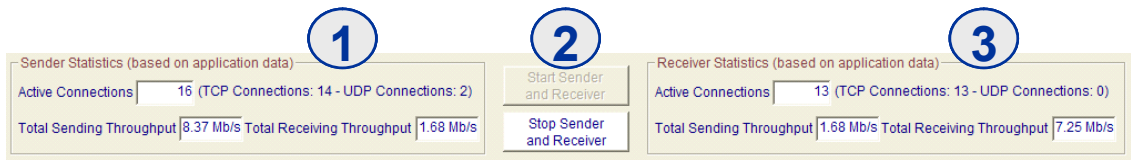
10.2.6.4 Help/About LanTrafficV2

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

10.3 Total statistics

Total statistics for the **Sender** ① and **Receiver** ③ are displayed in the lower part of the **LanTraffic V2** 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 10.2.3.2.



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:

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

10.3.1 Sender statistics

For the Sender tab, the following statistics are displayed:

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

10.3.2 Receiver statistics

For the Receiver tab, following statistics are displayed:

- **Active connections:** Number of current running connections on the Local Receiver part. More details are displayed: number of TCP Receiver connections and number of UDP Receiver connections.
- **Total Sending Throughput:** Instant throughput of all echoing connections sent back from Local Receiver to Remote Sender, or Absorber-Generator.
- **Total Receiving Throughput:** Instant throughput of all receiving connections.


10.4 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.

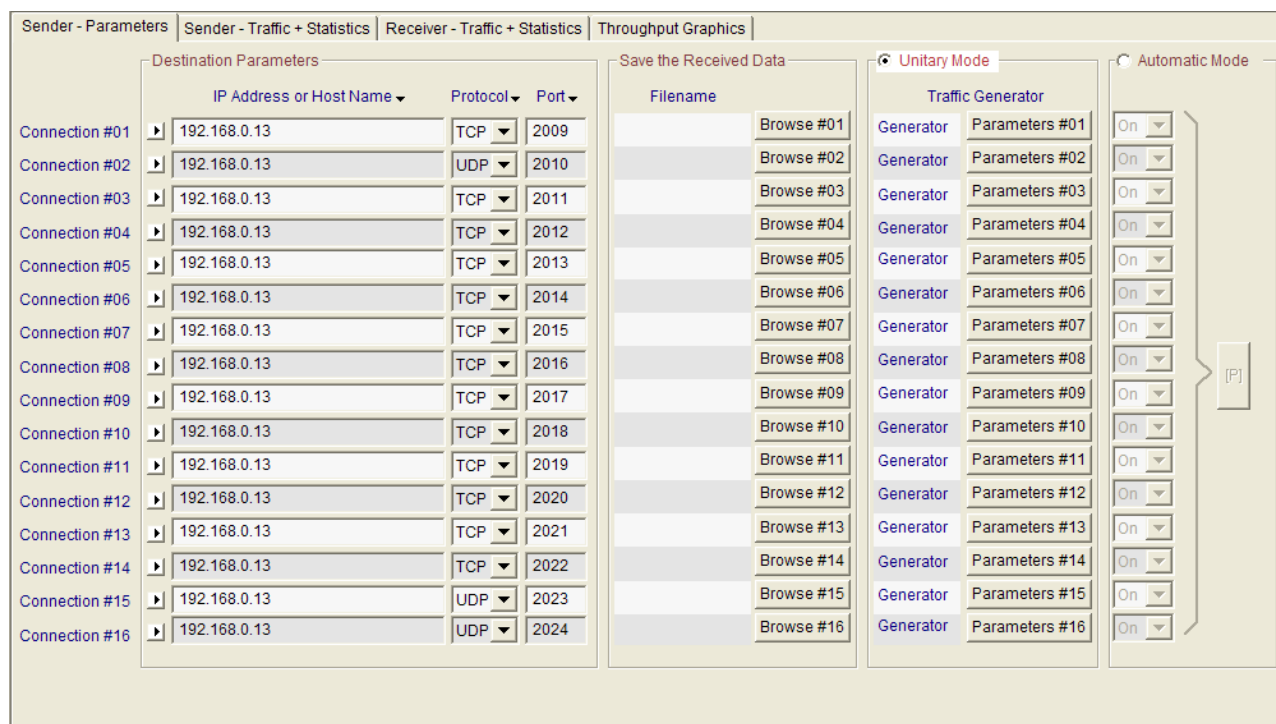
Sender part is represented in two tabs. The first one "Sender-Parameters" is used to configure connections and testing mode. The second one "Sender-Traffic + Statistics" is used to command the traffic generation and visualize the traffic statistics.

10.4.1 Sender - Parameters tab

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

- Selecting the interface and the IP version (when IPv6 is installed) for each connection, by clicking the black arrow .
- Entering 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 Absorber-Generator mode for the Remote Receiver part.
- Selecting and configuring the testing mode: Unitary or Automatic.
- Configuring the generator: for each connection when the Unitary mode is selected or globally when the Automatic mode is selected.

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



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

Tab 1: "Sender – Parameters"

10.4.1.1 Destination parameters

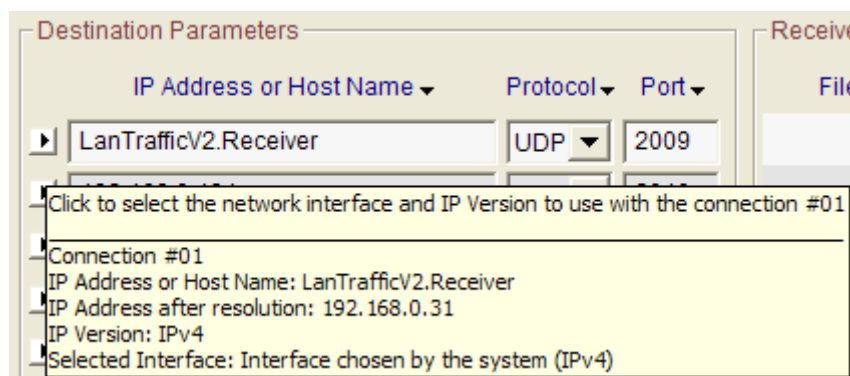
Located at the left part of the tab, this area allows configuring the destination parameters of each sending connection. You can enter the following information:

Network interface selection and IP version ▾	The black arrow has two purposes: <ul style="list-style-type: none"> • 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

10.4.1.1.1 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").

10.4.1.1.2 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** 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** 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.

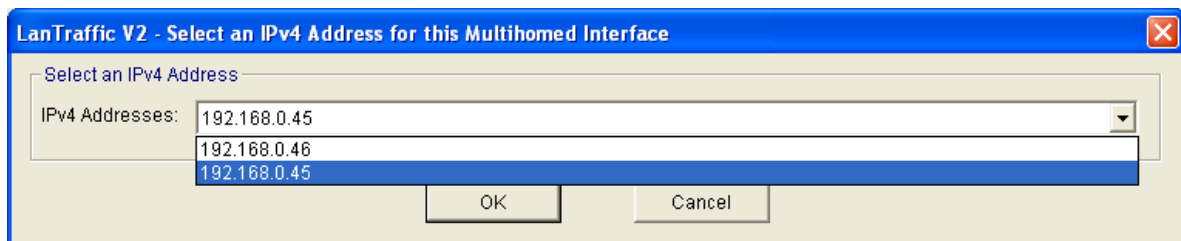
(2) The IP version selection is available:

- with Windows XP
- If IPv6 features are installed on the target machine. Please refer to the Windows XP/2003 Server documentation to install the IPv6 stack.
- You can allow **LanTraffic V2** 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** 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 10.4.1.1.3) 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** 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.

10.4.1.1.3 IP Address translation mechanism

LanTraffic V2 tries to translate – e.g. to resolve - the IP address from a canonical to a numerical format. This operation is called the *IP address translation mechanism*. When the 'IP Address or Host Name' field or Interface parameters changes, when you move from 'IP Address or Host Name' field to another field, 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** 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).

10.4.1.1.4 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)

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

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

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

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

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

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

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

(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.

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

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

10.4.1.1.5 IP address floating menu

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

IP Address or Host Name	Protocol	Port	Filename
192.168.0.13	TCP	2010	

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

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

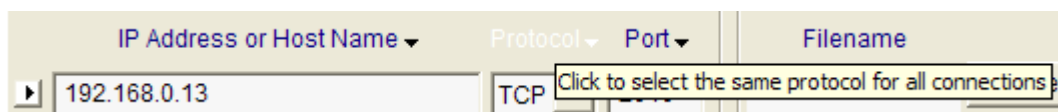
Destination Parameters		Save the Receiver	
	IP Address or Host Name	Protocol	Port
Connection #01	192.168.0.13	TCP	2009

Copy the IP Address from Connection #01 to all Connections

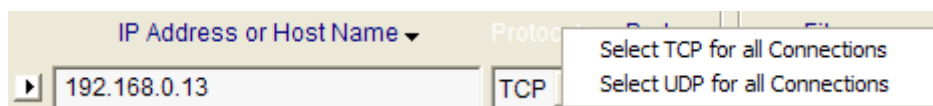
With this function the IP Address field from connection #01 is copied out on all connections from #02 to #16.

10.4.1.1.6 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:



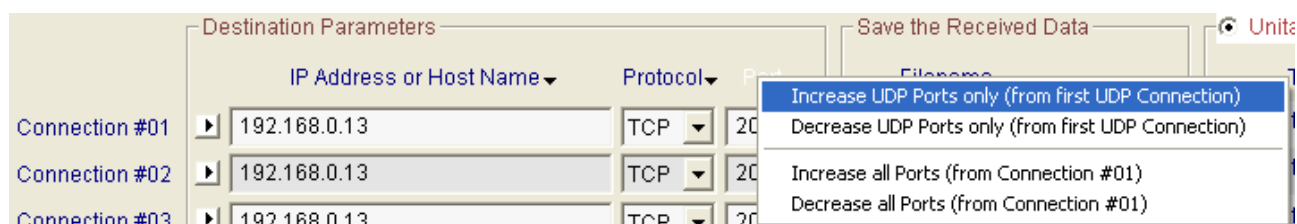
This menu helps to set the same protocol for all connections.

10.4.1.1.7 Port floating menu

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



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



With this menu, you can:

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

10.4.1.2 Save the Received Data

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

A Browse button allows an easy file selection.

10.4.1.3 Configure the Unitary Mode

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

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

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

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

- Traffic generator type: Packets generator, mathematical law or file to send,
- Data size and packets parameters: data size, inter packet delay, RTT option (RTT: Round Trip Time), TOS value (Type Of Service i.e. DSCP) – 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.

LanTraffic V2 - Traffic Generator Parameters - Sender Unitary Testing Mode (connection #01)

Step1: Select the traffic generator type
First select the traffic generator which is going to be used on this connection.

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

Packet Contents (00 to FF hexa byte)

☒ Packets Generator

☐ Mathematical Law

☐ File to send

Step2: Specify data size and packets parameters
In this step, define data size and packets parameters as well as the delay between each sent packet or specify values for some IP header fields.

TCP or UDP Data Size (1 to 65,535 bytes)

☒ Fixed

☐ Randomized min max

☐ Alternated size-1 size-2

☐ Increasing / Decreasing min max step

Inter Packet Delay (0 to 9,999 ms)

☒ Fixed (See FOREWARNINGS menu please)

☐ Randomized min max

☐ Alternated value-1 value-2

☐ Increasing / Decreasing min max step

☐ Mathematical Law

RTT Option ☐ Yes ☒ No

TOS (1 hexa byte) Value

Time To Live (TTL) Value

Step 3 (Optional): Enable a throughput limit
When one of these two options is selected, LanTraffic V2 generates the traffic with best effort to respect the throughput chosen.

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

☐ Use value

☒ Inter Packet Delay adjusted by LanTraffic V2 automatically

☐ TCP or UDP Data Size adjusted by LanTraffic V2 automatically

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

☐ Use value (except for TCP connection)

OK Cancel Help

Unitary testing parameters window (IPv4)

10.4.1.3.1 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)

10.4.1.3.1.1 Packets Generator

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

Packets Generator Parameters

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

Packet Contents (00 to FF hexa byte)

☒ Fixed

☐ Randomized min max

☐ Alternated value-1 value-2

☐ Increasing / Decreasing min max step

Packets Generator parameters

▪ Packets number

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

▪ Packet contents (00 to FF hexa byte)

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

The packet contents can be configured as follows:

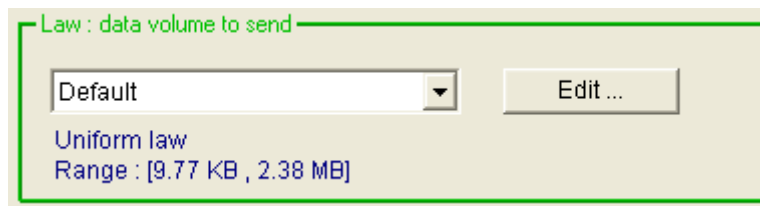
- **Fixed:** each packet has the same content.
- **Randomized:** **LanTraffic V2** computes random packet content included in a user-defined range (min to max).
- **Alternated:** **LanTraffic V2** uses the first value (value-1) for odd packets and the second value (value-2) for even packets.
- **Increasing/Decreasing:**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



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

10.4.1.3.1.2 Mathematical law

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



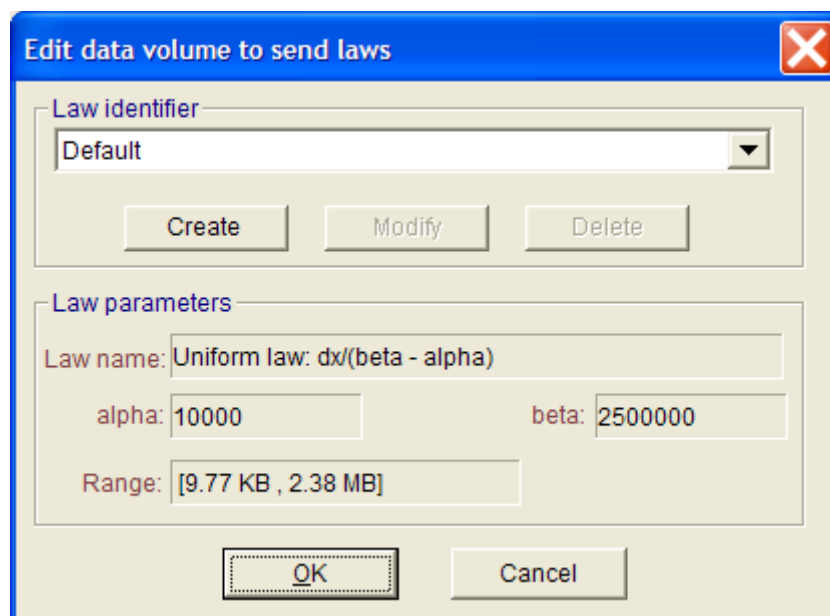
LanTraffic V2 unitary testing mode offers four mathematical laws related to the data volume:

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

These laws are presented in details in the Annex PART 13.

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

To add a new data volume to send law:

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

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



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



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

10.4.1.3.1.3 File to send

With this selection **LanTraffic V2** 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.

10.4.1.3.2 Step 2: Specify data size and packets parameters

10.4.1.3.2.1 Data Size

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

TCP or UDP Data Size (1 to 65,535 bytes)

☒ Fixed

☐ Randomized min max

☐ Alternated size-1 size-2

☐ Increasing / Decreasing min max step

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

- **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** 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** uses the first value for odd packets and the second value for even packets.
- **Increasing/Decreasing:** the size of each packet varies in a range defined by the user, from the minimal to the maximal value. Each size is incremented by the step value (0 is an invalid value). When the maximal value is reached, the packet size decreases step by step until the minimal value.



*It is important to note that **LanTraffic V2** requires a minimal packet size when the RTT mode is selected, to add a CRC, a sequence number and the timestamp. Therefore the minimal packet size with RTT mode active is 14 bytes (see paragraph 10.4.1.3.2.3 about the RTT option).*

10.4.1.3.2.2 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** 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** 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).

10.4.1.3.2.3 RTT option

When 'Yes' is selected, **LanTraffic V2** 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 10.4.1.2).

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

10.4.1.3.2.4 The TOS field (IPv4 only) / DSCP

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

TOS (1 hexa byte)

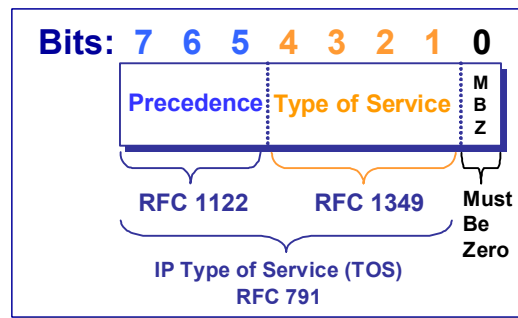
Value

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

Example: value = 24 (or in binary: **0010 1000**) means:

Precedence bits 7-5 (COS) = 001 (priority)

Type of Service bits 4-1 (TOS) = 0100 (maximize throughput)



IPv4 Type of Service byte

The TOS value entered is included without modification in the IP header i.e. **LanTraffic V2** doesn't change what you set in the TOS byte.

Use of DSCP (Differentiated Services Code Point)

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 have nothing to do with the quality of service. They are spare bits in the IP Header used by the Explicit Congestion Notification (see RFC 3168 for more details).

The DSCP totally overlaps the Precedence field.

This is why the values of DSCP have been carefully chosen to be backward compatible.

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 DSCPs are defined as following:

DSCP	Service	TOS byte in hexadecimal to be used by LanTraffic V2 (if ECT = 0 and CE = 0)
0	Best effort	00
8	Class 1	20
10	Class 1, gold (AF11)	28
12	Class 1, silver (AF12)	30
14	Class 1, bronze (AF13)	38
16	Class 2	40
18	Class 2, gold (AF21)	48
20	Class 2, silver (AF22)	50
22	Class 2, bronze (AF23)	58
24	Class 3	60
26	Class 3, gold (AF31)	68
28	Class 3, silver (AF32)	70
30	Class 3, bronze (AF33)	78
32	Class 4	80
34	Class 4, gold (AF41)	88
36	Class 4, silver (AF42)	90
38	Class 4, bronze (AF43)	98
40	Express forwarding	A0
46	Expedited forwarding (EF)	B8
48	Control	C0
56	Control	E0



To obtain a Windows NT 4.0 IP_TOS behavior's like on Windows 2000/XP, a new registry key must be added on Windows 2000/XP. It is necessary to edit the Registry and modify this key in order to use the TOS byte with LanTraffic V2.



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.

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

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

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

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

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

NOTE: The registry key is one path.

On the Edit menu, click Add Value, and then type DisableUserTOSSetting. Click REG_DWORD in the Data Type box, and then click OK. Enter 0 in the prompt box. Quit Registry Editor, and then restart the computer.

10.4.1.3.2.5 The TTL field

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

10.4.1.3.3 Step 3 (optional): Activate a throughput limit

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

Step 3 (Optional): Enable a throughput limit

When one of these two options is selected, LanTraffic V2 generates the traffic with best effort to respect the throughput chosen.

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

☐ Use value
☒ Inter Packet Delay adjusted by LanTraffic V2 automatically
 ☐ TCP or UDP Data Size adjusted by LanTraffic V2 automatically

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

☐ Use value (except for TCP connection)

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 average throughput in Kbps in the edit box and select one of the two parameters (packet size or inter packet delay). **LanTraffic V2** will automatically adapt data traffic generation with adjustment of packet size or inter packet delay (user choice) up to the throughput requested by the user.

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

Step 3 (Optional): Enable a throughput limit

When one of these two options is selected, LanTraffic V2 generates the traffic with best effort to respect the throughput chosen.

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

☐ Use value
☒ Inter Packet Delay adjusted by LanTraffic V2 automatically
 ☐ TCP or UDP Data Size adjusted by LanTraffic V2 automatically

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

☐ Use value (except for TCP connection)

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

10.4.1.4 Configure the Automatic Mode

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

As 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.

The screenshot shows the LanTraffic V2 application window. The 'Sender - Parameters' tab is active. It features a table for defining connections, a section for saving received data, and a traffic generator section. The 'Automatic Mode' is selected, and a bracket labeled '[P]' groups the 'On' status dropdowns for all connections. At the bottom, there are statistics for sender and receiver, and buttons to start or stop the sender and receiver.

Destination Parameters			
	IP Address or Host Name	Protocol	Port
Connection #01	192.168.0.35	UDP	2009
Connection #02	192.168.0.35	TCP	2010
Connection #03	192.168.0.35	TCP	2011
Connection #04	192.168.0.35	TCP	2012
Connection #05	192.168.0.35	TCP	2013
Connection #06	192.168.0.35	TCP	2014
Connection #07	192.168.0.35	TCP	2015
Connection #08	192.168.0.35	TCP	2016
Connection #09	192.168.0.35	TCP	2017
Connection #10	192.168.0.35	TCP	2018
Connection #11	192.168.0.35	TCP	2019
Connection #12	192.168.0.35	TCP	2020
Connection #13	192.168.0.35	TCP	2021
Connection #14	192.168.0.35	UDP	2022
Connection #15	192.168.0.35	UDP	2023
Connection #16	192.168.0.35	UDP	2024

Save the Received Data	
Filename	Browse
	Browse #01
	Browse #02
	Browse #03
	Browse #04
	Browse #05
	Browse #06
	Browse #07
	Browse #08
	Browse #09
	Browse #10
	Browse #11
	Browse #12
	Browse #13
	Browse #14
	Browse #15
	Browse #16

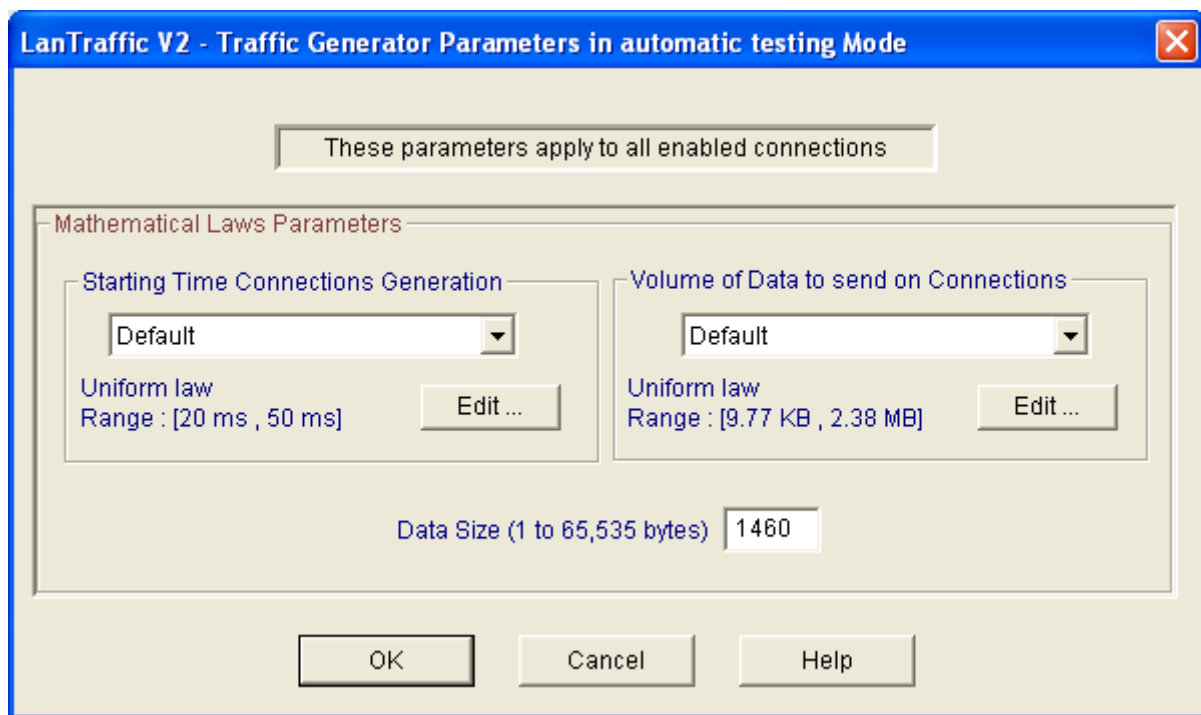
Traffic Generator		
Generator	Parameters	
Generator	Parameters #01	On
Generator	Parameters #02	On
Generator	Parameters #03	On
Generator	Parameters #04	On
Generator	Parameters #05	On
Generator	Parameters #06	On
Generator	Parameters #07	On
Generator	Parameters #08	On
Generator	Parameters #09	On
Generator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

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

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

Start Sender and Receiver Stop Sender and Receiver

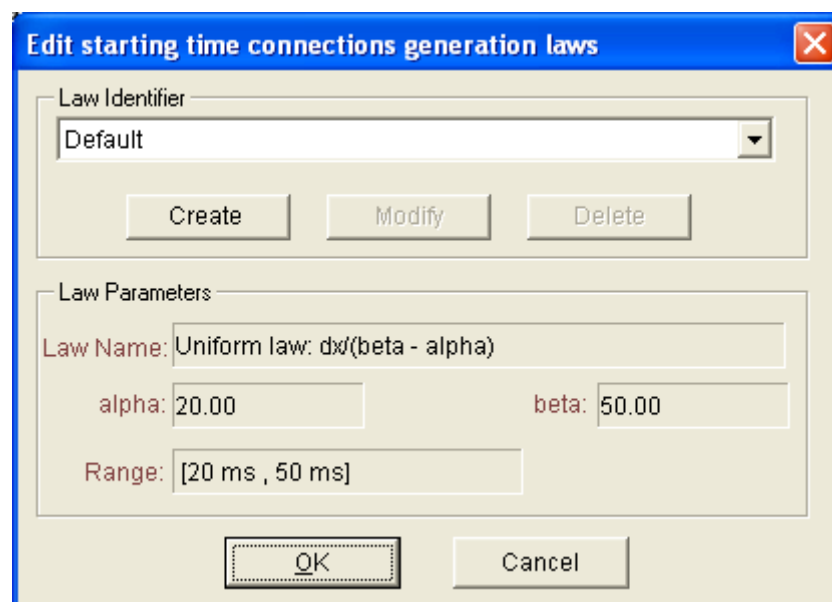
By clicking on the '[P]' button (P as Parameters), the following window is displayed allowing to configure the automatic testing mode parameters:



Automatic testing parameters window

10.4.1.4.1 Starting time connections generation laws

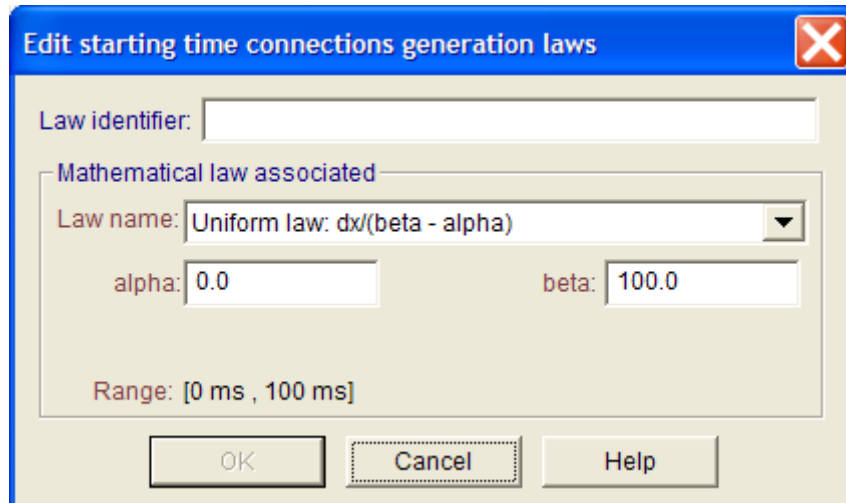
Starting time connection laws regulate the timing between the beginning of two connections. The available mathematical laws for starting time connection are Uniform and Exponential laws. (Mathematical laws are presented in details in Annex part). You can add, modify or delete a law by pressing the "Edit"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



Starting time connections generation law window

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

- 1) Press the “Create” button and then a new window will appear:

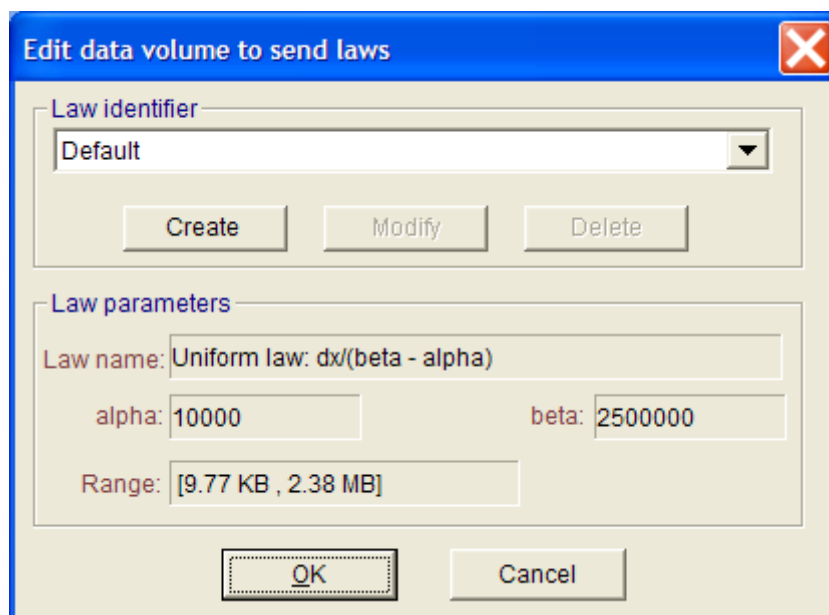
A dialog box titled "Edit starting time connections generation laws" with a blue header bar and a red close button. It contains a "Law identifier" text field. Below it is a section titled "Mathematical law associated" containing a "Law name" dropdown menu showing "Uniform law: dx/(beta - alpha)". Below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

Edit starting time connections generation law window

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

10.4.1.4.2 Data volume to send laws

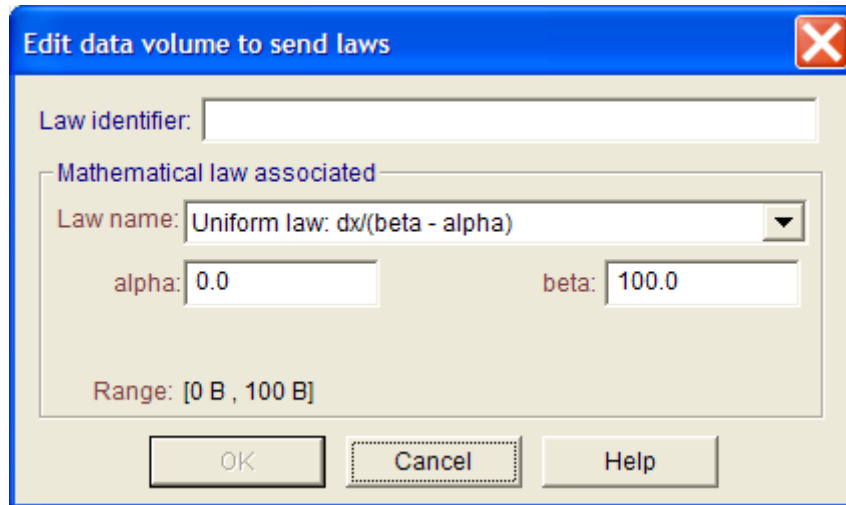
Data volume laws regulate the data volume to send for connection. The available mathematical laws for data volume to send are: Uniform, Exponential and Pareto laws. (Mathematical laws are presented in details in Annex Part). You can add, modify or delete a law by pressing the “Edit” button.

A dialog box titled "Edit data volume to send laws" with a blue header bar and a red close button. It features a "Law identifier" dropdown menu currently set to "Default". Below this are three buttons: "Create", "Modify", and "Delete". A section titled "Law parameters" contains a "Law name" dropdown menu showing "Uniform law: dx/(beta - alpha)". Below this are two text fields: "alpha:" with the value "10000" and "beta:" with the value "2500000". At the bottom of this section is a "Range:" label followed by "[9.77 KB , 2.38 MB]". At the very bottom of the dialog are two buttons: "OK" and "Cancel".

Volume law window

To add a new data volume to send law:

1. Press the “Create” button and the following window is displayed:



Edit data volume law window

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



According to the operating system used (Windows 98, Me, NT4, 2000 or XP), the WinSock 2 interface could present number-limits of the incoming simultaneous calls. Consequence for LanTraffic V2 is the presence of “connection failed”, particularly when 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”. To reduce these failures, decrease the frequency of connections or increase the data volume.

10.4.1.4.3 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.

10.4.2 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.

Sender - Parameters

Sender - Traffic + Statistics

Receiver - Traffic + Statistics

Throughput Graphics

Destination Parameters

Statistics (based on application data)

Clear on Stop

Unitary Mode

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

Export Statistics into a File

Parameters

Export is disabled

Choose Columns

Reset Display

Stop #01

Stop #02

Start #03

Start #04

Start #05

Start #06

Start #07

Start #08

Start #09

Start #10

Start #11

Start #12

Start #13

Start #14

Start #15

Start #16

Start All Connections

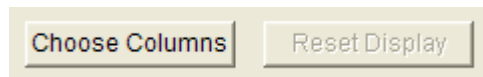
Stop All Connections

Tab 2: “Sender - Traffic + Statistics”

10.4.2.1 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.

10.4.2.2 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.

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

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

Examples:

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

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

Note: the warning message isn't 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 has sent since the connection is started.
Tx Pkts Throughput	Tx Pkts Throughput (Tx = Transmit) is the mean number of packets that LanTraffic V2 is sending per second. This value is only available with UDP connections. The calculation of this value is based on the sampling period defined by the throughput sampling period in the 'Configuration/General Parameters' menu.
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 has sent since the connection is started.

Receiving statistics

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

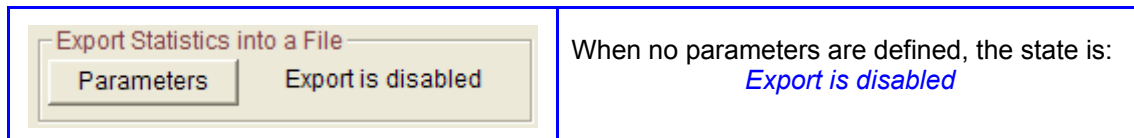
Other statistics

Jitter	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 = Absorber Generator mode) or the two-ways variation mean (remote Receiver = Echoer mode).
Remaining Volume	'Remaining Volume' is the number of bytes that LanTraffic V2 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 which was sent by LanTraffic V2 . This value is calculated if the RTT option is selected on the local Sender Traffic Generator and if the remote Receiver works in Echoer mode.
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 Absorber Generator or Echoer.

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

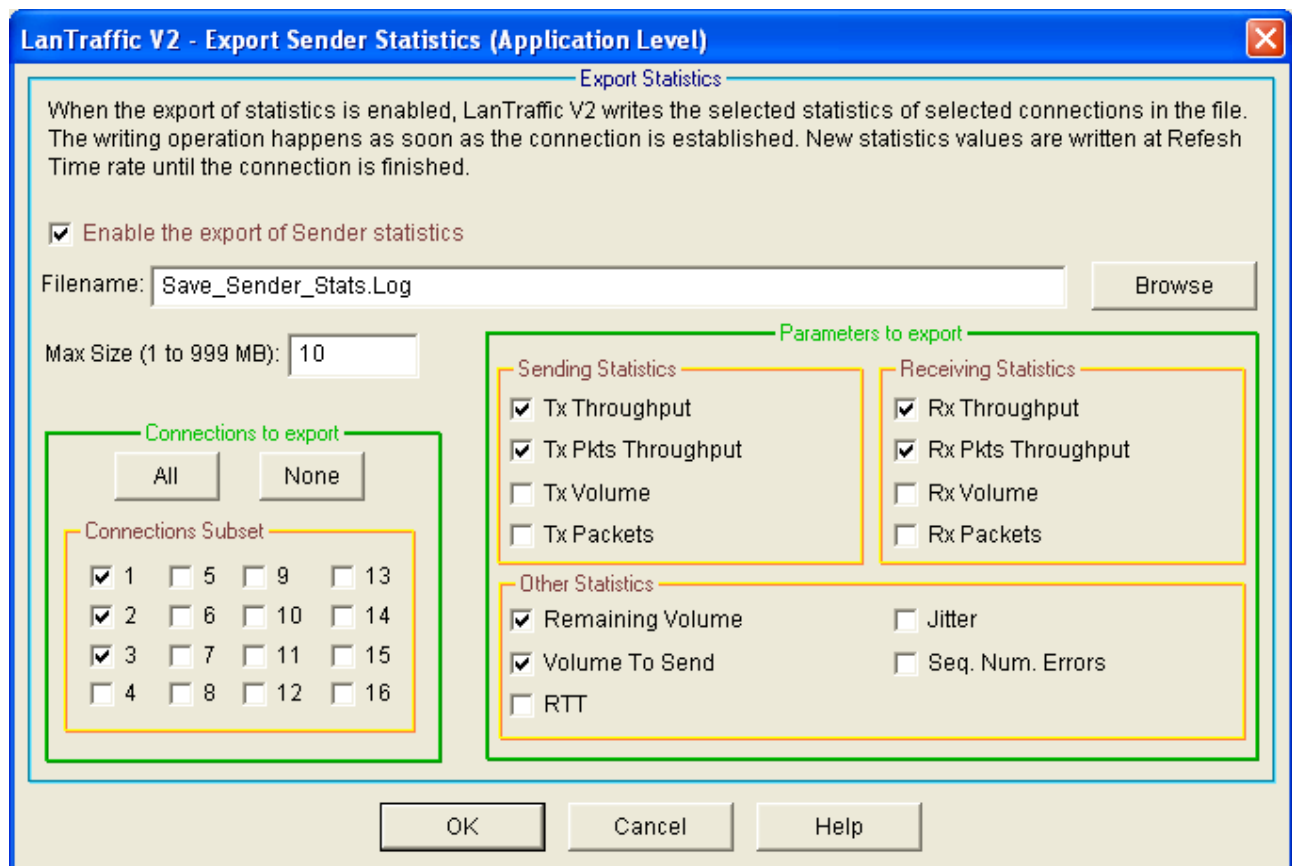
10.4.2.3 Export Statistics into a File

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

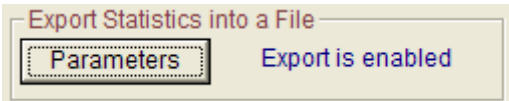



Then a new window allows defining parameters for the export process:

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

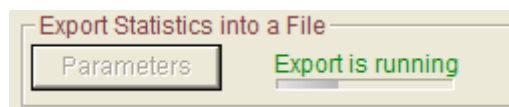


Then press OK to validate, and a new state is displayed:

	<p>When parameters have been defined and the export process is enabled, the state is: <i>Export is enabled</i></p>
---	--

	<p><i>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.</i></p>
---	--

The statistics file is updated with the same refresh period than the statistics displayed. A special mark is added to keep special TCP and UDP events e.g. Begin and End of sending traffic. When you reset statistics, the displayed values and the exported values are reset. Statistics are saved into the file as soon as the 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:



10.4.2.3.1 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 i	Parameter ...
---------------------------	------	------	-------------	-------------	---------------

with:

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

Next lines: numerical values

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

Additional marks for TCP and UDP connection events

Connection #nn (TCP or UDP) 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** for the line.

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

Additional mark for TCP or UDP disconnection events

Connection Cnx #n (TCP or UDP) 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**.

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 Pkts Throughput" and "Rx Pkts Throughput" are filled with the "N/A" symbol when the protocol used for the concerned connection is not UDP.

In addition, 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".

10.4.2.3.2 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


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

Starting session 09/26/2005 at 14:51:11.765 (UTC Time)

LanTrafficV2 Sender

Connection # (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	09/26/2005	14:51:11.781	0.00	0.00	0	0.00	0.00	0	N/A	N/A
Connection #02 (TCP) START	09/26/2005	14:51:11.843	0.00	0.00	0	0.00	0.00	0	0	0
Connection #16 (TCP) START	09/26/2005	14:51:11.843	0.00	0.00	0	0.00	0.00	0	0	0
Connection #01 (UDP)	09/26/2005	14:51:12.531	66.16	48.48	34	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	09/26/2005	14:51:12.531	63.88	44.20	31	0.00	0.00	0	0	0
Connection #16 (TCP)	09/26/2005	14:51:12.531	63.88	48.48	34	63.88	45.63	32	7	0
Connection #01 (UDP)	09/26/2005	14:51:14.546	289.72	186.78	131	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	09/26/2005	14:51:14.546	292.00	186.78	131	0.00	0.00	0	0	0
Connection #16 (TCP)	09/26/2005	14:51:14.546	292.00	186.78	131	292.00	186.78	130	5	0
Connection #01 (UDP)	09/26/2005	14:51:16.546	517.84	329.36	231	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	09/26/2005	14:51:16.546	517.84	329.36	231	0.00	0.00	0	0	0
Connection #16 (TCP)	09/26/2005	14:51:16.546	520.13	329.36	231	520.13	329.36	229	5	0
Connection #01 (UDP)	09/26/2005	14:51:18.531	568.03	474.79	333	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	09/26/2005	14:51:18.531	568.03	473.36	332	0.00	0.00	0	0	0
Connection #16 (TCP)	09/26/2005	14:51:18.531	568.03	473.36	332	568.03	471.93	329	4	0
Connection #01 (UDP)	09/26/2005	14:51:20.531	568.03	614.51	431	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	09/26/2005	14:51:20.531	568.03	620.21	435	0.00	0.00	0	0	0
Connection #16 (TCP)	09/26/2005	14:51:20.531	568.03	615.94	432	568.03	615.94	430	5	0
Connection #01 (UDP)	09/26/2005	14:51:22.531	568.03	759.94	533	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	09/26/2005	14:51:22.531	565.75	759.94	533	0.00	0.00	0	0	0
Connection #16 (TCP)	09/26/2005	14:51:22.531	568.03	759.94	533	568.03	759.94	525	7	0
Connection #01 (UDP)	09/26/2005	14:51:24.531	570.31	905.37	635	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	09/26/2005	14:51:24.531	570.31	903.95	634	0.00	0.00	0	0	0
Connection #16 (TCP)	09/26/2005	14:51:24.531	570.31	899.67	631	568.03	898.24	622	7	0
Connection #01 (UDP)	09/26/2005	14:51:26.546	572.59	1045.10	733	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	09/26/2005	14:51:26.546	572.59	1042.25	731	0.00	0.00	0	0	0
Connection #16 (TCP)	09/26/2005	14:51:26.546	568.03	1042.25	731	568.03	1042.25	717	8	0
***	***	***	***	***	***	***	***	***	***	***
***	***	***	***	***	***	***	***	***	***	***
Connection #01 (UDP)	09/26/2005	14:54:26.687	568.03	13864.30	9724	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	09/26/2005	14:54:26.687	570.31	13868.57	9727	0.00	0.00	0	0	0
Connection #16 (TCP)	09/26/2005	14:54:26.687	570.31	13877.13	9733	568.03	13874.28	9613	9	0
Connection #01 (UDP)	09/26/2005	14:54:28.687	570.31	14012.58	9828	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	09/26/2005	14:54:28.687	568.03	14016.86	9831	0.00	0.00	0	0	0
Connection #16 (TCP)	09/26/2005	14:54:28.687	570.31	14019.71	9833	570.31	14016.86	9711	9	0
Connection #01 (UDP)	09/26/2005	14:54:30.921	568.03	14166.56	9936	0.00	0.00	0	N/A	N/A
Connection #02 (TCP)	09/26/2005	14:54:30.921	570.31	14170.84	9939	0.00	0.00	0	0	0
Connection #16 (TCP)	09/26/2005	14:54:30.921	568.03	14175.12	9942	570.31	14173.69	9820	9	0
Connection #02 (TCP) END	09/26/2005	14:54:32.078	568.03	14257.81	10000	0.00	0.00	0	0	0
Connection #16 (TCP) END	09/26/2005	14:54:32.531	524.69	14257.81	10000	526.97	14257.81	9879	9	0
Connection #01 (UDP)	09/26/2005	14:54:32.906	538.38	14257.81	10000	0.00	0.00	0	N/A	N/A
Connection #01 (UDP) END	09/26/2005	14:54:32.937	538.38	14257.81	10000	0.00	0.00	0	N/A	N/A

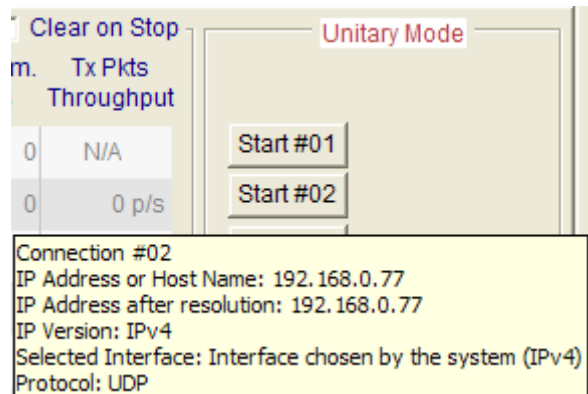
10.4.2.4 Run the Unitary Mode



The screenshot shows a panel titled 'Unitary Mode'. It contains a vertical list of buttons labeled 'Start #01' through 'Start #16'. To the right of these buttons are two larger buttons: 'Start All Connections' and 'Stop All Connections'.

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:



The tooltip shows a table with columns 'Clear on Stop', 'm.', 'Tx Pkts', and 'Throughput'. Below the table, it lists connection details for Connection #02.

Clear on Stop	m.	Tx Pkts	Throughput
0		N/A	
0			0 p/s

Connection #02
 IP Address or Host Name: 192.168.0.77
 IP Address after resolution: 192.168.0.77
 IP Version: IPv4
 Selected Interface: Interface chosen by the system (IPv4)
 Protocol: UDP

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

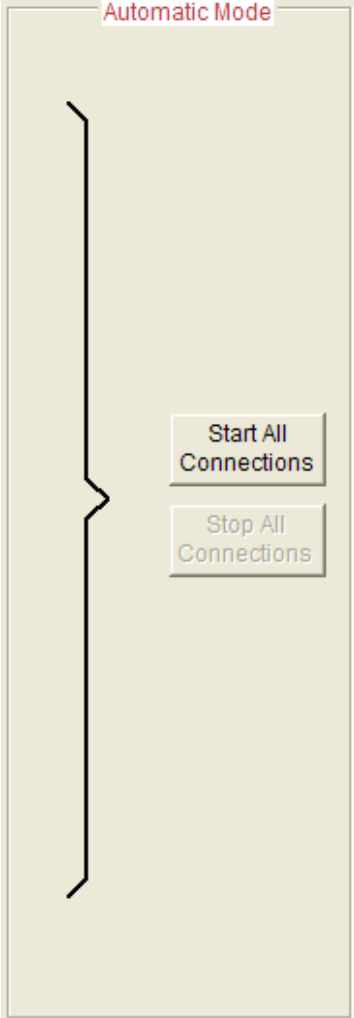
The "Sender – Traffic + Statistics" summary tooltip displays:

- 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.

10.4.2.5 Run the Automatic Mode

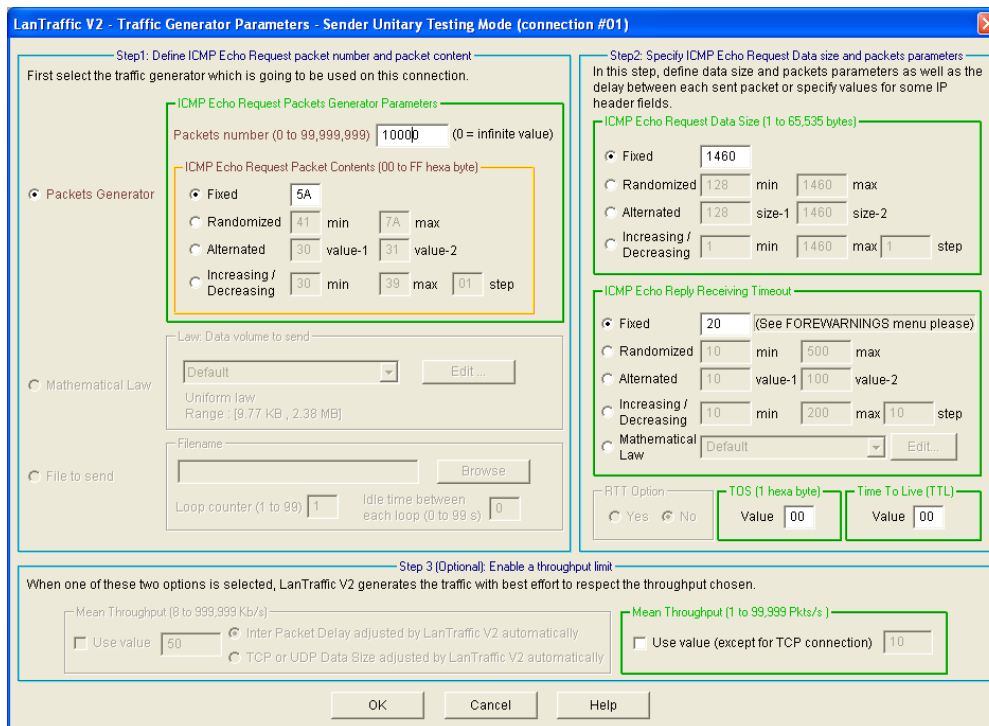
	<p>The Automatic mode is chosen in the "Sender – Parameters" tab.</p> <p>The automatic testing mode can be launched from the Automatic Mode area as shown on the left.</p> <p>In this area, there are two buttons to start and stop all enabled connections: 'Start All Connections' and 'Stop All Connections'.</p> <p>To carry out the automatic testing session:</p> <ol style="list-style-type: none">1 <i>In Tab 2: "Sender - Traffic + Statistics"</i> ⇒ If the Sender connections are active, stop all running connections by pressing the "Stop All Connections" button.2 <i>In Tab 1: "Sender - Parameters"</i> ⇒ Select the Automatic Mode.3 <i>In Tab 1 "Sender - Parameters":</i> ⇒ If necessary, configure the automatic parameters by pressing the "[P]" button and enable or disable connections by using the ON/OFF combo box.4 <i>In Tab 2: "Sender - Traffic + Statistics":</i> ⇒ Press the "Start All Connections" button to start all enabled connections.
--	---

10.4.3 Using ICMP capacity of the Sender

LanTraffic V2 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.
- 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 10.4.1.3

Destination Parameters			Statistics (based on application data)				Unitary Mode
Connection #01	IP Address or Host Name	Port	Seq. Num. Errors	RTT	Tx Packets	Rx Packets	Stop #01
	192.168.0.120	N/A	4	3 ms	4068 p	4063 p	

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 average Round Trip Time.
- Seq. Num. Errors (Sequence Numbering Errors): this value represents the number of replies that “LanTraffic V2” does not receive.

10.5 The Receiver part

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

Receiver - Parameter + Statistics tab

By using this tab, you can:

- Configure 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'.

Listening To ...			Coming From ...	Working Mode		Statistics (based on application data)				
Connection	Port	Protocol	Remote IP Address or Host Name	Working Mode	Browse	Rx Throughput	Rx Volume	Tx Throughput	Tx Volume	Jitter
Connection #01	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #02	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #03	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #04	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #05	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #06	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #07	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #08	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #09	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #10	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #11	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #12	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #13	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #14	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #15	2009	TCP	ANY_ADDRESS	Absorber	Browse					
Connection #16	2009	TCP	ANY_ADDRESS	Absorber	Browse					

Export Statistics into a File
Parameters Export is disabled

Start Receiving Traffic Stop Receiving Traffic

Choose Columns Reset Display

Tab 3 "Receiver - Traffic + Statistics"

10.5.1 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 10.4.1.1.4).

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.

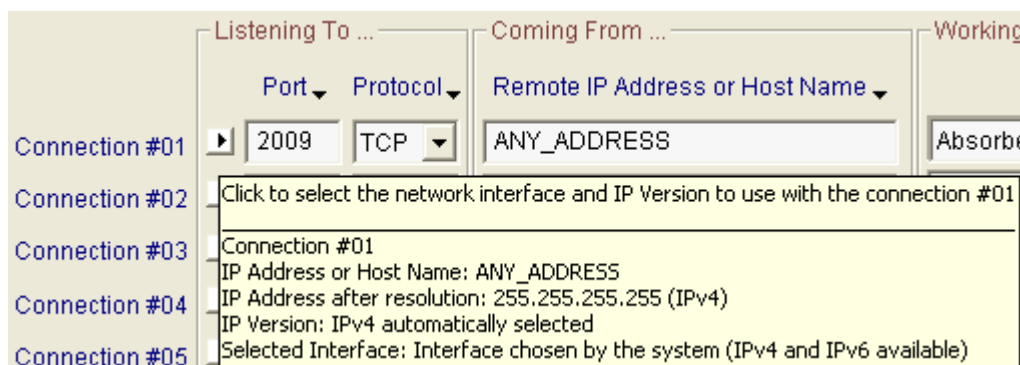
10.5.2 Listening To ...

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 	<i>The black arrow has two purposes:</i> <ul style="list-style-type: none"> • 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).

10.5.2.1 Summary of the connection parameters

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



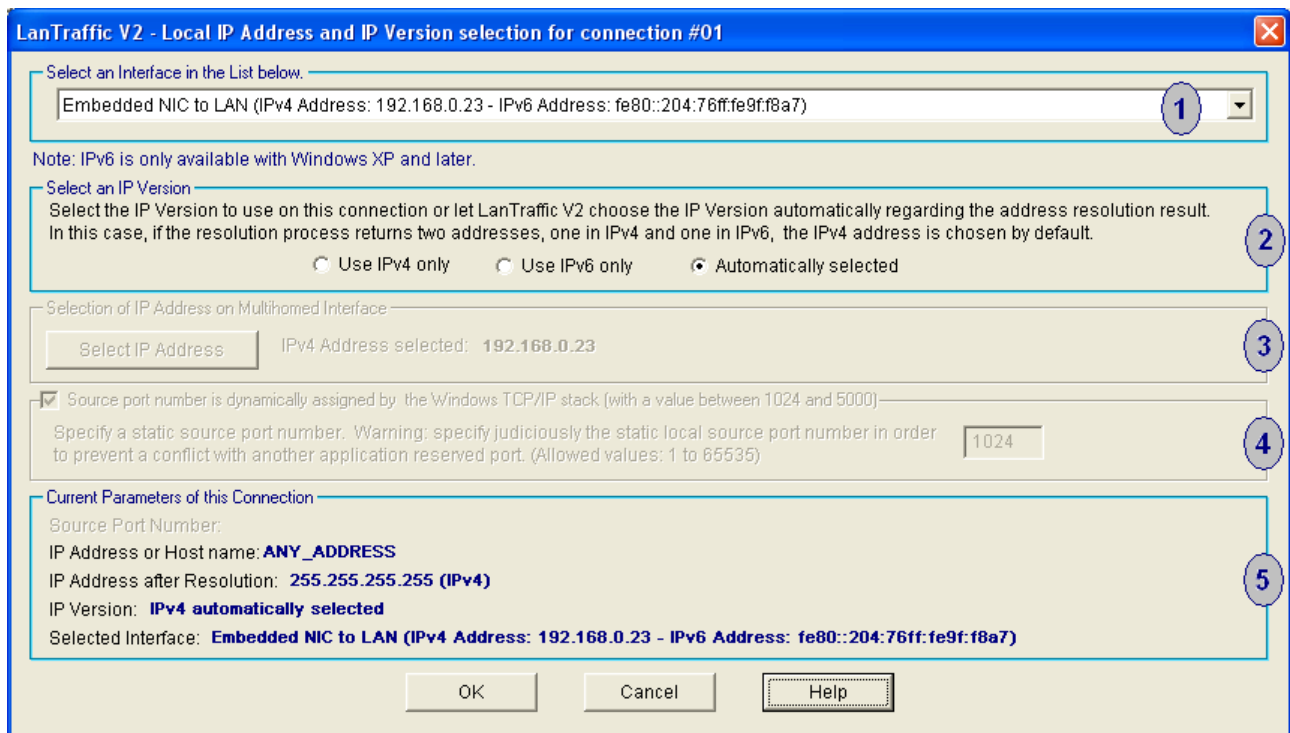
Receiver connection tooltip

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”).

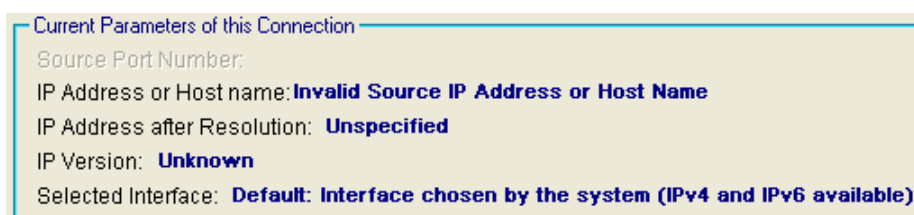
10.5.2.2 Select the network interface, IP version and local IP address

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** 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** 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:

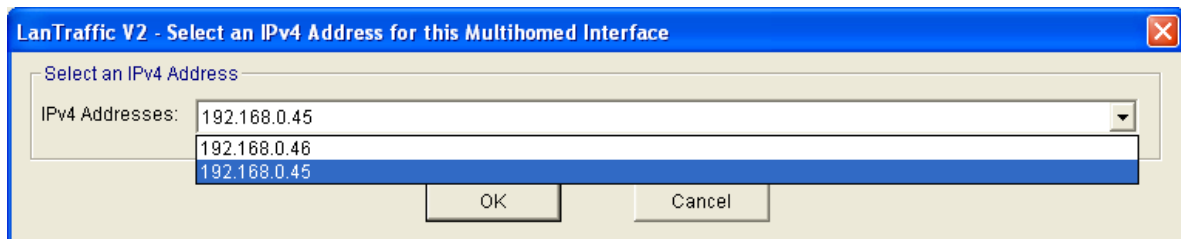
- with Windows XP (or later)
- If IPv6 features are installed on the target machine. Please refer to the Windows XP documentation to install the IPv6 stack.
- You can allow **LanTraffic V2** to choose automatically the good IP version regarding the address or host name resolution result. If a canonical name corresponds at the same time to an IPv4 and IPv6 addresses, **LanTraffic V2** 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 10.4.1.1.3) 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** 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.



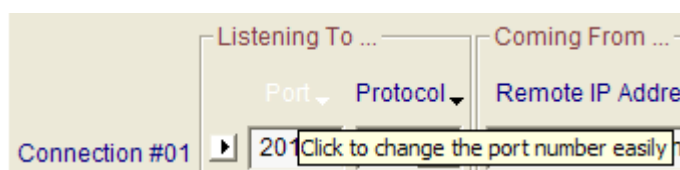
When you click on the OK button, if the interface selected or IP version has changed, the IP address translation is automatically started. It may be time consuming.

So, you can configure various incoming connection criteria:

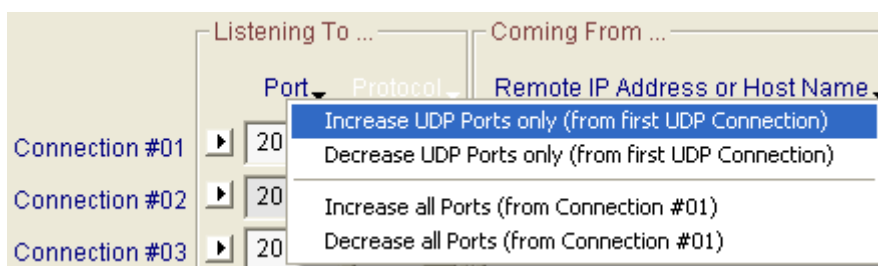
- **Interface:** you limit a connection to a specific Interface or let the Operating System to return connections from any interfaces.
- **IP version:** when an Interface offers the two IP versions, you can select the IP version expected or not. By default, the automatic selection is activated.
- **When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

10.5.2.3 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:

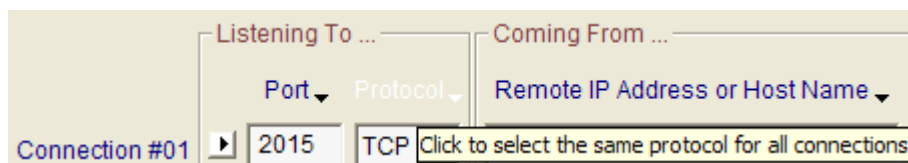


With this menu, you can:

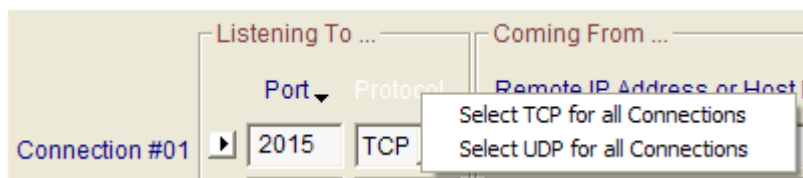
- Set the port number increasingly or decreasingly for all UDP connections, based on the port number of the first UDP connection,
- Set the port number increasingly or decreasingly for all connections, based on the port number of the first connection without taking into account the protocol in use.

10.5.2.4 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:



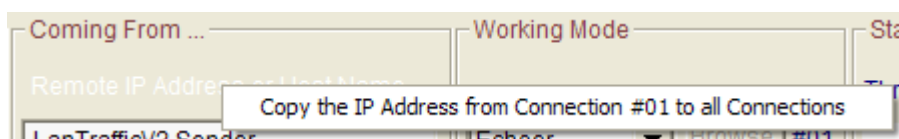
This menu helps to set the same protocol for all connections.

10.5.3 Coming From ...

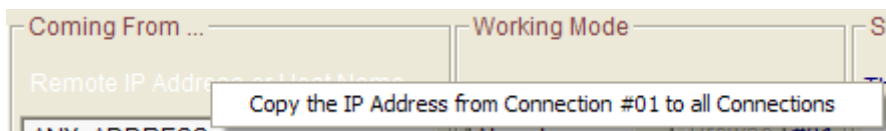
Remote IP address or Host Name:	<p><i>Enter the IP address (numerical format) or Host Name (canonical format), with the help of AutoComplete when active.</i></p> <p><i>By default, the value is ANY_ADDRESS (This address is a mask to accept connection from any source address. It applies on both IPv4 and IPv6).</i></p>
--	---

10.5.3.1 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.

10.5.3.2 IP Address translation mechanism

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

10.5.4 Working Mode

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

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

10.5.4.1 Absorber mode

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

LanTraffic V2
Local Sender

Connection # n

LanTraffic V2

Remote Receiver (absorber mode)
(no specific treatment for each received IP packet)

10.5.4.2 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.

LanTraffic V2
Local Sender

Connection # m

LanTraffic V2

Remote Receiver (absorber file mode)
(each received IP packet is saved in a file)



10.5.4.3 Echoer mode

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

LanTraffic V2
Local Sender

Connection # p

LanTraffic V2

Remote Receiver (echoer mode)
(each received IP packet on the connection is sent to the transmitter)

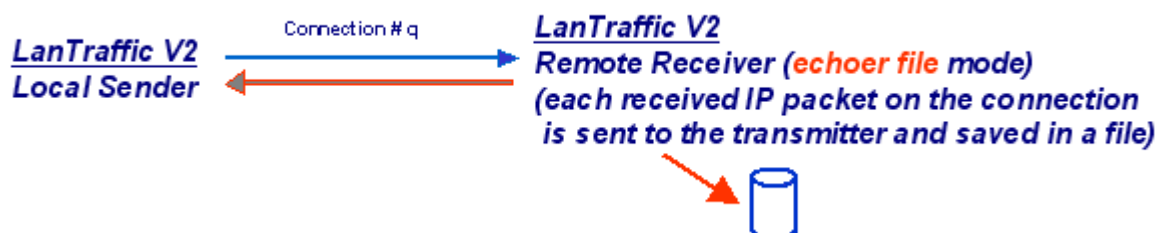
With UDP protocol, echoer mode is available only if a connected sender IP address is specified.



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

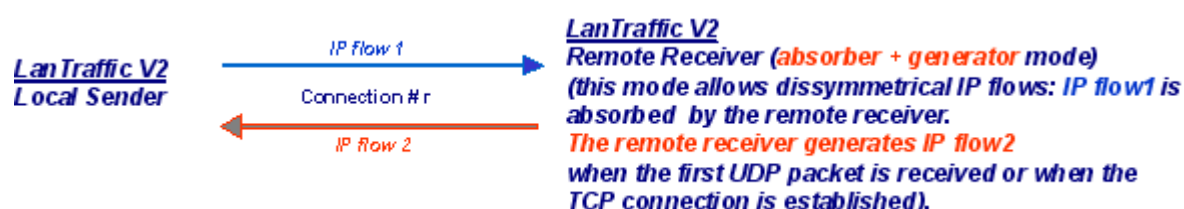
10.5.4.4 Echoer File mode

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



10.5.4.5 Absorber + Generator mode

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



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

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

When you select the "Absorber gen." mode for a connection (#01 in the example above), a 'Param.' Button is displayed in order to specify 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).

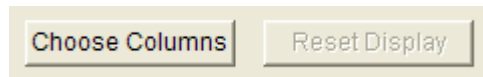
For a TCP connection, *IP flow 2* is generated as soon as the TCP connection will be established between the 'Local Sender' and the 'Remote Receiver' modules. It stops when 'Local Sender' stops the connection or at the end of the 'Remote Receiver' Traffic generator.

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.

10.5.4.6 Disable mode

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

10.5.5 Statistics



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

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

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

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

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

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

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

Example:

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

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

List of the 13 statistic parameters calculated for the Receiver***Sending statistics***

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

Receiving statistics

Rx Packets	Rx Packets (Rx = Receive) is the number of packets that LanTraffic V2 has received since the connection is started.
Rx Pkts Throughput	Rx Pkts Throughput (Rx = Receive) is the mean number of packets that LanTraffic V2 is receiving per second. This value is only available with UDP connections. The calculation of this value is based on the sampling period defined by the throughput sampling period in the 'Configuration/General Parameters' menu.
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 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 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 Absorber Generator or Echoer.
Volume To Send	'Volume To Send' is the number of bytes that " LanTraffic V2 should send. This information is available for two Traffic Generator Types only (Mathematical law and File to Send).

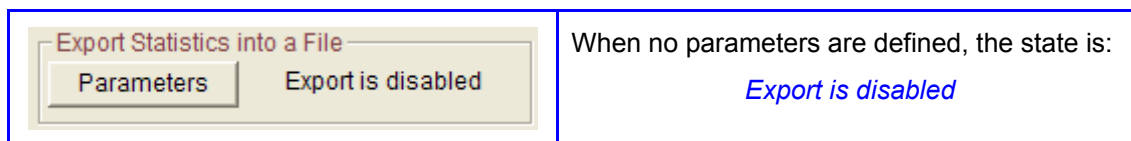
By pressing the 'Start Receiving Traffic' button, all connected sender information and working mode information are grayed,
Disabled connections statistics fields are empty on gray background,
UDP enabled connections statistics fields are filled with “00” value on white background,
TCP connections statistics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

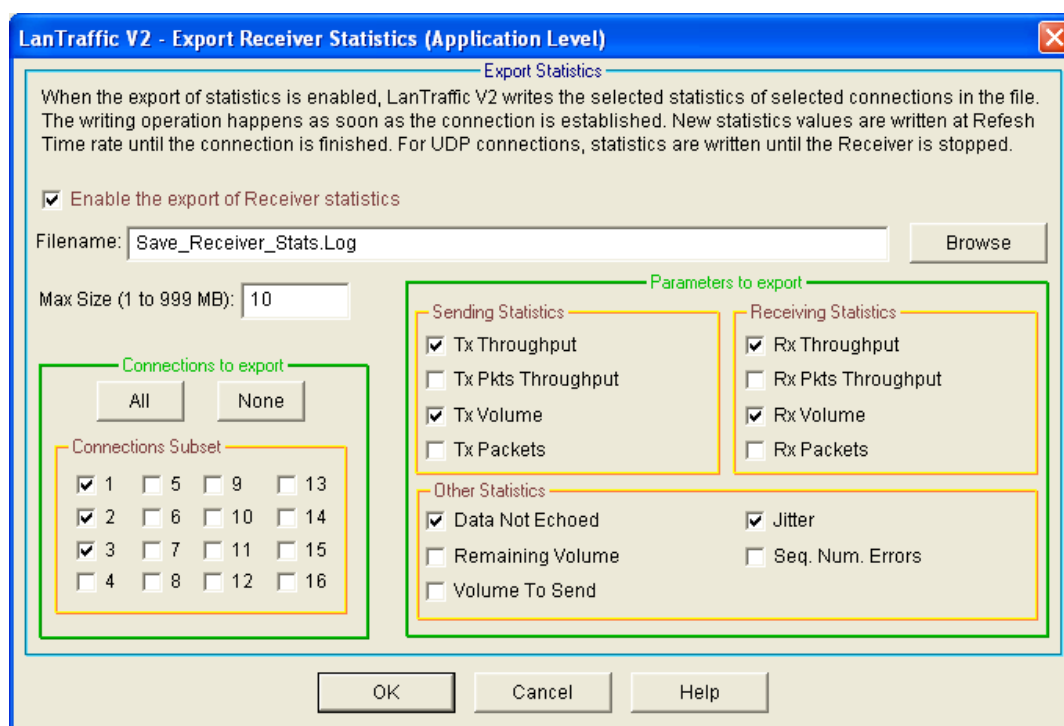
10.5.6 Export Statistics into a File

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

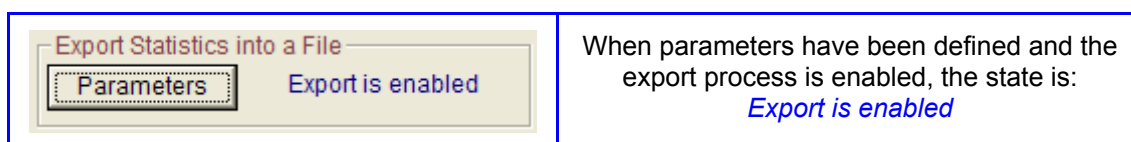


Then a new window allows defining parameters for the export process:

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



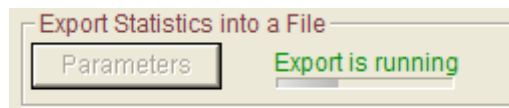
Then press OK to validate, and a new state is displayed:



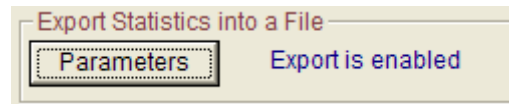
Do not specify the same filename to save statistics for the Sender and the Receiver parts; if you do so, a warning message is displayed.

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

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



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



10.5.6.1 Receiver statistics file format

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

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

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

with

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

Next lines: numerical values

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

Additional marks for TCP and UDP connection events

Connection #nn (TCP or UDP) 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** for the line.

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

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**.

Idle connections

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

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

In addition, 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”.

10.5.6.2 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

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 09/26/2005 at 16:26:10.500 (UTC Time)

LanTrafficV2 Receiver

Connection # (Protocol)	Date	Time	Rx Throughput (Kb/s)	Rx Pkts Throughput (Pkts/s)	Rx Packets (Pkts)	Jitter (ms)	Seq. Num. Errors
Connection #03 (UDP) START	09/26/2005	16:26:10.546	0.00	0	0	N/A	N/A
Connection #03 (UDP)	09/26/2005	16:26:10.609	0.00	0	0	N/A	N/A
Connection #03 (UDP)	09/26/2005	16:26:11.437	0.00	0	1	0	N/A
Connection #01 (TCP) START	09/26/2005	16:26:11.484	0.00	N/A	0	N/A	N/A
Connection #02 (TCP) START	09/26/2005	16:26:11.484	0.00	N/A	0	N/A	N/A
Connection #01 (TCP)	09/26/2005	16:26:13.453	109.50	N/A	98	0	N/A
Connection #02 (TCP)	09/26/2005	16:26:13.453	109.50	N/A	98	0	N/A
Connection #03 (UDP)	09/26/2005	16:26:13.453	109.50	9	101	0	N/A
Connection #01 (TCP)	09/26/2005	16:26:15.453	337.63	N/A	195	0	N/A
Connection #02 (TCP)	09/26/2005	16:26:15.453	337.63	N/A	198	0	N/A
Connection #03 (UDP)	09/26/2005	16:26:15.453	337.63	29	201	0	N/A
Connection #01 (TCP)	09/26/2005	16:26:17.453	565.75	N/A	293	0	N/A
Connection #02 (TCP)	09/26/2005	16:26:17.453	565.75	N/A	297	0	N/A
Connection #03 (UDP)	09/26/2005	16:26:17.453	565.75	49	301	0	N/A
Connection #01 (TCP)	09/26/2005	16:26:19.437	574.88	N/A	392	0	N/A
Connection #02 (TCP)	09/26/2005	16:26:19.437	574.88	N/A	397	0	N/A
Connection #03 (UDP)	09/26/2005	16:26:19.437	572.59	50	401	0	N/A
Connection #01 (TCP)	09/26/2005	16:26:21.437	574.88	N/A	491	1	N/A
Connection #02 (TCP)	09/26/2005	16:26:21.437	570.31	N/A	496	0	N/A
Connection #03 (UDP)	09/26/2005	16:26:21.437	570.31	50	500	0	N/A
Connection #01 (TCP)	09/26/2005	16:26:23.437	574.88	N/A	587	0	N/A
Connection #02 (TCP)	09/26/2005	16:26:23.437	574.88	N/A	592	0	N/A
Connection #03 (UDP)	09/26/2005	16:26:23.437	572.59	50	597	0	N/A
Connection #01 (TCP)	09/26/2005	16:26:25.453	570.31	N/A	688	1	N/A
Connection #02 (TCP)	09/26/2005	16:26:25.453	570.31	N/A	693	0	N/A
Connection #03 (UDP)	09/26/2005	16:26:25.453	570.31	50	701	0	N/A
Connection #01 (TCP)	09/26/2005	16:26:27.453	574.88	N/A	787	1	N/A
Connection #02 (TCP)	09/26/2005	16:26:27.453	574.88	N/A	792	1	N/A
Connection #03 (UDP)	09/26/2005	16:26:27.453	572.59	50	801	0	N/A
Connection #01 (TCP)	09/26/2005	16:26:29.437	574.88	N/A	883	1	N/A
Connection #02 (TCP)	09/26/2005	16:26:29.437	574.88	N/A	888	1	N/A
Connection #03 (UDP)	09/26/2005	16:26:29.437	572.59	50	897	0	N/A
Connection #01 (TCP)	09/26/2005	16:26:31.453	570.31	N/A	984	0	N/A
Connection #02 (TCP)	09/26/2005	16:26:31.453	570.31	N/A	986	0	N/A
Connection #03 (UDP)	09/26/2005	16:26:31.453	570.31	50	1000	0	N/A
Connection #01 (TCP) END	09/26/2005	16:26:31.984	570.31	N/A	984	1	N/A
Connection #02 (TCP) END	09/26/2005	16:26:32.000	568.03	N/A	987	0	N/A
***	***	***	***	***	***	***	***
Connection #03 (UDP)	09/26/2005	16:27:45.437	0.00	0	1000	0	N/A
Connection #03 (UDP)	09/26/2005	16:27:47.437	0.00	0	1000	0	N/A

10.6 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.



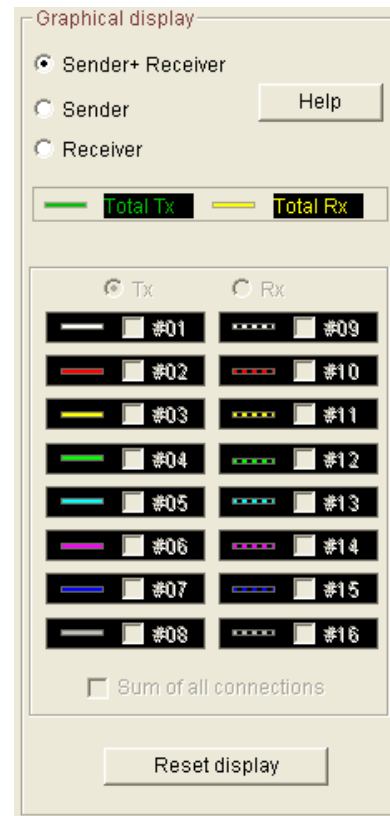
This snapshot shows 6 curves for connections #01 up to #06 for the Tx (Transmit) part of the Sender.

10.6.1 The Graphical Display object

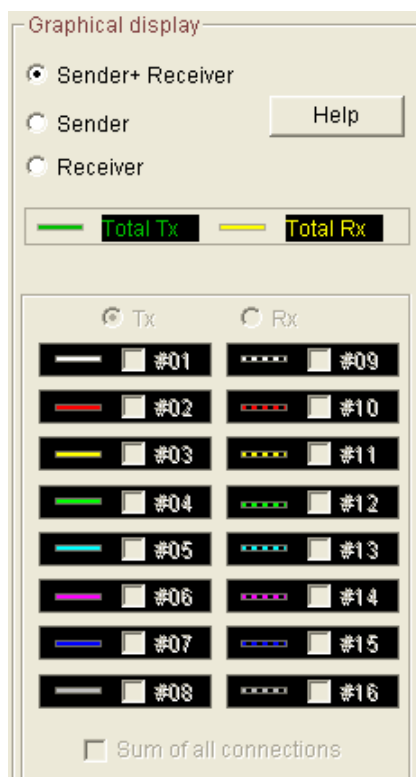
This object allows selecting curves to display with three choices:

- 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:

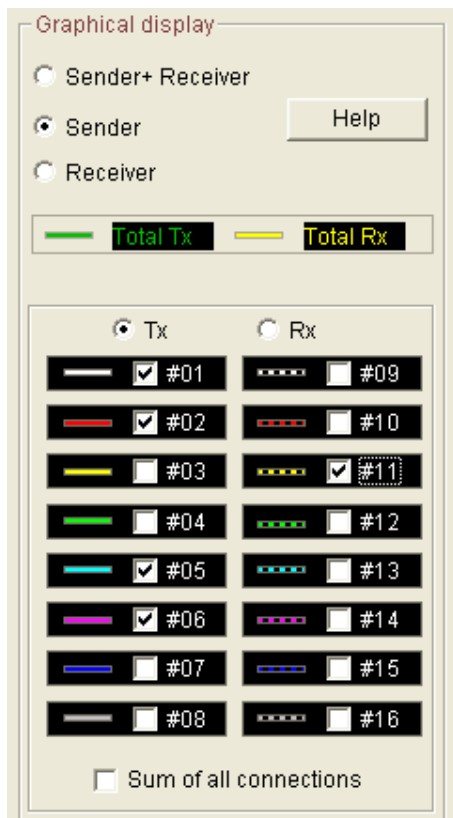


Total Tx (green curve) represents 'Total **LanTraffic V2** sending throughput' = total sending throughput of the Sender + total echoing throughput of the Receiver.

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

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

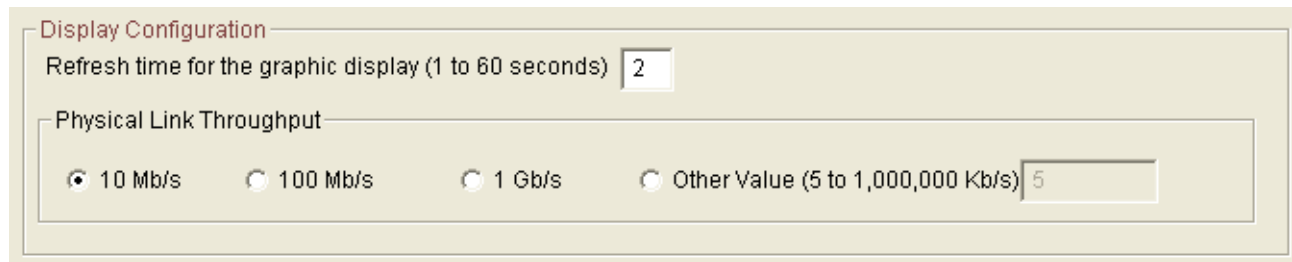
One or more connections can be selected (via the #i check box) and a colored curve is displayed for each selected connection. Up to 16 connections can be displayed on the graphic.

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

10.6.2 The Display Configuration object



Display Configuration

Refresh time for the graphic display (1 to 60 seconds)

Physical Link Throughput

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

Refresh time defines the time represented by one pixel on the graph. With value = 1, a new point is drawn every second. In this case, the graph shows an approximately 3-mn period.

Notice that **LanTraffic V2** 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 or any other value expressed in Kb/s limited to 1,000,000.

PART 11 Command Line Parameters

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

Example of a script:

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

General rule

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

Context filename

The context filename is a set of parameters for **LanTraffic V2**. This set can be saved in a file and reloaded later in such a way the user 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\file.ctx"`.
The " symbol is necessary to use spaces in filenames or directories.

Starting the "LanTraffic V2" Receiver part

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

Syntax: **-R**

Starting the "LanTraffic V2" Sender part

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

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

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

Where **Option** may be:

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

Stopping the "LanTraffic V2" Sender and Receiver parts

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

Syntax: **-STOP**

Unload the "LanTraffic V2" application

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

Syntax: **-UNLOAD**

Command line samples

- **LanTrafficV2 -R**

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

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

This command line launches **LanTraffic V2** 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 -SAI**

This command line starts **LanTraffic V2** 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** and load 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).

Error return code

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

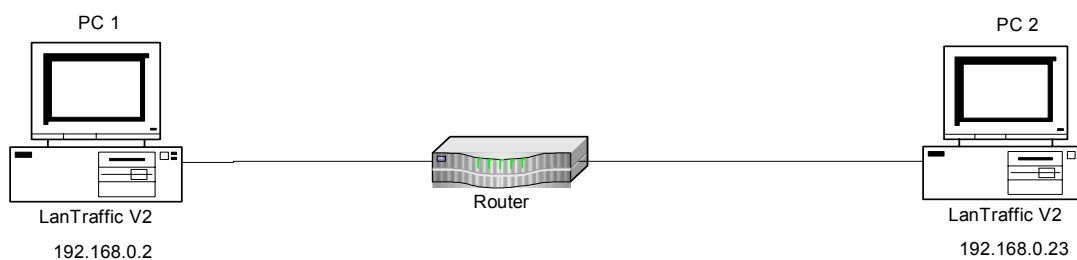
PART 12 How To Do ...

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

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

12.1 Checking router configuration

With this sample, it is shown how to check if a router is able to handle the TOS field in the IP header (see the TOS byte in paragraph 10.4.1.3.2.4).



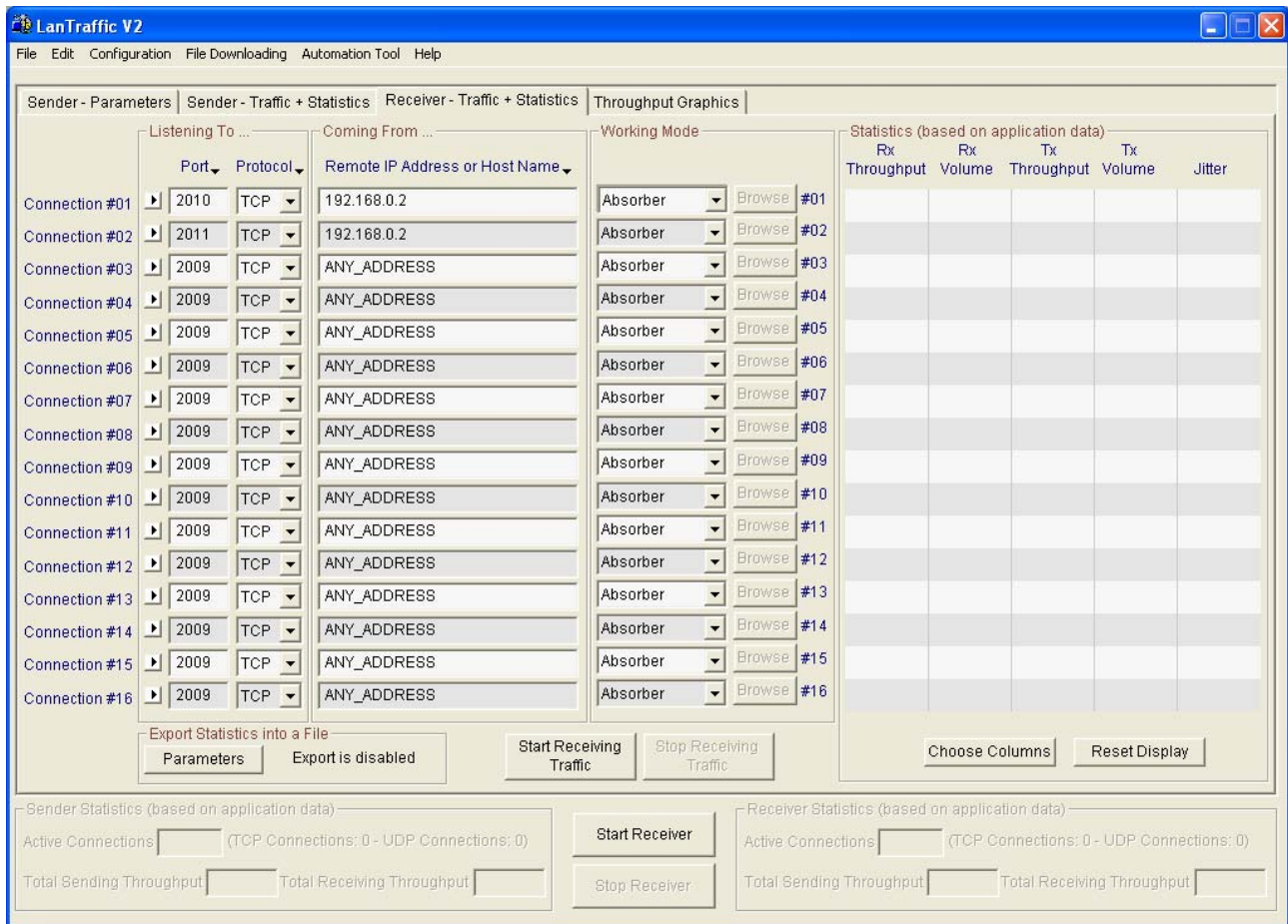
PC #1 is the Sender and PC #2 is the Receiver.

12.1.1 PC #2 parameters

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

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

The screenshot below shows the configuration at this point.



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

12.1.2 PC #1 parameters

PC #1 acts as the Sender.

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

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

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

LanTraffic V2 - Traffic Generator Parameters - Sender Unitary Testing Mode (connection #02)

Step1: Select the traffic generator type
First select the traffic generator which is going to be used on this connection.

☒ Packets Generator

Packets Generator Parameters

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

Packet Contents (00 to FF hexa byte)

☒ Fixed

☐ Randomized min max

☐ Alternated value-1 value-2

☐ Increasing / Decreasing min max step

☐ Mathematical Law

Law: Data volume to send: Edit...

Uniform law
Range : [9.77 KB , 2.38 MB]

☐ File to send

Filename: Browse

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

Step2: Specify data size and packets parameters
In this step, define data size and packets parameters as well as the delay between each sent packet or specify values for some IP header fields.

TCP or UDP Data Size (1 to 65,535 bytes)

☒ Fixed

☐ Randomized min max

☐ Alternated size-1 size-2

☐ Increasing / Decreasing min max step

Inter Packet Delay (0 to 9,999 ms)

☒ Fixed (See FOREWARNINGS menu please)

☐ Randomized min max

☐ Alternated value-1 value-2

☐ Increasing / Decreasing min max step

☐ Mathematical Law

Law: Edit...

RTT Option ☐ Yes ☒ No

TOS (1 hexa byte) Value

Time To Live (TTL) Value

Step 3 (Optional): Enable a throughput limit
When one of these two options is selected, LanTraffic V2 generates the traffic with best effort to respect the throughput chosen.

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

☐ Use value ☒ Inter Packet Delay adjusted by LanTraffic V2 automatically

☐ TCP or UDP Data Size adjusted by LanTraffic V2 automatically

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

☐ Use value (except for TCP connection)

OK Cancel Help

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

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

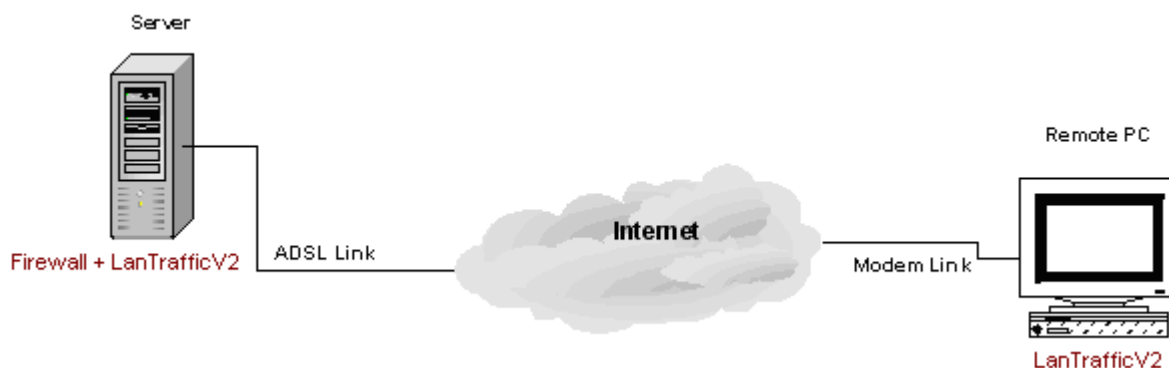
12.1.3 What should happen?

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

12.2 Checking a firewall configuration

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

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



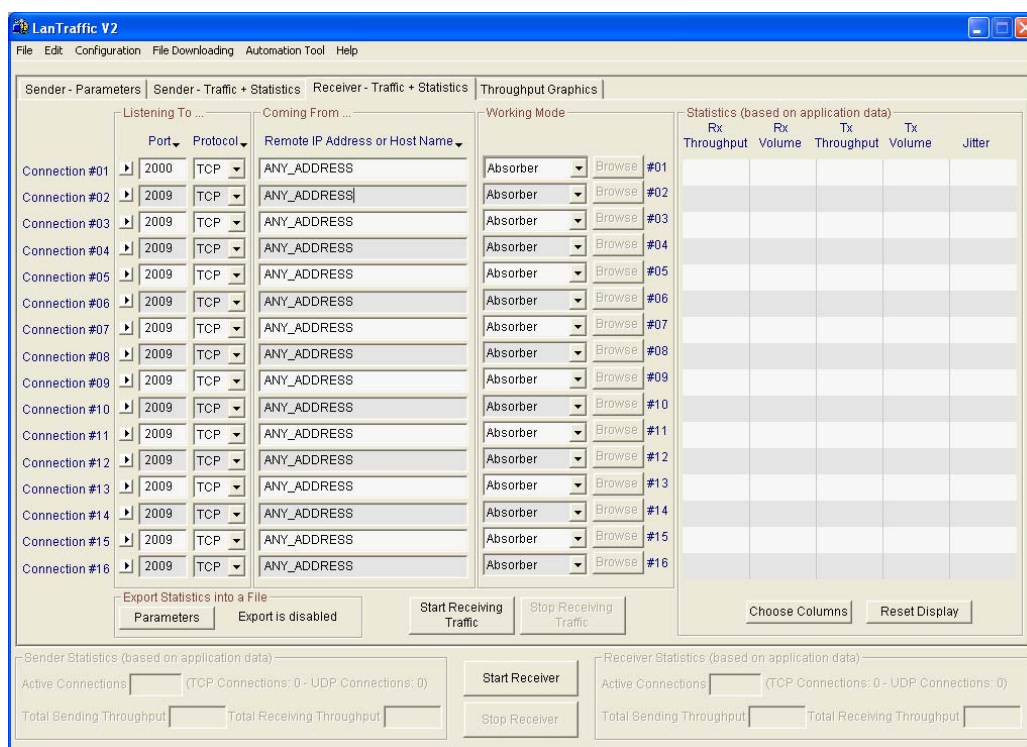
12.2.1 LanTraffic V2 parameters on the server

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

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

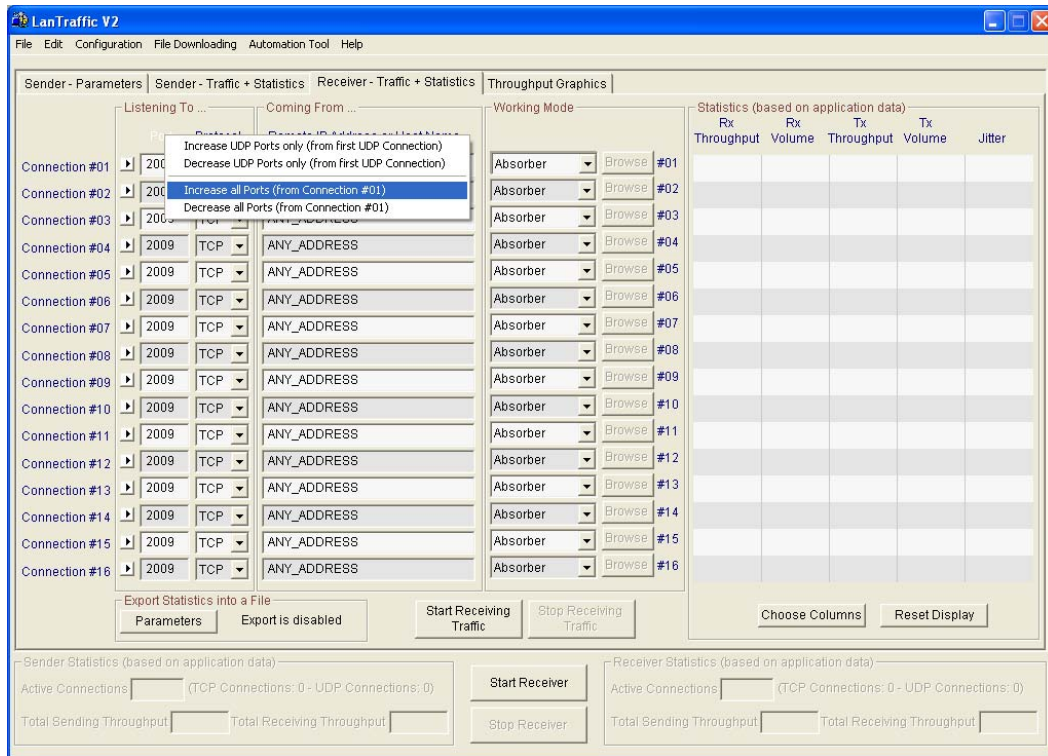
In this example we check the TCP connections port from 2000 to 2015. You can adapt this range and the protocol to your specific environment.

Let's start with the connection #1.



To access incoming TCP connection coming from any Sender, the IP address 'ANY_ADDRESS' has been selected. The port number is 2000 and the protocol is configured with TCP.

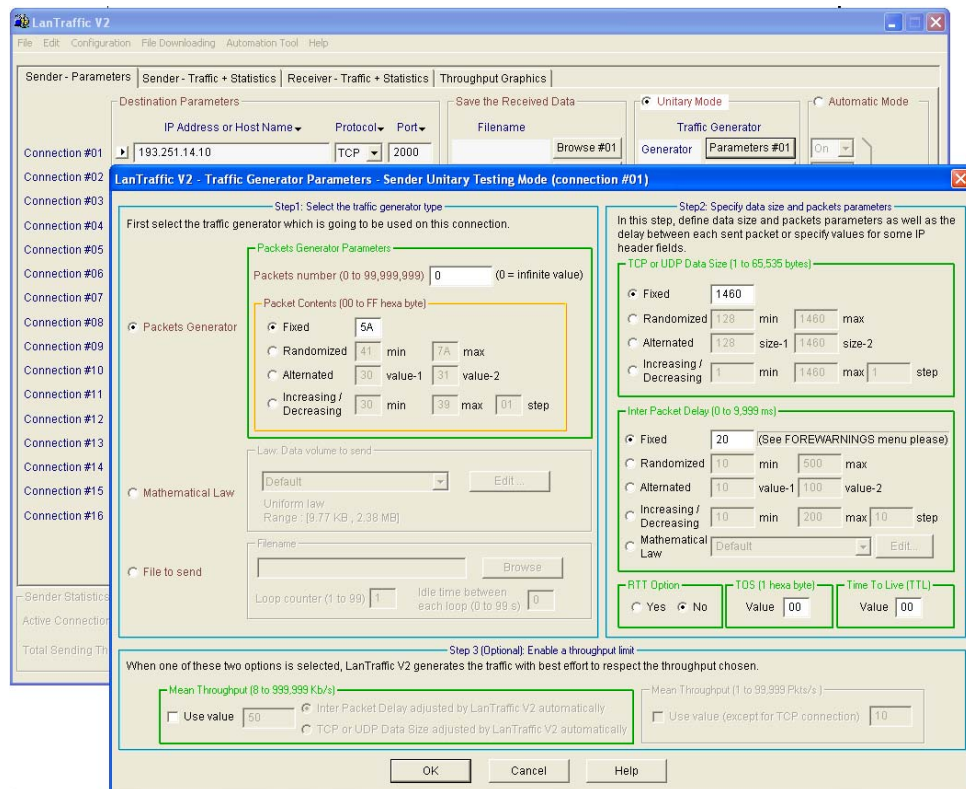
To easily increase the port number for each connection, you can use the 'Port floating menu' as shown below:



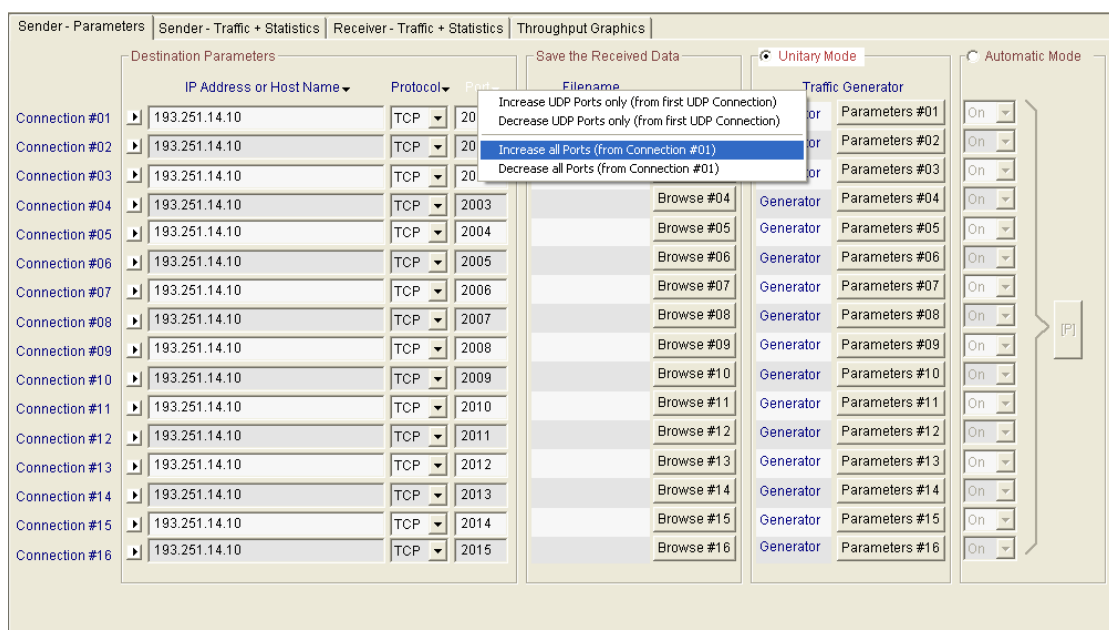
You are ready to start the Server by pressing the 'Start Receiving Traffic' button.

12.2.2 LanTraffic V2 parameters for the Remote PC

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



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



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

12.2.3 What result can you expect?

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

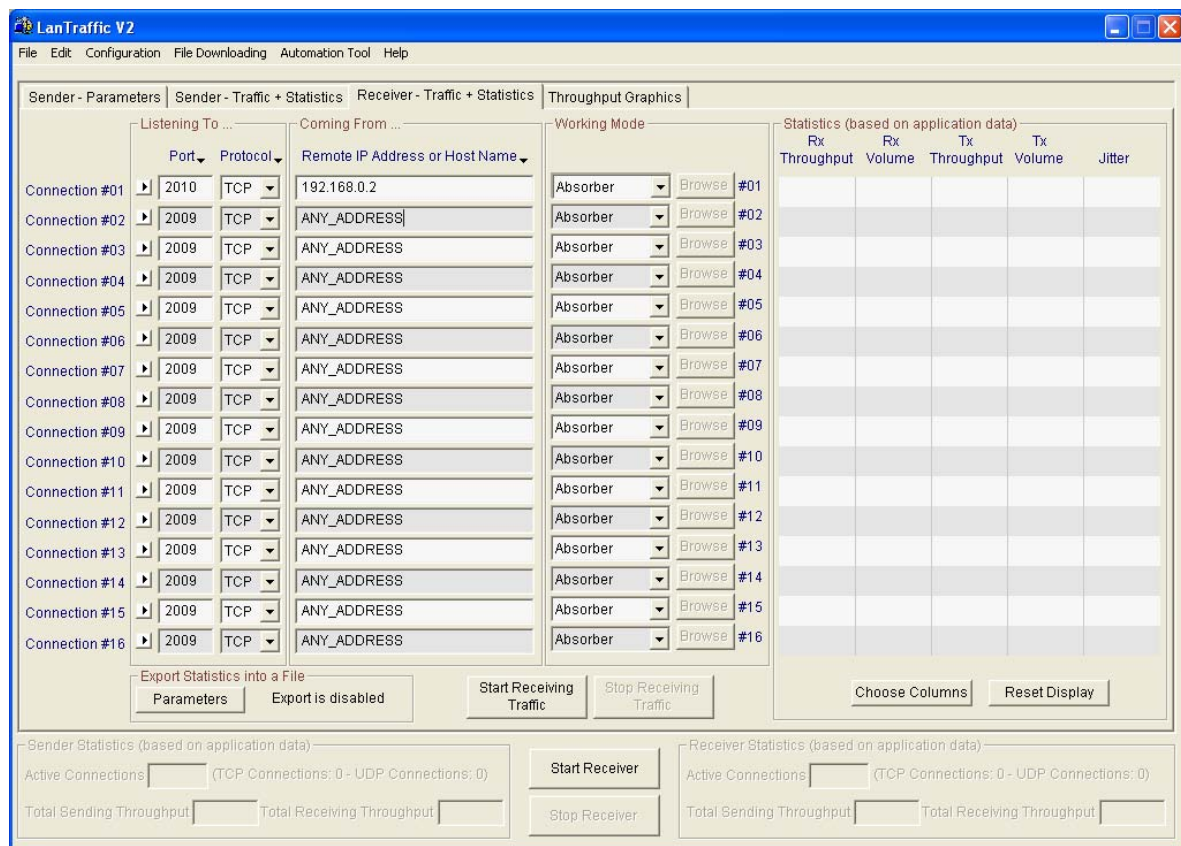
12.3 Checking the best throughput

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



12.3.1 PC #2 parameters

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



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

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

12.3.2 PC #1 parameters

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

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

LanTraffic V2 - Traffic Generator Parameters - Sender Unitary Testing Mode (connection #01)

Step1: Select the traffic generator type
First select the traffic generator which is going to be used on this connection.

Packets Generator Parameters

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

Packet Contents (00 to FF hexa byte)

☒ Fixed min max

☐ Randomized value-1 value-2

☐ Alternated min max step

☐ Increasing / Decreasing

Law: Data volume to send

☐ Mathematical Law

Uniform law
Range : [9.77 KB , 2.38 MB]

☐ File to send

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

Step2: Specify data size and packets parameters
In this step, define data size and packets parameters as well as the delay between each sent packet or specify values for some IP header fields.

TCP or UDP Data Size (1 to 65,535 bytes)

☒ Fixed

☐ Randomized min max

☐ Alternated size-1 size-2

☐ Increasing / Decreasing min max step

Inter Packet Delay (0 to 9,999 ms)

☒ Fixed (See FOREWARNINGS menu please)

☐ Randomized min max

☐ Alternated value-1 value-2

☐ Increasing / Decreasing min max step

☐ Mathematical Law

RTT Option ☐ Yes ☒ No

TOS (1 hexa byte) Value

Time To Live (TTL) Value

Step 3 (Optional): Enable a throughput limit
When one of these two options is selected, LanTraffic V2 generates the traffic with best effort to respect the throughput chosen.

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

☐ Use value ☒ Inter Packet Delay adjusted by LanTraffic V2 automatically

☐ TCP or UDP Data Size adjusted by LanTraffic V2 automatically

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

☐ Use value (except for TCP connection)

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

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

Columns 'Throughput' for the PC #2 Sender and PC #1 Receiver will show throughputs. Best throughput depends mainly on the CPU, the memory and the NIC quality.

If the PCs you are using are different, **choose the most powerful PC as Receiver.**

12.4 ADSL connection simulation

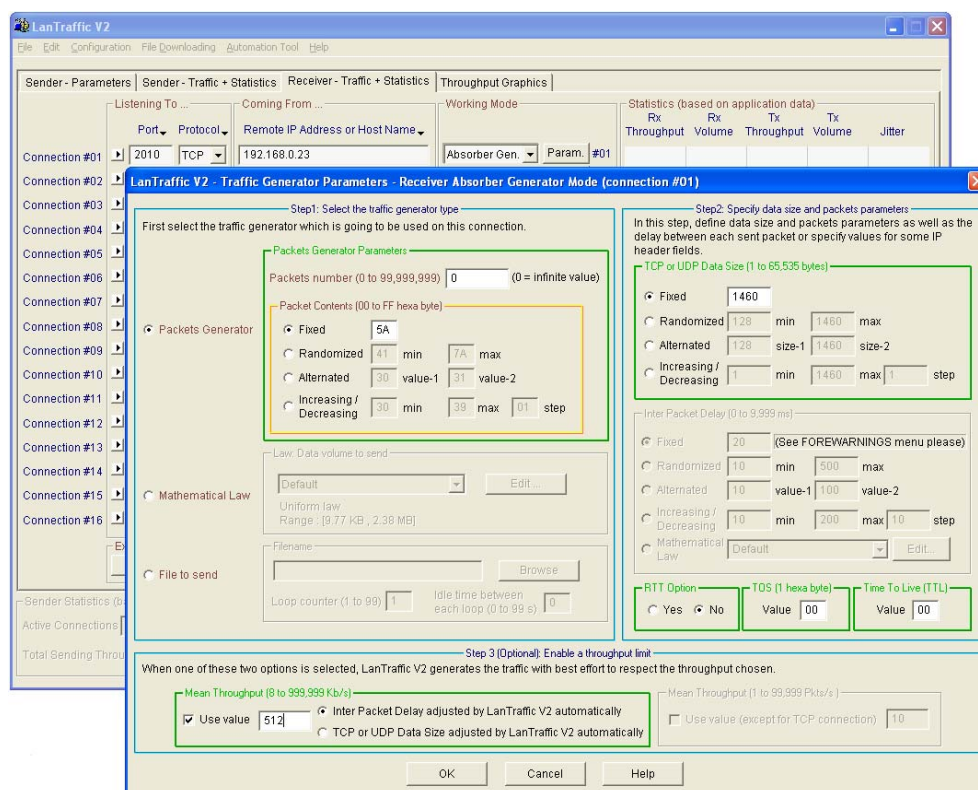
LanTraffic V2 can be used to simulate an ADSL connection, which is asymmetrical by nature. The next figure is one of those that can be used. Hub or router may also be used to connect the 2 PCs.



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

12.4.1 PC #2 parameters

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



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

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

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

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

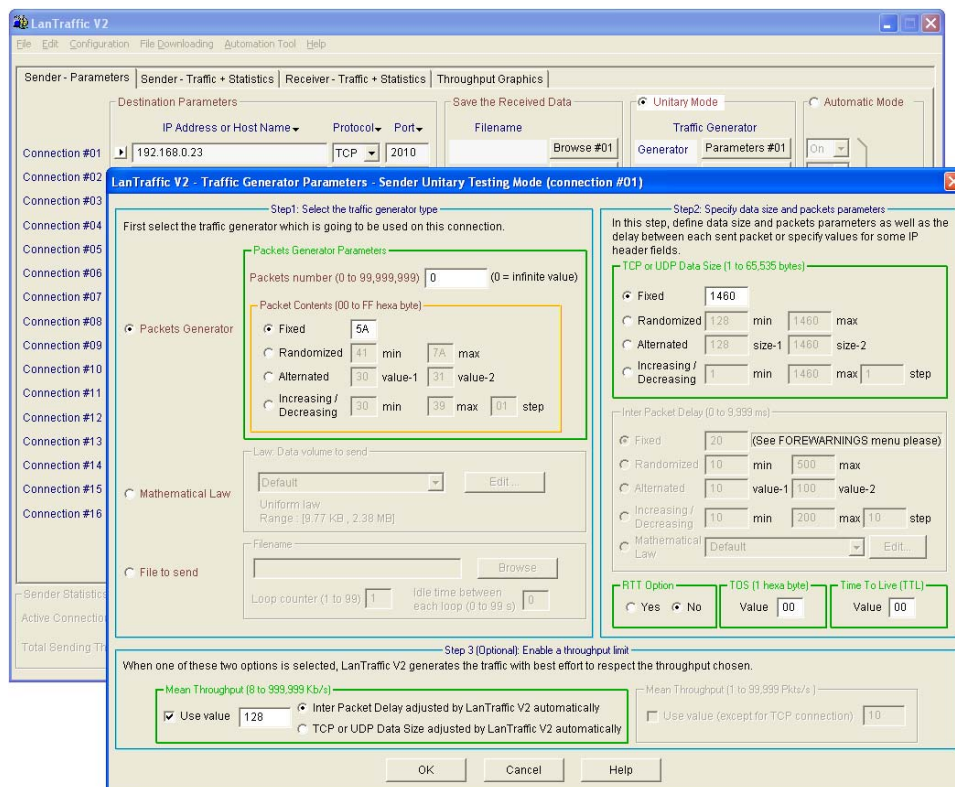
To establish the connection go to the PC #1.



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

12.4.2 PC #1 parameters

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



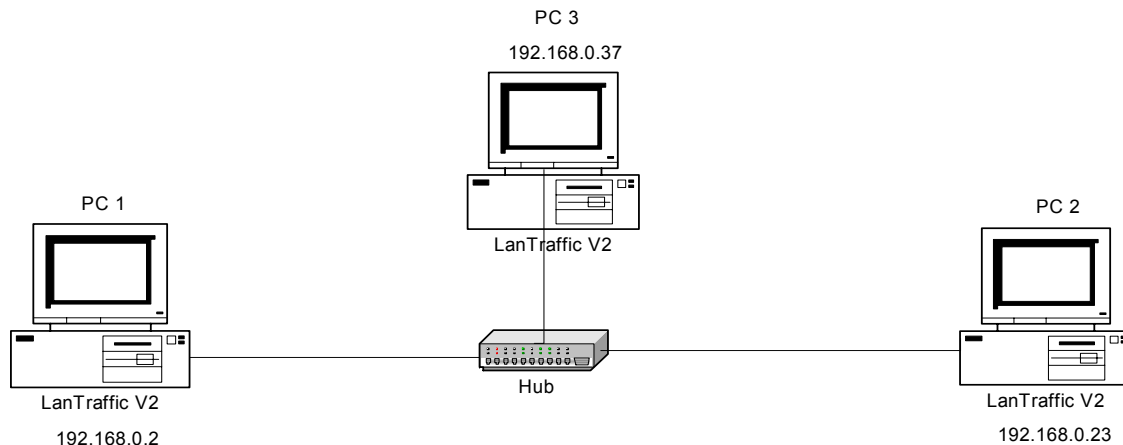
The connection #01 will be used in this example. Enter the IP address of PC #2 (192.168.0.23), select the TCP protocol and enter the port number 2010 (same as PC #2). To change the traffic generator, click on the 'Parameters #01' button. Select the unlimited packet number with 0 in the packet number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

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

12.5 Generating multicast IP traffic

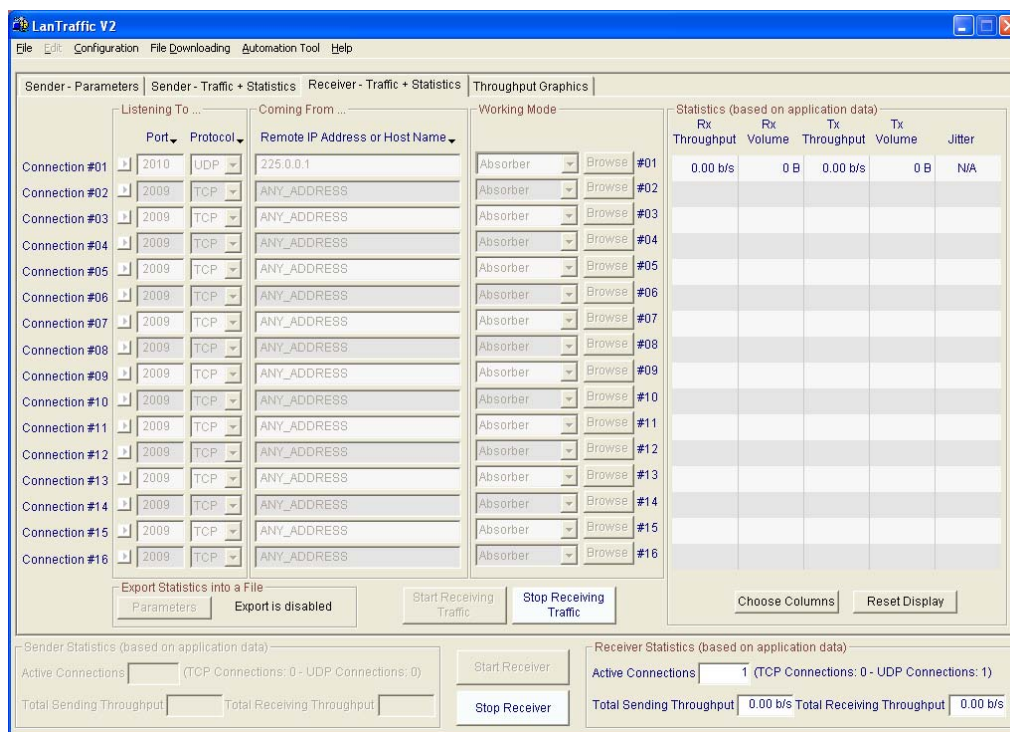
The next figure shows how to generate IPv4 multicast traffic.

Multicast traffic is based on the UDP protocol. Its characteristic is that multiple receivers can get data from one source – or sender – just indicating from which source they would like to receive data.



12.5.1 PC #2 and PC #3 parameters

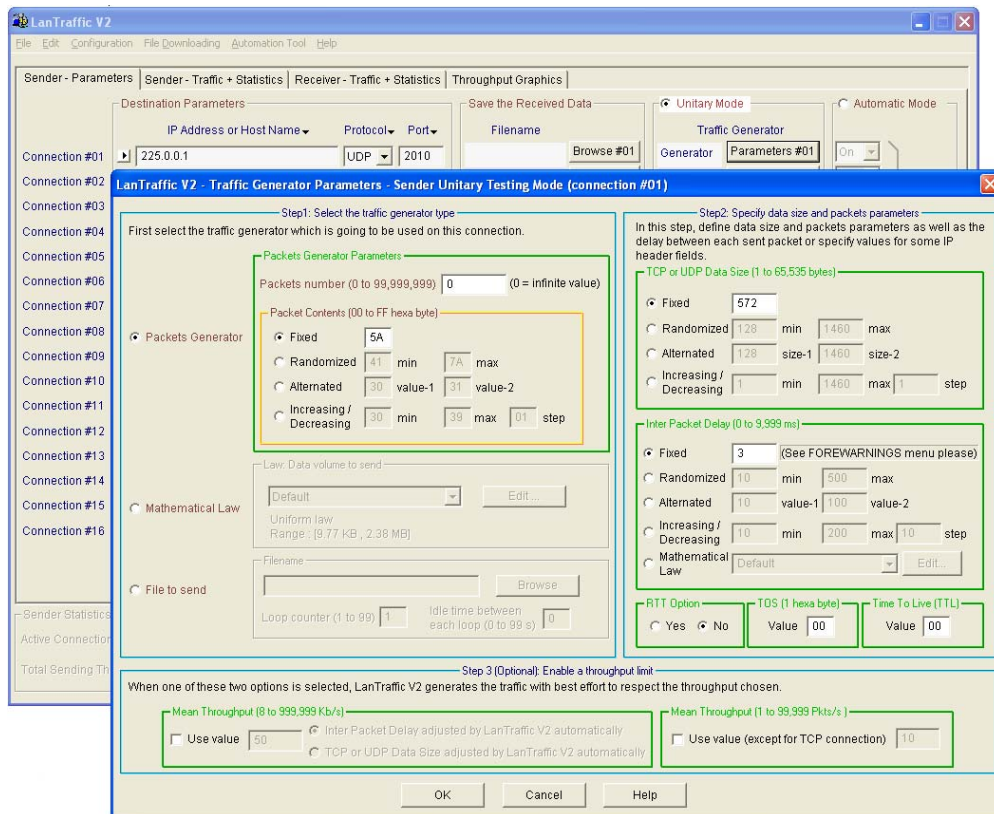
Let us assume PC #2 and PC #3 are set in the Receiver mode, whereas PC #1 is the Sender (server). Start **LanTraffic V2** on PC #2 and select the "Receiver – Traffic + Statistics" tab.



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

12.5.2 PC #1 parameters

PC #1 is used as the Sender. Start **LanTraffic V2** and select the "Sender – Parameters" tab.



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

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

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

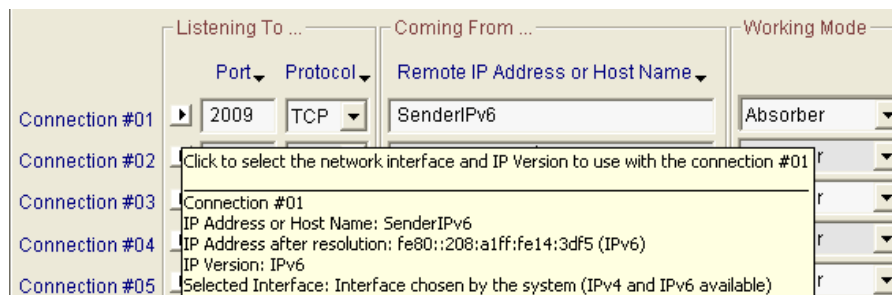
12.6 IPV6 connection

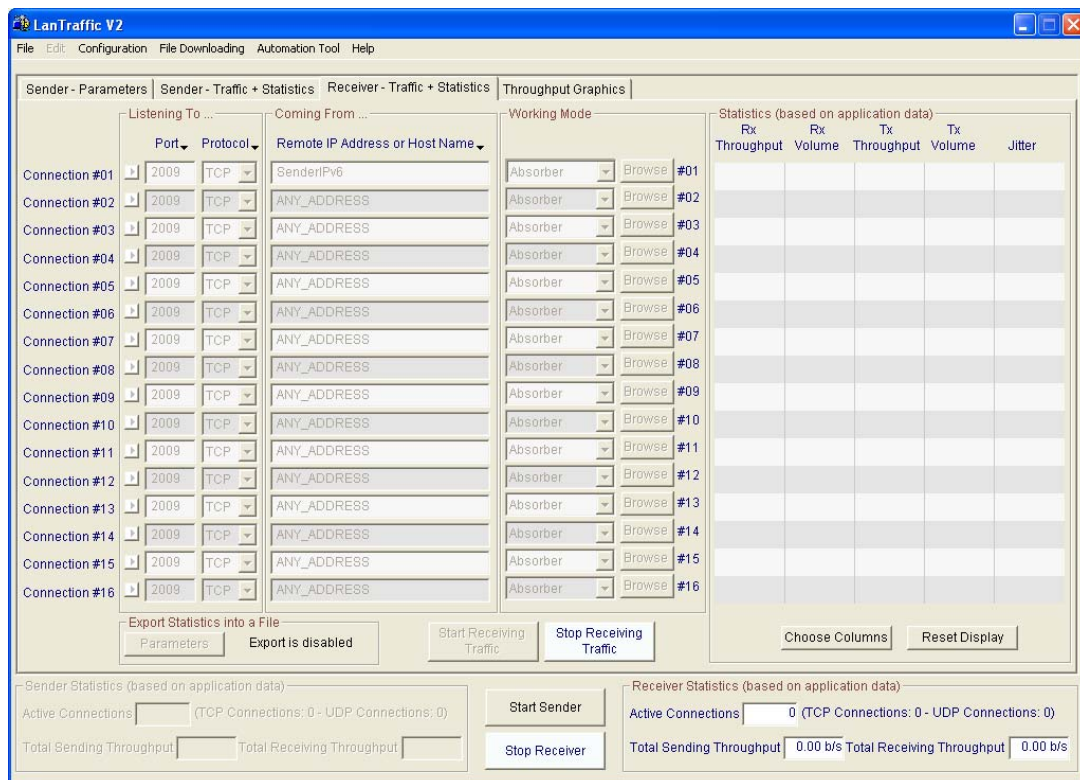
To check the IPv6 throughput between two PCs, you may use a crossed-cable or a switch as shown below.



12.6.1 PC #2 parameters

Start "LanTrafficV2" on PC #2 and select the "Receiver - Traffic + Statistics" tab. Enter the canonical name of the IPv6 sender. You may check parameters using the black arrow tooltip by moving the mouse over the arrow of the connection #01.



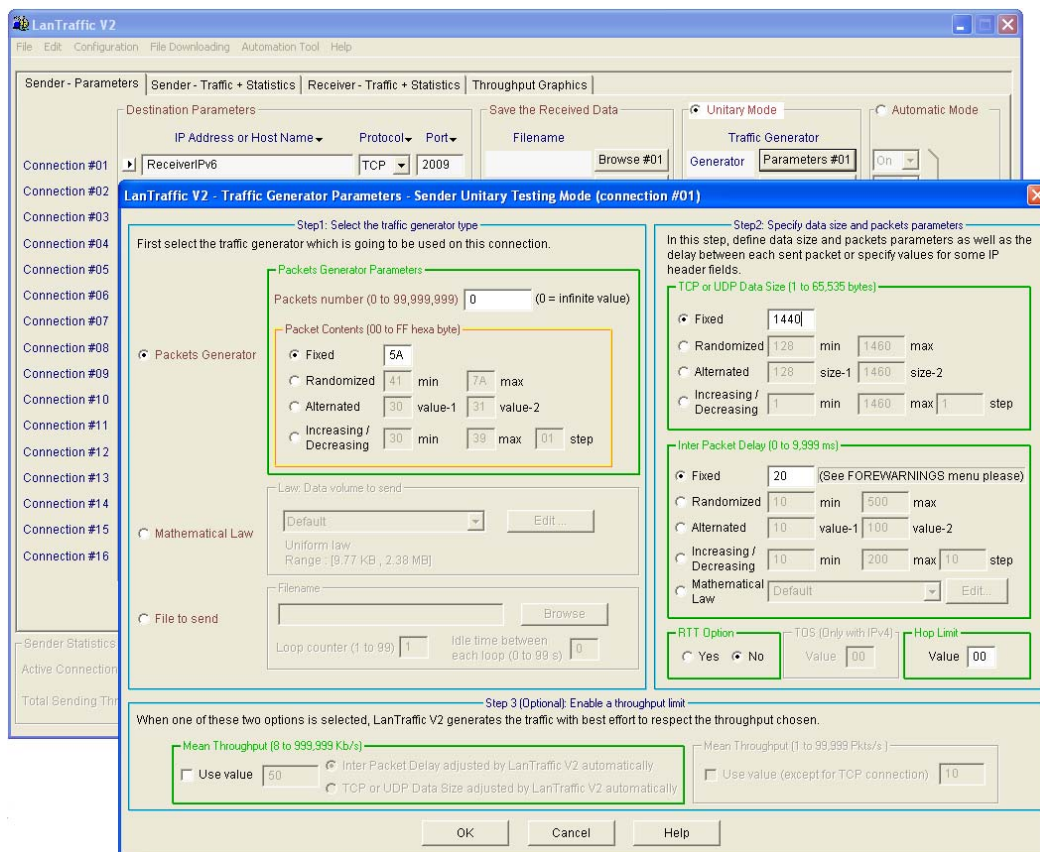


Assuming the connection #01 will be used, the port number here is arbitrary selected to 2009. Select the TCP protocol and the receiving working mode to 'Absorber'. Start the Receiver by pressing the 'Start Receiving Traffic' button.

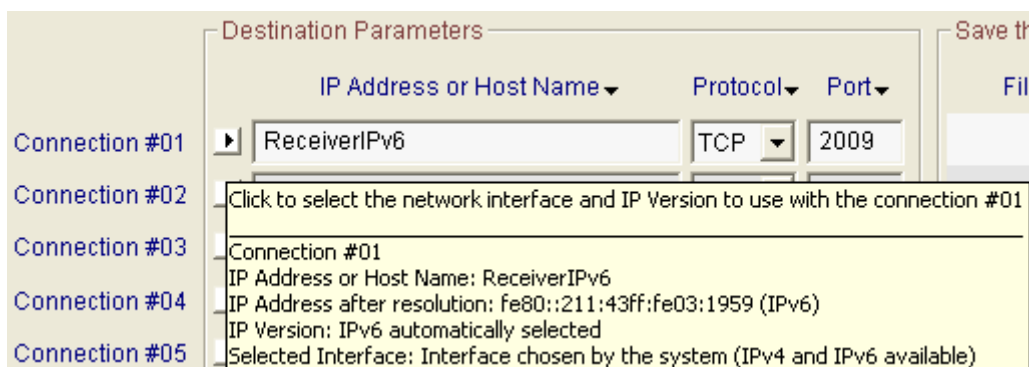
12.6.2 PC #1 parameters

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

The connection #01 will be used in this example. Enter a canonical IPv6 address for PC #2, select the TCP protocol and enter the port number 2009 (same as PC #2). To change the traffic generator, click on the 'Parameters #01' button.



Select the unlimited packet number with 0 in the packet number field; the packet size is the best with 1440 bytes long. The inter-packet delay should be 0 for the maximum throughput. The summary tooltip may be used to check the IP version parameters.



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

The throughput columns for the PC #2 Sender and PC #1 Receiver will show the throughputs. Best throughput depends mainly on the CPU, the memory and the NIC quality.

If the PCs you are using are different, **choose the most powerful PC as the Receiver.**

12.7 Source/Local IP Address and Interface requirements

With **LanTraffic V2** version 2.4, interface selection is not required anymore to carry out unicast or multicast exchanges.

“LanTraffic V2” acting as:	Sender (UDP, TCP and ICMP)		Receiver (UDP and TCP)	
	IPv4	IPv6	IPv4	IPv6
Unicast exchange	<i>Interface selection is not required</i>	Interface selection is required	<i>Interface selection is not required</i>	<i>Interface selection is not required</i>
Multicast exchange	<i>Interface selection is not required</i>	<i>Interface selection is not required</i>	<i>Interface selection is not required</i>	<i>Interface selection is not required</i>

Consequences when an Interface is selected

For the **LanTraffic V2 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 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**.
2. With TCP protocol, **LanTraffic V2** 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 13 Annexes

13.1 Mathematical laws used by LanTraffic V2

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

The mathematical laws are used:

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

Hereafter is a detailed presentation of each mathematical law.

13.1.1 Uniform law

- *Presentation*

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

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

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

- *Mathematical function*

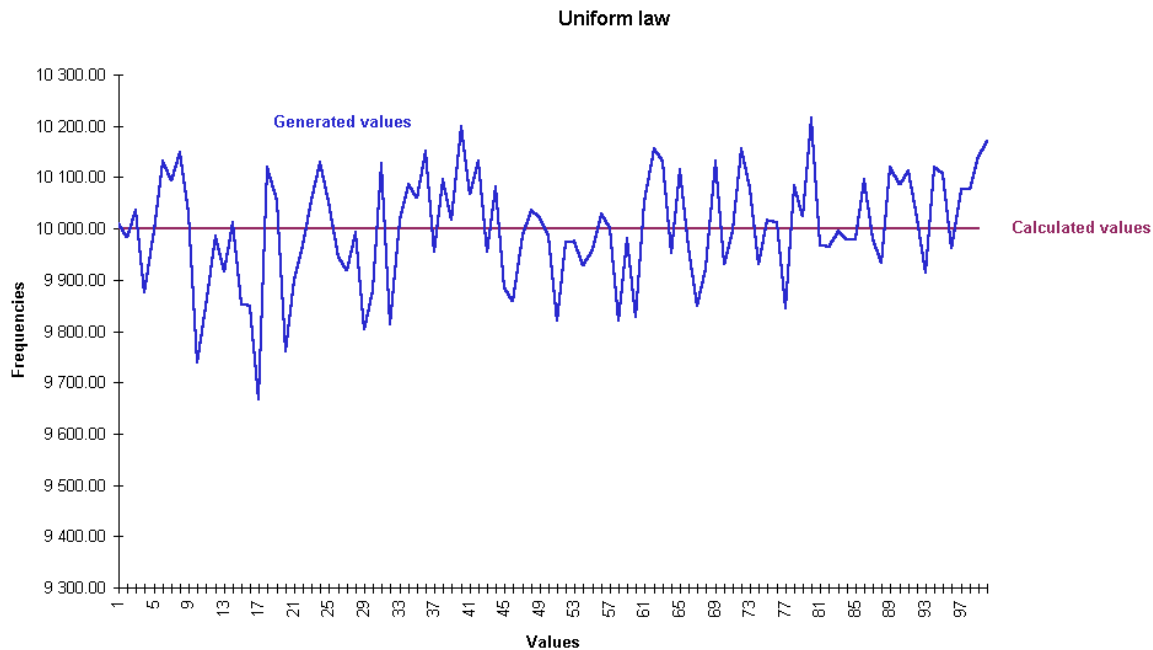
Uniform law on (α, β) range

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

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

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

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



13.1.2 Exponential law

- *Presentation*

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

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

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

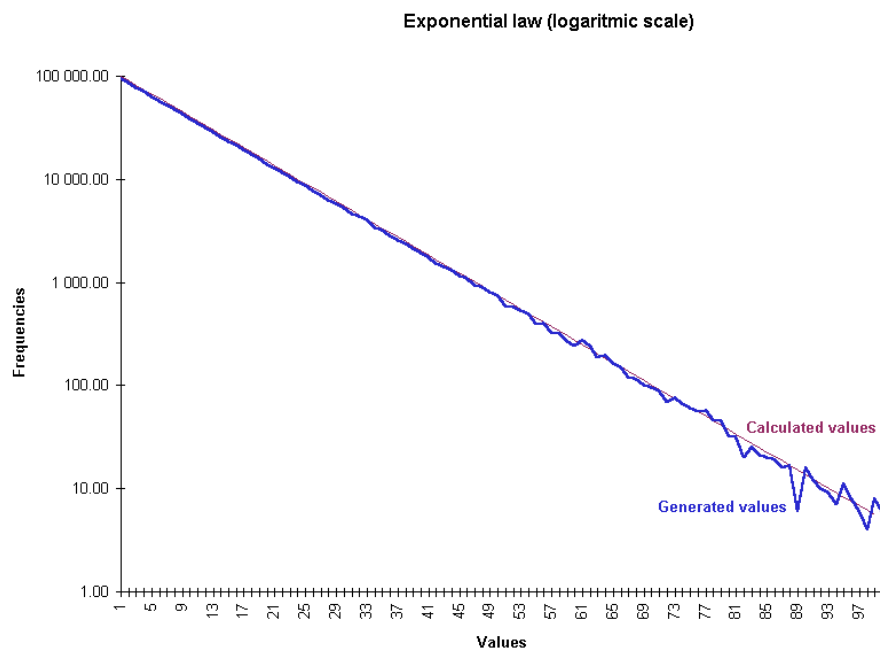
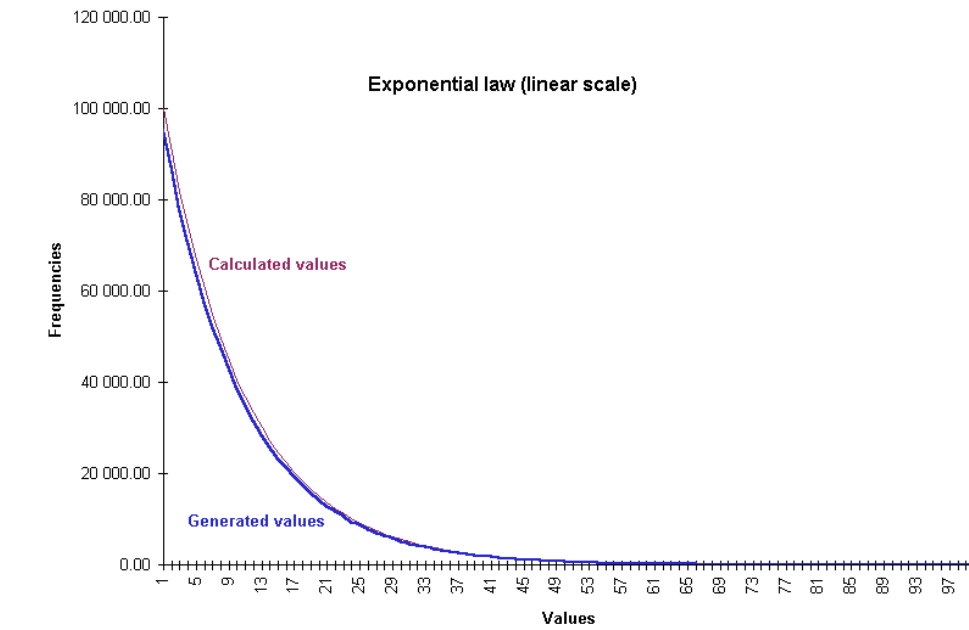
- *Mathematical function*

Exponential law ($\lambda > 0$)

$$\begin{aligned} f(x) &= \lambda e^{-\lambda x} & \text{if } x \geq 0 \\ f(x) &= 0 & \text{if } x < 0 \end{aligned}$$

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

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



❖ *Exponential law - Table of generated values:*

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

13.1.3 Pareto Law

- *Presentation*

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

The Pareto law is based on two parameters: a and β . a unit is the final unit of the volume. β does not have unit because it represents a coefficient of variation of result around the a value.

The following values have been noticed:

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

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

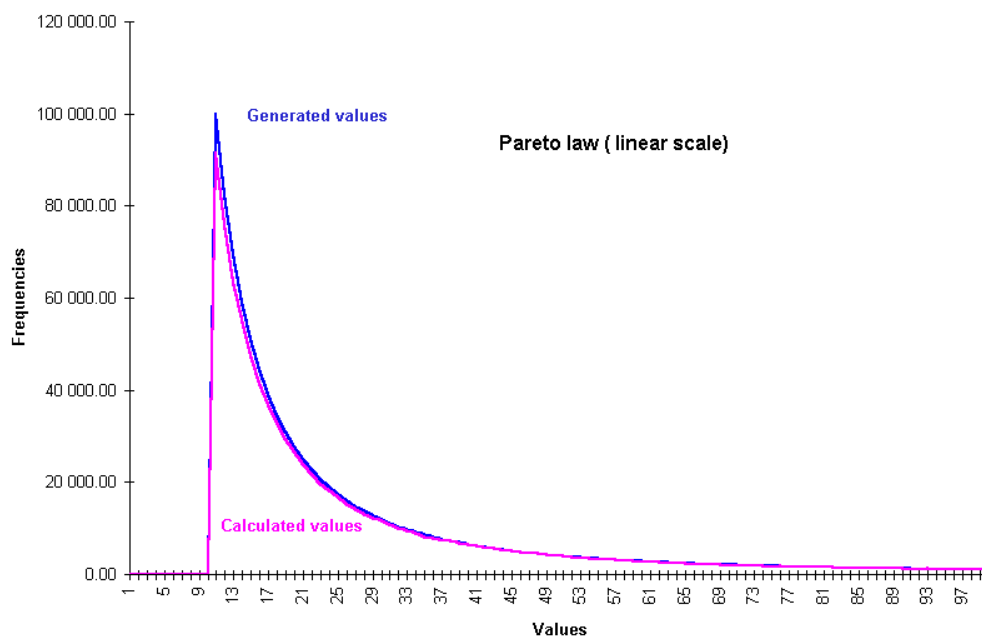
- *Mathematical function*

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

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

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

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



13.1.4 Gauss law

- *Presentation*

The Gauss law has two parameters: μ (average) and σ (standard deviation).

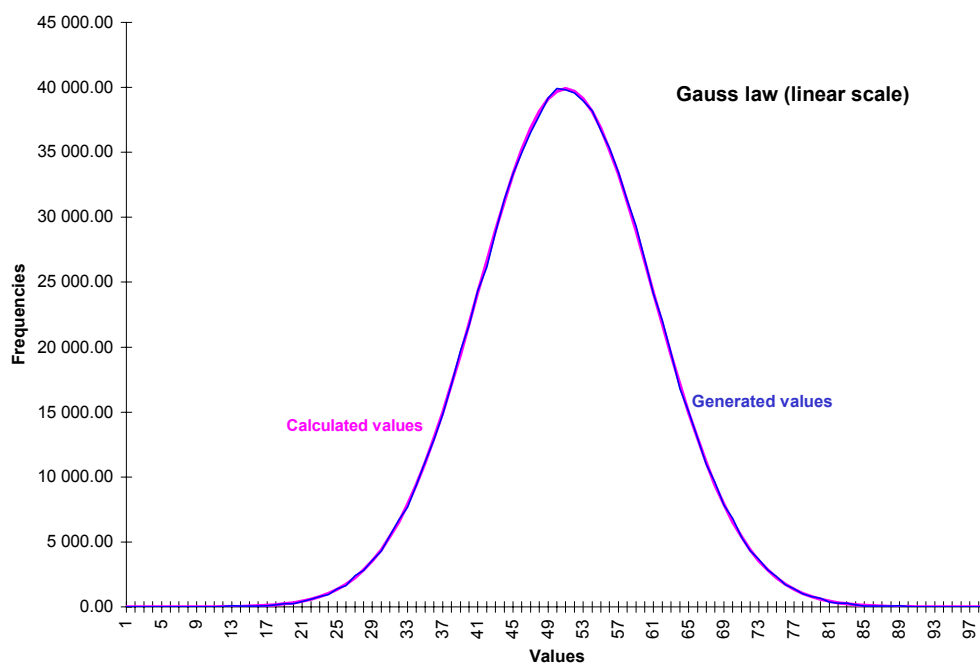
With this law, unit used is millisecond for starting time connection generation laws and byte for data volume to send laws.

- *Mathematical function*

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

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

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



13.2 LanTraffic V2 Traces

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

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

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

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



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

13.3 LanTraffic V2 configuration parameters saved in the Registry

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

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



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

13.3.1 General configuration parameters

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

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



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

13.3.2 Help configuration parameters



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

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

13.4 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 = 20 ms
		RTT option	No
		TOS 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 Buffer size	
Receive buffer size	8192
Transmit buffer size	8192

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]