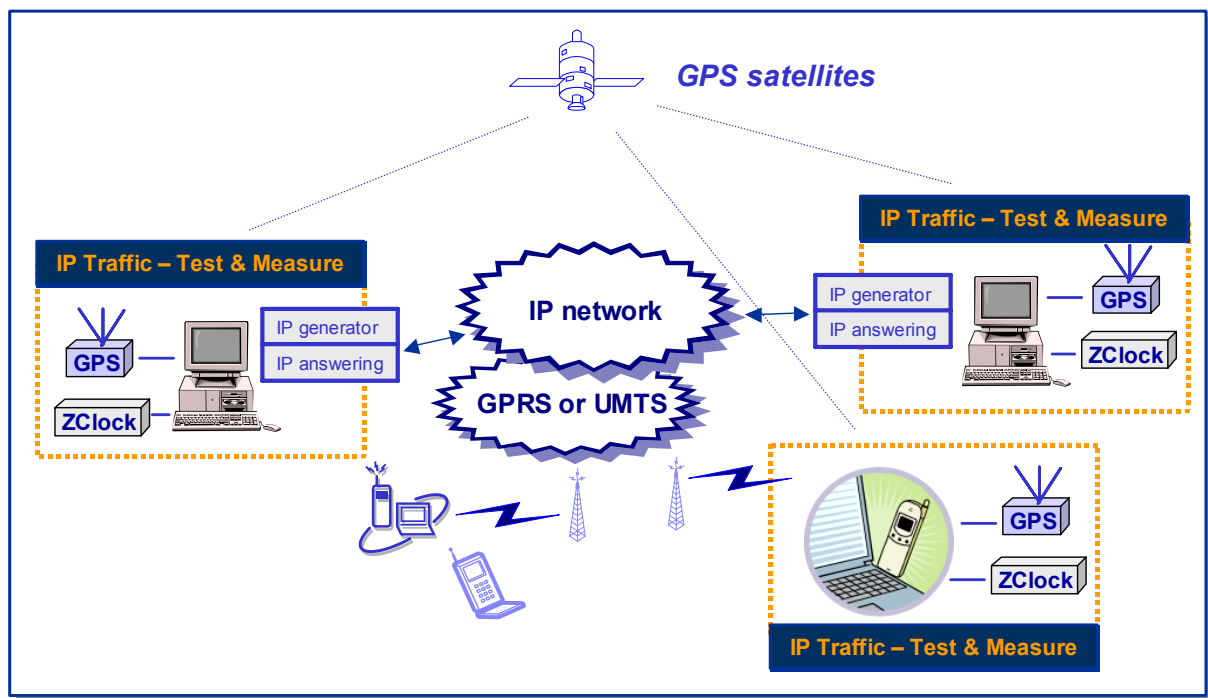




# ***IP Traffic -Test & Measure***

***Version 2.3***

**Traffic Generator and Measurement Tool for Wired,  
Wireless, Satellite, PLC or Mobile IP Networks**



## ***User Guide***

## **WARNING**

*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.*

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

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

*This guide allows the user to discover "IP Traffic – Test & Measure" and is not an exhaustive user manual.*

## **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>  
E-mail: [contact@zti-telecom.com](mailto:contact@zti-telecom.com) or [contact@zti.fr](mailto:contact@zti.fr) (marketing & sales)  
[support@zti-telecom.com](mailto:support@zti-telecom.com) or [support@zti.fr](mailto:support@zti.fr) (technical support)

Copyright (C) ZTI 2000-2005  
France Telecom licensed product.  
Reproduction rights reserved.

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.

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

## Software License Agreement

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

### **COPYRIGHT**

*The enclosed Software and documentation (here after called the Products) remains ZTI property.*

The products are protected by French copyright laws and international treaties.

ZTI grants you the right to use the products according to the following:

### **USE OF THE SOFTWARE**

You may:

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

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

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

### **SOFTWARE PROTECTION**

The "IP Traffic – Test & Measure" software is licensed on a per workstation basis. You will need to purchase a separate license for each machine that you install it. Each licensed copy of the software installed on a workstation has a unique Site Code, which requires the corresponding unique Site Key to be entered before the tool is operational.

### **LIMITED WARRANTY**

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

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

In no event, ZTI will be liable for any kind of direct or indirect damages caused by the Products.

### **JURISDICTION**

This agreement will be governed by French laws.

All disputes arising out of or in connection with this Agreement shall be finally settled by the court of GUINGUAMP in France.

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

## Table of contents

<b>Part 0: Preface</b>	<b>6</b>
0.1 ORGANIZATION OF THIS MANUAL .....	6
0.2 MINIMUM SYSTEM REQUIREMENTS .....	7
0.3 TECHNICAL SUPPORT .....	7
<b>Part 1: Product Overview</b>	<b>8</b>
1.1 GENERAL DESCRIPTION .....	8
1.2 ARCHITECTURE .....	11
1.3 HARDWARE OPTIONS AVAILABLE .....	12
1.4 "IP TRAFFIC – TEST & MEASURE" KEY FEATURES .....	13
1.5 REFERENCE .....	18
<b>Part 2: Install and Uninstall "IP Traffic - Test &amp; Measure"</b>	<b>19</b>
2.1 INSTALL "IP TRAFFIC - TEST & MEASURE" FROM A DOWNLOADED TRIAL VERSION .....	19
2.2 INSTALL "IP TRAFFIC - TEST & MEASURE" FROM THE CD-ROM.....	23
2.3 UNINSTALL "IP TRAFFIC - TEST & MEASURE" .....	26
<b>Part 3: License Configuration and License Transfers</b>	<b>27</b>
3.1 TO CONFIGURE A LICENSE .....	27
3.2 LICENSE TRANSFERS .....	29
3.2.1 <i>Direct Transfer: move the license from one local directory to another</i>	30
3.2.2 <i>Transfer by media (floppy disk or USB key) from a source PC to a target PC</i>	31
3.3 KILL A LICENSE .....	37
<b>Part 4: Hardware Installation (GPS Kit and ZClock)</b>	<b>38</b>
4.1 CONFIGURATION 1: "IP TRAFFIC – TEST & MEASURE" + GPS KIT .....	38
4.2 CONFIGURATION 2: "IP TRAFFIC – TEST & MEASURE" + ZCLOCK.....	39
4.3 CONFIGURATION 3: "IP TRAFFIC – TEST & MEASURE" + GPS KIT + ZCLOCK .....	40
<b>Part 5: Graphical User Interface</b>	<b>41</b>
5.1 MAIN WINDOW.....	41
5.2 DISPLAY GENERAL RULES OF THE "IP TRAFFIC – TEST & MEASURE" GUI.....	42
5.3 USED UNITS IN INFORMATION DISPLAY .....	43
5.3.1 <i>Volume units</i>	43
5.3.2 <i>Throughput units</i>	43
5.3.3 <i>Duration units</i>	43
<b>Part 6: Using "IP Traffic – Test &amp; Measure"</b>	<b>44</b>
6.1 MAIN STEPS .....	44
6.2 LAUNCH "IP TRAFFIC – TEST & MEASURE" .....	45
6.3 MENU DESCRIPTION .....	46
6.3.1 <i>File Menu</i>	46
6.3.2 <i>Edit menu</i>	47
6.3.3 <i>Configuration menu</i>	49
6.3.4 <i>Tools menu</i>	57
6.3.5 <i>File downloading menu</i>	58
6.3.6 <i>Automation Tool menu</i>	60
6.3.7 <i>Help Menu</i>	60
6.3.8 <i>Operating mode menu</i>	63
6.4 MAIN WINDOW: THE FIVE TABS.....	64
6.5 MAIN WINDOW: THE ACTIVITY DISPLAY.....	64
6.6 MAIN WINDOW: THE GENERAL COMMANDS.....	65

6.7 THE 'IP GENERATOR – PARAMETERS' TAB .....	65
6.7.1 Destination Parameters .....	67
6.7.2 Configure the unitary mode .....	72
6.7.3 Configure the automatic mode .....	82
6.7.4 Configure the replay sniffed traffic mode .....	86
6.8 THE 'IP GENERATOR – TRAFFIC + STATISTICS' TAB .....	87
6.8.1 Destination Parameters area .....	88
6.8.2 Statistics (Application Level) .....	88
6.8.3 Run an unitary testing session .....	94
6.8.4 Run an automatic testing session .....	95
6.8.5 Run a replay traffic session .....	96
6.8.6 Using ICMP capacity of the Traffic Generator .....	97
6.9 THE 'IP ANSWERING' TAB .....	98
6.9.1 Duplicate parameters of a connection onto others .....	98
6.9.2 Listening To ... .....	99
6.9.3 Coming From ... .....	103
6.9.4 Receiving working mode .....	104
6.9.5 'IP Answering' Statistics .....	107
6.9.6 "Export IP Answering statistics in a file" parameters .....	109
6.10 THE 'TRAFFIC SNIFFER' TAB .....	114
6.10.1 Capture Parameters .....	115
6.10.2 Capture sniffed traffic into a file .....	117
6.10.3 Run analysis algorithm .....	117
6.11 THE 'TRAFFIC OBSERVER' TAB .....	119
6.11.1 "IP Traffic – Test & Measure": On-line and Off-line modes for statistics .....	120
6.11.2 Objects and command buttons .....	121
6.11.3 Values and statistics display .....	134
<b>Part 7: Calculation Mode for the Statistics</b> .....	<b>141</b>
7.1 INTRODUCTION .....	141
7.2 STATISTICS COMPUTED BY "IP TRAFFIC – TEST & MEASURE" .....	142
7.2.1 Reference points to compute the statistics .....	142
7.2.2 Statistics description .....	143
7.3 GENERAL PARAMETERS USED TO CALCULATE THE STATISTICS .....	145
7.4 DETAILED DESCRIPTION FOR CALCULATION OF THE STATISTICS .....	147
7.4.1 The 'IP Generator – Traffic + Statistics' tab .....	147
7.4.2 The 'IP Answering – Parameters + Statistics' tab .....	148
7.4.3 The 'Traffic Observer' tab .....	149
<b>Part 8: Annexes</b> .....	<b>151</b>
8.1 DESCRIPTION OF THE MATHEMATICAL LAWS USED BY "IP TRAFFIC – TEST & MEASURE" .....	151
8.1.1 Uniform Law .....	151
8.1.2 Exponential Law .....	152
8.1.3 Law of Pareto .....	154
8.1.4 Gauss law .....	155
8.2 "IP TRAFFIC – TEST & MEASURE" TRACES .....	156
8.3 CONFIGURATION PARAMETERS SAVED IN THE REGISTRY DATABASE .....	156
8.4 DEFAULT VALUE OF A CONTEXT .....	158
8.5 EXTERNAL FILE FOR THE 'IP GENERATOR' MODULE .....	160
8.6 EXTERNAL DLL FOR THE 'IP GENERATOR' MODULE .....	160
8.6.1 TrafficInit .....	161
8.6.2 PacketDelay .....	161
8.6.3 PacketData .....	162
<b>Part 9: Examples of sniffed traffic files</b> .....	<b>163</b>

## Part 0: Preface

### 0.1 Organization of this manual

This user guide is aimed at helping you to discover and use “IP Traffic – Test & Measure”. This manual is organized as follows:

- **Part 1: Product Overview**  
Part 1 briefly describes “IP Traffic – Test & Measure” and its features, and explains how to contact the ZTI Technical Support Center.
- **Part 2: Install, Uninstall "IP Traffic – Test & Measure"**  
Part 2 explains how to install and uninstall the software.
- **Part 3: License configuration and License transfers**  
Part 3 explains how to configure a license and move a license (direct transfer or floppy disk transfer).
- **Part 4: Hardware Installation (GPS Kit and ZClock)**  
Part 4 explains how to connect the GPS Kit via a serial cable and ZClock via a parallel cable to the PC.
- **Part 5: Graphical User Interface**  
Part 5 presents the “IP Traffic – Test & Measure” Graphical User Interface, i.e. the main rules and principles of representation and display.
- **Part 6: Using "IP Traffic – Test & Measure"**  
Part 6 explains how to use the “IP Traffic – Test & Measure” software. This part includes menu and functionality description. It is based on Windows and Tabs description. Each Tab is presented separately.
- **Part 7: Calculation Mode for the Statistics**  
This part describes the rules and methods used to calculate statistics displayed by “IP Traffic – Test & Measure”.
- **Part 8: Annex**  
Describes additional information about the mathematical laws used by “IP Traffic – Test & Measure”, “IP Traffic – Test & Measure” traces, configuration parameters saved in the Registry database, default values of a new context, information on external objects for the ‘IP Generator’ module (file or DLL).
- **Part 9: Examples of sniffed traffic files**  
Six sample files (containing IP packets captured with the 'Traffic Sniffer') are provided with the “IP Traffic – Test & Measure” software. These files can be used with the off-line mode of the 'Traffic Observer'.

## 0.2 Minimum System Requirements

The “IP Traffic – Test & Measure” software requires the following minimum system requirements to operate properly:

- Windows 98, 2000 or XP
- Pentium processor
- 30 Mb free hard disk space
- 1024 x 768 display
- To use the GPS kit: 1 serial interface
- To use the ZClock module: 1 parallel interface (with the EPP mode)

## 0.3 Technical Support

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

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

You can contact Technical Support by:

Email	Send as many details as possible to <a href="mailto:support@zti-telecom.com">support@zti-telecom.com</a> or <a href="mailto:support@zti.fr">support@zti.fr</a>
Fax	Send as many details as possible to +33 2 96 48 14 85
Telephone	Telephone support is available from 09:30 am to 06:00 pm (GMT Time +1 or +2), Monday to Friday. Call +33 2 96 48 43 43

Before contacting Technical Support, please record the following information:

- Product name and version.
- Demo version or licensed product.
- System configuration.
- Problem details: settings, error messages,...
- If the issue can be reproduced, the details on how to create the issue.

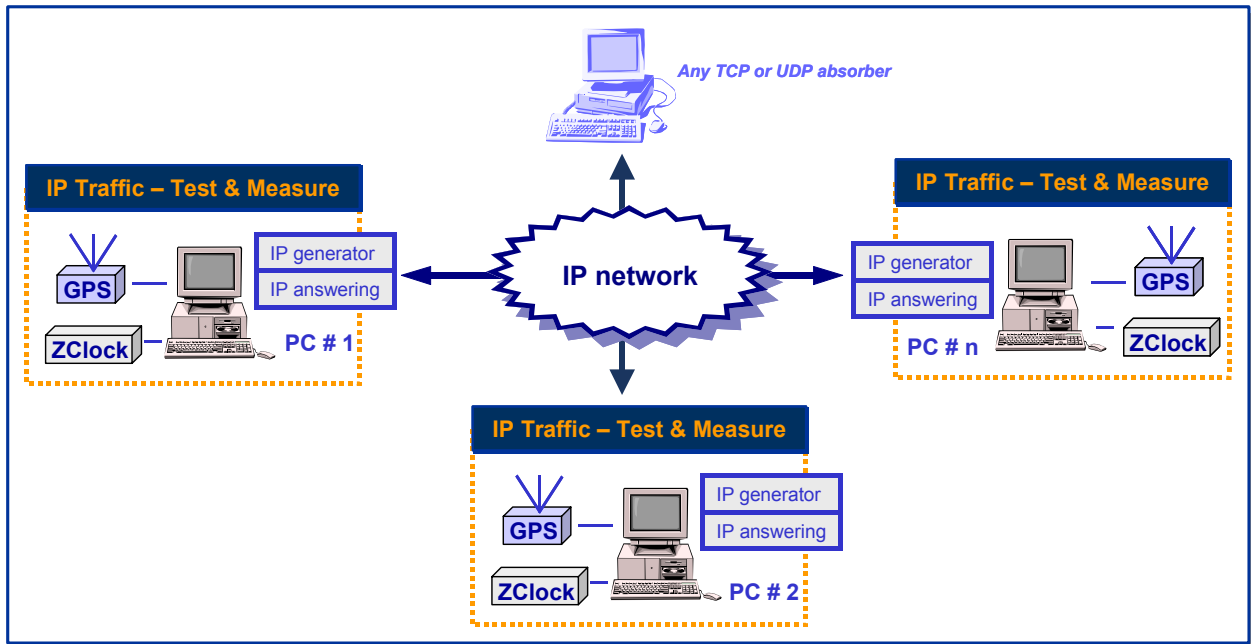
## Part 1: Product Overview

### 1.1 General Description

The "IP Traffic – Test & Measure" software is a connection and data generation tool for IP networks. Data flows use TCP (Transmission Control Protocol), UDP (User Datagram Protocol) or ICMP (Internet Control Message Protocol) protocols, which are used by mailing exchanges, file transfers, ping programs and World Wide Web transmissions.

"IP Traffic – Test & Measure" needs at least two PCs running on Windows 98, 2000 or XP. The screen resolution must be at least 1024x768.

Various testing configurations can be implemented using more than two PCs. "IP Traffic – Test & Measure" establishes TCP or UDP connections between PCs through IP networks.



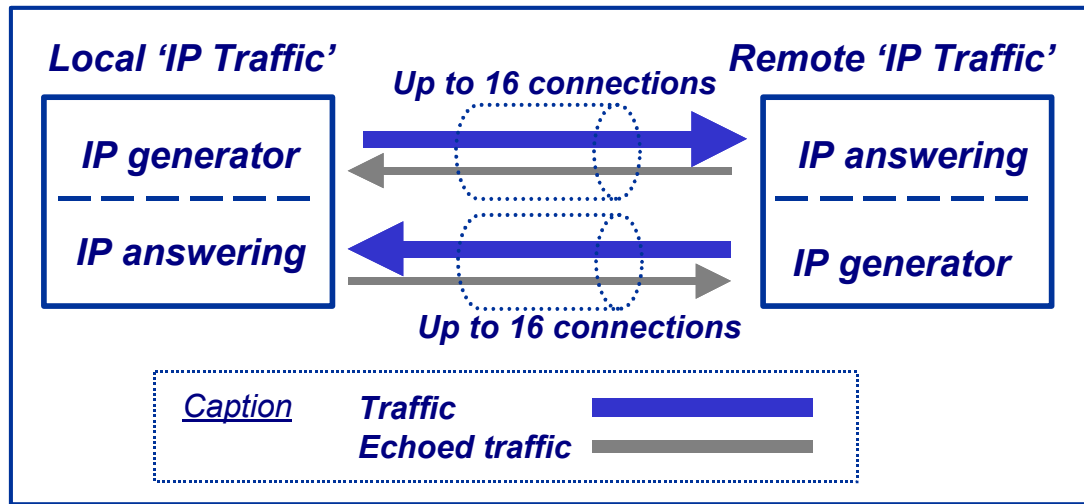
"IP Traffic – Test & Measure" is an IP software testing tool using the Microsoft Windows TCP/IP stack (Winsock2 interface). So, "IP Traffic – Test & Measure" is independent of any transmission or telecom link and can use any transmission link managed by the Windows operating system: LAN (Ethernet, Token-ring, hyperlan...), WLAN, WAN (modem, ISDN, ATM, satellite link...), remote access, mobile or cellular networks,

"IP Traffic – Test & Measure" can be used with two optional external products in order to have a very precise time reference to realize measurements with a high accuracy: a GPS kit and a very precise clock (ZClock) manufactured by ZTI (see next paragraph for more information).



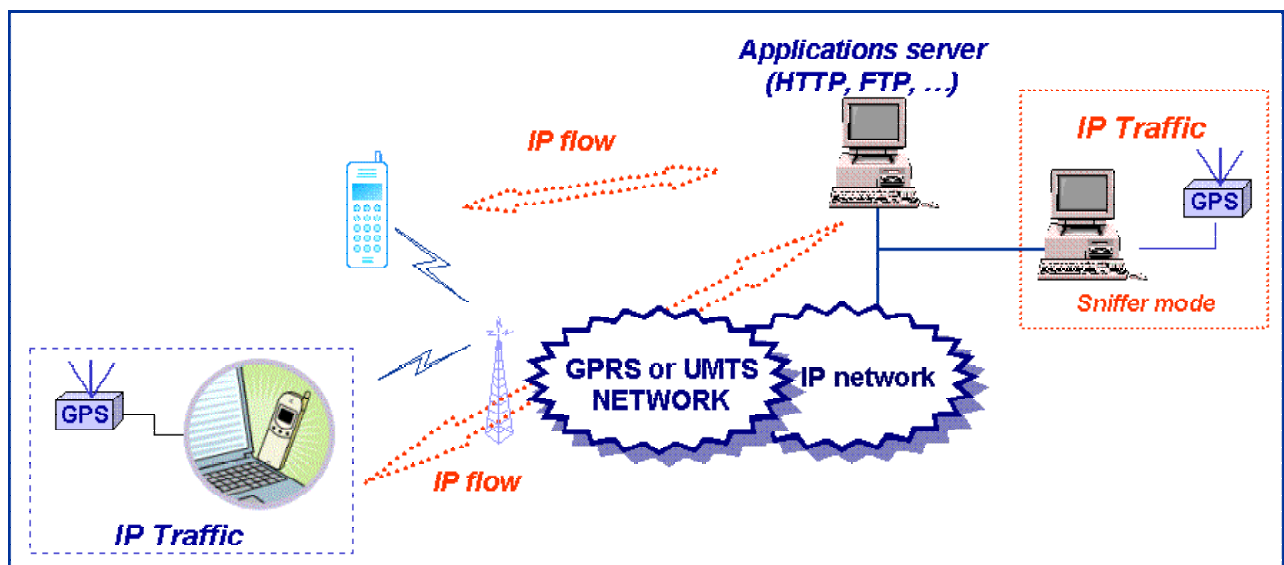
The "IP Traffic – Test & Measure" testing tool is composed of four modules: 'IP Generator', 'IP Answering', 'Traffic Sniffer' and 'Traffic Observer'.

- **Module 1: 'IP Generator'** to generate IP traffic on 16 simultaneous connections.
- **Module 2: 'IP Answering'** able to receive IP traffic on 16 simultaneous connections with different working modes (Absorber, Absorber file, Echoer, Echoer file and Absorber + Generator).



*The 'IP Generator' and 'IP Answering' modules*

- **Module 3: 'Traffic Sniffer'** to capture traffic files at the driver level (under the TCP/IP stack) in order to calculate traffic statistics and timestamp IP packets. These traffic files can be replayed by the 'IP Generator' module.



*"IP Traffic – Test & Measure": sniffer mode*

"IP Traffic – Test & Measure" can be used to capture IP traffic with the 'Traffic Sniffer': for example, the IP flows between a mobile and an application server (web, video telephony...) can be captured and saved in a file. IP packets are time stamped, in order to replay IP traffic with the same timing as for the capture. The user can then use an internal "IP Traffic – Test & Measure" algorithm in order to obtain two traffic files (traffic client file and traffic server file). These traffic files can be used by the 'IP Traffic' generator as source traffic.

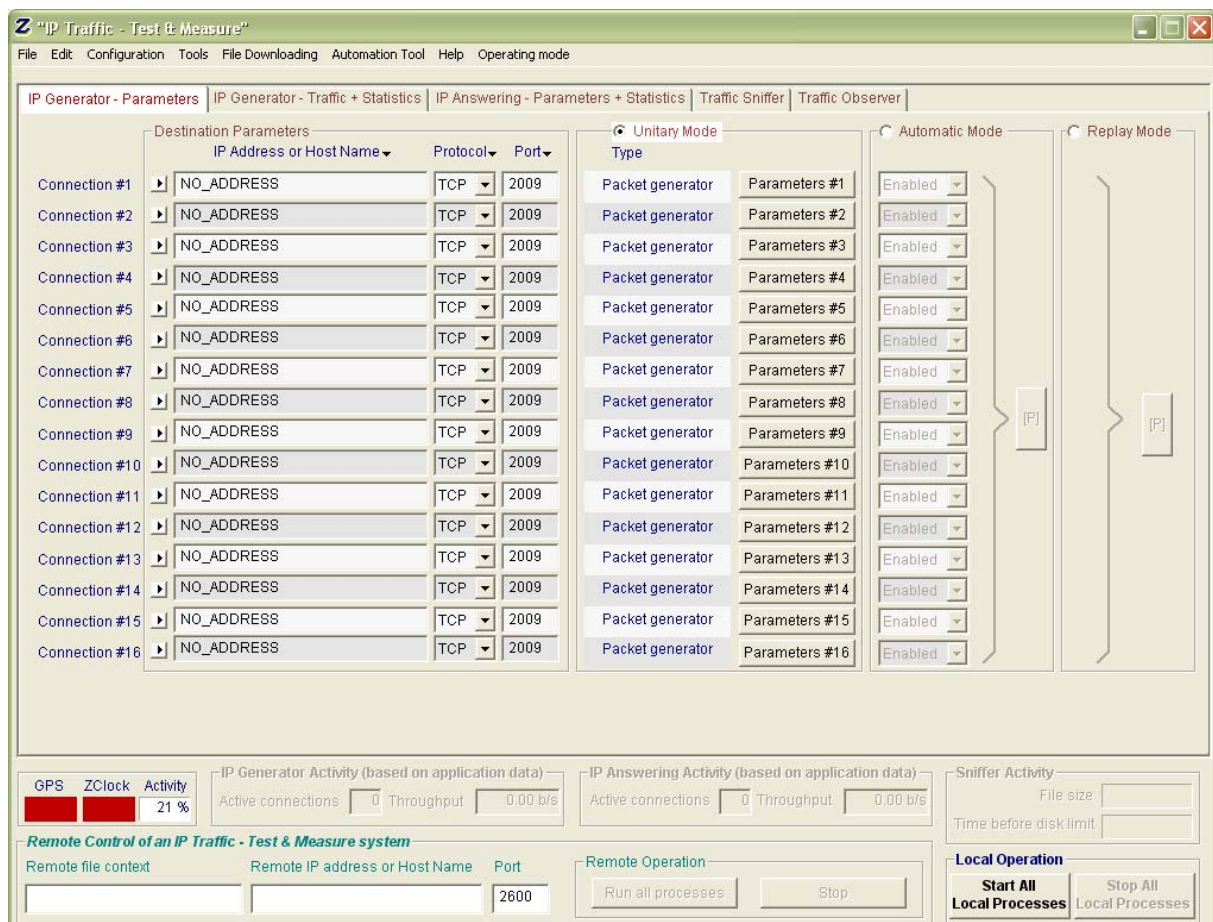
- **Module 4: the 'Traffic Observer'** is a powerful **graphic tool** to display and visualize traffic statistics on IP connections. Statistics are displayed in real time [on-line mode] or by using an

off-line mode [user can replay traffic files by using a 'video recorder' mode (play, pause, stop) with index management].

### "IP Traffic" can be operated with two main modes:

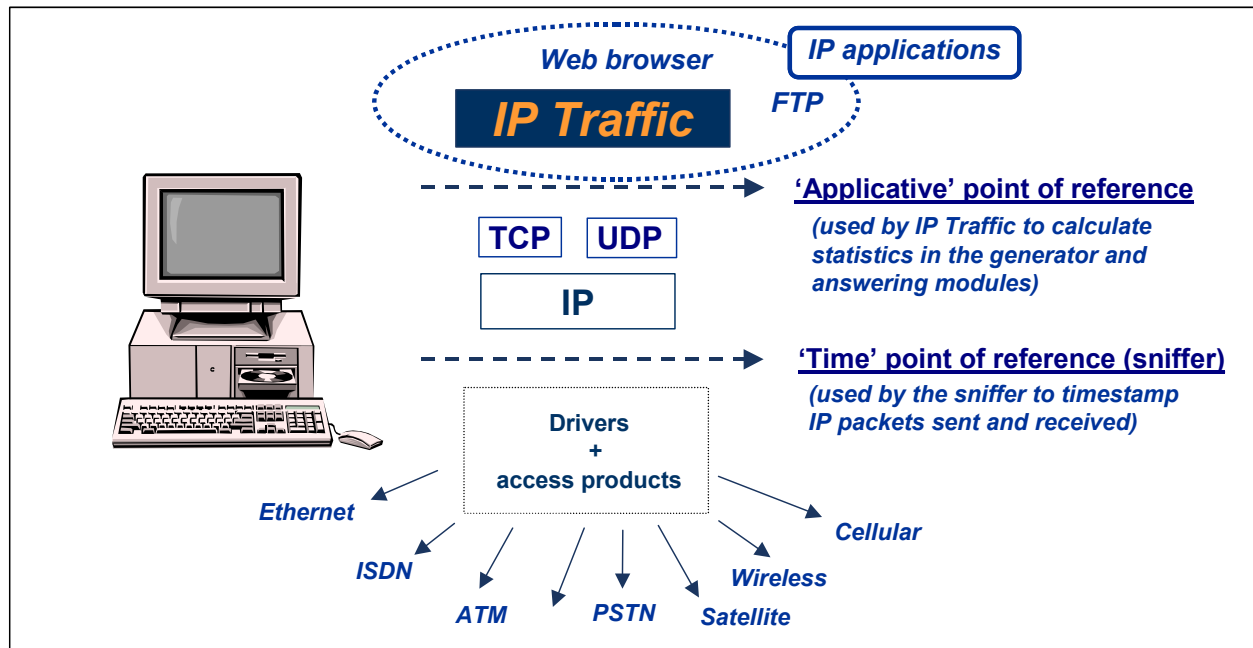
- The **normal** mode: the user can access all commands and functionalities
- The **remote control** mode: the user can't access locally commands of the "IP Traffic - Test & Measure" software. It's mainly used for control by a remote "IP Traffic – Test & Measure" system. It's very useful for example to use an "IP Traffic – Test & Measure" system as a server that the user can operate remotely.

The design of the "IP Traffic – Test & Measure" man machine interface offers a main window allowing easy access to all functionalities and commands. Counters and Indicators give an overview of the overall traffic activities.



**"IP Traffic – Test & Measure" main window**

## 1.2 Architecture



Two points of reference are used by the "IP Traffic – Test & Measure" software.

### 'Applicative' point of reference

In the 'IP Generator' and the 'IP Answering' modules, statistics (e.g. throughput, RTT...) are calculated at the application level (above the TCP/IP stack). These statistics refer to data sent or received by the "IP Traffic – Test & Measure" application, and are independent of the protocol (TCP or UDP).

### 'Time' point of reference

The Traffic Sniffer uses this point of reference in order to timestamp IP packets sent and received. Timestamp of packets is made at the nearest of the physical link (under the TCP/IP stack). Therefore, "IP Traffic – Test & Measure" can identify lost and retransmitted IP packets. Values and statistics of the 'Traffic Observer' tab use this point of reference.

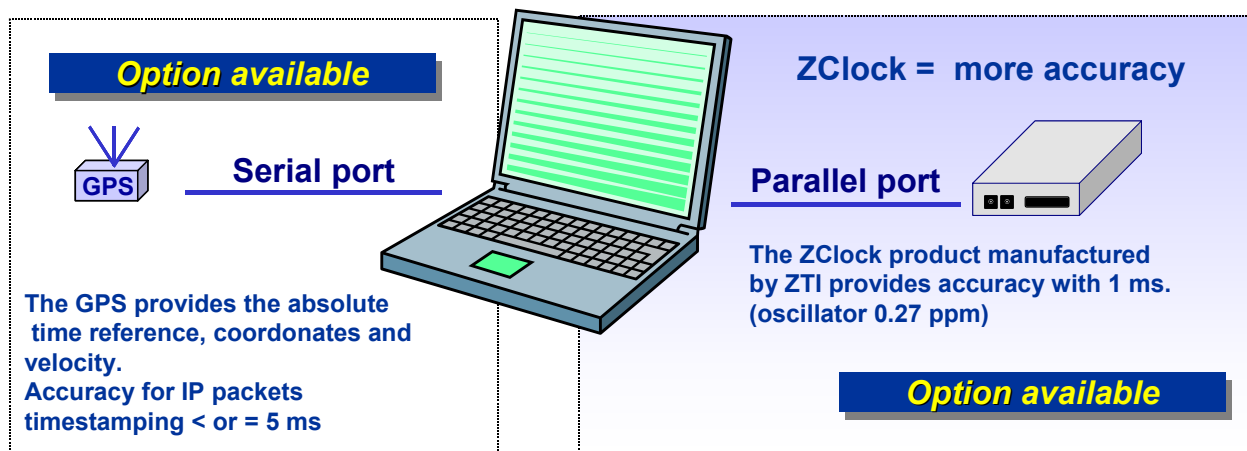
**Note:** see Part 7 for more information to know how "IP Traffic – Test & Measure" computes statistics.

In order to have a good accuracy to timestamp IP packets, additional hardware options are available as described in the following paragraph.

When no additional hardware is used, the 'Traffic Sniffer' uses the PC internal clock to timestamp IP packets sent and received. Because, the PC internal clock can't provide an absolute time reference, and needs to be synchronized with all the PCs internal clocks used by "IP Traffic – Test & Measure" ZTI recommends an additional hardware option to allow precise time propagation delays calculations into IP networks.

## 1.3 Hardware Options Available

In order to free "IP Traffic" from the constraints related to the use of the PC internal clock, ZTI proposes two optional systems, allowing the Traffic Sniffer to timestamp sent and received IP packets with more accuracy.



With the GPS Kit and ZClock options, 4 configurations to use the "IP Traffic – Test & Measure" software:

Configuration	Description	Absolute Time reference	Accuracy for Measurement
0	"IP Traffic – Test & Measure"	No or user defined	Not defined (PC clock used)
1	"IP Traffic – Test & Measure" + GPS	GPS	5 milliseconds
2	"IP Traffic – Test & Measure" + ZClock	No or user defined (ZClock is initialized with the PC clock)	1 millisecond
3	"IP Traffic – Test & Measure" + GPS + ZClock	GPS (ZClock is initialized with the GPS time)	1 millisecond

***It is recommended to use ZClock to have the best accuracy for measurement.***

The GPS and ZClock systems provide time reference with more accuracy than the PC internal clock. The ZClock product provides a very precise clock time reference (by the use of a high stability quartz oscillator < +/- 1.10<sup>-9</sup> on 1 day), and authorizes to lose the GPS signal, without yet losing the time reference. For example, whereas GPS signal on a mobile system is lost in a tunnel, ZClock continues to timestamp the IP packets in a precise way.

The GPS system provides an absolute time reference. So each IP Traffic system equipped with one GPS system will have the same time reference. By using only the GPS system and the internal PC clock, accuracy for IP packets time stamping is < or = 5 milliseconds.

The ZClock product provides a very precise clock with a high stability (long term stability is < 1 ms for 1 hour on 1 year). When used with IP Traffic, accuracy is one (1) millisecond for IP packets time stamping.

When the GPS time signal is available, IP traffic initializes the ZClock product with this time reference. Even if the GPS signal is lost during many hours, the accuracy of one (1) millisecond is preserved.

## 1.4 "IP Traffic – Test & Measure" key features

### Module 1: 'IP Generator' Overview with TCP or UDP protocol

- The '**IP Generator**' module generates up to 16 simultaneous unicast – or multicast UDP - connections. Connections can be generated following three different testing modes:

⇒ **Unitary mode**: for each IP connection, you can select the traffic generator data source (*internal* or *external*), define a time code option (time code is added as data in the packet data), specify the ToS (Type of Service) byte, specify the Time To Live (TTL) and if needed save incoming traffic in a file.

**Internal data generator** with five parameter groups:

- Data to send: automatic data generation by using a mathematical law, packet generator (fix, random, alternate and increasing / decreasing) or file to send
- TCP or UDP Data size: fix, random, alternate and increasing / decreasing
- Inter packet delay: fix, random, alternate, increasing / decreasing or use of a mathematical law
- Mean Throughput for the connection in Kb/s: data size or inter packet delay adjustable
- Mean Packet Throughput for the connection in p/s (packets per second) : this option is only available with UDP connection
- Save generated traffic in a file

**External data source generator**: select a file or an external DLL providing traffic to send (packet starting time, size, contents, inter packet delay...) and if needed use of a loop counter with an idle time between each loop.

⇒ **Automatic mode**: use of a mathematical law for connections generation starting time and another mathematical law for data volume to send, in order to generate up to 16 outgoing IP connections.

⇒ **Replay sniffed traffic**: use of a traffic file previously captured by the Traffic Sniffer and the 'IP Generator' module replays this traffic file with timing accordingly to time capture (IP resolution addressing is made by the user before replay). A repeat counter can be defined with an idle time between each replay.

- **Statistics**: different statistics parameters are displayed by the 'IP Generator' module for each connection
  - 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)
  - Seq. numb errors (sequence numbering errors)
  - Mean RTT (Round Trip Time)
  - Jitter

These statistics can be saved in a file defined by the user.

### **Module 1: 'IP Generator' Overview with ICMP protocol**

- The '**IP Generator**' module generates up to 16 simultaneous connections. Connections can be generated following only one testing mode when using ICMP protocol:

⇒ **Unitary mode**: for each IP connection, only the **internal** data source is allowed. Moreover you can specify the ToS (Type of Service) byte or specify the Time To Live (TTL).

**Internal data generator** proposed three parameter groups. Below are listed the different possibilities offer with ICMP protocol:

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

- **Statistics**: different statistics parameters are displayed by the IP Generator module for each connection:
  - Sent ICMP requests (Tx Packets)
  - Received ICMP replies (Rx Packets, responses sent by the target remote)
  - Seq. numb errors (sequence numbering errors)
  - Mean RTT (Round Trip Time)

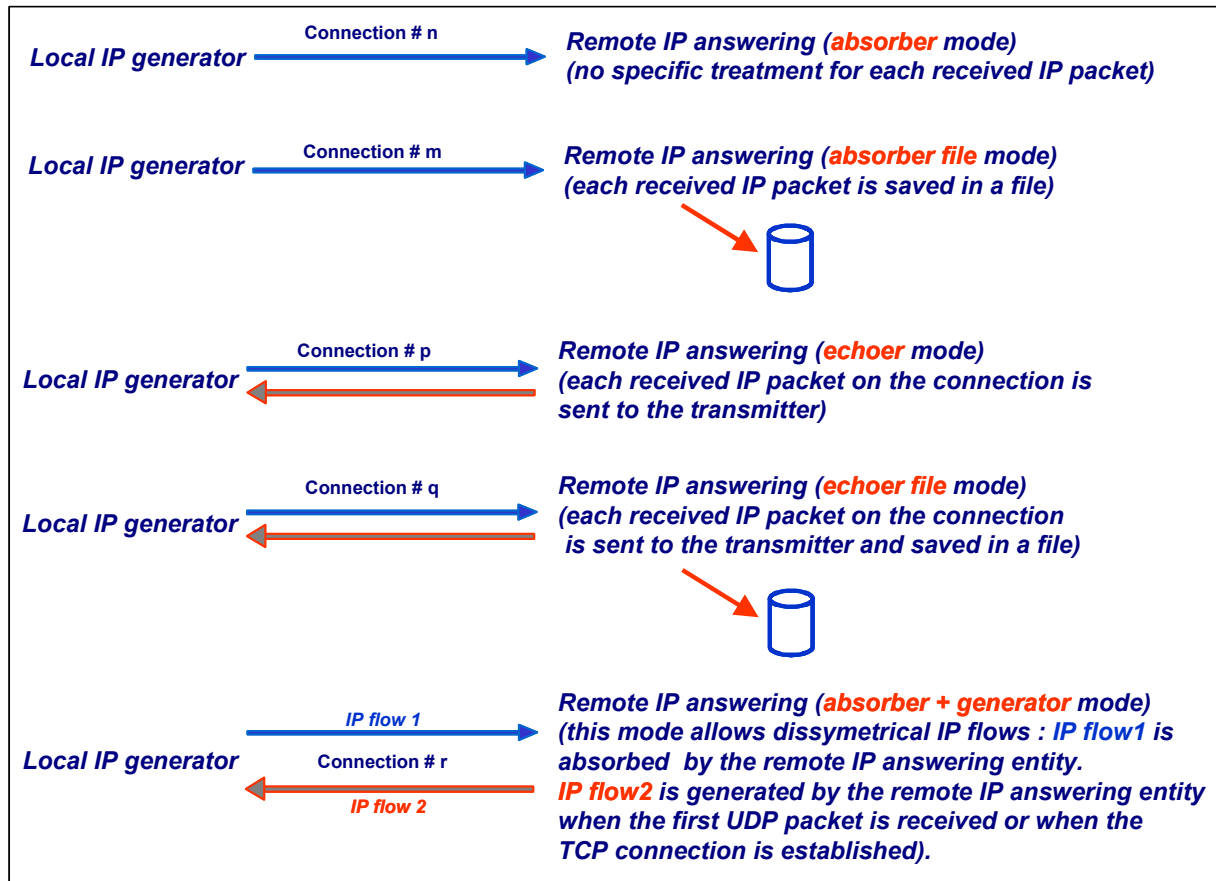
These statistics can be saved in a file defined by the user.



## Module 2: 'IP Answering' Overview

- The '**IP Answering**' module receives traffic (up to 16 simultaneous connections), and operates for each connection following different working modes: '**Absorber**', '**Absorber file**', '**Echoer**', '**Echoer file**', '**Absorber + Generator**' or '**Disable**'.

In this User Guide, we will consider that the Local machine is used for generating IP traffic and the Remote one is used for IP answering.



- **Statistics:** different statistics parameters are displayed by the IP Answering module for each connection:
  - 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)
  - Seq. numb errors (sequence numbering errors)
  - Data not echoed
  - Jitter

These statistics can be saved in a file defined by the user.

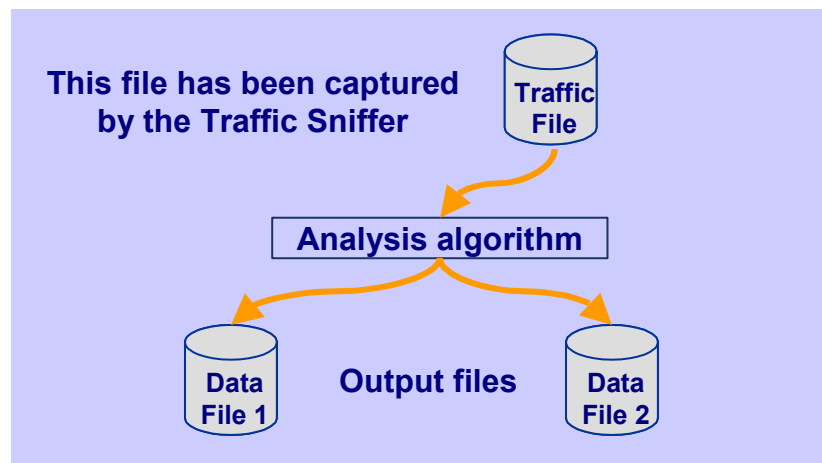
### Module 3: 'Traffic Sniffer' Overview

Sent and received IP packets are time stamped by the 'Traffic Sniffer' and then saved in a file in order to generate capture traffic files.

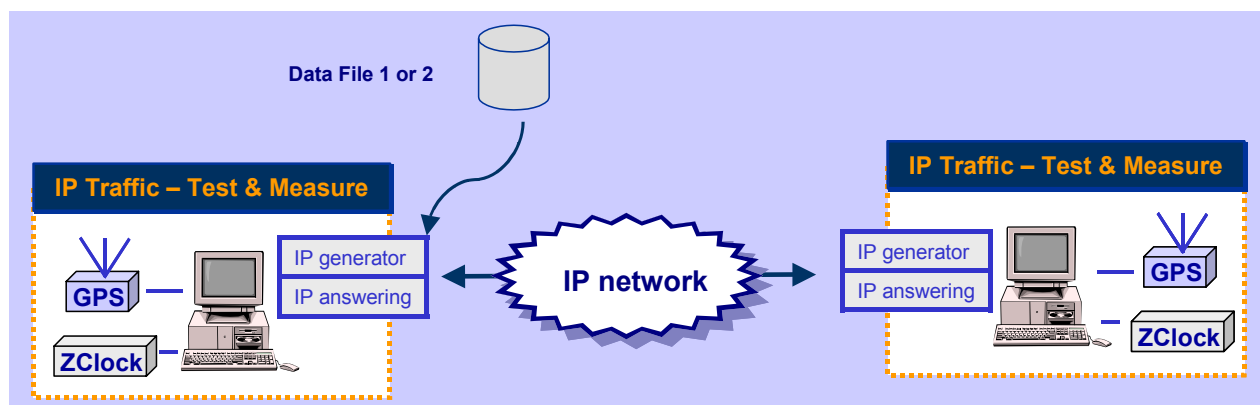
User can define IP filters to capture IP traffic in a file.

In the example above, the 'Traffic Sniffer' is activated on each system to generate a traffic file. Two traffic files are produced: File A and File B. These traffic files A and B can then be used by the 'Traffic Observer' in order to calculate off-line statistics (such as the packet transit delay).

From one traffic file captured by the 'Traffic Sniffer', an analysis algorithm produces two data files as shown below (because a traffic file contains IP packets sent and received):



Then it is possible to use a data file generated in order to replay traffic via the 'IP Generator' module:

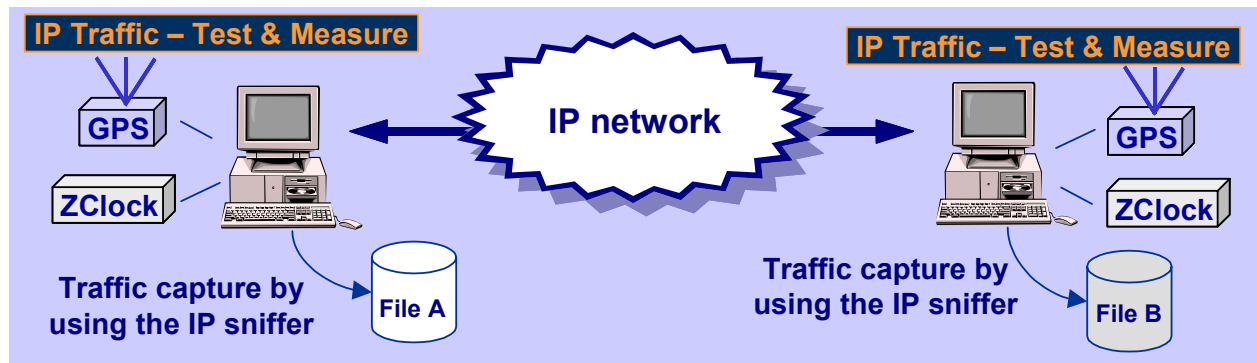




## **Module 4: 'Traffic Observer' Overview**

The 'Traffic Observer' displays statistics for the 'IP Generator' or the 'IP Answering' modules according two modes: on-line (real time) and off-line (batch mode).

The off-line mode allows calculating statistics parameters (e.g. 'Packet Erasure Rate' and 'Packet Transit Delay') needing to have time stamped packets from the local and the remote systems.



This mode uses and analyzes the two traffic files (Files A and B in the schema) captured by the 'Traffic Sniffer'.

### **□ Features available with the on-line mode**

- ⇒ Select 'IP Generator' or 'IP Answering' display
- ⇒ Display of statistic parameters in a table for 16 connections:
  - IP throughput snapshot
  - IP throughput average
  - UDP or TCP throughput
  - Inter packet delay

Or

Graphic statistics display for the following parameters with triggers defined by user

- IP throughput
- Inter packet delay

*The graphic display enables to choose 'all connections' or a specific connection (from 1 to 16) and to calculate in real time the following parameters: average, standard deviation and confidence distance*

- ⇒ Export statistics in a file with filters defined by user
- ⇒ Reset statistics
- ⇒ Help window

### **□ Features available with the off-line mode**

- ⇒ Select 'IP Generator' or 'IP Answering' display
- ⇒ Load traffic files and process analysis for these files to detect that these files are coherent
- ⇒ User can replay traffic files by using a 'video recorder' mode (play, pause, stop) with index management (next, add, remove)
- ⇒ Display of statistic parameters in a table for 16 connections:
  - IP throughput snapshot
  - IP throughput average
  - UDP or TCP throughput
  - Inter packet delay
  - Packet erasure rate
  - Packet transit delay

Or

Graphic statistics display for the following parameters with triggers defined by user

- IP throughput
- Inter packet delay
- PER (Packet Erasure Rate) quality
- Packet transit delay

*The graphic display enables to choose ‘all connections’ or a specific connection (from 1 to 16) and to calculate the following parameters: average, standard deviation and confidence distance.*

Or

**Packet statistics:** display of packets sent and lost with transit delay

- ⇒ Export statistics in a file with filters defined by user
- ⇒ Reset statistics
- ⇒ Help window

## 1.5 Reference

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

## Part 2: Install and Uninstall "IP Traffic - Test & Measure"

To install this software testing tool, you need a PC with [at least a 1024 x 768 display screen resolution](#) and [Windows 98, 2000 or XP](#).

*Note: the "IP Traffic – Test & Measure" software is also named "IP Traffic" in this document.*

### Warning:

*\* To run "IP Traffic – Test & Measure" your computer's screen resolution must be configured on 1024 X 768 (at least). Please note that you should mask the task bar in a 1024x768 screen resolution, so you could have an optimal view of the software interface.*

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

### Note:

*It is advisable to first close anti-virus application before installing this software.*

The "IP Traffic – Test & Measure" software is configured by default with a 15-days limited license. When the time limit expires, "IP Traffic - Test & Measure" will cease to run. See part 2 below for more information about the license program.

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

### 2.1 Install "IP Traffic - Test & Measure" from a downloaded trial version

### Warning:

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

### Notes:

*The installation procedure is a standard installation program.*

*Please note that the install procedure of the "IP Traffic - Test & Measure" software will be different in the last part, depending on the target Operating System: Windows 98 or Windows 2000 / XP.*

- If you have downloaded the "IP Traffic – Test & Measure" software trial version from our website, you have downloaded the file [Setup\\_IPTraffic.zip](#) that includes the documentation and the file [Setup\\_IPTraffic.exe](#).
- Run Setup\_IPTraffic.exe and follow the "IP Traffic - Test & Measure" setup instructions to proceed with the installation.

By default, the "IP Traffic - Test & Measure" software will be installed in the following directory (C: is used as example):

C:\Program Files\IP Traffic with the following subdirectories:

C:\Program Files\IP Traffic  
 C:\Program Files\IP Traffic\Samples  
 C:\Program Files\IP Traffic\Samples\DataFile (for the IP Generator)  
 C:\Program Files\IP Traffic\Samples\User\_DLL (for the IP Generator)

- The following step of the installation procedure depends on the target Operating System (Windows 98 or Windows 2000/XP). Follow the instructions relating to your Operating System in the table below:

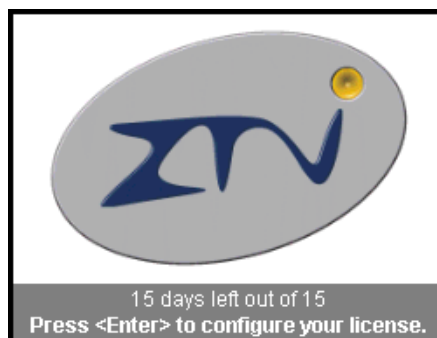
<i>Windows 98 install</i>	<i>Windows 2000/XP install</i>
<p>Just before the end of the installation, the WinPcap Setup Program is automatically launched in order to install the packet capture driver used by "IP Traffic - Test &amp; Measure".</p> <p>You will find below the different windows displayed by WinPcap 3.0 during the install procedure.</p> <p>Once the install procedure of WinPcap is finished, you can end the "IP Traffic - Test &amp; Measure" installation procedure.</p> <p>You must then <b>reboot</b> your PC.</p>	<p>The installation procedure automatically installs the packet capture driver named 'znpf.sys' on your system in the 'IP Traffic' directory.</p> <p>When the installation is finished, you don't need to reboot your computer to consider changes.</p>

#### Start Menu shortcuts created:

Start > Programs > **IP Traffic**

- ⇒ **IP Traffic – User Guide**
- ⇒ **Automation Tool – User Guide**
- ⇒ **Read Me First**
- ⇒ **License help**
- ⇒ **Uninstall IP Traffic**
- ⇒ **IP Traffic – Test & Measure** (click to run the "IP Traffic – Test & Measure" software)
- ⇒ **Automation Tool for 'IP Traffic – Test & Measure'**

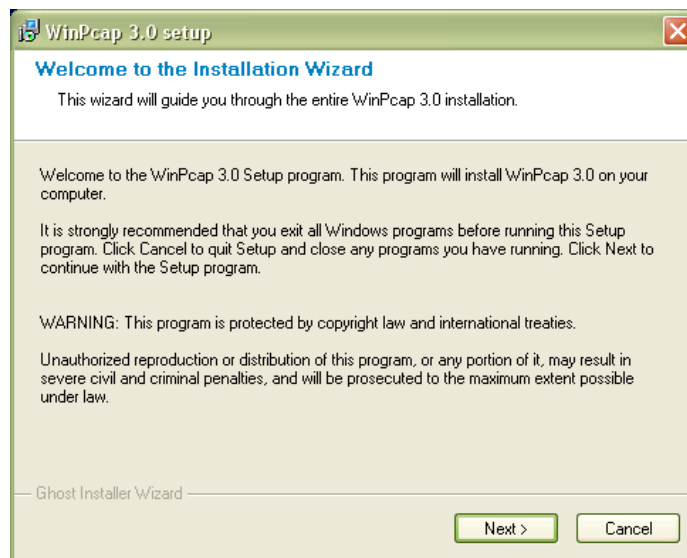
With "IP Traffic - Test & Measure" trial version, when you launch "IP Traffic - Test & Measure" for the first time, a message is displayed showing remaining days of use (for example, 15 days left out of 15 in the following example):



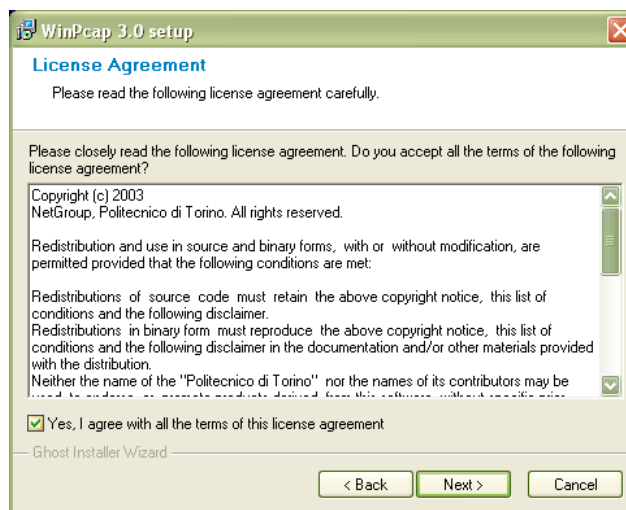
*Please refer to the third paragraph to configure your license.*

## **Automatic install of the packet capture driver by WinPcap for Windows 98**

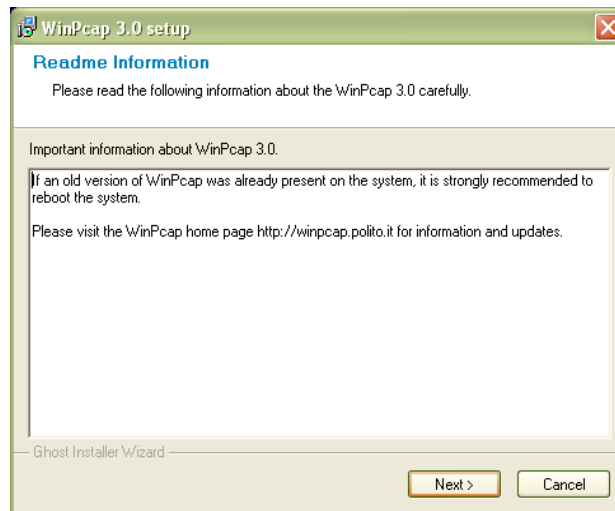
*Note: the WinPcap program includes software developed by the Politecnico di Torino and its contributors.*



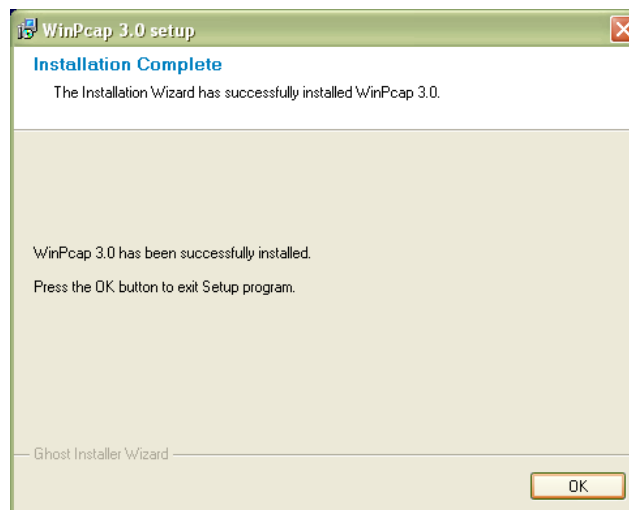
Then press Next to continue and display the License Agreement.



Once you have checked "Yes, I agree with all the terms of this license agreement", then press Next to continue.



Press Next to continue.



## 2.2 Install “IP Traffic - Test & Measure” from the CD-ROM

### Warning:

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

### Notes:

*The installation procedure is a standard installation program.*

*Please note that the install procedure of the "IP Traffic - Test & Measure" software will be different in the last part, depending on the target Operating System: Windows 98 or Windows 2000 / XP.*

- First, insert the «IP Traffic - Test & Measure» CD-ROM on disk drive.
- Click on “Start”, “Execute” and type “CD-ROM unit>:\Setup\_IPTraffic.exe”. Follow the “IP Traffic - Test & Measure” setup instructions to proceed with the installation. By default, the “IP Traffic - Test & Measure” software will be installed in the following directory (C: is used as example):

C:\Program Files\IP Traffic with the following subdirectories:

C:\Program Files\IP Traffic  
 C:\Program Files\IP Traffic\Samples  
 C:\Program Files\IP Traffic\Samples\DataFile (for the IP generator)  
 C:\Program Files\IP Traffic\Samples\User\_DLL (for the IP generator)

- The following step of the installation procedure depends on the target Operating System (Windows 98 or Windows 2000/XP). Follow the instructions relating to your Operating System in the table below:

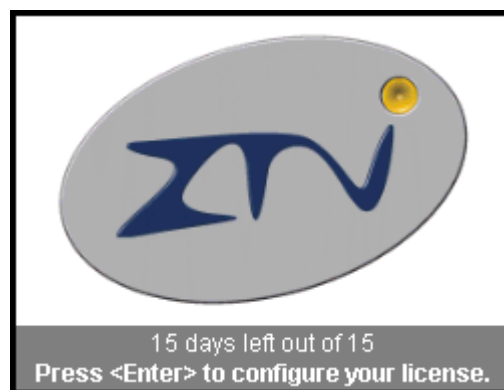
<i>Windows 98 install</i>	<i>Windows 2000/XP install</i>
<p>Just before the end of the installation, the WinPcap Setup Program is automatically launched in order to install the packet capture driver used by “IP Traffic - Test &amp; Measure”.</p> <p>You will find below the different windows displayed by WinPcap 3.0 during the install procedure.</p> <p>Once the install procedure of WinPcap is finished, you can end the “IP Traffic - Test &amp; Measure” installation procedure.</p> <p>You must then <b>reboot</b> your PC.</p>	<p>The installation procedure automatically installs the packet capture driver named ‘znpf.sys’ on your system in the ‘IP Traffic’ directory.</p> <p><b>When the installation is finished, you don’t need to reboot your computer to consider changes.</b></p>

## Start Menu shortcuts created:

Start > Programs > **IP Traffic**

- ⇒ **IP Traffic – User Guide**
- ⇒ **Automation Tool – User Guide**
- ⇒ **Read Me First**
- ⇒ **License help**
- ⇒ **Uninstall IP Traffic**
- ⇒ **IP Traffic – Test & Measure** (click to run the "IP Traffic – Test & Measure" software)
- ⇒ **Automation Tool for 'IP Traffic – Test & Measure'**

When you launch "IP Traffic - Test & Measure" for the first time, a message is displayed showing remaining days of use, even if you have bought an unlimited license (for example, 15 days left out of 15 in the following example):

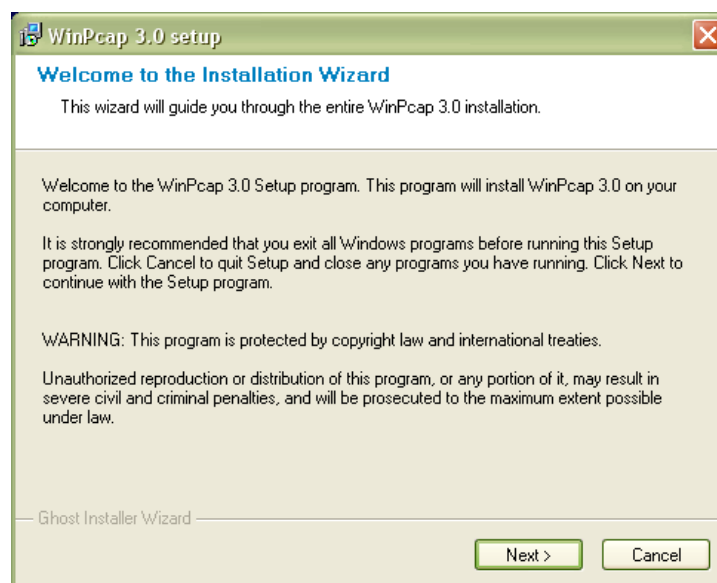


*Please refer to the third paragraph to configure your unlimited license.*

## **Automatic install of the packet capture driver by WinPcap for Windows 98**

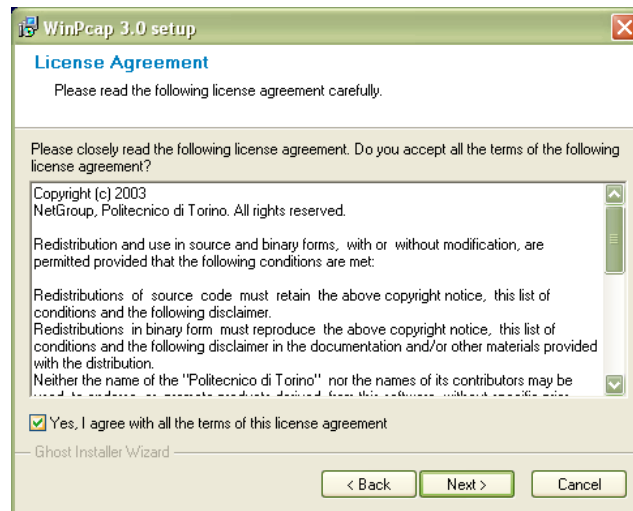
### Note:

*The WinPcap program includes software developed by the Polytecnico di Torino and its contributors.*

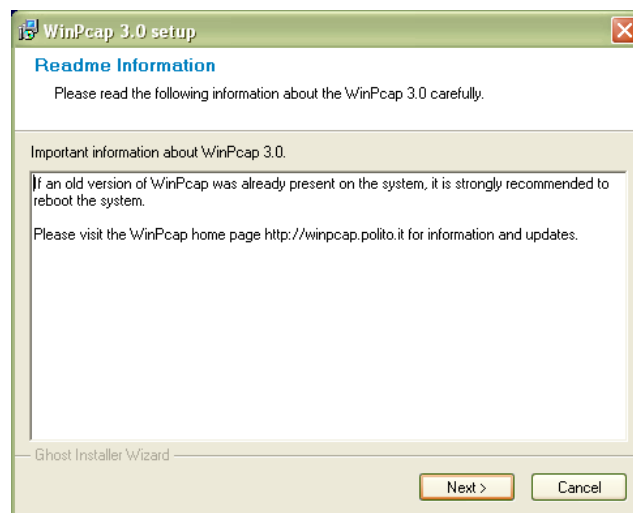


Then press Next to continue and display the License Agreement.

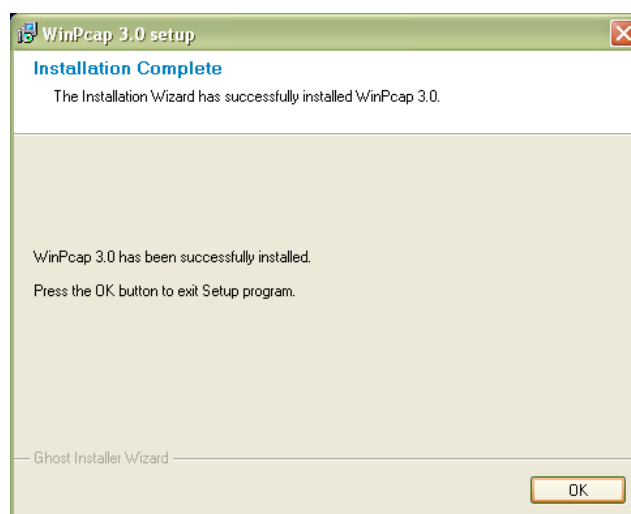




Once you have checked "Yes, I agree with all the terms of this license agreement", then press Next to continue.



Press Next to continue.



## 2.3 Uninstall “IP Traffic - Test & Measure”

The uninstall procedure is a standard uninstall program.

In the “Start > Programs > IP Traffic” Menu, select “Uninstall IP Traffic”.

<i>Windows 98 uninstall</i>	<i>Windows 2000/XP uninstall</i>
<p>Then delete all remaining files in the directory "C:\Program Files\IP Traffic".</p> <p>To uninstall the packet capture driver installed by the WinPcap Setup program, select the 'Add/Remove programs' icon of the "Control Panel" and then uninstall the "WinPcap 3.0" program.</p> <p><a href="#">Then reboot your PC.</a></p>	<p>Then delete all remaining files in the directory "C:\Program Files\IP Traffic".</p>

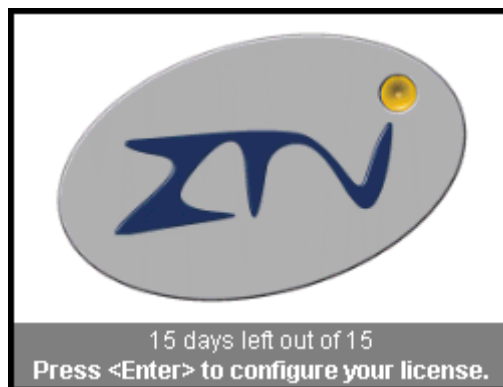
## Part 3: License Configuration and License Transfers

### 3.1 To configure a license

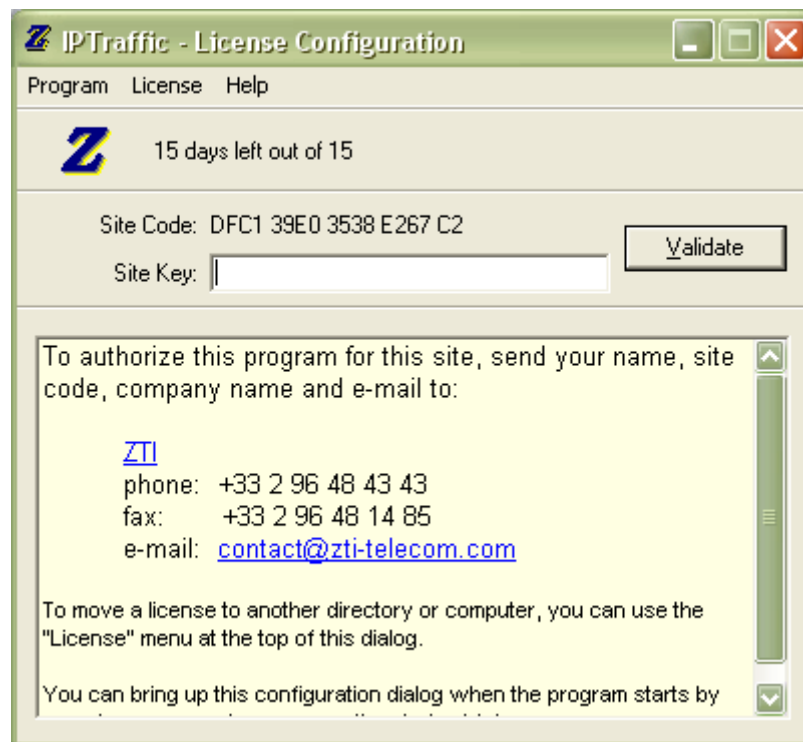
Note:

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

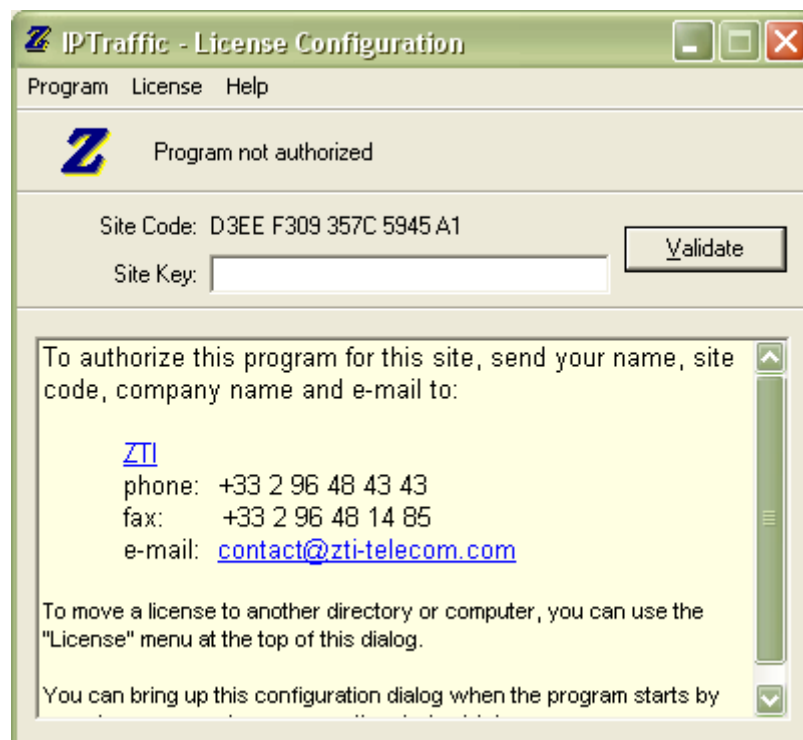
If you wish to configure your license before trial period end, please press **Enter** when the following message is displayed:



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



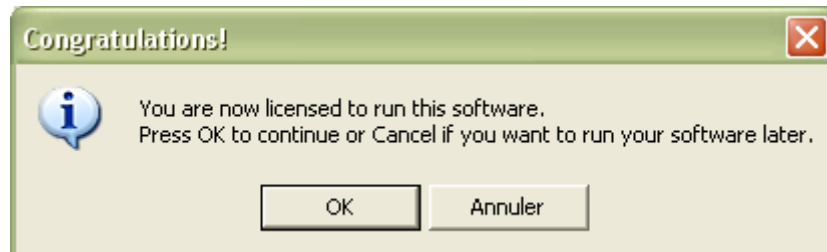
*Note: at the end of the trial period when you launch "IP Traffic – Test & Measure", the same license configuration dialog appears, with a specific mention instead of the remaining days of use: "Program not authorized".*



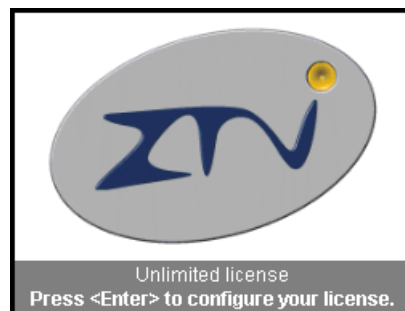
To get the 'Site Key' and obtain an unlimited version, please send your name, 'Site Code' (specific to your installation), company name, e-mail and preferred method of payment (if you haven't bought the "IP Traffic – Test & Measure" software yet) to: [contact@zti-telecom.com](mailto:contact@zti-telecom.com)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

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

If you have already bought the license, please email your Site Code and we will email you back the Site Key. After you have entered your Site Key, you get the following message:



*Note: you will see the following dialog when you launch "IP Traffic – Test & Measure" if you have an unlimited license:*



## 3.2 License Transfers

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

Licenses can be transferred using one of the following methods:

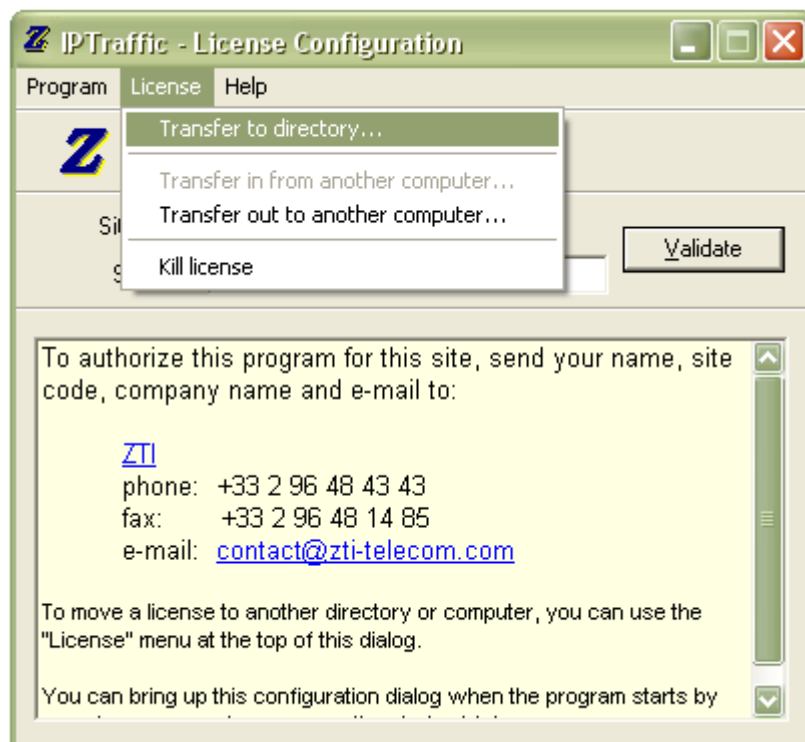
- ⇒ **Direct transfer:** move the license to another directory on the same PC or between two networked PCs.
- ⇒ **Transfer by media:** move the license from a source PC to a target PC by using a floppy disk or USB key.

**Warning:**  
Be careful when using USB keys in particular with a Windows 2000 system. When you unplug the USB key, you should use, before any removing of the USB key, the Unplug/Eject system by clicking on the Unplug/Eject icon present on the systray bar (placed on the bottom right corner of your screen). A "hot unplug" is unsafe and can damage all data contained on the USB key.

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

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

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



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

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

*Note: a floppy disk or USB key is needed for this kind of transfer.*

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

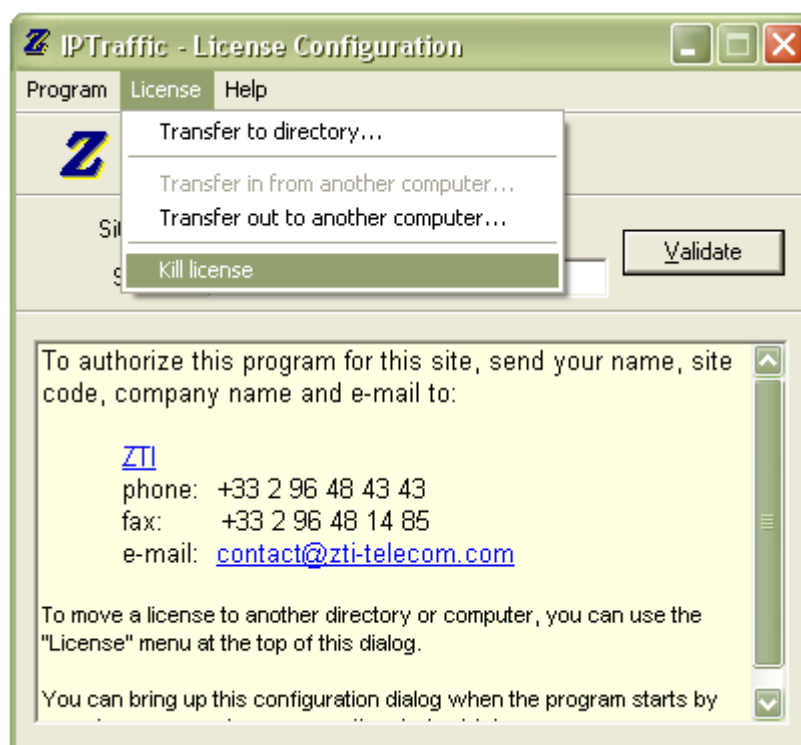
**Point 1:** First install the program on the target PC (PC # 2).

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

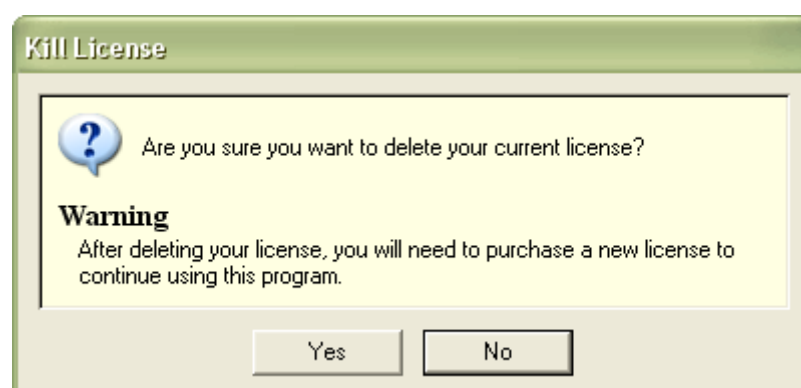
You need to kill the license if the "Transfer in from another computer ..." item of the license menu is disabled.

To kill the license, please proceed as follows.

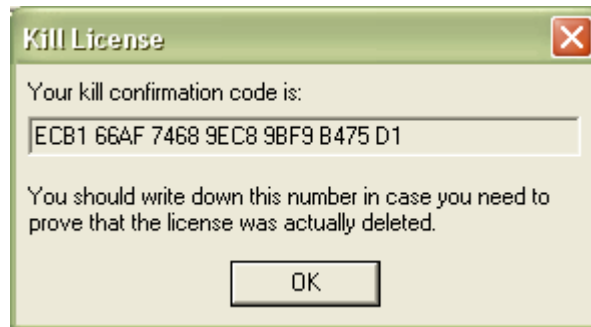
When the license configuration window appears, press **Enter** and select in the menu "License > Kill license".



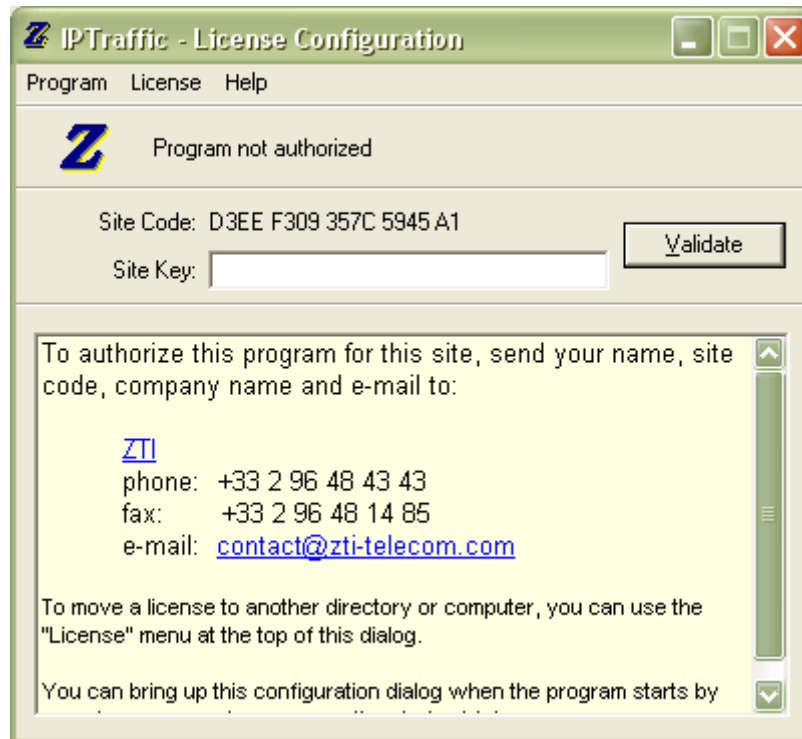
A message box appears, press 'Yes' to kill the license.



And a kill confirmation code is displayed.

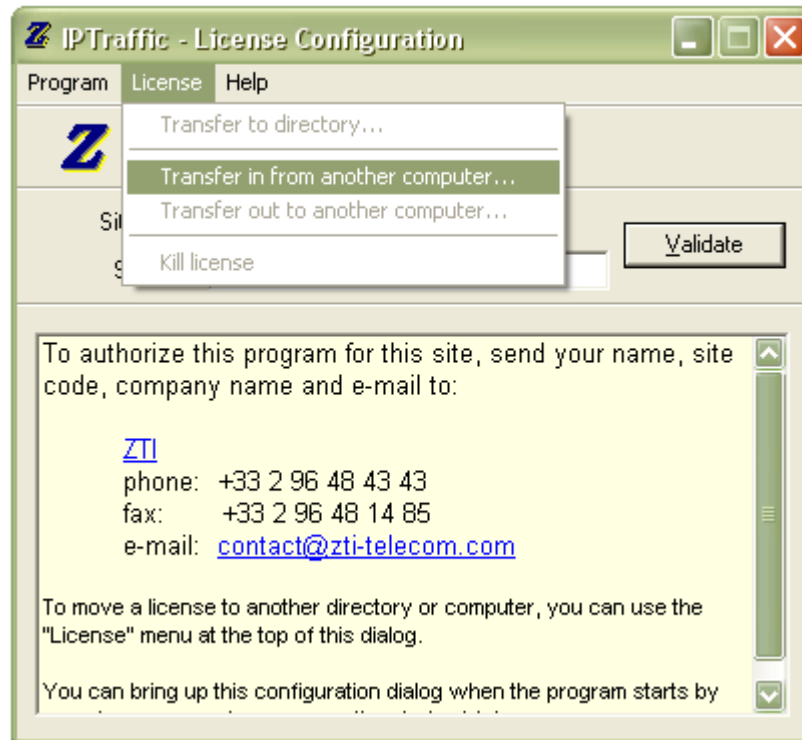


The license window displays now "Program not authorized" as following:

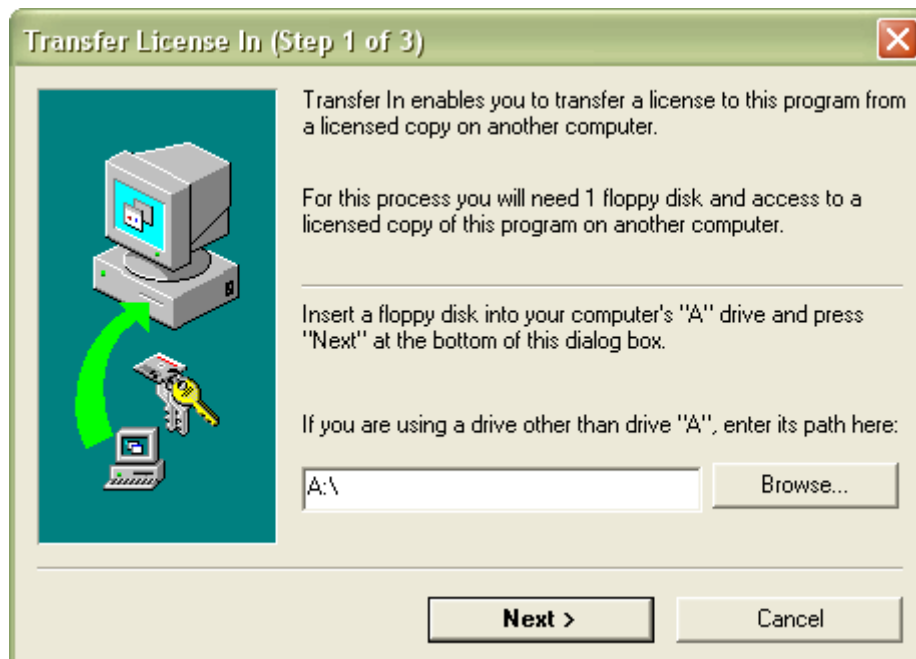




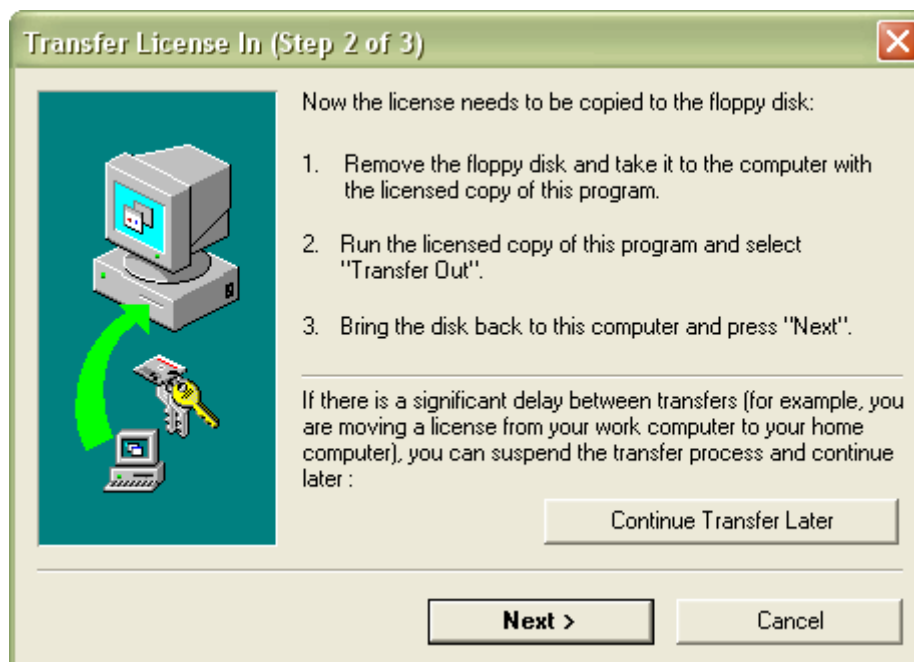
**Point 3:** select in the license menu, the item: "License > Transfer in from another computer ..."



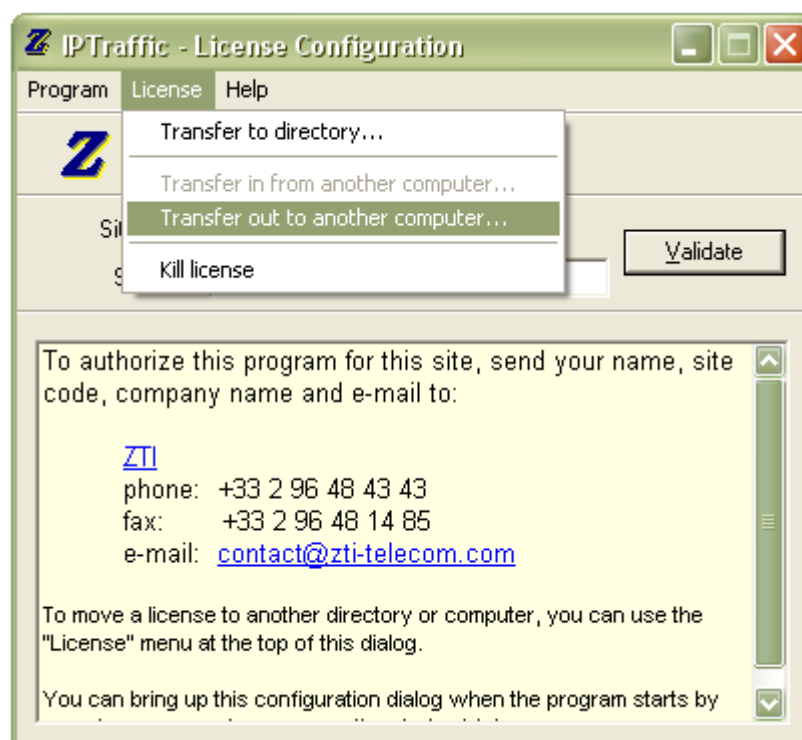
and the "Transfer License In (Step 1 of 3)" window is displayed:



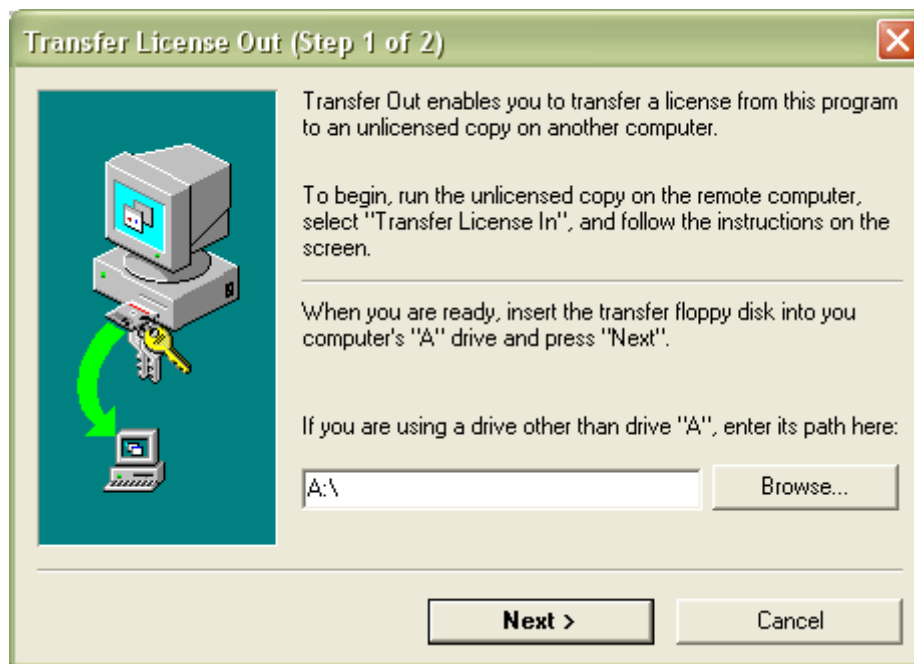
**Point 4:** Insert a floppy disk or use a USB key as requested in step 1 of 3 and specify the path. Then press "Next >" and the "Transfer License In (Step 2 of 3)" window is displayed:



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

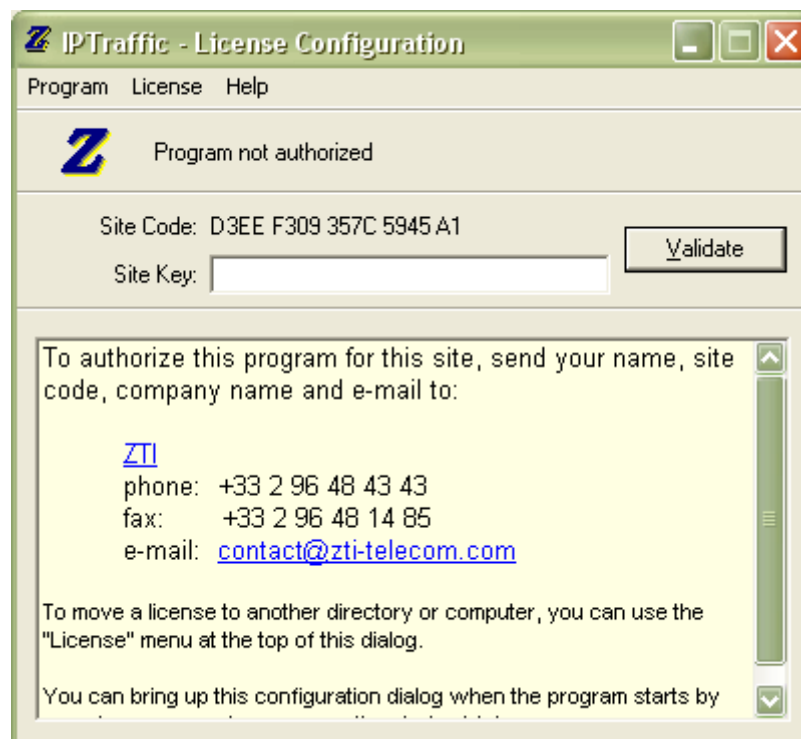


Then the following window is displayed:



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

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



*Note: you can check that the license is no more available on the source PC since the "IP Traffic – Test & Measure" software license is on a per workstation basis.  
Contact us to get information on site license ([contact@zti.fr](mailto:contact@zti.fr) or [contact@zti-telecom.com](mailto:contact@zti-telecom.com)).*

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

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

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



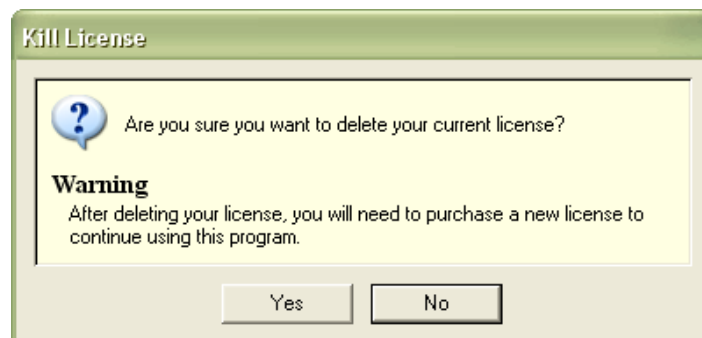
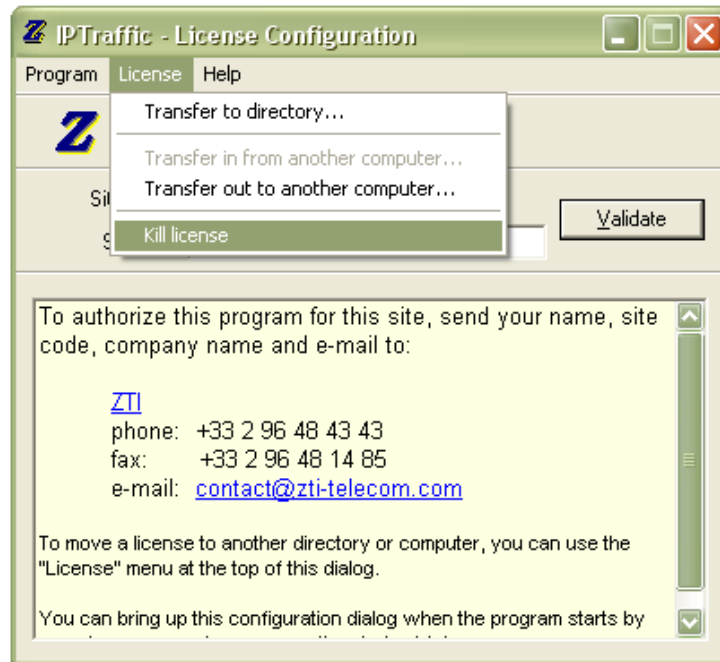
Click Finish to continue.

### 3.3 Kill a license

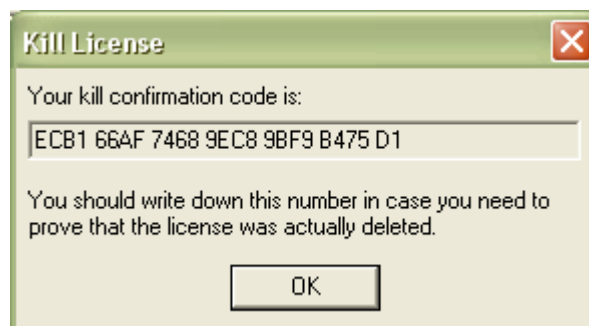
If you would like to transfer an unlimited license key onto a PC where a trial period is still active, you should first kill the active trial period. If you don't kill the active trial period, you will not be able to transfer an unlimited license.

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

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



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

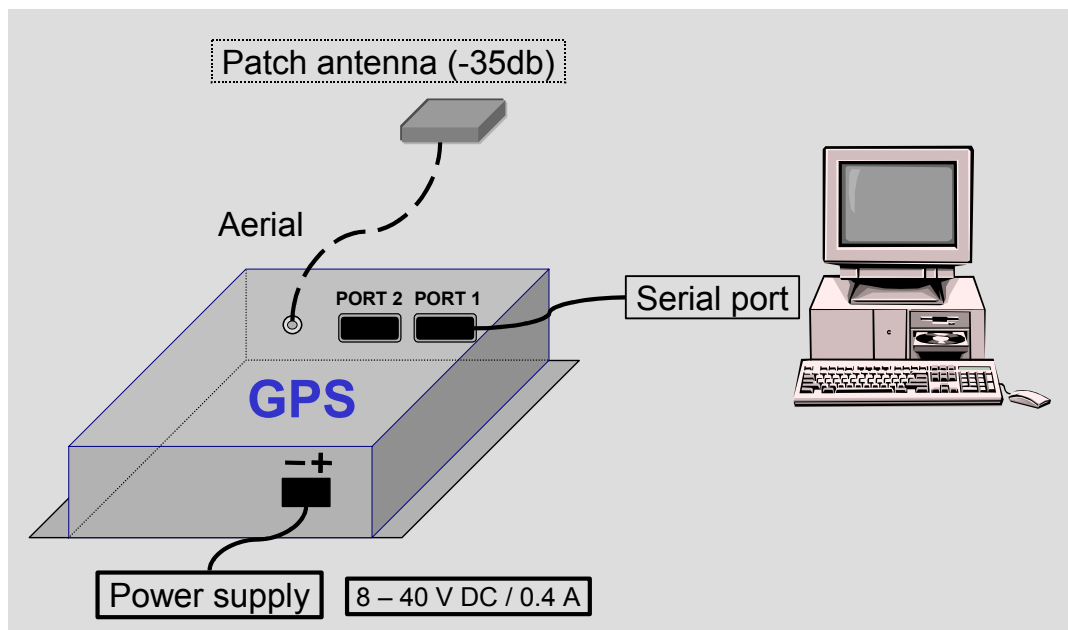
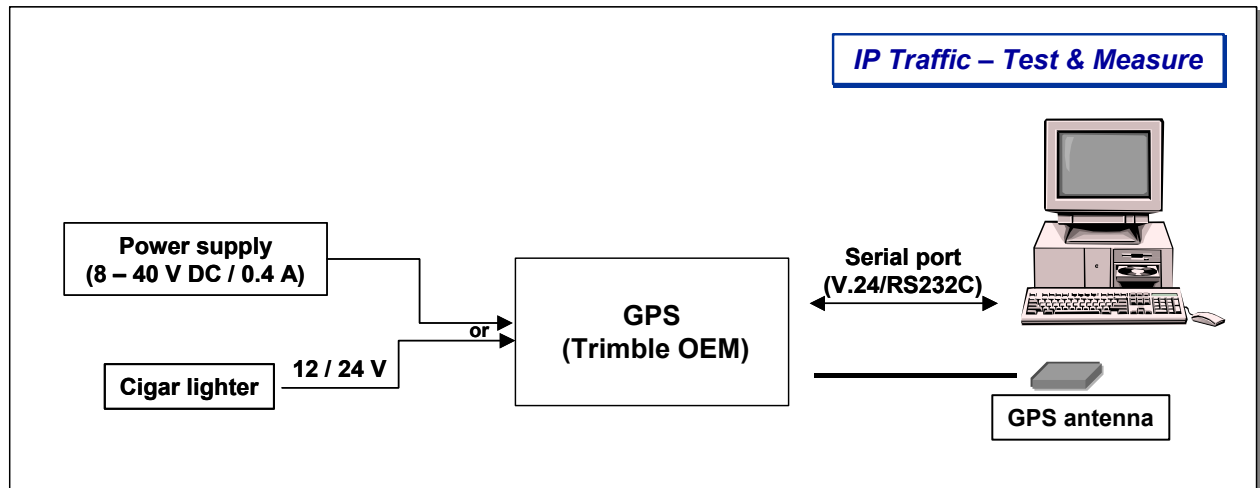


## Part 4: Hardware Installation (GPS Kit and ZClock)

### 4.1 Configuration 1: "IP Traffic – Test & Measure" + GPS Kit

The GPS kit is provided with the GPS box, a serial cable and a –35 db patch antenna. This GPS provides an absolute time reference (accuracy:  $\pm 500$  nanoseconds).

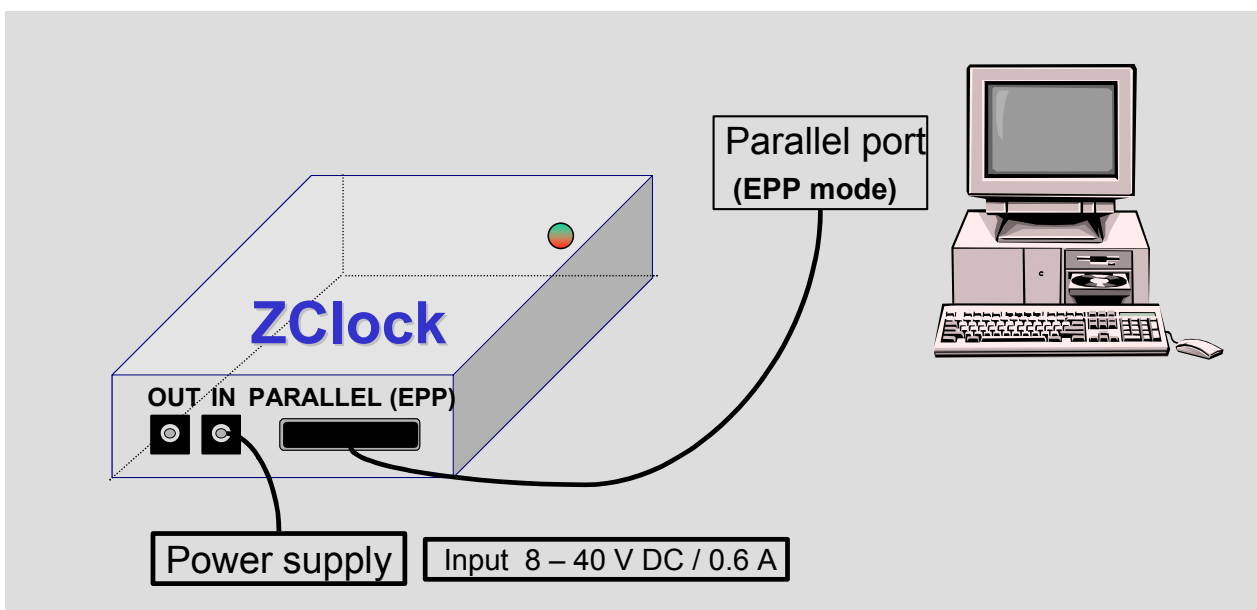
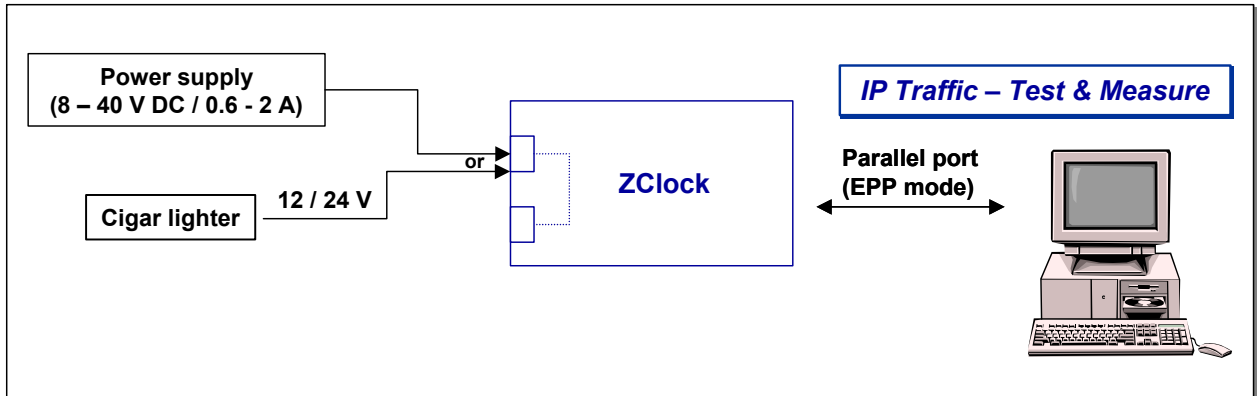
By using this GPS kit (Trimble OEM), the accuracy for IP packets time stamping is  $\leq 5$  milliseconds.



## 4.2 Configuration 2: "IP Traffic – Test & Measure" + ZClock

The ZClock module is provided with a parallel cable and the PC must operate in the EPP (Enhanced Parallel Port) mode.

In this configuration, there is no absolute time reference. User can use an external system in order to provide the time reference to the PC. ZClock is initialized with the PC clock time reference. By using ZClock, the accuracy for IP packets time stamping is  $\pm 1$  millisecond.

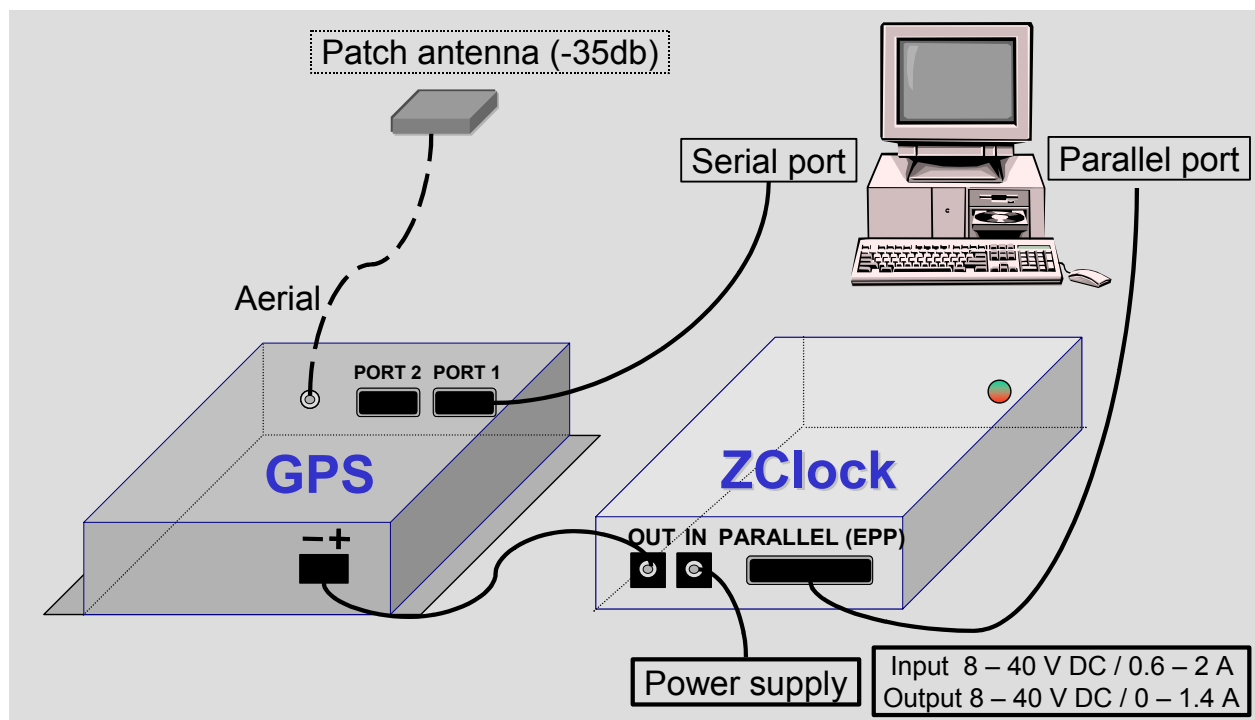
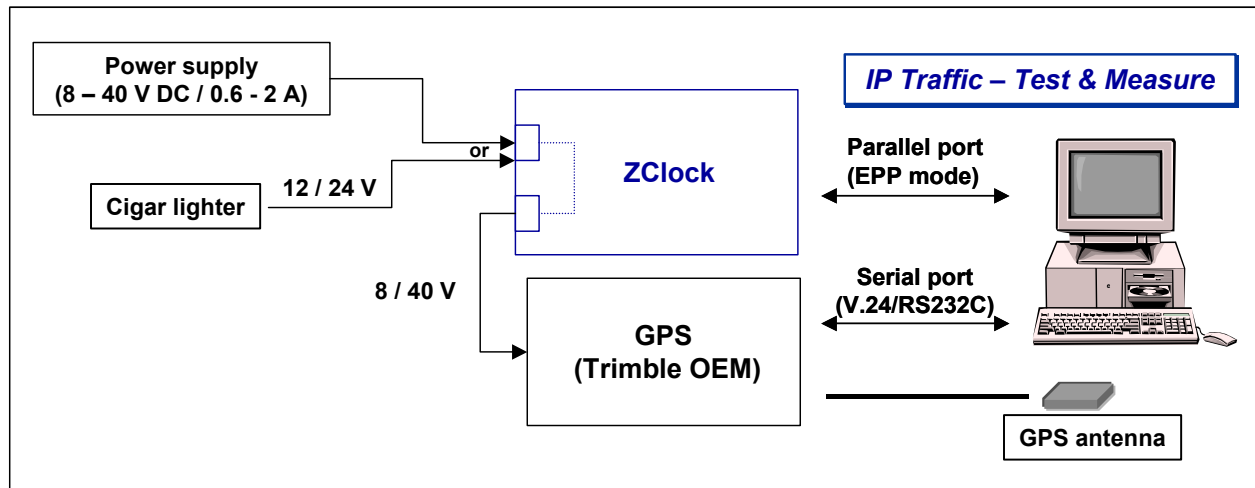


### 4.3 Configuration 3: "IP Traffic – Test & Measure" + GPS Kit + ZClock

The GPS Kit is provided with the GPS box, a serial cable and a –35 db patch antenna. This GPS provides an absolute time reference (accuracy:  $\pm 500$  nanoseconds).

The ZClock module is provided with a parallel cable and the PC must operate in the EPP (Enhanced Parallel Port) mode.

The GPS time reference is used to initialize ZClock. By using the GPS and ZClock, time stamping of IP packets by the Traffic Sniffer is made with an accuracy of  $\pm 1$  millisecond.

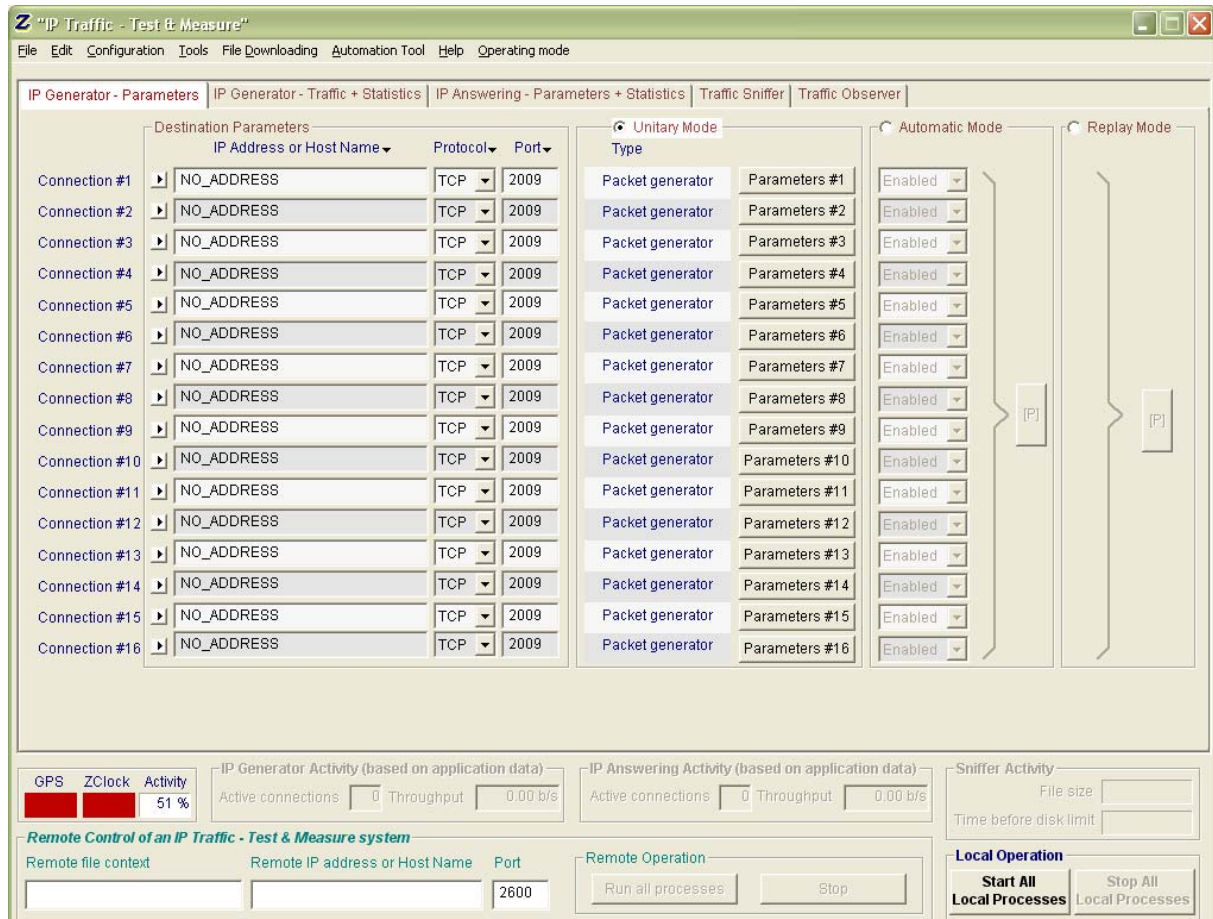




## Part 5: Graphical User Interface

### 5.1 Main Window

When you launch “IP Traffic – Test & Measure” (after the adapter selection on Windows 98), the following window is displayed:



**“IP Traffic – Test & Measure” main window**

The “IP Traffic – Test & Measure” main window is composed of four parts:

- **Menu bar:** File, Edit, Configuration, Tools, File downloading, Automation Tool, Help, Operating mode.
- **Tabs area:** this main area displays the five tabs. To view a tab, click on the tab title.
- **Activity display:** ‘GPS’ state, ‘ZClock’ state, ‘Activity’ parameter, ‘IP Generator Activity’, ‘IP Answering Activity’ and ‘Sniffer Activity’.
- **General commands:** for remote control or local operations.

Menu bar, activity display and global commands are always visible whatever the tab displayed.

## 5.2 Display General Rules of the “IP Traffic – Test & Measure” GUI

The fields of the “IP Traffic – Test & Measure” software interface can be filled following four situations:

### ❖ Fields in which the user can enter values

All the fields in which the user can enter or choose values are recognizable by black writing on gray or white background color.

### ❖ Statistics fields

Statistics fields are automatically filled. The user, who can only configure the refresh time of statistics display, cannot modify them or reset statistics display by pressing “Reset statistics” 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 for informational use only

These fields are filled automatically by “IP Traffic – Test & Measure” after the user had entered or selected parameters. They are displayed as reminder and will be modified by another user action.

### ❖ Fields turned out of reach further to user action

User actions and parameters selection may turn some “IP Traffic – Test & Measure” 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. The user has to stop running connection to change connection’s parameters.
- When a testing mode (unitary or automatic) is selected, it is impossible to change parameters of the unselected testing mode.
- If the user enters a no valid value in a field, the connection could be disabled or actions button in configuration windows could become out of reach.

## 5.3 Used Units in Information Display

All information used by “IP Traffic – Test & Measure” is displayed with its unit; unit is changing in order to limit figure size.

### 5.3.1 Volume units

Display	Meaning
10 B	10 Bytes
1 KB	1 Kilo Bytes (1024 bytes)
1 MB	1 Mega Bytes (1048576 bytes)
1 GB	1 Giga Bytes (1073741824 bytes)
1 TB	1 Tera Bytes (1099511627776 bytes)
1.23 <sup>65</sup>	1.23 x 10 <sup>65</sup> Bytes
1 p	1 packet

### 5.3.2 Throughput units

Display	Meaning
10 b/s	10 bits per second
1 Kb/s	1 Kilo bits per second (1024 b/s)
1 Mb/s	1 Mega bits per second (1048576 b/s)
1 Gb/s	1 Giga bits per second (1073741824 b/s)
1 Tb/s	1 Tera bits per second (1099511627776 b/s)
1.23 <sup>65</sup>	1.23 x 10 <sup>65</sup> bits per second
1 p/s	Packet per second

#### Note: Throughput computing

“IP Traffic – Test & Measure” displayed throughput corresponds to MTU data (transmitted bytes) on the sampling period (defined in the configuration menu) and brings back to a bytes/second number.

The displayed throughput is an “Application” throughput. At some instant, it could be different from physical network throughput because data can be split and buffered at various system levels.

### 5.3.3 Duration units

Display	Meaning
31 ms	31 milliseconds
1s	1 second
1mn32s	1 minute 32 seconds
1h24mn	1 hour 24 minutes
>24h	Time superior to 24 hours

## Part 6: Using "IP Traffic – Test & Measure"

### 6.1 Main steps

The main steps to use "IP Traffic – Test & Measure" are:

◆ **To send data:**

1. *In Tab 1 'IP Generator – Parameters':*

Configure IP Generator parameters (IP address or Host Name, port number, and protocol),  
Select and configure testing mode,

2. *In Tab 2 'IP Generator – Traffic + Statistics':*

Run connections,

3. Results: see and exploit statistics in the 'Traffic Observer' tab.

◆ **To receive data:**

1. *In Tab 3 'IP Answering - Parameters + Statistics'*

Configure IP Answering parameters (connected remote, working mode),

2. *In Tab 3 'IP Answering - Parameters + Statistics':*

Start receiving connections,

3. Results: see and exploit statistics in the "Traffic Observer" tab.

*Note about the context file:*



*In order to avoid entering again all parameters for a new testing session, or creating again mathematical laws, all the "IP Traffic – Test & Measure" parameters can be saved in a context file (see File menu description below).*

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

## 6.2 Launch “IP Traffic – Test & Measure”

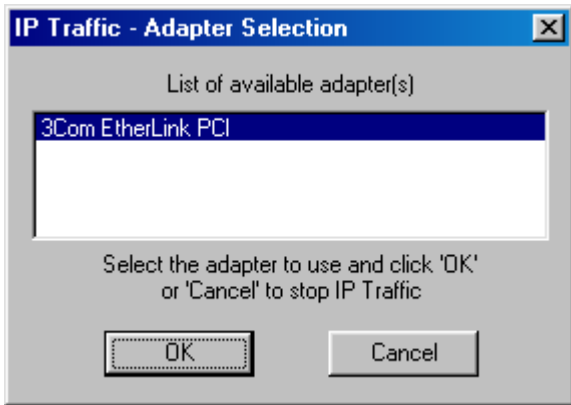
In the ‘Start > programs > IP Traffic’ Menu, select “IP Traffic – Test & Measure” and click. The software is launched.

*Step 1: depending of your license, you will get the following license window:*

Limited license	Unlimited license
	

**If you need to configure your license press <Enter>. Otherwise don’t press any key: after a few second this window will automatically disappear.**

*Step 2: depending of the operating system, you will get the following window*

Windows 98	Windows 2000 or XP
<p>The user must first select the adapter needed to send and receive IP traffic.</p>  <p>For example, select the 3Com Ethernet adapter in this desktop configuration and then press OK.</p> <p>After a while due to initializations, the “IP Traffic – Test &amp; Measure” main window is displayed.</p>	<p>After a while due to initializations, the “IP Traffic – Test &amp; Measure” main window is displayed.</p>

## 6.3 Menu description

### 6.3.1 File Menu



#### 6.3.1.1 [File/New](#)

This command opens a new default context in “IP Traffic – Test & Measure”. Before opening a new default context, running connections must be stopped. The default values of a new context are presented in the Annex part.

#### 6.3.1.2 [File/Open](#)

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

Note:

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

#### 6.3.1.3 [File/Save](#)

“Save” option allows saving the entire configuration parameters and parameters of the laws defined in the opened context file.

#### 6.3.1.4 [File/Save as](#)

This option allows saving all the configuration parameters and parameters of the laws defined in a context file (.CTX file), which name is requested in a standard enter dialog box.

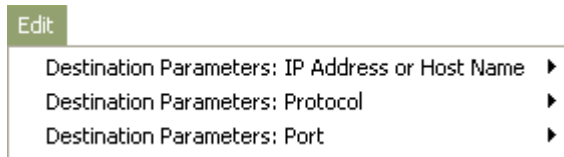
#### 6.3.1.5 [File/Recent Contexts](#)

This option allows charging the 4 most recent used context files (.CTX file).

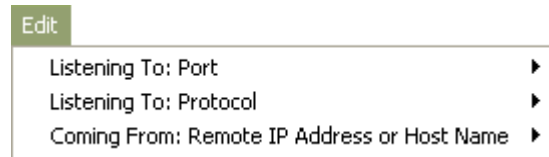
#### 6.3.1.6 [File/Exit](#)

This command stops “IP Traffic – Test & Measure”. To stop “IP Traffic – Test & Measure”, all active connections (‘IP Generator’ and ‘IP Answering’) shall be stopped. A message box will ask you to save or not changes made to parameters in a context file.

## 6.3.2 Edit menu



*Active tab: “IP Generator – Parameters”*



*Active tab: “IP Answering – Parameters + Statistics”*

### 6.3.2.1 Edit/Destination Parameters: IP Address or Host Name (for IP Generator)

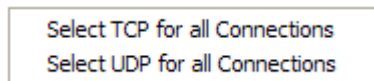
One option is available:



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

### 6.3.2.2 Edit/Destination Parameters: Protocol (for IP Generator)

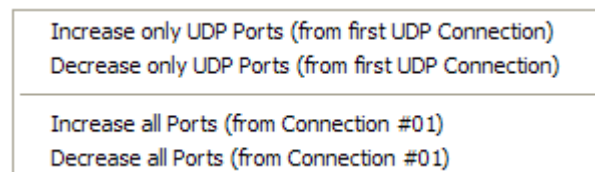
Two options are available:



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

### 6.3.2.3 Edit/Destination Parameters: Port (for IP Generator)

Four options are available:



With this menu, you can:

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

#### 6.3.2.4 [Edit/Listening To: Port \(for IP Answering\)](#)

Four options are available:

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

With this menu, you can:

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

#### 6.3.2.5 [Edit/Listening To: Protocol \(for IP Answering\)](#)

Two 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.

#### 6.3.2.6 [Edit/Coming From: Remote IP Address or Host Name \(for IP Answering\)](#)

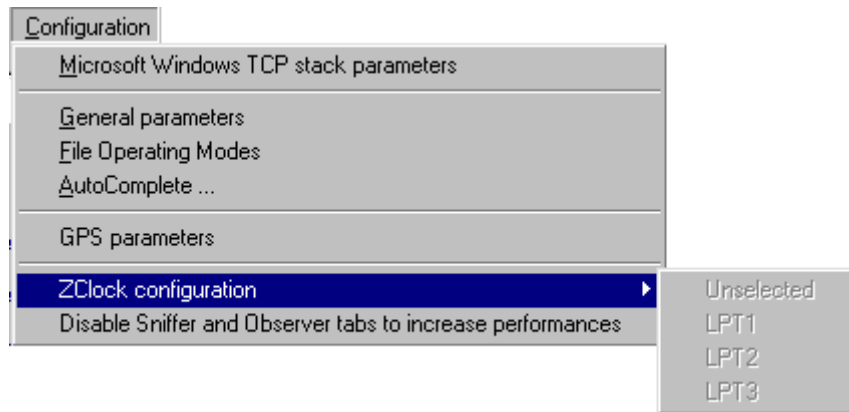
One option is available:

Copy the IP Address from Connection #01 to all Connections
--

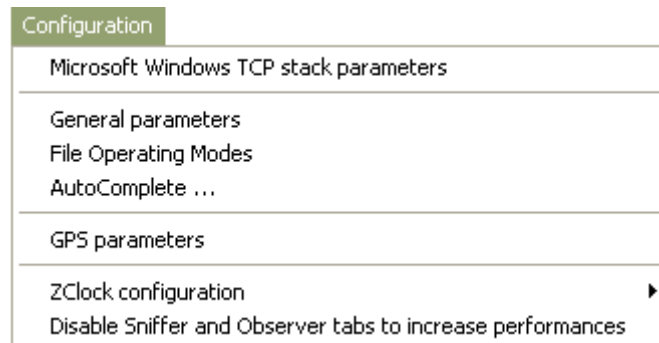
By selecting this item, the IP Address field from connection #01 is recopied for all connections from #02 to #16.



### 6.3.3 Configuration menu



*Windows 98*



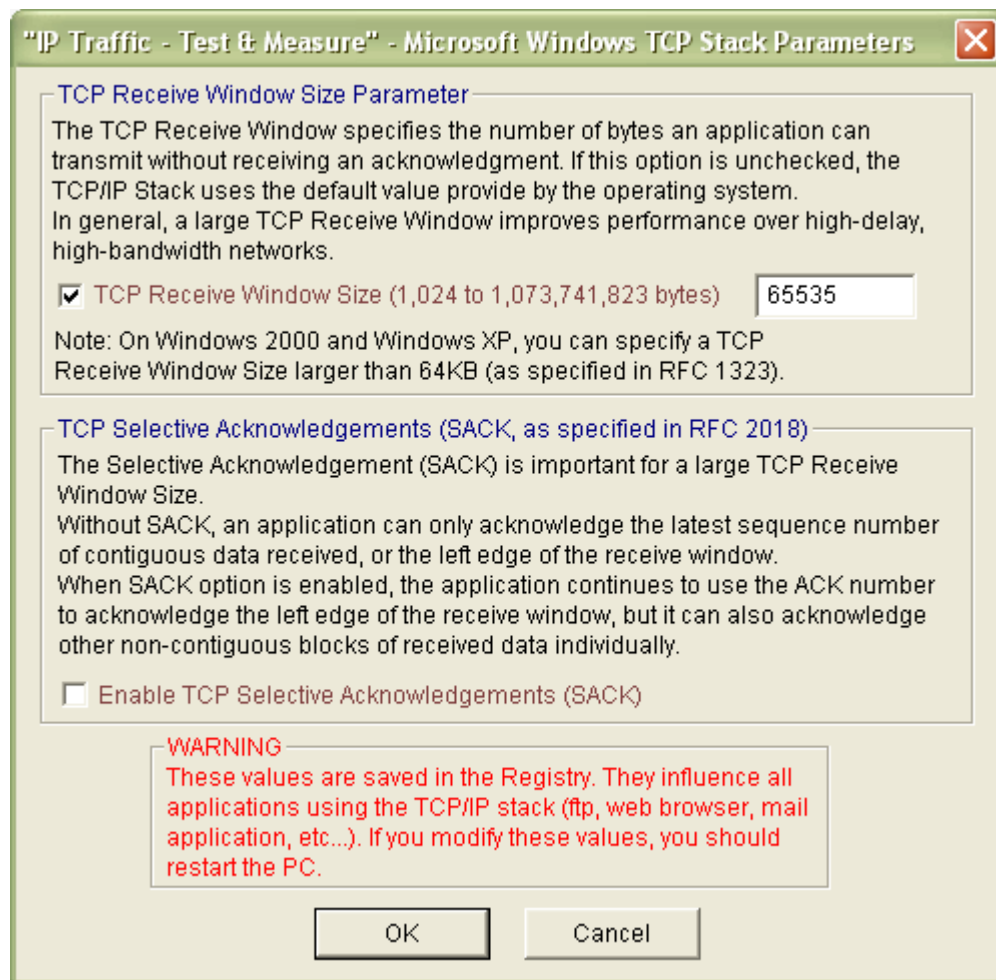
*Windows 2000 or XP*

#### 6.3.3.1 Microsoft Windows TCP Stack Parameters

"IP Traffic – Test & Measure" uses the Microsoft TCP/IP stack via the Winsock2 interface (or API). This interface enables modifying some parameters of the Microsoft TCP/IP stack.

"IP Traffic – Test & Measure" enables modifying the TCP Receive Window size and enables the TCP Selective Acknowledgements.

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



Microsoft Windows TCP 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 on the registry depend on the operating system:

- Windows 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).

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



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

### 6.3.3.2 *General parameters*

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

*General parameters window*

#### *Parameters applying to the GUI display*

Refresh time: the value entered in this field configures the display refresh time for all statistics displayed in "IP Traffic – Test & Measure".

Throughput sampling period: the value entered in this field is used to compute the throughput for the 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, "IP Traffic – Test & Measure" continues TCP data acquisition during a time defined by this timeout. If this value equals zero, "IP Traffic – Test & Measure" 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, "IP Traffic – Test & Measure" continues UDP data acquisition during a time defined by this timeout. If this value equals zero, "IP Traffic – Test & Measure" 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.

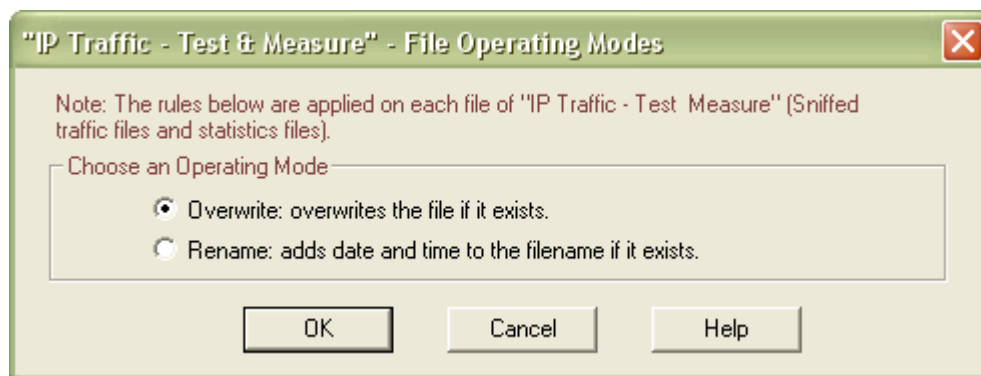
Transmit buffer size: this value is saved in the current context only and is used when sending data to the Microsoft Winsock2 interface.

### *Acquisition period for statistics*

This parameter is used to define the polling driver time in order to get statistics by the "IP Traffic – Test & Measure" application. This parameter defines the period to compute statistical average presented in the 'Traffic Observer' tab.

#### **6.3.3.3** *File Operating Modes*

This command allows selecting the file operation mode for every file generated by "IP Traffic – Test & Measure" except the context file. When selected, the following window is displayed:



*File Operating Modes window*

#### *Overwrite*

If you choose this mode, each time you start an export statistics process or the traffic capture, IP Traffic overwrites the file you have defined if it exists.

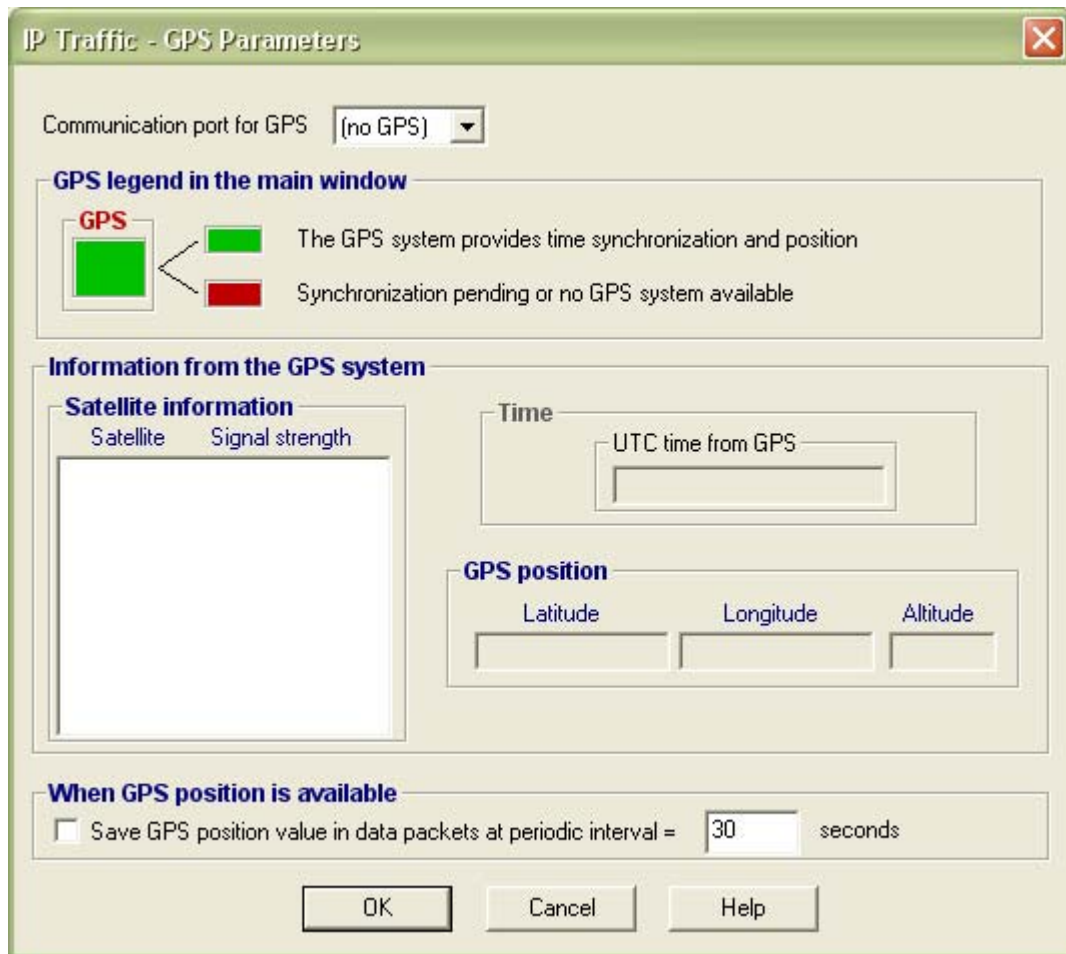
#### *Rename*

By choosing this mode, IP Traffic adds a suffix to the file name, if the file still exists. The suffix follows the format: mmddyyyy\_hhmmss

Example: For a file name IPGenerator\_Statistics, the resulting file name generated by IP Traffic will be IPGenerator\_Statistics\_01242004\_193020.

#### 6.3.3.4 GPS parameters

This command allows configuring parameters applying to the GPS system connected to the PC via a serial link.



This window is divided into four sections:

- **Communication port for GPS:** to select the GPS communication port (COM1 to COM6) or not (no GPS).
- **GPS legend in the main window:** colored icons giving information on the state of the GPS system (see the GPS color box on the lower left of the "IP Traffic – Test & Measure" main window)
  - ⇒ **Green color:** the GPS system provides complete timing and position information (3D). For this state, the GPS system is synchronized with at least four satellites.
  - ⇒ **Red color:** no information is available via the GPS system: either the GPS system is not operational (no GPS system or no power by example), or there is not enough satellites seen by the GPS to get precise timing information and position. In this case, change the position of the outdoor antenna of the GPS system and wait some minutes to see the result.

- *Information from the GPS system:*

⇒ Satellite information: for each satellite recognized by the GPS, satellite number and signal level is displayed.

Satellite information	
Satellite	Signal strength
20	9.00
24	11.00
28	7.00
7	8.20
(1)	---
(11)	1.60
(14)	0.00
(19)	0.00

In this example, 8 satellites are displayed, and only the satellites number 20, 24, 28 and 7 have a significant level.

*Satellite information*

XX means that the satellite XX is used for computation.

[XX] means that the satellite XX is not used for computation (time and localization).

*Signal strength information*

xx.yy indicates the signal level

--- means that the signal level is not significant

⇒ Time: time provided by the GPS system (GMT time).

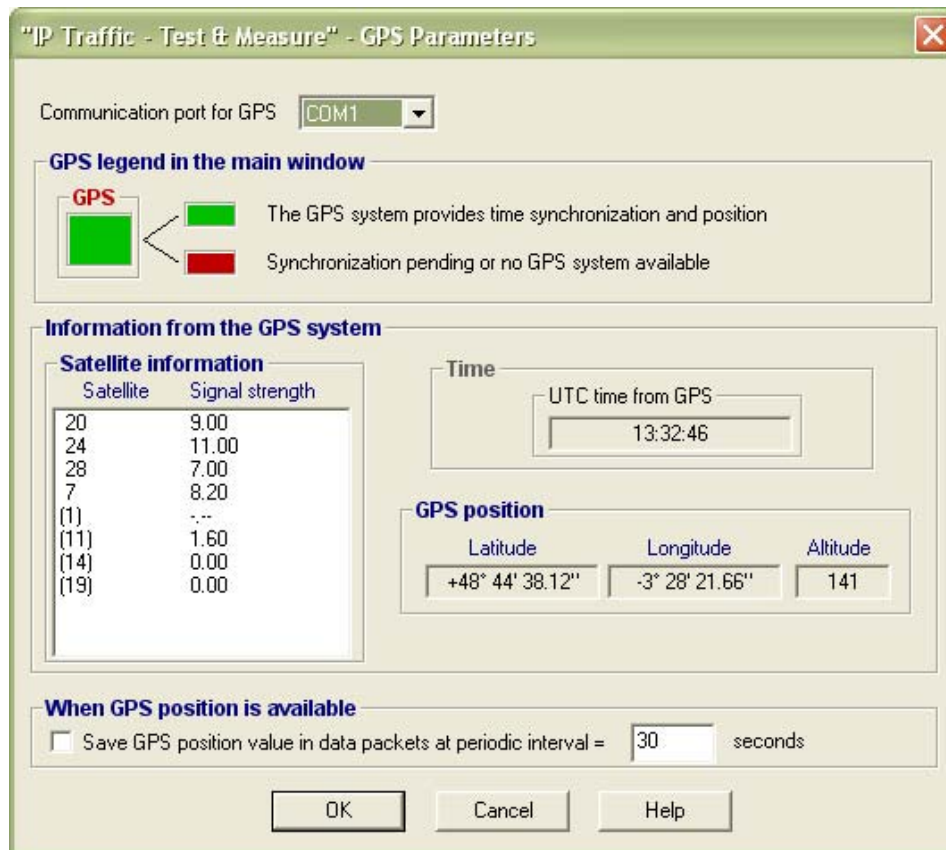
⇒ GPS position: 3D reference (latitude, longitude and altitude).

- *When GPS position is available*: GPS position (latitude, longitude and altitude) can be added for data packets at a user-defined rate. This additional information is stored by "IP Traffic – Test & Measure" in specific record of the Traffic sniffed file and it is not included in the data packets.

In the "GPS parameters" window, a **Help** button delivers information about 'How GPS works' and how to use it.

*Example of GPS parameters window (obtained in Lannion, FRANCE)*

In this example, four satellites have a significant level, and GPS position is available.



### 6.3.3.5 AutoComplete

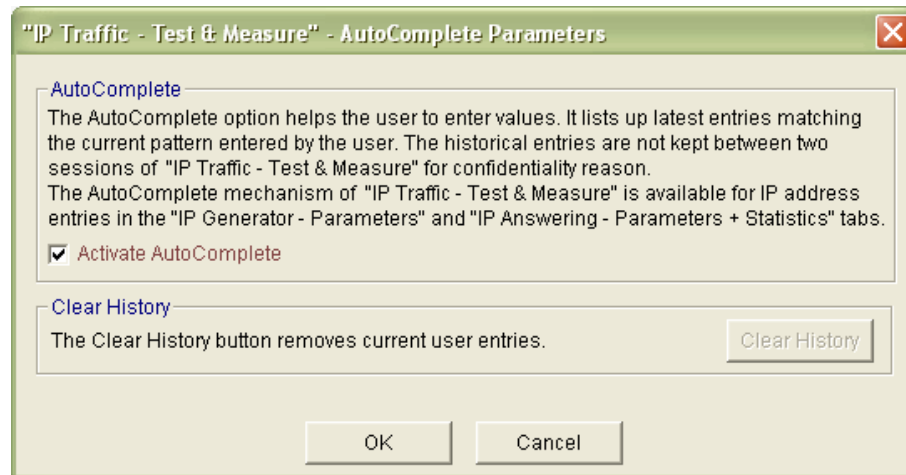
The AutoComplete option is a help mechanism to input values for the user. It lists possible entries that match user entries typed before. The AutoComplete mechanism with "IP Traffic – Test & Measure" is available for IP address entries in the "IP Generator – Parameters" and "IP Answering – Parameters + Statistics" tabs.



There are 3 different historical records:

- Historical record for IP address entry in the IP Generator tab,
- Historical record for IP address entry in the IP Answering tab
- Historical record for IP address in the File Downloading dialog box.
- Historical record for IP address on the Remote Control panel
- Historical record for IP address entry in user-defined filter edition window on the Traffic Sniffer tab.

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



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

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

- **NO\_ADDRESS:** this is the default IP Address of the Traffic Generator - a void address, used to disable the connection.
- **ANY\_ADDRESS:** this is the default IP Address of the Answering, used to accept any incoming connection.

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

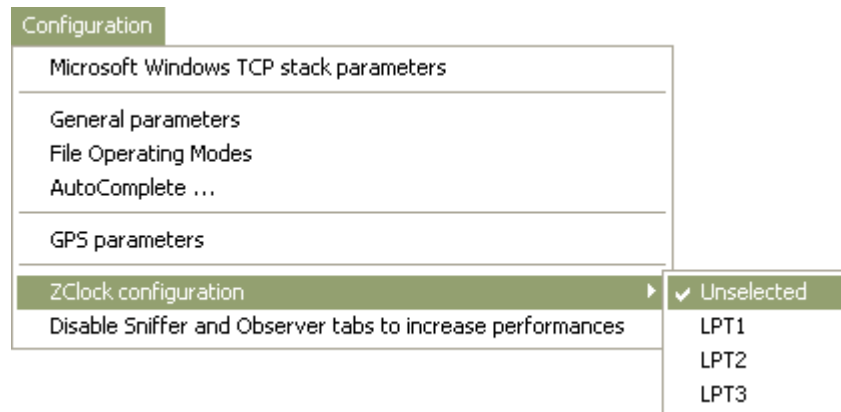
*Note: the historical record is associated to the "IP Traffic – Test & Measure" session. For confidential reasons, the historical record is not kept between sessions and is lost at the end of the "IP Traffic – Test & Measure" session.*



### 6.3.3.6 ZClock configuration

This item allows configuring parameters applying to the ZClock module connected to the PC via a parallel cable in EPP mode. You can configure the EPP mode at boot time in the Setup menu or by using the specific driver of the addition card - PCI and PC card add-ons supporting EPP mode are commonly available.

You can select the parallel port to use ZClock with "IP Traffic – Test & Measure".

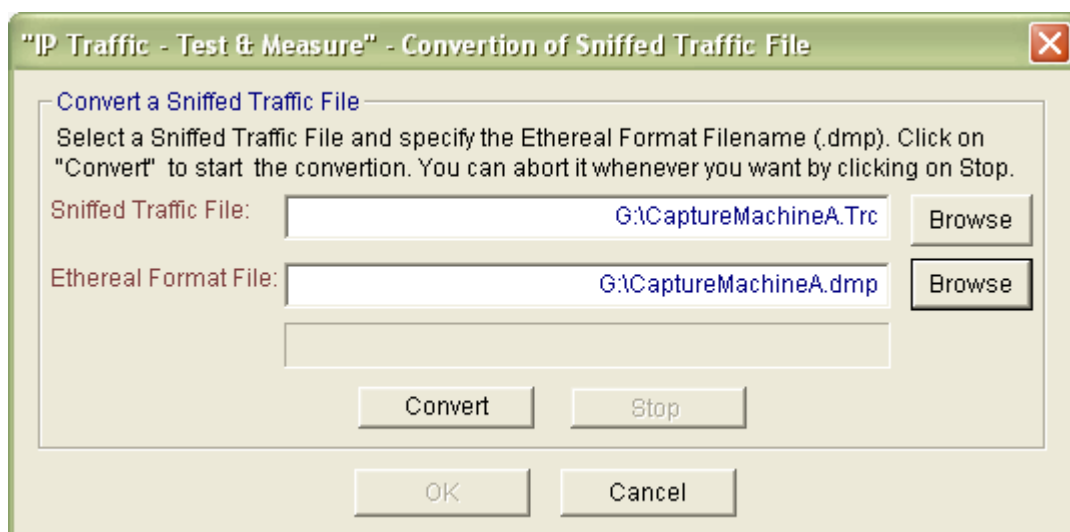
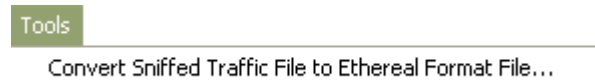


### 6.3.3.7 Disable 'Traffic Sniffer' and 'Traffic Observer' tabs to increase performances

This item allows disabling the 'Traffic Sniffer' and 'Traffic Observer' tabs in order to free processors and memory resources for traffic generation on slow computers.

When this option is selected, IP level statistics (and graphics) as well as the sniffer features are not available any more.

## 6.3.4 Tools menu



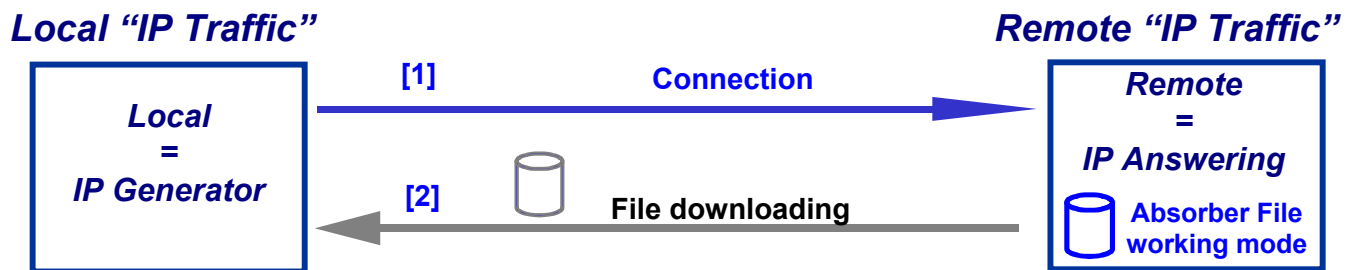
This tool allows converting the Sniffed Traffic files by "IP Traffic" to Ethereal Standard format. By realizing this operation, the result file (dmp) can be opened by a Network Analyzer software such as Ethereal or Network Instruments Observer.

### 6.3.5 File downloading menu

#### File Downloading

This command allows downloading a file from one "IP Traffic – Test & Measure" machine to another one. In order to avoid confusion, "Local" and "Remote" terms are used to indicate the machines for this command.

File Downloading is mainly used when a receiving connection is operating in Absorber File working mode. It is aimed at repatriating the absorbed file from IP Answering to IP Generator, as shown in the following scheme (any file from the remote machine can be downloaded).



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

[1] The Remote 'IP Answering' stocks received data in a file.

[2] The user of the Local 'IP Generator' 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 at repatriating the absorbed file from the 'IP Answering' part to compare it to the file sent by the 'IP Generator' part, as shown below.

The Remote 'IP Answering' is configured in the Absorber file Mode, for TCP connection.

The Local 'IP Generator' establishes a TCP connection and sends data from a file.

When the connection is finished, the 'IP Generator' uses the File downloading function to get received data from the Remote 'IP Answering'. The user of Local 'IP Generator' can check if data transfer was successful.

## Process a file downloading

When clicking on the file downloading command, the following window is displayed:

*File downloading window*

**To process a file transfer, do the following steps:**

On local and remote machines:

**[1]** Configure port number – Port number must be the same for local and remote machines.

On local machine:

**[2]** Give the name and path of the remote file to download. To be downloaded, file must not be read or enriched on the remote machine at the same time.

**[3]** Give the IP address of the remote machine from which file is downloaded.

**[4]** Give local name of the destination file.

**[5]** Press the "Start" button to begin file downloading from remote machine.

"OK" button allows saving the entered parameters and closes the window.

Note:

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

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

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

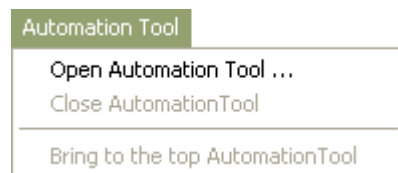
- Remote IP address is the IP address of the machine from which you want to download the file.
- Port number is the port number for file downloading (it must be the same for remote and local machines).
- Local filename downloaded by remote is the name of the downloaded file.
- Data volume to send is the total volume of the file to download.
- Data remaining volume is the volume still to send.

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

#### File downloading is working as follows:

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

### 6.3.6 Automation Tool menu



#### 6.3.6.1 Open

The Open command launches the "Automation Tool for IP Traffic".

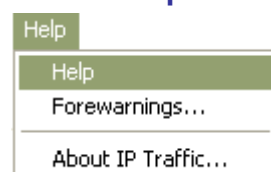
#### 6.3.6.2 Close

The Close command stops the "Automation Tool for IP Traffic".

#### 6.3.6.3 Bring to the top

The Bring to the top command displays the "Automation Tool for IP Traffic" on the top of other windows.

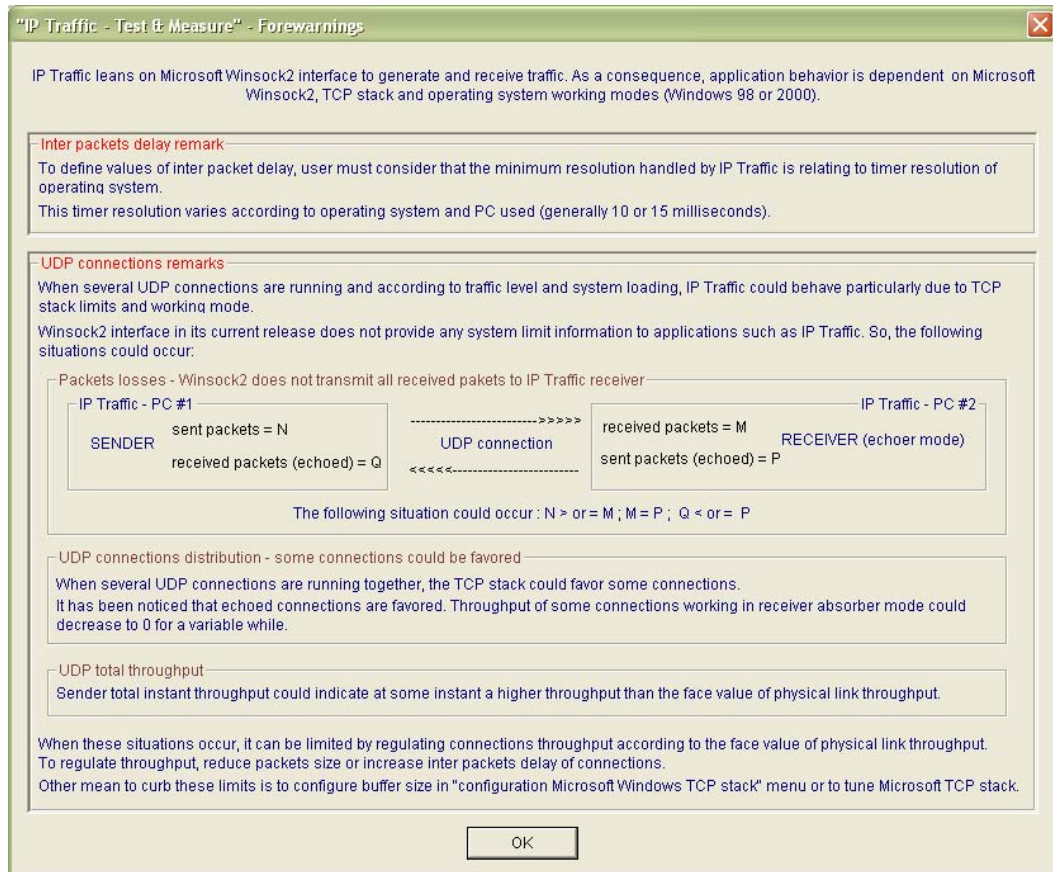
### 6.3.7 Help Menu



### 6.3.7.1 [Help](#)

Help command displays help on "IP Traffic – Test & Measure". Pressing «F1» key can also activate help.

### 6.3.7.2 [Forewarnings menu](#)



This menu is aimed at informing "IP Traffic – Test & Measure" special behaviors due to system limits.

"IP Traffic – Test & Measure" leans on Microsoft Winsock 2 Interface to generate and receive TCP or UDP traffic. Therefore, "IP Traffic – Test & Measure" application behavior, as any Winsock 2 application, is dependent on Winsock 2 Interface, Microsoft TCP Stack and operating system working modes.

#### 6.3.7.2.1 *Inter packets Delay*

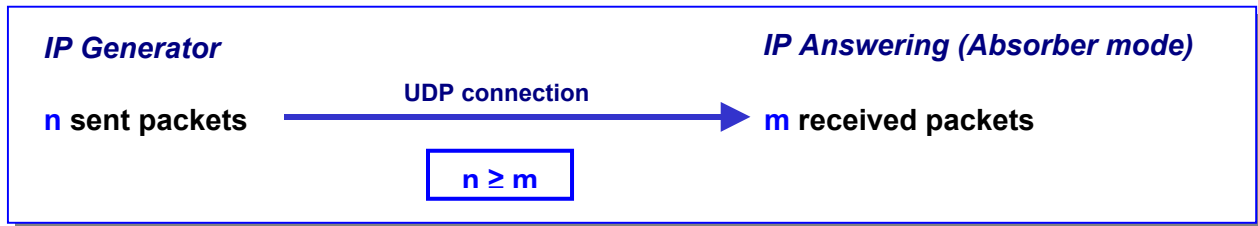
When defining Inter packet delay, the user must consider that minimum resolution handled by "IP Traffic – Test & Measure" is related to timer resolution of operating system. This timer resolution varies according to the used operating system and PC. Usually, timer resolution is 10 or 15 ms.

#### 6.3.7.2.2 *UDP connections*

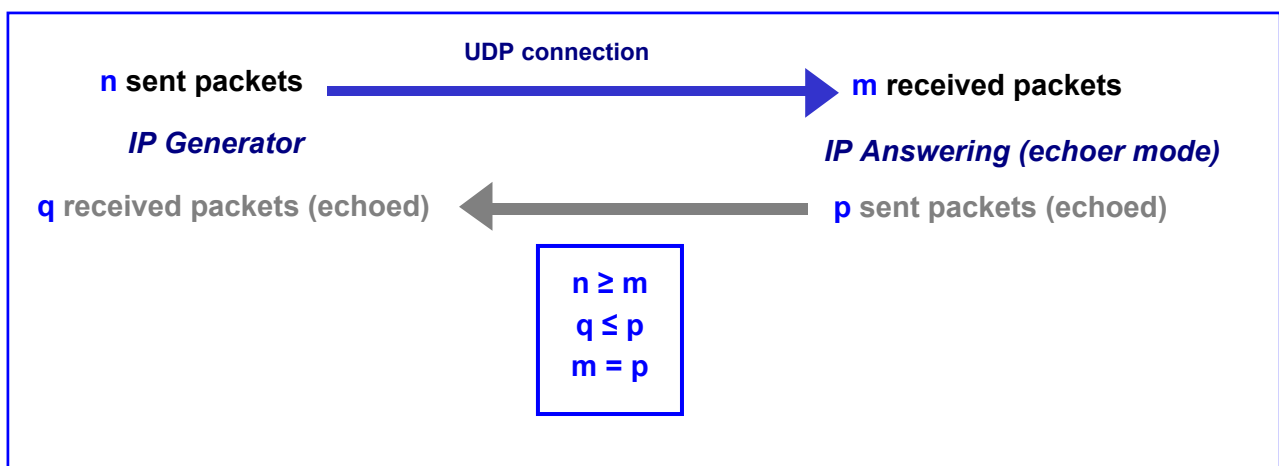
When several UDP connections are running and according to traffic level and system loading, "IP Traffic – Test & Measure" application could behave particularly due to TCP stack limits and working mode.

### Packet losses

- ❖ UDP connection from Local IP Generator to Remote IP Answering - the working mode of the Remote IP Answering is absorber.



- ❖ UDP connection from Local IP Generator to Remote IP Answering - the working mode of the Remote IP Answering is echoer.



In this case, number of received packets (m) will be equal to the number of echoed packet (p) in the 'IP Answering' part. Nevertheless, the number of received packets (q) in the 'IP Generator' part could be inferior to the number of packets (p) sent by the Remote 'IP Answering' in echoer mode.

### UDP connection distribution

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

Throughput of some connections working in the 'IP Answering' absorber mode could decrease to zero for a variable while.

### UDP total throughput

IP Generator total instant throughput could indicate at some instant a higher throughput than the face value of physical link throughput.

When these situations occur, it can be limited by regulating connections throughput according to the face value of physical link throughput. To regulate throughput, reduce packets size or increase inter packets delay of connections. Other mean to curb these limits is to configure buffer size in "configuration-Microsoft Windows TCP stack" menu or to tune the Microsoft TCP stack.

#### 6.3.7.3 About "IP Traffic – Test & Measure" ...

"About" command displays the version number and copyright of the "IP Traffic – Test & Measure" software and ZTI contact information.

### 6.3.8 Operating mode menu

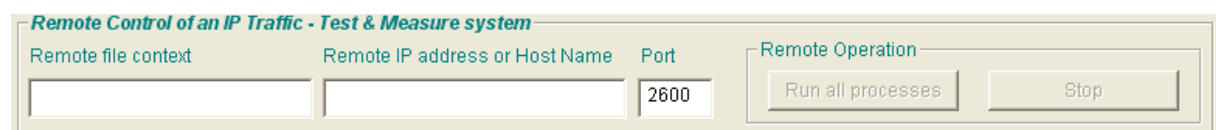


#### 6.3.8.1 Local mode

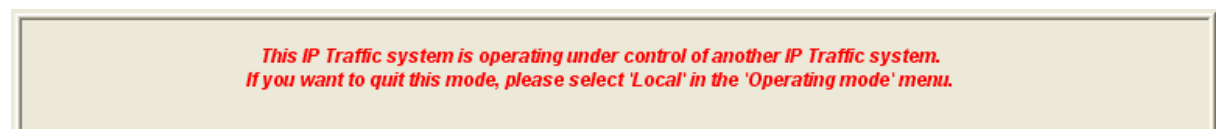
By selecting this mode, all "IP Traffic – Test & Measure" functionalities and commands are available.

#### 6.3.8.2 Remote control mode

**The "Remote" item is enabled only if you have previously filled in the port number in the "Remote control of an «IP Traffic – Test & Measure» system" (for example, 2600 in the example below). Therefore, this system will wait an incoming TCP connection on this port in order to operate under control of a remote system.**

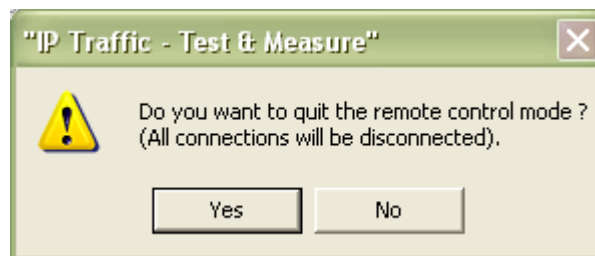


When the remote control mode is selected, a message is displayed at the bottom of the "IP Traffic – Test & Measure" main window as described below, and all button commands and tabs are inhibited.



The "Traffic Observer" tab is displayed and you can see the connections activity if any.

To quit this mode, select the item menu "Normal" of the Operating mode menu. A message is then displayed:



Press OK to return in normal operating mode.

A remote "IP Traffic – Test & Measure" system can operate with another "IP Traffic – Test & Measure" system in remote control mode by using commands at the bottom of the "IP Traffic – Test & Measure" main window (left part):



First, you define the remote context file to load on the remote "IP Traffic – Test & Measure" machine, and define the remote IP address and port number.

*Note: the remote "IP Traffic – Test & Measure" machine must be set before in the 'Remote' mode (by using the 'Remote' item of the 'Operating mode' menu).*

When the "Run all processes" button is pressed, a TCP connection is established with the remote system in order to supervise the link between the two systems.



Then the context filename previously defined is sent to the remote. The remote system loads this file context and then executes the "Run all processes". This specific TCP connection between local and remote is stopped when you press the "Stop" button of the 'Remote operations' on the local system.

## 6.4 Main window: the five tabs

### Tabs general presentation:

"IP Traffic – Test & Measure" presents five tabs:

IP Generator - Parameters	IP Generator - Traffic + Statistics	IP Answering - Parameters + Statistics	Traffic Sniffer	Traffic Observer
---------------------------	-------------------------------------	--	-----------------	------------------

*"IP Traffic – Test & Measure" tabs titles*

- ⇒ The first two tabs are related to the 'IP Generator' module. They are named "**IP Generator - Parameters**" and "**IP Generator - Traffic + Statistics**".
- ⇒ The third one is related to the 'IP Answering' module, it is named "**IP Answering - Parameters + Statistics**".

For the first three tabs related to the 'IP Generator' and 'IP Answering' modules, each one of the 16 connections is represented by one line (from "connection #1" to "connection #16"). Columns represent parameters or status of connections and statistics.

- ⇒ The fourth tab concerns the management of the Sniffer allowing IP traffic capture: the "**Traffic Sniffer**".
- ⇒ The fifth tab is named "**Traffic Observer**": all statistics and graphs are displayed in this tab with many user commands and parameters.

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

## 6.5 Main window: the activity display

"IP Traffic – Test & Measure" displays four information areas:

<div>GPS ZClock Activity</div> <div> <div></div> <div></div> <div>7 %</div> </div>	<div>IP Generator Activity (based on application data)</div> <div>Active connections 16 Throughput 7.25 Mb/s</div>	<div>IP Answering Activity (based on application data)</div> <div>Active connections 16 Throughput 7.25 Mb/s</div>	<div>Sniffer Activity</div> <div>File size 8 B</div> <div>Time before disk limit &gt;24 h</div>
--	--	--	---

- The left area contains three indicators:
  - The **GPS** colored status (green or red). If green, GPS is present and operational.
  - The **ZClock** colored status (green or red). If green, ZClock is present and operational.
  - The **Activity** counter expressed in % indicating the general O.S. activity
- **IP Generator Activity** with the total number of active connections and the total throughput for these connections.
- **IP Answering Activity** with the total number of active connections and the total throughput for these connections.
- **Sniffer Activity** to indicate the current Sniffer activity (saving files) with the current total file size already saved on disk and time available before disk limit.

Statistics display refresh time, and sampling period to compute throughputs are configured in *Configuration / General Parameters* menu.



## 6.6 Main window: the general commands

"IP Traffic – Test & Measure" offers two command blocks at the bottom of the main window:

- On the left: commands for **Remote control of an "IP Traffic – Test & Measure" system**

For remote control, you must first specify the following parameters:

- ⇒ Remote file context: filename of the "IP Traffic – Test & Measure" context to load
- ⇒ The remote IP address
- ⇒ The associated Port number

Then you control the remote "IP Traffic – Test & Measure" system with these commands:

- ⇒ **Run all processes**: the 'IP Generator' and 'IP Answering' modules of the remote system are started.
- ⇒ **Stop**: the 'IP Generator' and 'IP Answering' modules of the remote system are stopped.

### Note:

*The previous commands are used to control a remote "IP Traffic – Test & Measure" system. The remote system must be switched before in 'Remote control mode' by using the "Operating mode" menu (and you must specify on this remote system the same port number as the one defined previously for the local system).*

- On the right: **Local Operation**

The user can launch four main functionalities independently: IP Traffic Generator ("Run All Connections"), IP Answering ("Start receiving traffic"), Traffic Sniffer ("Start") and Export statistics of the Traffic Observer tab ("Start").

The command button "**Start All Local Processes**" is used to activate simultaneously these functions. The command button "**Stop All Local Processes Stop**" stops all active functions.

### Note:

*User must first define if the start commands for the 'Traffic Sniffer' and the export of statistics in the 'Traffic Observer' tab are included in the "Run all processes" command. [See check boxes in the 'Traffic Sniffer' (Enable automatic start in local operation) and in the parameters button of 'Export statistics' in the 'Traffic Observer' (Enable automatic export in local operation)].*

## 6.7 The 'IP Generator – Parameters' tab

The 'IP Generator' module is composed of two tabs:

- ⇒ **IP Generator – Parameters** tab: to configure connections and testing mode.
- ⇒ **IP Generator – Traffic + statistics** tab: to command traffic generation and visualize traffic statistics.

The "IP Generator – Parameters" tab is described in this chapter. The "IP Generator – Traffic + statistics" tab is explained in the next chapter.

The 'IP Generator' module handles up to 16 simultaneous connections and traffic can be generated following three exclusive testing modes:

- Unitary mode
- Automatic mode
- Replay sniffed traffic

The “IP Generator – Parameters” tab allows to:

- ⇒ Enter destination parameters (IP address, port number, protocol) for each connection.
- ⇒ Select files in which save received data when connections are working in echoer mode on remote IP Answering part.
- ⇒ Select and configure the testing mode: Unitary, Automatic or Replay.


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

IP Generator - Parameters				IP Generator - Traffic + Statistics				IP Answering - Parameters + Statistics				Traffic Sniffer				Traffic Observer							
<b>Destination Parameters</b>								<b>Unitary Mode</b>								<b>Automatic Mode</b>				<b>Replay Mode</b>			
IP Address or Host Name ▼				Protocol ▼		Port ▼		Type															
Connection #1 ▶	192.168.0.30	UDP ▼	2009	Mathematical law	Parameters #1	Enabled ▼																	
Connection #2 ▶	192.168.0.30	UDP ▼	2010	Packet generator	Parameters #2	Enabled ▼																	
Connection #3 ▶	192.168.0.30	UDP ▼	2011	File to send	Parameters #3	Enabled ▼																	
Connection #4 ▶	192.168.0.30	UDP ▼	2012	User file	Parameters #4	Enabled ▼																	
Connection #5 ▶	192.168.0.30	UDP ▼	2013	User DLL	Parameters #5	Enabled ▼																	
Connection #6 ▶	NO_ADDRESS	TCP ▼	2014	Packet generator	Parameters #6	Enabled ▼																	
Connection #7 ▶	192.168.0.30	TCP ▼	2015	Packet generator	Parameters #7	Enabled ▼																	
Connection #8 ▶	192.168.0.30	TCP ▼	2016	Packet generator	Parameters #8	Enabled ▼																	
Connection #9 ▶	192.168.0.30	TCP ▼	2017	Packet generator	Parameters #9	Enabled ▼																	
Connection #10 ▶	192.168.0.30	TCP ▼	2018	Packet generator	Parameters #10	Enabled ▼																	
Connection #11 ▶	192.168.0.30	TCP ▼	2019	Packet generator	Parameters #11	Enabled ▼																	
Connection #12 ▶	192.168.0.30	TCP ▼	2020	Packet generator	Parameters #12	Enabled ▼																	
Connection #13 ▶	192.168.0.30	TCP ▼	2021	Packet generator	Parameters #13	Enabled ▼																	
Connection #14 ▶	192.168.0.30	TCP ▼	2022	Packet generator	Parameters #14	Enabled ▼																	
Connection #15 ▶	192.168.0.30	UDP ▼	2023	Packet generator	Parameters #15	Enabled ▼																	
Connection #16 ▶	192.168.0.30	TCP ▼	2024	Packet generator	Parameters #16	Enabled ▼																	

Tab 1: IP Generator – Parameters

### 6.7.1 Destination Parameters

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

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

#### 6.7.1.1 Summary of connection parameters

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

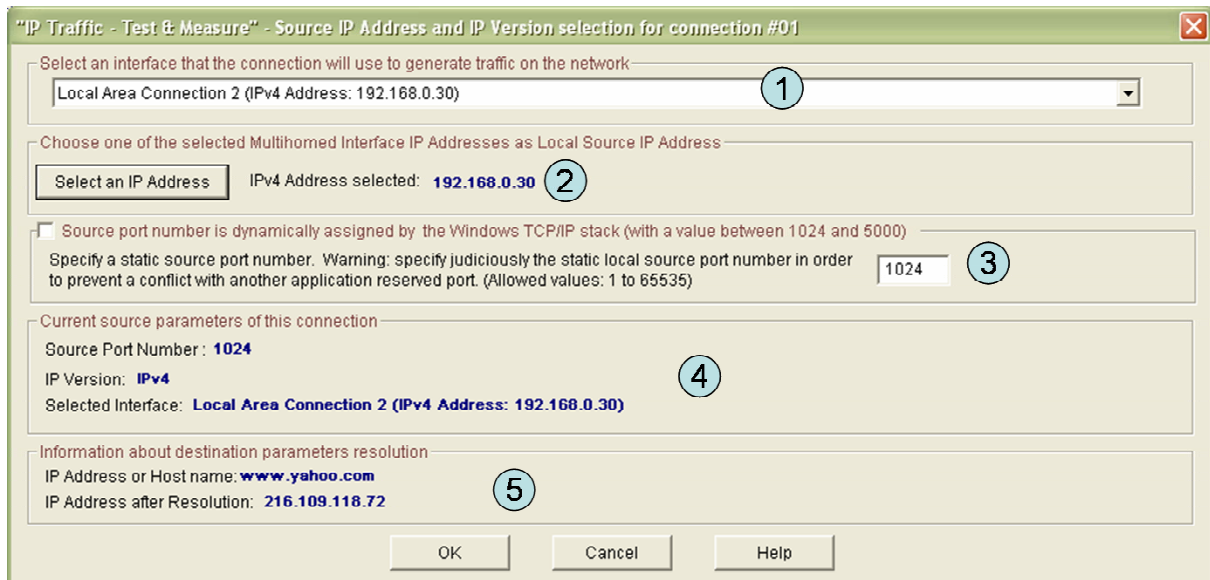


The tooltip for the IP Generator connection includes 5 items:

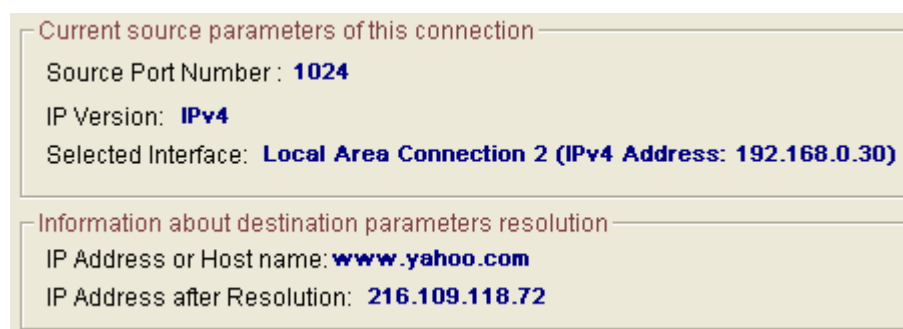
- First item is the connection number the tooltip refers to.
- Next item is the IP address defined by the user.
- Next item is the IP address translated when IP Translation address has succeeded (e.g. the address is not NO\_ADDRESS nor 0.0.0.0).
- Next item is the IP version currently selected.
- Last item is the interface name selected. The name displayed is the name of the connection presented in the “Settings/Network and Dial-up Connections” Start menu of the operating system (Default is “Interface chosen by the system”).

### 6.7.1.2 Select the network interface, source IP address and source port number

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

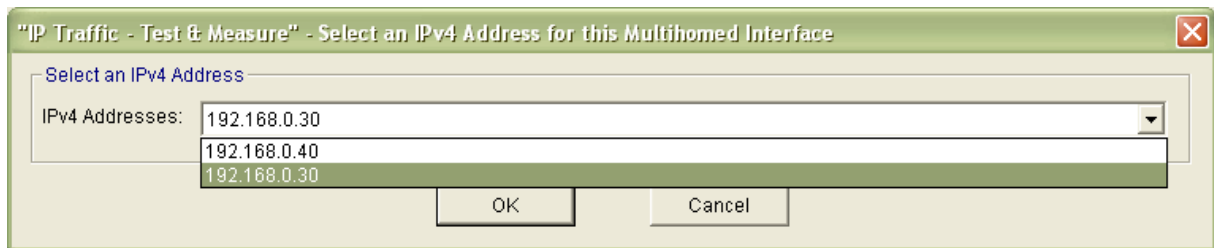


- The **network interface** selection is optional. It is used to force connections to be established using a specific interface.
  - By default:  
The IP stack resolves the network interface selection to send packets to the remote. The IP stack uses the destination IP address to select the network interface.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



- Network 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.
- **Select IP address button** is available when multiple IP addresses are attached to the network interface. This network configuration is also known as 'multihomed' interface. Selection of a Source IP address is generally not required: "IP Traffic – Test & Measure" uses the default IP address of the interface to establish connections. It may be useful to change the source IP address when routing priority or policy is defined.

Example of IP address selection for a multihomed interface:



*Note: select an IP address is not available if the default interface 'Interface chosen by the system' is selected.*

- **Specification of the source local port number** is by default disabled. In this case, the system automatically chooses the source port number for any connection generating traffic. In order to take care of respecting the rules of a firewall for example, the source port number can be user defined.
- **Current parameters of this connection** area are an abstract for the connection. It summarizes IP address, numerical IP address format, IP version and interface selection.
  - IP addresses are static. The IP address translation will process only when you click on OK.
  - Current network interface is dynamically updated with the user selection.

*Warning:*  
 When you click on the OK button, if the network interface is selected, the IP address translation is automatically started. It may be time consuming.

### 6.7.1.3 IP Address translation mechanism

"IP Traffic – Test & Measure" 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 Network Interface parameters changes, when you move from 'IP Address or Host Name' field to another field or another tab, when the Enter key is pressed or when Network Interface parameters change, automatically starts the IP address translation mechanism.

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

If network environment changes – e.g. a new DNS has been defined - you should press the Enter key in the 'IP Address or Host Name' field to force "IP Traffic – Test & Measure" restart the translation mechanism for this connection.

*Note:*  
 When the IP address translation failed, the IP address is written **red** on white. This connection cannot be started: the "Run" button in the 'IP Generator – Traffic + Statistics' tab is grayed.

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

- the focus leaves the 'IP Address or Host Name' field,
- you press the Enter key while the focus is in the 'IP Address or Host Name' field,
- another tab is selected,
- you duplicate parameters from one connection to another one,

- you change the Network Interface parameters.

#### 6.7.1.4 Description of the Copy/Paste mechanism

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

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

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

Destination Parameters			
	IP Address or Host Name	Protocol	Port
Connection #1	192.168.0.13	TCP	2009
Connection #2	NO_ADDRESS	TCP	2009
Connection #3	NO_ADDRESS	TCP	2009

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

	IP Address or Host Name	Protocol	Port
Connection #1	192.168.0.13	TCP	2009



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

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

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

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



(Copy mode)

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

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

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

#### 6.7.1.5 *Description of the floating menu mechanism*

In the Destination Parameters object, the labels 'IP address', 'Port' and 'Protocol' are mouse sensitive.



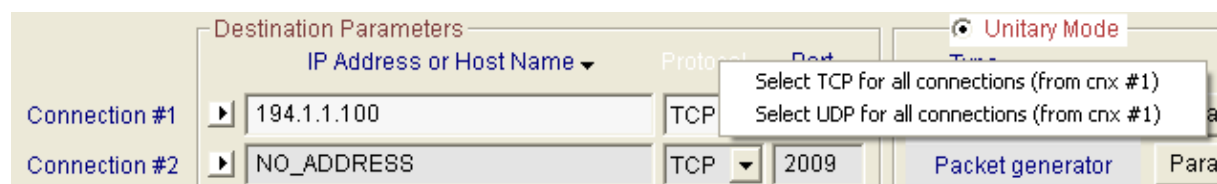
When the mouse is located on the 'IP Address or Host Name' text area for example, the text color changes to white. Then click left your mouse to display the associated menu.

#### *Floating menu for the 'IP Address or Host Name' label*



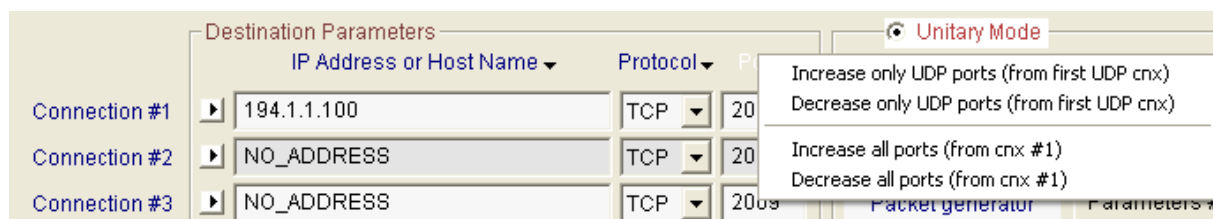
With this function, you can duplicate the IP address or the Host name from the first connection to the others fifteen connections.

#### *Floating menu for the 'Protocol' label*



This menu helps to set the same protocol to every connection.

#### *Floating menu for the 'Port' label*



With this menu you can:

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



## 6.7.2 Configure the unitary mode

Type	Parameters
Mathematical law	Parameters #1
Packet generator	Parameters #2
File to send	Parameters #3
User file	Parameters #4
User DLL	Parameters #5
Packet generator	Parameters #6
Packet generator	Parameters #7
Packet generator	Parameters #8
File to send	Parameters #9
Mathematical law	Parameters #10
Packet generator	Parameters #11
User DLL	Parameters #12
User file	Parameters #13
Packet generator	Parameters #14
Packet generator	Parameters #15
Packet generator	Parameters #16

The unitary mode is one of the three testing modes offered by the ‘IP Generator’ module. Note that each testing mode is exclusive, i.e. it is impossible to mix connections in unitary testing mode and connections in another mode.

Unitary mode is configured in Tab 1 “IP Generator - Parameters” and launched from Tab 2 “IP Generator - Traffic + Statistics”.

To run or configure unitary testing session, you must first select ‘Unitary mode’.

By pressing “Parameter #n” buttons, a parameters window is displayed and the parameters for this connection can be configured.

The main selected unitary testing parameter of connection #n is reminded beside the “Parameters #n” button: Mathematical law, Packet generator, File to send, User file or User DLL.

When the “Parameters #n” button is pressed, the following window is displayed.

**Mode 1: Using the Internal Data Generator**

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

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

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

- ☒ Fix
- ☐ Random  min  max
- ☐ Alternate  value-1  value-2
- ☐ Increasing / Decreasing  min  max  step

**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)

**Step 2: Specify Data size and packets parameters**  
In this step, define Data Size and packets parameters as well as the delay between each sent packet.

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

- ☒ Fix
- ☐ Random  min  max
- ☐ Alternate  size-1  size-2
- ☐ Increasing / Decreasing  min  max  step

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

- ☒ Fix  (See Forewarnings menu please)
- ☐ Random  min  max
- ☐ Alternate  value-1  value-2
- ☐ Increasing / Decreasing  min  max  step
- ☐ Mathematical law

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

**Mean Throughput (8 to 999,999 Kb/s)**  
☐ Use value  ☒ Inter Packet Delay automatically adjusted by IP Traffic ☐ TCP or UDP Data Size automatically adjusted by IP Traffic

**Mean Packet Throughput (1 to 99,999 Pkts/s)**  
☐ Use value (only for UDP connection)

**Mode 2: Using the External Data Source Generator** ( ☒ User file or ☐ User DLL )

**Filename**   **Loop counter**  **Idle time between each loop (sec.)**

**Options**

**Timecode (RTT) option**  
If RTT is activated when using Mode 1, the minimum "Data Size" defined in Step2 must be greater 26 bytes. ☐ Yes ☒ No

**Tos (1 hexa byte)** Value  **Time To Live (TTL)** Value

**Save incoming data traffic (needs remote in echo mode)**   **Save generated traffic into file (only data are saved)**

Unitary testing parameters window



This window is divided into three main areas:

- Mode 1: Using the Internal data generator
- Mode 2: Using the External data source generator (allowing to use an user file or an user DLL)
- Options:
  - Time code option (used to calculate the RTT – Round Trip Time and Jitter, if the remote is operating in the echoer mode)
  - TOS (Type of Service) byte (hex value)
  - TTL (Time To Live) byte (hex value)
  - Save incoming data traffic in a file for this connection (if the remote is operating with the echoer mode)
  - Save generated traffic into a file for this connection

The "OK" button validates new entered parameters for this connection and closes the window.

*Note: The first parameter to configure a unitary testing session is to select the mode between the internal data generator or the external data source generator.*

### 6.7.2.1 Mode 1: Using the Internal data generator

**Mode 1: Using the Internal Data Generator**

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

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

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

- ☒ Fix
- ☐ Random  min  max
- ☐ Alternate  value-1  value-2
- ☐ Increasing / Decreasing  min  max  step

Law : data volume to send

☐ Mathematical law  
Uniform law  
Range : [9.77 KB , 2.38 MB]

☐ File to send  
Filename

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

**Step 2: Specify Data size and packets parameters**  
In this step, define Data Size and packets parameters as well as the delay between each sent packet.

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

- ☒ Fix
- ☐ Random  min  max
- ☐ Alternate  size-1  size-2
- ☐ Increasing / Decreasing  min  max  step

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

- ☒ Fix  (See Forewarnings menu please)
- ☐ Random  min  max
- ☐ Alternate  value-1  value-2
- ☐ Increasing / Decreasing  min  max  step
- ☐ Mathematical law

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

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

- ☐ Use value
- ☒ Inter Packet Delay automatically adjusted by IP Traffic
- ☐ TCP or UDP Data Size automatically adjusted by IP Traffic

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

- ☐ Use value (only for UDP connection)

This area is divided into three parts:

- Step 1: Select the traffic generator type
- Step 2: Specify Data size and packets parameters
  - Data size (in bytes)
  - Inter packet delay (in milliseconds)
- Step 3 (Optional): Activate a throughput limit
  - Mean throughput (in Kb/s)
  - Mean packet throughput (in Pkts/s, only for UDP connection)

#### 6.7.2.1.1 Step 1: Select the traffic generator type

This area is divided into three parts corresponding to the three types of data source; beside each data source selection is a sub-area that displays data source parameters:

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

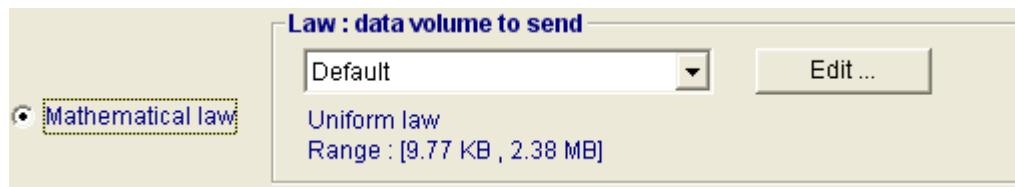
#### Mathematical law

In the unitary mode, the offered mathematical law is a data volume to send law. Volume will impact on the duration of the connection.

"IP Traffic – Test & Measure" unitary mode offers four mathematical laws related to data volume:

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

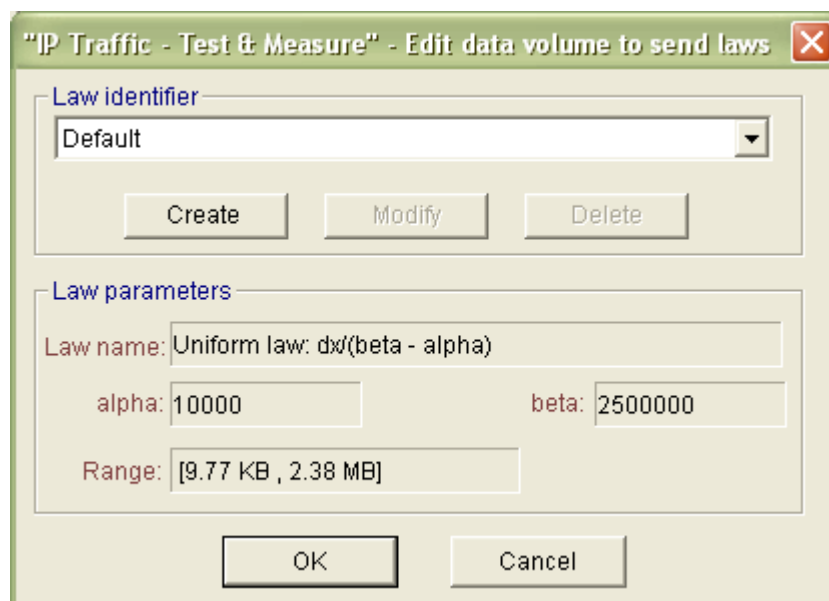
These laws are presented in details in the [Annex Part](#).



Mathematical law for the unitary testing selection

In the "Law: data volume to send" sub-area, a list box allows selecting 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 laws by pressing the "Edit" button. Then a new window is displayed:



Edit data volume to send laws

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

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

*Edit data volume to send laws 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 the "OK" button.
5. Your new law is selected in the parent window
6. Repeat operation 1 to 5 to create other laws.

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

Note: Laws created from this window will also be available for the Automatic mode.

### Packets Generator

When the Packet Generator data source is selected, "IP Traffic – Test & Measure" generates n IP packets for this connection. Packet contents can also be configured.

## ⇒ Packets number

You specify the number of packets to send in the "Packets generator" sub-area. The number of packets to send is limited to 99,999,999. Zero value means infinite (Zero is the default value).

## ⇒ Packet contents

A content is one hex byte. Accepted values are all combinations from 00 to FF. If a no valid value is entered, it will be automatically replaced by FF.

You can configure packet contents as follows:

- **Fix:** each packet has the same content.
- **Random:** "IP Traffic – Test & Measure" computes random packet content included in a range (min to max).
- **Alternate:** you define two values. "IP Traffic – Test & Measure" 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 range from the minimal to the maximal value; each packet content following is incremented by the step value (0 is an invalid value). When the maximal value is reached, the packet content decreases by the step value, until the minimal value is reached.

### Note:

When 'Packets generator' data source is selected, the 'Volume to send' and the 'Remaining volume' statistics cannot be computed. In the statistics fields of the tab 2 "IP Generator - Traffic + Statistics", "N/A" will be displayed in "Sent" and "Remain" columns.

## File to send

With this selection, "IP Traffic – Test & Measure" sends the content of the file defined in "Filename" sub-area. The "Browse" button allows selecting easily the file to send.

Note: it is not allowed to send an empty file.

With the two input fields "**Loop counter**" and "**Idle time between each loop (sec.)**", you can specify how many times this file must be sent and the idle time (expressed in seconds) before sending the file again. Note that the remote IP Answering should be configured accordingly to accept an idle time greater than the 'Idle time between each loop value'.

### 6.7.2.1.2 Step 2: Specify Data size and packets parameters

#### Data Size

This parameter defines the size of transmitted packets.

The maximum accepted value is 65 535. 0 (null) is not a valid value. By default, the entered value is 1460.

Data size can be configured as follows:

- **Fix:** each packet has the same size. The last packet may have an inferior size to fit the data volume to send when a mathematical law or file to send data source is selected.
- **Random:** "IP Traffic – Test & Measure" computes a random data size included in a range for each packet to send.
- **Alternate:** "IP Traffic – Test & Measure" 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 from the minimal to the maximal value, each size is incremented by step value (0 is an invalid value). When the maximal value is reached, the data size decreases step by step until the minimal value.

#### Note:

*It is important to notice that "IP Traffic – Test & Measure" requires a minimal data size when the RTT mode is selected, to add a CRC, a sequence number and the timestamp. Therefore, the minimal data size with RTT mode active is 15 bytes (see paragraph 2.3 about the RTT option).*

#### Note:

*The TCP or UDP data size is the data payload, not including headers (MAC, IP and protocol headers). It is not the frame size e.g. Ethernet frame size.*

*When UDP is used, the data size, greater than the MTU, generates IP fragmentation.*

*If TCP is used, the TCP protocol can aggregate packets with a size smaller than the MTU. To avoid aggregation, you should configure IP Traffic – Test & Measure with a TCP No Delay option set (see **Erreur ! Source du renvoi introuvable.** for more details)*

### Inter Packet Delay

This parameter allows defining the time interval between two packets to send. Values are limited to 9999 milliseconds i.e. 10 seconds. A value of zero means no inter packet delay.

The Inter Packet Delay can be configured as follows:

- **Fix:** inter packet delay is the same for all transmitted packets.
- **Random:** "IP Traffic – Test & Measure" computes a random inter packet delay included in a range you have specified for each packet to send.
- **Alternate:** "IP Traffic – Test & Measure" uses the first value for odd packets and the second value for even packets.
- **Increasing/Decreasing:** inter packet delay varies in a range from the minimal to the maximal value; each inter packet delay is incremented by the step (0 is not an accepted value for step). When the maximal value is reached, inter packet delay decreases by step value until the minimal value is reached.
- **Mathematical law:** you can choose between one of the fourth available laws: Uniform, Exponential, Pareto and Gauss.

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

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

With this feature, you can define a throughput limit for this connection (in Kilo bits per second) with the check box 'Use value'. You specify the average throughput in Kbps in the edit box and select one of the two parameters (data size or inter packet delay). "IP Traffic - Test & Measure" automatically adapts data traffic generation with adjustment of data 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 (p/s):

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

### 6.7.2.2 [Mode 2: Using the External data source generator \(allowing to use an user file or DLL\)](#)

If you select the external data source generator, the following area is active:

Two external data sources (file or DLL) are selectable, and you specify which filename to use:

- ⇒ **User file:** this external data file is provided by the user (see file format in Part 8-5). It contains different parameters: data, data size, inter packet delay...
- ⇒ **User DLL:** "IP Traffic – Test & Measure" invokes the user DLL each time data is needed to send (see Part 8-6 for more information)

*Note: when the 'User file' parameter is selected two parameters can be defined allowing sending the same file many times:*

- *Loop counter,*
- *Idle time (expressed in seconds) between each loop.*

### 6.7.2.3 [Options](#)

#### 6.7.2.3.1 *Time code option*

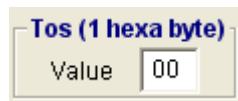
When this option is selected, "IP Traffic – Test & Measure" will add RTT (Round Trip Time) information to packets. The RTT header format (in the little endian notation) is:

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

This information is used in conjunction with connections running in the echoer mode on the Remote IP Answering module. Each echoed packet is analyzed by the Local 'IP Generator' module. When the RTT header is found, the RTT value is computed and displayed in statistics.

For the remote IP Answering module, the RTT information is checked to update 'sequencing errors' statistics.

### 6.7.2.3.2 The TOS byte

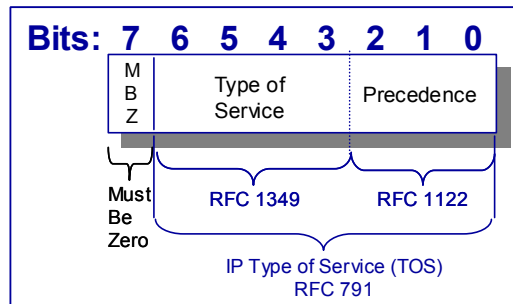


You can input the TOS value (by default, TOS = 00) used for each packet sent on the IP connection.

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

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

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



IPv4 Type of Service byte

**Important note for Windows 2000 and XP:** to allow IP\_TOS, a new registry key is added on Windows 2000 and XP.

It is necessary to edit the Registry and modify this key in order to use the TOS byte of "IP Traffic – Test & Measure".

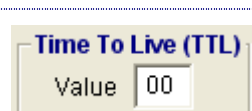
**WARNING:** Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved.

For information about how to edit the registry, view the "Changing Keys and Values" Help topic in Registry Editor (Regedit.exe) or the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedit.exe. Note that you should back up the registry before you edit it. If you are running Windows 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 and XP:

1. Start Registry Editor (Regedit.exe).
2. Go to the following key:  
HKEY\_LOCAL\_MACHINE on Local Machine\System\CurrentControlSet\Services\Tcpip\Parameters\  
**NOTE:** The registry key is one path.
3. On the **Edit** menu, click **Add Value**, and then type **DisableUserTOSSetting**. Click **REG\_DWORD** in the **Data Type** box, and then click **OK**.
4. Enter **0** in the prompt box.
5. Quit Registry Editor, and then restart the computer.

### 6.7.2.3.3 The TTL field

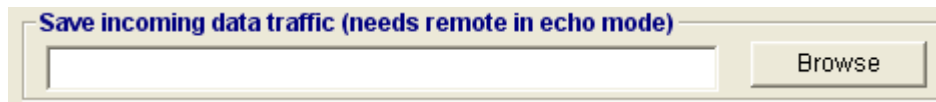


The user can input the TTL/Hop Limit value (hexadecimal) used for each packet sent on the connection.

Default value = 00



#### 6.7.2.3.4 *Save incoming data traffic or generated traffic into a file*



The dialog box has a title bar that reads "Save incoming data traffic (needs remote in echo mode)". Below the title bar is a text input field and a "Browse" button.

With this feature, you save in a file all incoming data traffic on the considered connection. The remote 'IP Answering' module must be set before in "Echoer" or "Echoer file" mode.

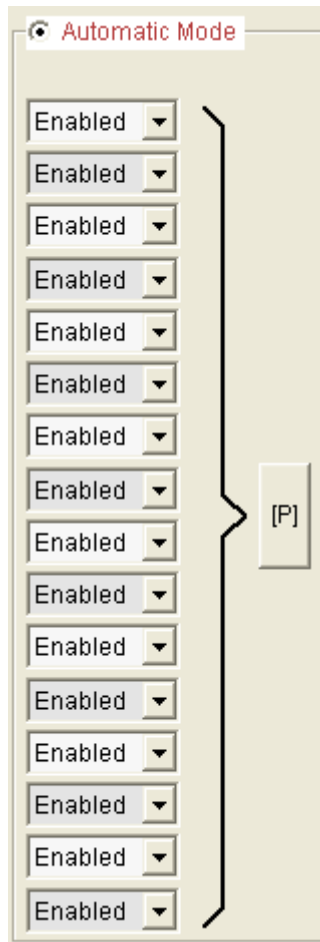
If the internal traffic generator is used and a file has been specified:



The dialog box has a title bar that reads "Save generated traffic into file (only data are saved)". Below the title bar is a text input field and a "Browse" button.

then it would be possible to compare the two files: sent data and received data on this connection.

### 6.7.3 Configure the automatic mode

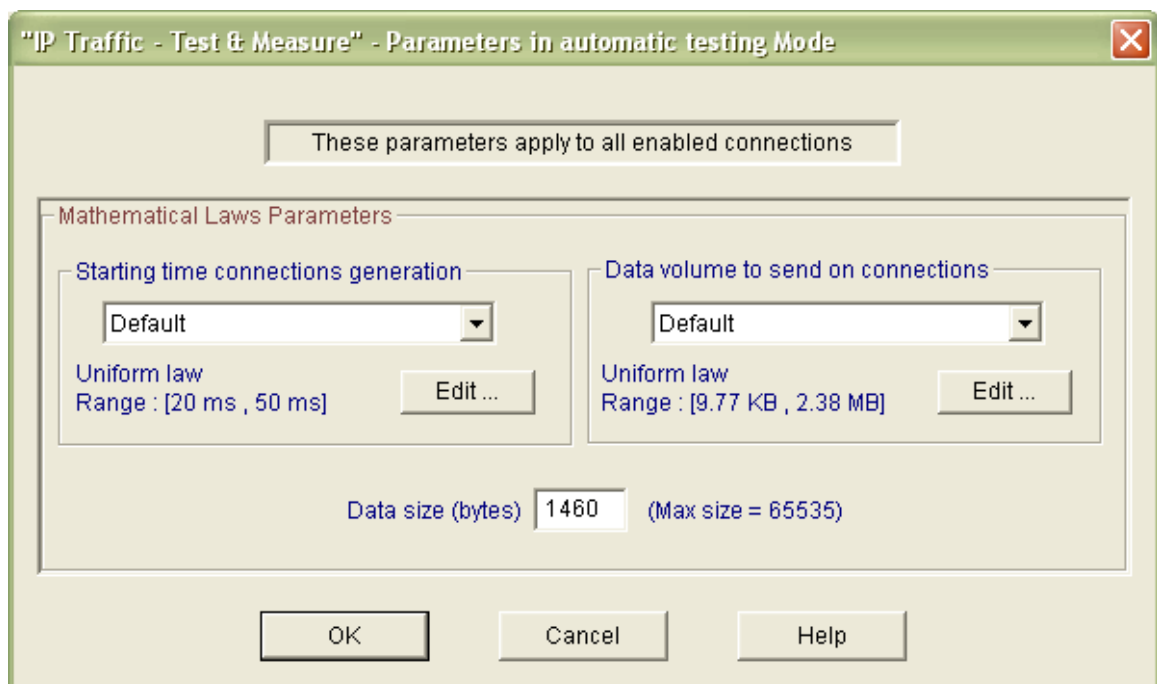


Automatic mode is a mode in which all enabled connections are generated in loop, according to a "Starting time connections generation" law and a "Data volume to send" law.

As the unitary mode, the automatic mode is configured in Tab 1 "IP Generator – Parameters" and is run in Tab 2 "IP Generator – Traffic +Statistics".

Once automatic mode is selected in Tab 1, the user can choose to enable or disable each connection by using the combo-box.

By clicking on the "[P]" button, the following window is displayed, allowing configuring the automatic mode parameters:



Automatic testing parameters window

### 3.1 Starting time connections generation laws

Starting time connection laws regulate the timing between starting of two connections. The available mathematical laws for starting time connection are Uniform and Exponential laws. (Mathematical laws are presented in details in [Annex part](#)).

To modify, delete or add a law, click on the "Edit" button. Then the following window is displayed:

This window is composed of three areas:

- ["Law identifier"](#)  
This area allows selecting, creating, modifying or deleting an existing law.
- ["Law parameters"](#)  
This area displays the parameters associated to the selected law.
- [Action buttons](#)  
  - "OK" button: to quit the law-editing window and accept all changes.
  - "Cancel" button: to ignore all modifications made since the window has been opened.

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

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

*Edit starting time connections generation law window*

2. Select one mathematical law: Uniform or Exponential.
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. The new law is selected in the parent window.
6. Repeat operation 1 to 5 to create other laws

### 3.2 Data volume to send laws

Data volume laws define the data volume to send for a connection. The available mathematical laws for data volume to send are: Uniform, Exponential, Pareto and Gauss 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:

*Edit data volume to send laws*

### 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: 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 "OK" button.
5. You new law is selected in the parent window
6. Repeat operation 1 to 5 to create other laws

**Note:**

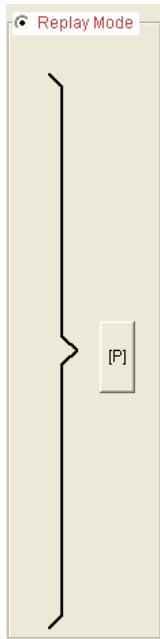
Up to the used OS (Windows 98, 2000 or XP), WinSock 2 Interface could present number-limits of the incoming simultaneous calls. Consequence for "IP Traffic – Test & Measure" is the presence of "connection failed", particularly when connections frequency is very near (inferior to 150 ms), and when the data volume to transmit is very small, which implies to make many connections. These connection failures do not disturb "IP Traffic – Test & Measure". To reduce these failures, increase the frequency of connection or the data volume.

### 3.3 Data size

In the automatic mode, entering a value (in bytes) in «Mathematical laws parameters» window configures the data size.

The data size is limited to 65,535 bytes.

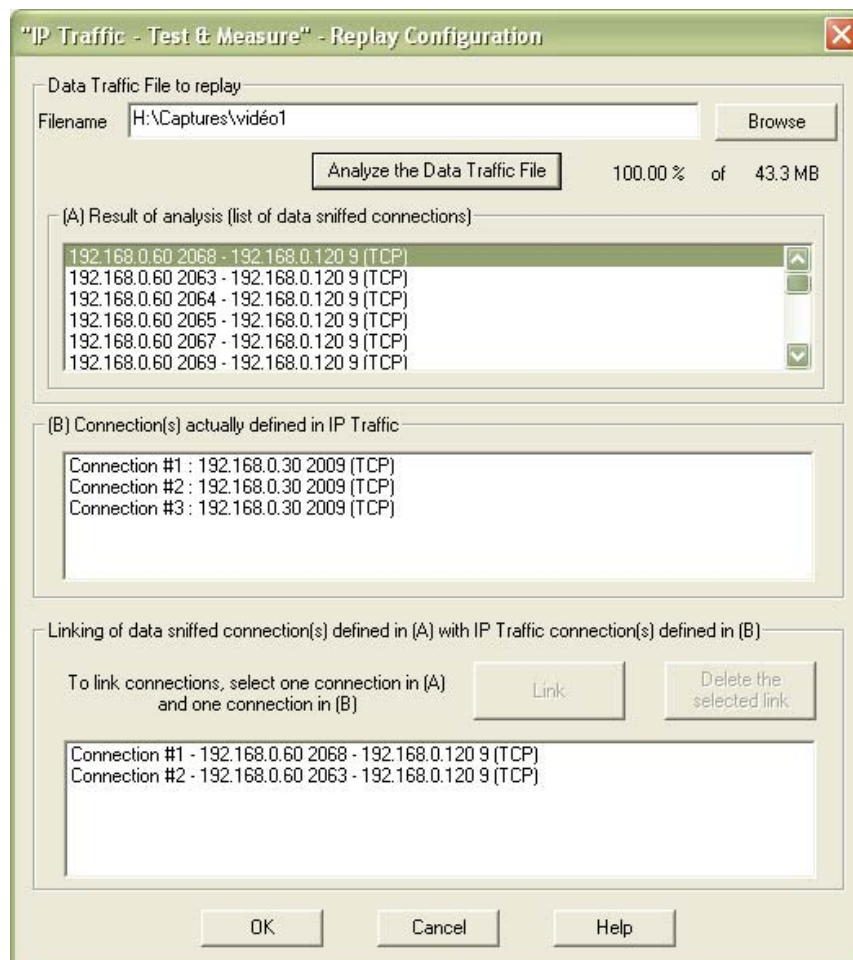
#### 6.7.4 Configure the replay sniffed traffic mode



In this mode, "IP Traffic – Test & Measure" uses traffic files captured by the "Traffic Sniffer" (see tab 4).

When you click on the command button "[P]", the following window is displayed.

First, select a 'Data traffic file to replay' and then press the "Analyze the data traffic file" button. At the end of the process, an indication is displayed: "100.00% of xxx KB" (where xxx is the file size).



After the analysis of the data traffic file, all IP connections founded in the sniffed traffic file are then displayed in the “(A) Result of analysis (list of data sniffed connections)” object.

Connections that have already been defined in the current IP Generator module are displayed in the “(B) Connection(s) already defined in IP Traffic” object.

Then you must link one ‘data sniffed connection’ to one ‘defined connection’ by pressing the “Link” button. If needed, one association can be removed by pressing the “Delete the selected link” button.

Once the needed links have been defined, press OK. “IP Traffic – Test & Measure” is ready to replay traffic on actually defined connections of the ‘IP Generator’ by using data of connections from the ‘data traffic file to replay’ specified by the different links made by the user.

## 6.8 The ‘IP Generator – Traffic + Statistics’ tab

This second tab related to the IP Generator module allows:

- To visualize destination parameters and traffic statistics for each connection,
- To save traffic statistics for all or a set of active connections of the IP Generator module in a file,
- If unitary mode is selected in Tab 1, to control traffic generation in unitary mode, i.e. to start and to stop each connection,
- If automatic mode is selected in Tab 1, to command traffic generation in automatic mode, i.e. to start and to stop all enabled connections,
- If replay sniffed traffic mode is selected in Tab 1, to command replay traffic generation on connection(s).

The “IP Generator - Traffic + Statistics” tab is divided into five areas. Each area is presented in the following paragraphs.

IP Generator - Parameters

IP Generator - Traffic + Statistics

IP Answering - Parameters + Statistics

Traffic Sniffer

Traffic Observer

Clear on Stop

Unitary Mode

Destination Parameters			Statistics (based on application data)							
	IP Address or Host Name	Port	Tx Throughput	Tx Volume	Tx Packets	Rx Throughput	Rx Volume	Rx Packets	Jitter	
Connection #01	192.168.0.120	9	568 Kb/s	630 KB	442 p	0.00 b/s	0 B	0 p	N/S	
Connection #02	192.168.0.120	7	570 Kb/s	636 KB	446 p	570 Kb/s	636 KB	435 p	N/S	
Connection #03	192.168.0.120	9	570 Kb/s	633 KB	444 p	0.00 b/s	0 B	0 p	N/S	
Connection #04	192.168.0.120	9	570 Kb/s	626 KB	439 p	0.00 b/s	0 B	0 p	N/S	
Connection #05	192.168.0.120	7	570 Kb/s	627 KB	440 p	570 Kb/s	627 KB	440 p	N/S	
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

Start #01

Start #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

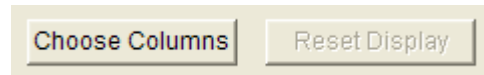
Tab 2: “IP Generator - Traffic + Statistics”

## 6.8.1 Destination Parameters area

In this area, the destination parameters (IP address and port number) of each connection are shown for information. These parameters can be modified in the "IP Generator –Parameters" tab, when all connections are stopped.

## 6.8.2 Statistics (Application Level)

The statistics are displayed for each connection in the "Statistics" area:



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

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

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

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

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



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

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

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

Examples of warning messages:

- Connection failed: no response from the Remote. Please check your parameters.
- Connection pending: "IP Traffic – Test & Measure" is waiting for the Remote response.
- Connection reset: the Remote has reset the connection.

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

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



### 6.8.2.1 Transmitting statistics

◆ Tx Packets	Tx Packets (Tx = Transmit) is the number of packets that “IP Traffic – Test & Measure” has sent since the connection started.
◆ Tx Pkts Throughput	Tx Pkts Throughput (Tx = Transmit) is the mean number of packets that “IP Traffic – Test & Measure” 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 “IP Traffic – Test & Measure” has sent since the connection started.

### 6.8.2.2 Receiving statistics

◆ Rx Packets	Rx Packets (Rx = Receive) is the number of packets that “IP Traffic – Test & Measure” has received since the connection is started.
◆ Rx Pkts Throughput	Rx Pkts Throughput (Rx = Receive) is the mean number of packets that “IP Traffic – Test & Measure” 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 “IP Traffic – Test & Measure” has received since the connection is started.

### 6.8.2.3 Other statistics

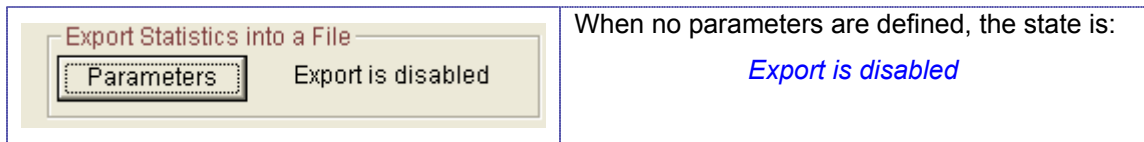
◆ Jitter	Jitter is the mean variation of delays on packets received. This value is only available when Timecode option is selected (for the local 'IP Generator'). This value corresponds to either the mean one-way variation (remote 'IP Answering' = Absorber Generator mode) or the mean two-ways variation (remote 'IP Answering' = Echoer mode).
◆ Remaining Volume	'Remaining Volume' is the number of bytes that “IP Traffic – Test & Measure” has still not sent. 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 “IP Traffic – Test & Measure”. This value is calculated if the Timecode option is selected for the local 'IP Generator' and if the remote 'IP Answering' works in the Echoer mode.
◆ Seq. Numb. Errors	'Seq. Numb. Errors' (Sequence Number Errors) is the sum of the Out Of Sequence packets number (OOS) and the number of lost packets. This value is only available if the Timecode option is selected (for the local 'IP Generator') and if the working mode of the remote 'IP Answering' is Absorber Generator or Echoer.
◆ Volume To Send	'Volume To Send' is the number of bytes that “IP Traffic – Test & Measure” should send. This information is only available for two Traffic Generator types: Mathematical law and File to Send.

When you press the “Stop all connections” button, statistics remain displayed in black writing on gray background.

If a connection cannot be activated (in case of invalid parameters), the statistics fields are empty on gray background.

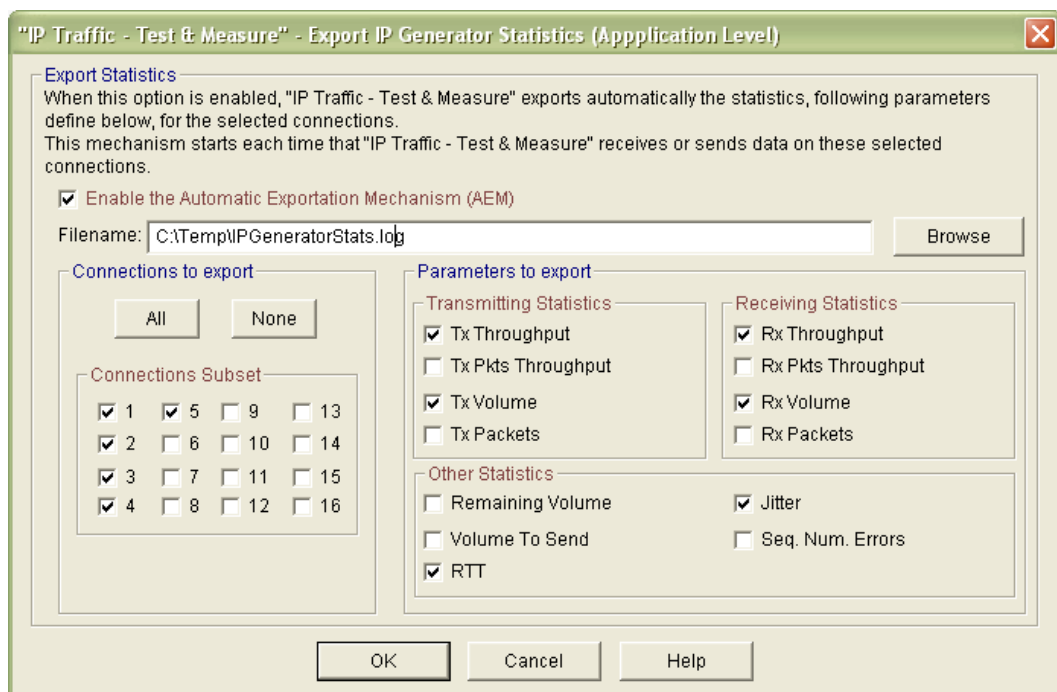
#### 6.8.2.4 Export statistics in a file

To export all or part of **statistics** into a file, click on the 'Parameters' button when enabled (i.e. if connections of the IP Generator 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 identification of the needed connections,
- The parameters to export (up to 13).



"Export IP Answering Statistics"

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



Note: do not specify the same filename to save statistics for the 'IP Generator' and the 'IP Answering' parts else a warning message is displayed.

The statistics file is updated with the same refresh period than the statistics displayed.

A special mark is added to keep special TCP and UDP events e.g. Start and End of sending traffic.

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

Statistics are saved into the file as soon as connections of the IP Generator 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:



To export all or part of statistics displayed (in other words, there is the possibility of saving all the statistics even those which are not displayed) in a file, you can use the parameters connection and statistics dialog.

#### 6.8.2.4.1 The IP Generator statistics file format

**The IP Generator statistics file is formatted line by line as follows (example):**

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

**Second line:** IP Traffic - Test & Measure IP Generator

**Third line:** (Only seven statistics headers are showed here. Statistics headers can be up to thirteen)

<u>Cnx#i</u> (Protocol)	<u>Date</u>	<u>Time</u>	<u>Throughput</u> (Kb/s)	<u>Data</u> sent (*)	<u>Data</u> Received (*)	<u>Volume</u> to send (KB)	<u>Remaining</u> volume (KB)	<u>Seq.</u> <u>Num.</u> <u>Errors</u>	<u>RTT</u> (ms)
----------------------------	-------------	-------------	-----------------------------	-------------------------	-----------------------------	-------------------------------	---------------------------------	---	--------------------

**Next lines:**

<u>Cnx#i</u> (TCP, UDP or ICMP)	<u>MM/DD/YYYY</u>	<u>HH:MM:SS.mmm</u>	<u>nnn.nn</u>	<u>nnn.nn</u>	<u>nnn.nn</u>	<u>Nnn.nn</u>	<u>nnn.nn</u>	<u>X</u>	<u>X</u>
---------------------------------------	-------------------	---------------------	---------------	---------------	---------------	---------------	---------------	----------	----------

#### Additional mark for TCP connection events

Cnx #n (TCP) START This mark indicates the connection #n starts (n: from 01 to 16). When this mark is included in the IP Generator traces, numerical values are set to 0.

Cnx #n (TCP) END This mark indicates the connection #n has stopped. Numerical values are latest values computed by "IP Traffic – Test & Measure".

#### Additional mark for TCP or UDP disconnection events

Cnx #n (TCP) ERROR This mark indicates the reason of the disconnection if this one is not produced by the click on 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 IP Generator traces, numerical values are replaced by the error message returned by "IP Traffic – Test & Measure".

## Idle connections

When the connection is idle, 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 'IP Generator' 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”.

## Export an IP Generator file sample

In this example, 3 connections have been selected with all parameters exported. For each connection, the 'IP Answering' is operating with the echoer mode.

- Connection #01 is configured with the TCP protocol and uses the internal data generator.
- Connection #02 is configured with the UDP protocol and uses the internal data generator.
- Connection #03 is configured with the TCP protocol and uses the “File to send” generator.

The “Refresh time” parameter is set to 2 seconds.

Starting session 04/01/2005 at 15:37:06.343								
IP Traffic - Test & Measure IP Generator								
Cnx#i (Protocol)	Date	Time	Tx Throughput (Kb/s)	Tx Volume (KB)	Rx Throughput (Kb/s)	Rx Volume (KB)	Remaining Volume (KB)	Volume To Send (KB)
Cnx#2 (UDP) START	04/01/2005	15:37:06.437	0.00	0.00	0.00	0.00	N/A	N/A
Cnx#3 (TCP) START	04/01/2005	15:37:07.703	0.00	0.00	0.00	0.00	0.00	0.00
Cnx#1 (TCP) START	04/01/2005	15:37:07.718	0.00	0.00	0.00	0.00	N/A	N/A
Cnx#1 (TCP)	04/01/2005	15:37:08.296	0.00	41.35	0.00	39.92	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:08.296	0.00	41.35	0.00	41.35	N/A	N/A
Cnx#3 (TCP)	04/01/2005	15:37:08.296	0.00	139.73	0.00	139.73	5626.08	5765.81
Cnx#1 (TCP)	04/01/2005	15:37:10.281	193.91	181.07	193.91	181.07	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:10.281	196.19	183.93	196.19	183.93	N/A	N/A
Cnx#3 (TCP)	04/01/2005	15:37:10.281	666.13	611.66	661.56	610.23	5154.15	5765.81
Cnx#1 (TCP)	04/01/2005	15:37:12.562	422.03	337.91	419.75	332.21	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:12.562	424.31	312.25	422.03	309.39	N/A	N/A
Cnx#3 (TCP)	04/01/2005	15:37:12.562	1453.16	1016.58	1450.88	1008.03	4749.23	5765.81
Cnx#1 (TCP)	04/01/2005	15:37:15.281	524.69	523.26	511.00	523.26	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:15.281	499.59	526.11	490.47	513.28	N/A	N/A
Cnx#3 (TCP)	04/01/2005	15:37:15.281	1610.56	1651.05	1608.28	1649.63	4114.75	5765.81
Cnx#1 (TCP)	04/01/2005	15:37:17.281	545.22	665.84	545.22	664.41	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:17.281	547.50	667.27	524.69	654.43	N/A	N/A
Cnx#3 (TCP)	04/01/2005	15:37:17.281	1649.34	2187.15	1651.63	2185.72	3578.66	5765.81
Cnx#1 (TCP)	04/01/2005	15:37:19.281	545.22	806.99	547.50	806.99	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:19.281	545.22	808.42	526.97	795.59	N/A	N/A
Cnx#3 (TCP)	04/01/2005	15:37:19.281	1683.56	2720.39	1683.56	2718.96	3045.42	5765.81
Cnx#1 (TCP)	04/01/2005	15:37:21.281	570.31	949.57	572.59	949.57	N/A	N/A

Cnx#2 (UDP)	04/01/2005	15:37:21.281	568.03	952.42	572.59	939.59	N/A	N/A
Cnx#3 (TCP)	04/01/2005	15:37:21.281	2112.44	3252.21	2121.56	3250.78	2513.60	5765.81
Cnx#1 (TCP)	04/01/2005	15:37:23.281	570.31	1092.15	570.31	1090.72	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:23.281	570.31	1093.57	570.31	1080.74	N/A	N/A
Cnx#3 (TCP)	04/01/2005	15:37:23.281	2153.50	3788.30	2148.94	3786.88	1977.51	5765.81
Cnx#1 (TCP)	04/01/2005	15:37:25.281	570.31	1233.30	570.31	1233.30	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:25.281	570.31	1236.15	570.31	1223.32	N/A	N/A
Cnx#3 (TCP)	04/01/2005	15:37:25.281	2144.38	4321.54	2146.66	4315.84	1444.27	5765.81
Cnx#1 (TCP)	04/01/2005	15:37:27.281	570.31	1378.73	570.31	1378.73	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:27.281	570.31	1380.16	570.31	1367.32	N/A	N/A
Cnx#3 (TCP)	04/01/2005	15:37:27.281	2139.81	4837.68	2139.81	4836.25	928.13	5765.81
Cnx#1 (TCP)	04/01/2005	15:37:29.281	570.31	1521.31	568.03	1515.61	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:29.281	570.31	1521.31	570.31	1507.05	N/A	N/A
Cnx#3 (TCP)	04/01/2005	15:37:29.281	2123.84	5345.25	2123.84	5343.83	420.55	5765.81
Cnx#1 (TCP)	04/01/2005	15:37:31.281	568.03	1663.89	568.03	1662.46	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:31.281	570.31	1665.31	568.03	1649.63	N/A	N/A
Cnx#3 (TCP)	04/01/2005	15:37:31.281	2073.66	5765.81	2073.66	5765.81	0.00	5765.81
Cnx#3 (TCP) END	04/01/2005	15:37:31.390	2073.66	5765.81	2073.66	5765.81	0.00	5765.81
Cnx#1 (TCP)	04/01/2005	15:37:33.281	568.03	1803.61	568.03	1803.61	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:33.281	570.31	1806.46	568.03	1790.78	N/A	N/A
Cnx#1 (TCP)	04/01/2005	15:37:35.281	568.03	1946.19	570.31	1946.19	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:35.281	570.31	1950.47	568.03	1936.21	N/A	N/A
Cnx#1 (TCP)	04/01/2005	15:37:37.281	568.03	2090.20	593.13	2090.20	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:37.281	570.31	2093.05	570.31	2078.79	N/A	N/A
Cnx#1 (TCP)	04/01/2005	15:37:39.265	570.31	2232.77	572.59	2232.77	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:39.265	572.59	2234.20	572.59	2218.52	N/A	N/A
Cnx#1 (TCP)	04/01/2005	15:37:41.281	570.31	2373.93	570.31	2372.50	N/A	N/A
Cnx#2 (UDP)	04/01/2005	15:37:41.281	570.31	2375.35	568.03	2359.67	N/A	N/A
Cnx#1 (TCP) END	04/01/2005	15:37:42.875	570.31	2448.07	570.31	2448.07	N/A	N/A
Cnx#2 (UDP) END	04/01/2005	15:37:43.078	568.03	2450.92	568.03	2436.66	N/A	N/A

*The delimiter mark used between each field is the tabulation character.*

### 6.8.3 Run an unitary testing session

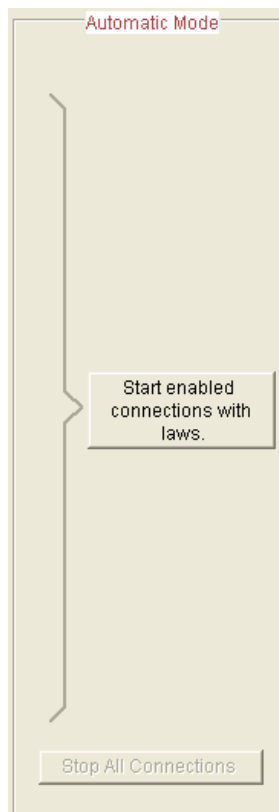


The unitary testing session can be started from the "Unitary mode" area in Tab 2 "IP Generator - Traffic + Statistics". From this area, you can start or stop connections in unitary testing separately or all together.

**To run an unitary mode session:**

1. *In Tab 2 "IP Generator - Traffic + Statistics":*  
 → If IP Generator connections are active, stop all running connections by pressing the "Stop All connections" button.
2. *In Tab 1 "IP Generator - Parameters":*  
 → Select unitary testing.
3. *In Tab 1 "IP Generator - Parameters":*  
 → If necessary configure unitary parameters for each connection by pressing the "Parameters #n" button.
4. *In Tab 2 "IP Generator - Traffic + Statistics":*  
 → Press the "Start All Connection" button to start all connections together or press the "Start #n" buttons to start connections one by one.

## 6.8.4 Run an automatic testing session

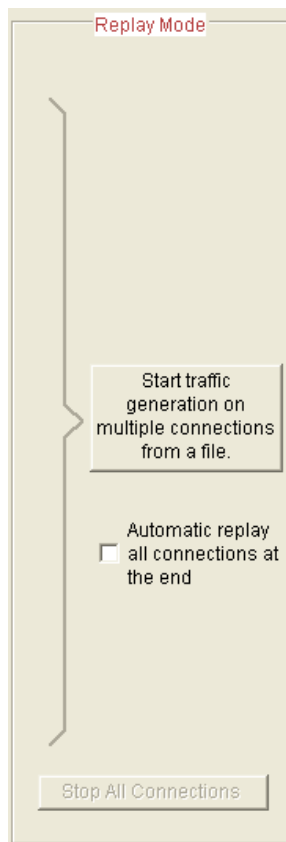


An automatic testing session is launched from the "Automatic Mode" area in Tab 2 "IP Generator - Traffic + Statistics". In this area, there is only one button to start and to stop all enabled connections in the automatic mode.

### To run an automatic mode session:

- 1 *In Tab 2 "IP Generator - Traffic + Statistics":*
  - If IP Generator connections are active, stop all running connections by pressing the "Stop All connections" button.
- 2 *In Tab 1 "IP Generator - Parameters":*
  - Select automatic testing.
- 3 *In Tab 1 "IP Generator - Parameters":*
  - If necessary, configure automatic parameters by pressing the "[P]" button and enable or disable connections by using the combo boxes.
- 4 *In Tab 2 "IP Generator - Traffic + Statistics":*
  - Press the "Start enabled connections with laws" button to start all enabled connections.

## 6.8.5 Run a replay traffic session



A replay traffic testing session is launched from the "Replay Mode" area in Tab 2 "IP Generator - Traffic + Statistics". In this area, there is only one button to start replay traffic from a traffic file on connections.

### To run a replay traffic session:

1. *In Tab 2 "IP Generator - Traffic + Statistics":*
  - If IP Generator connections are active, stop all running connections by pressing the "Stop All Connections" button.
2. *In Tab 1 "IP Generator - Parameters":*
  - Select the "Replay sniffed traffic" mode.
3. *In Tab 1 "IP Generator - Parameters":*
  - If necessary, configure and select the traffic file by pressing the "[P]" button.
4. *In Tab 2 "IP Generator - Traffic + Statistics":*
  - Press the "Start traffic generation on multiple connections from a file" button to start replay traffic generation.
5. *The option "Automatic replay at the end of all connections" restarts the replay of traffic generation when all connections are stopped.*



## 6.8.6 Using ICMP capacity of the Traffic Generator

“IP Traffic – Test & Measure” offers the possibility to generate ICMP Echo Request traffic. (the protocol used by Ping)

By using the ICMP protocol, only the unitary mode can be used. 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 specify.
- In the upper part of the Step 2, the ICMP Echo Request data size can be defined.
- The lower part of Steap 2 allows the definition of the replies timeout.

*Note: more information about these three areas is available in paragraph 6.7.2.1 Mode 1: Using the Internal data generator.*

For the “IP Generator – 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: this value represents the number of replies that “IP Traffic – Test & Measure” does not receive.

## 6.9 The ‘IP Answering’ tab

The ‘IP Answering’ part allows receiving UDP and TCP traffic in accordance with five different working modes: ‘Absorber’, ‘Absorber file’, ‘Echoer’, ‘Echoer file’ or ‘Absorber + Generator’.

### IP Answering - Parameter + Statistics tab

This third tab is related to the ‘IP Answering’ part activity to:

- Configure the “Listening to” parameters: network interface, port number and protocol of the listening port,
- Configure IP connected remote: source IP address or host name from which connection is received,
- Configure receiving working mode for each connection,
- Visualize the statistics for each connection,
- Save traffic statistics for all active connections of the IP Answering module in a file.

The tab is divided into four areas: Listening To ..., Coming From ..., Receiving Working Mode and Statistics (calculated at the application level).

Tab 3: “IP Answering - Parameters + Statistics”

### 6.9.1 Duplicate parameters of a connection onto others


In order to facilitate input of the parameters for a connection, a *copy/paste mechanism* for all parameters of a connection is available (identical to the *copy/paste mechanism* for the IP Generator part – see 6.7.1.4).

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

## 6.9.2 Listening To ...

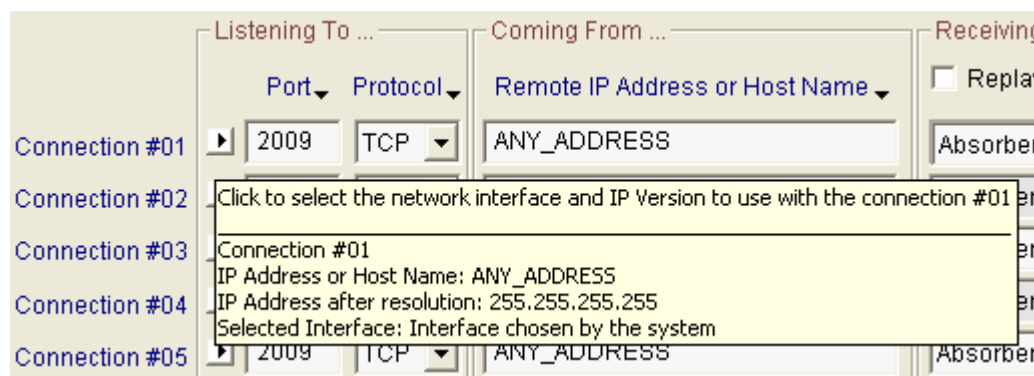
In this area, you configure each receiving connection with the following parameters corresponding to the connected sender from which connections are received:

In this area, you configure the parameters 'IP Traffic – Test & Measure' uses to listen to incoming connections. These parameters are:

<b>Network interface selection</b> 	<p><i>The black arrow has two purposes:</i></p> <ul style="list-style-type: none"> <li>• <i>To display a summary of the connection's parameters</i></li> <li>• <i>To select the network interface and the IP version for a connection.</i></li> </ul>
<b>Port</b>	<p>The port number is limited to 65,535. By default, the port number is 2009. In case of invalid value, the value is <b>red</b> colored.</p>
<b>Protocol</b>	TCP or UDP protocol (default = TCP protocol).

### 6.9.2.1 Summary of connection parameters

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



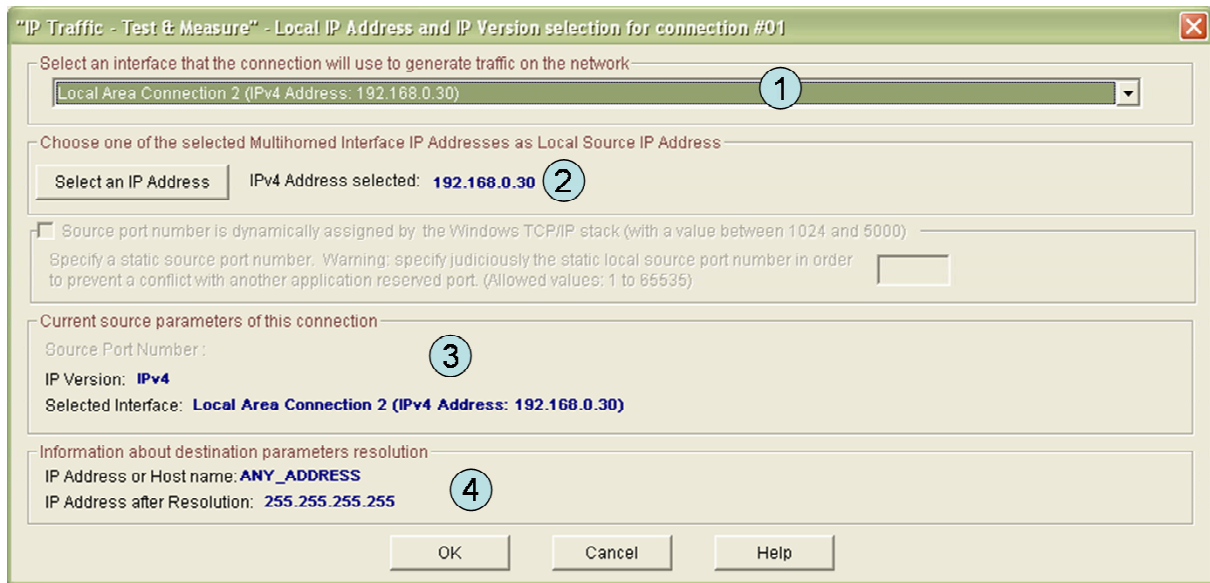
*IP Answering connection tooltip*

The tooltip for the IP Answering connection includes 4 items:

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

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

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



*Network interface, IP version and IP local address for an IP Answering's connection*

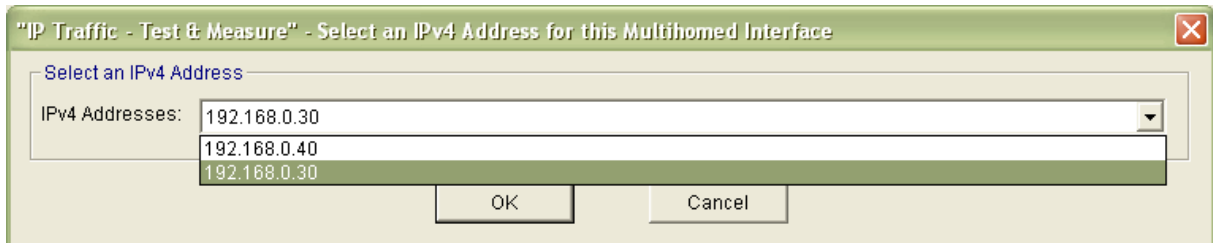
- (1) The **network interface** selection is optional. It is used to force connections to use a specific network interface.
- By default:
    - The IP stack resolves the network interface selection to receive packets from the remote.
    - The IP stack uses the destination IP address to select the network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



- Network interface types are restricted: only Ethernet and PPP are listed. A PPP interface should be in 'connected' state to belong to the interface list.
- (2) **Select IP address button** is available when multiple IP addresses are attached to the network interface. This network interface configuration is also known as 'multihomed'

interface. Selection of a Source IP address is generally not required: "IP Traffic – Test & Measure" uses the default IP address of the interface to establish connections. It may be useful when routing priority or policy is defined. This IP address is used to filter the coming connection. Only the coming connection, having the same destination IP address, is accepted by the IP Generator. In other cases, the connection is rejected.

Example of IP address selection for a multihomed interface:



Note:

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

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

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

Note:

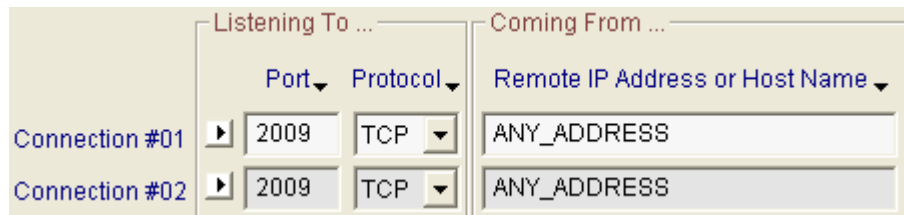
When you click on the OK button, if the network interface is selected, the IP address translation is automatically started. It may be time consuming.

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.
- When multiple IP addresses are attached to one interface, you should select the destination IP address the incoming connection should refer to. By default, the first IP address returned by the system is selected.

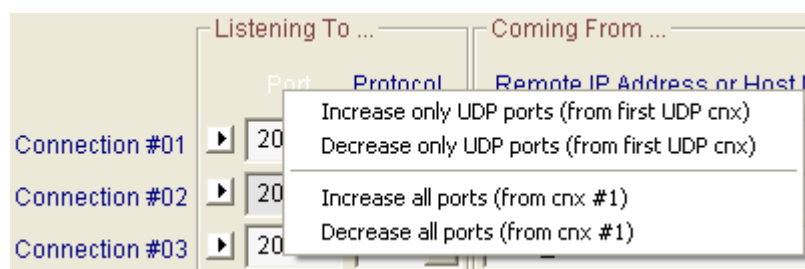
### 6.9.2.3 Description of the floating menu mechanism

In the 'Listening To' object, the labels 'Port' and 'Protocol' are mouse sensitive.



When the mouse is located on the 'Port' text area for example, the text color changes to white. Then click left your mouse to display the associated menu.

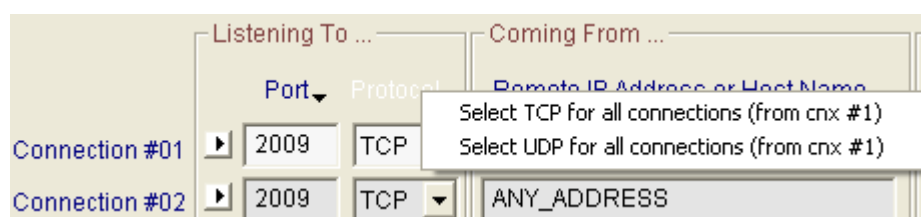
#### 6.9.2.3.1 *Floating menu for the 'Port' label*



With this menu you can:

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

#### 6.9.2.3.2 *Floating menu for the 'Protocol' label*



This menu helps to set the same protocol to every connection.

### 6.9.3 Coming From ...

#### Remote IP address or Host Name:

*Enter the IP address (numerical format) or Host Name (canonical format), with the help of AutoComplete when active. The IP address is not a mask.*

*By default, the value is ANY\_ADDRESS (This address is used to accept connection from any source address).*

#### 6.9.3.1 [IP address floating menu](#)

When the mouse is located, on the 'IP address' text area, the color changes to white.



Click on the left mouse button to display the short menu as above. With this function, the IP Address field from connection #01 is copied to all connections from #02 to #16.

#### 6.9.3.2 [IP Address translation mechanism](#)

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

Because the IP address translation mechanism is time consuming, a particular attention should apply when using IP canonical addresses. 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 "IP Traffic – Test & Measure" restart the translation mechanism for this connection.

#### Note:

*When the IP address translation failed, the IP address is written red on white. This connection cannot be started. If all connections have a red IP Address, the "Start Receiving Traffic" button in the 'IP Answering – Parameters + Statistics' tab is grayed*

#### Note:

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

- *the focus leaves the 'IP Address or Host Name' field,*
- *the focus is in the 'IP Address or Host Name' field and the user press the Enter key,*
- *another tab is selected,*
- *you duplicate parameters from one connection to another,*
- *you change the Interface parameters.*

## 6.9.4 Receiving working mode

"IP Traffic – Test & Measure" offers five different active working modes for the IP Answering part: '**Absorber**', '**Absorber File**', '**Echoer**', '**Echoer file**' or '**Absorber + Generator**'. A '**Disable**' (or inactive) mode is also available.

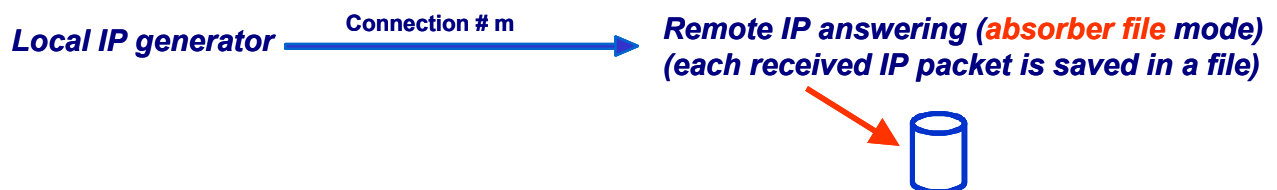
### 6.9.4.1 Absorber mode

With this working mode, "IP Traffic – Test & Measure" absorbs data on this connection.



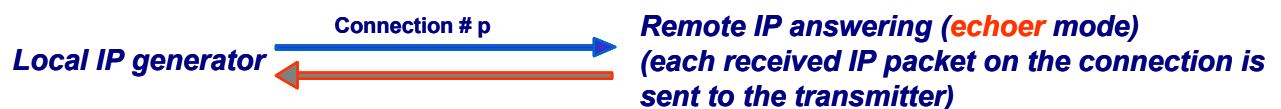
### 6.9.4.2 Absorber File mode

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



### 6.9.4.3 Echoer mode

When a receiving connection is operating in echoer mode, the received data are sent back to the 'IP Generator' module.



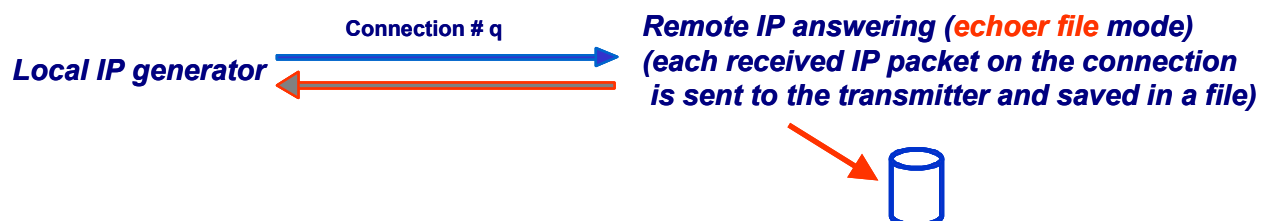
With UDP protocol, the 'Echoer' mode is available only if a connected 'IP Generator' address is specified.

#### Remind:

Echoed data can be saved in a file by the local 'IP Generator' module via the tab 1 "IP Generator - Parameters".

### 6.9.4.4 Echoer File mode

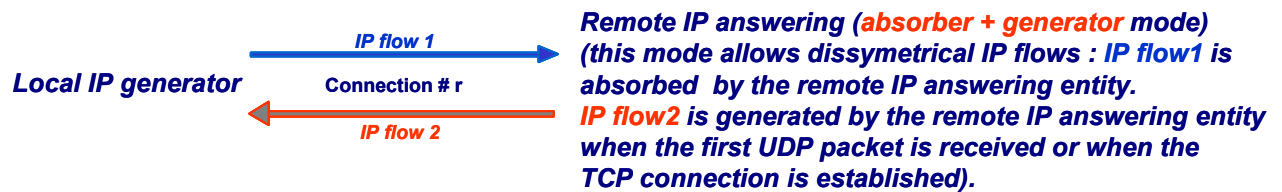
When a receiving connection is operating in this mode, the received data are sent back to the 'IP Generator' module and are saved in a file. The name of the file must be entered in the Filename field. A "Browse" button allows selecting the file easily.



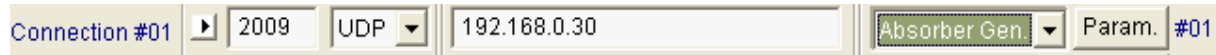
### 6.9.4.5 Absorber + Generator mode

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





Properties of the *IP flow 1* are defined at the local 'IP Generator' level and each IP packet received by the remote 'IP Answering' module is only used to compute statistics.



When you select the "Absorber gen." mode for a connection (#1 in the example above), a "Param." Button is displayed in order to specify the traffic parameters generated by the remote 'IP Answering' module (i.e. *IP flow 2*). When you press the "Param." button, an "IP Traffic – Parameters in unitary mode" window is displayed (the same as IP Generator – configure unitary testing mode). So you can input parameters for this *IP flow 2* as you like (for example, generate 10000 packets with an average throughput of 250 Kb/s).

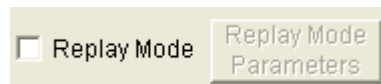
For a TCP connection, *IP flow 2* is generated as soon as the TCP connection will be established between the local 'IP Generator' and the remote 'IP Answering' modules.

For an UDP connection, *IP flow 2* is generated as soon as the remote 'IP Answering' module will receive the first UDP packet.

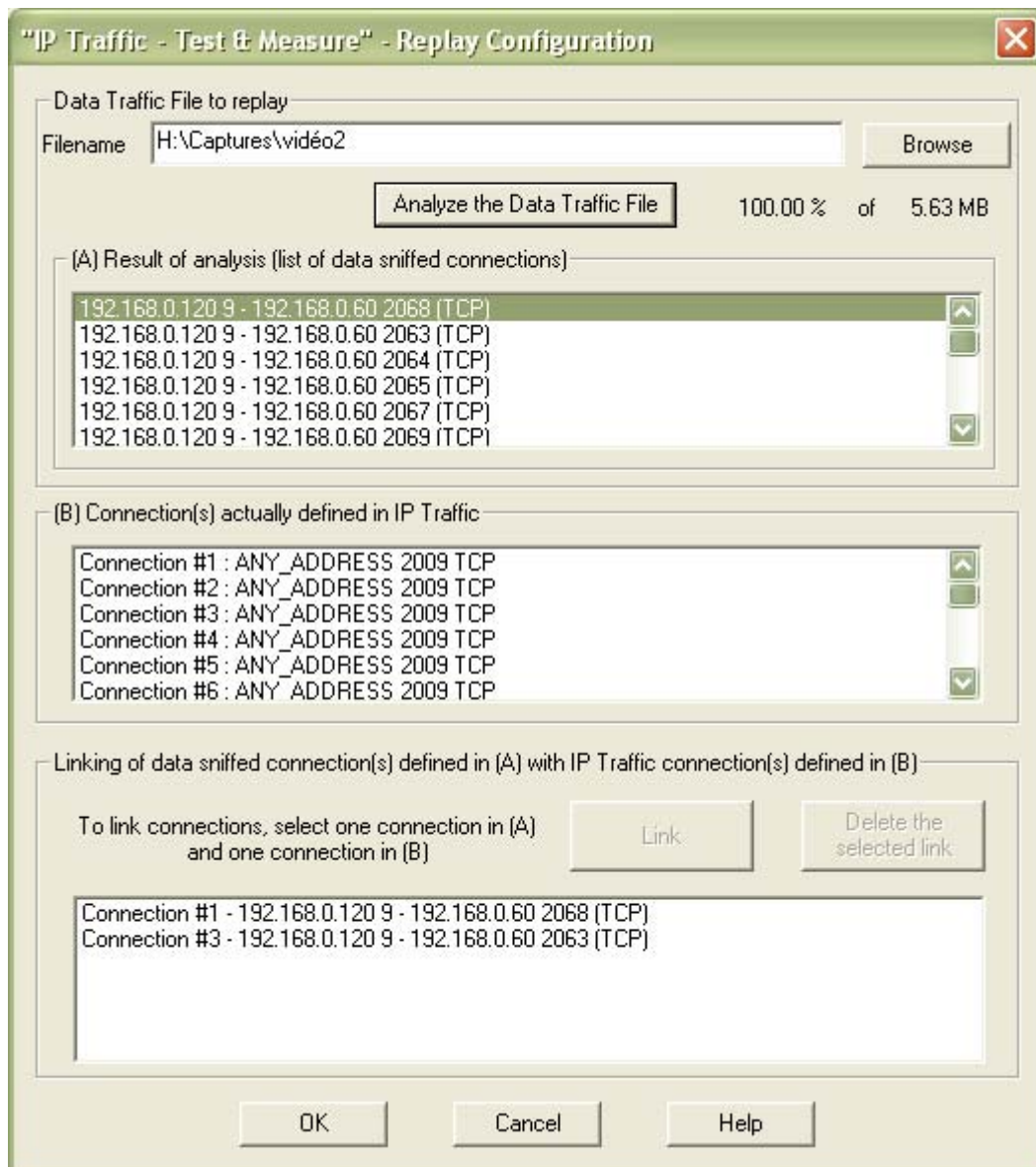
#### 6.9.4.6 Disable mode

When this mode is selected for a connection, "IP Traffic – Test & Measure" does not those parameters to establish a connection. The disabled connections are grayed when you start receiving traffic. Statistics fields of disabled connections are filled in with the following message: "Connection disabled". There is no statistics in the file for these connections.

#### 6.9.4.7 The command button: "Replay mode parameters"



The check box 'Replay mode' must be checked in order to access to the replay mode. By clicking on the "Replay Mode Parameters" button, the following window is displayed.



First, select a 'Data traffic file to replay' and then press the "Analyze the data traffic file" button. At the end of the process, an indication is displayed: "100.00% of xxx Kb" (where xxx is the file size).

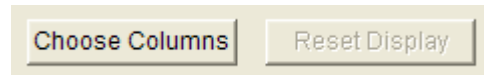
After the analysis of the data traffic file, all IP connections found in the sniffed traffic file are then displayed in the "(A) Result of analysis (list of data sniffed connections)" object.

Connections that have already been defined by the user in the current IP Answering module are displayed in the "(B) Connection(s) already defined in IP Traffic" object.

You must then link one 'data sniffed connection' to one 'defined connection' by pressing the "Link" button. If needed, one association can be removed by pressing the "Delete the selected link" button.

Once that the needed links have been defined, then press OK. "IP Traffic – Test & Measure" will replay traffic on actually defined connections of the 'IP Answering' module by using data of connections from the 'data traffic file to replay' specified by the different links you have made.

## 6.9.5 'IP Answering' 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 (see registry).  
*The IP Answering has ended the TCP connection because no data has been received (timeout defined with the TCPINACTIVITY parameter of "IP Traffic - Test & Measure" 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).				

#### 6.9.5.1 Transmitting statistics

◆ Tx Packets	Tx Packets (Tx = Transmit) is the number of packets that "IP Traffic - Test & Measure" has sent since the connection is started.
◆ Tx Pkts Throughput	Tx Pkts Throughput (Tx = Transmit) is the mean number of packets that "IP Traffic - Test & Measure" 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 "IP Traffic - Test & Measure" has sent since the connection is started.

#### 6.9.5.2 Receiving statistics

◆ Rx Packets	Rx Packets (Rx = Receive) is the number of packets that "IP Traffic - Test & Measure" has received since the connection is started.
◆ Rx Pkts Throughput	Rx Pkts Throughput (Rx = Receive) is the mean number of packets that "IP Traffic - Test & Measure" 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 "IP Traffic - Test & Measure" has received since the connection is started.

#### 6.9.5.3 Other statistics

◆ Data Not Echoed	'Data Not Echoed' is the number of bytes that the 'IP Answering' part couldn't echo. This value is only available if the 'IP Answering' part works in the Echoer mode.
◆ Jitter	Jitter is the mean variation of delays on packets received. This value is only available when Timecode option is selected (on the remote IP Generator). This value corresponds to the mean one-way variation only.
◆ Remaining Volume	'Remaining Volume' is the number of bytes that "IP Traffic - Test & Measure" has still not sent. This information is only available for two Traffic Generator types: Mathematical Law and File to Send.
◆ Seq. Numb. Errors	'Seq. Numb. Errors' (Sequence Number Errors) is the sum of the Out Of Sequence packets number (OOS) and the number of lost packets. This value is only available if the Timecode option is selected (for the remote 'IP Generator') and if the working mode of the local 'IP Answering' is Absorber Generator or Echoer.
◆ Volume To Send	'Volume To Send' is the number of bytes that "IP Traffic - Test & Measure" should send. This information is only available for two Traffic Generator types: Mathematical law and File to Send.

#### When pressing the "Start receiving traffic" button:

- All connected IP Generator information and working mode information are grayed,
- Disabled connections statistics fields are empty on gray background,

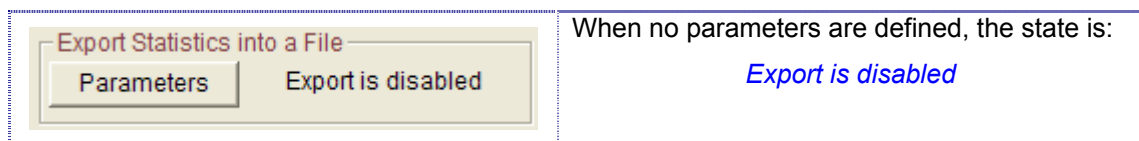
- UDP enabled connections statistics fields are filled in with "00" value on white background,
- TCP connections statistics fields are empty on white background (they will be filled in only when connection will be established).
- Statistics are exported into the file (see below)

#### When pressing the "Stop receiving traffic" button:

- Statistics fields are cleared up,
- 'Connected remote' and 'Working mode parameters' become available.

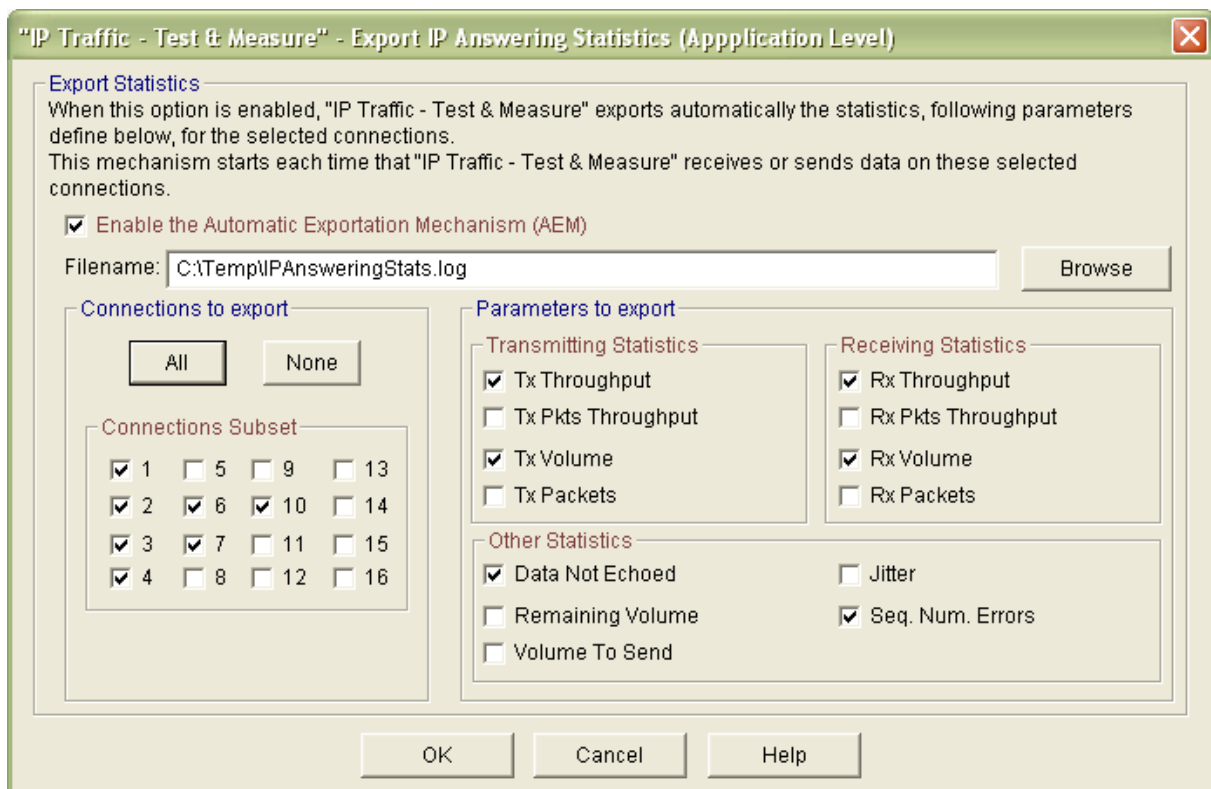
### 6.9.6 "Export IP Answering statistics in a file" parameters

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



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

- Enable or disable the export process,
- The filename (.log extension by default) of the export file,
- The identification of the needed connections,
- The parameters to export (up to 13).



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

Export Statistics into a File

Parameters

Export is enabled

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

Export is enabled

Note:

*Do not specify the same filename to save statistics for the 'IP Generator' and the 'IP Answering' parts; otherwise a warning message is displayed.*

The statistics file is updated at the same rate than the statistics are 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 IP Answering has been pressed and the 'Export is running' state is displayed:

Export Statistics into a File

Parameters

Export is running

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

Export Statistics into a File

Parameters

Export is enabled

#### 6.9.6.1 The 'IP Answering' statistics file format

**The IP Generator statistics file is formatted line by line as follows (example):**

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

**Second line:** IP Traffic - Test & Measure IP Answering

**Third line:** (Only five statistics headers are showed here. Statistics headers can be up to thirteen)

<u>Cnx#1</u> (Protocol)	<u>Date</u>	<u>Time</u>	<u>Throughput</u> <u>ut</u> (Kb/s)	<u>Data sent</u> (UDP:Packets/ TCP:KB)	<u>Data received</u> (UDP:Packets/ TCP:KB)	<u>Seq. Num.</u> <u>Errors</u>	<u>Data not echoed</u> (UDP:Packets/ TCP:KB)
----------------------------	-------------	-------------	--	--	--	-----------------------------------	--

**Other lines:**

Cnx #i (TCP or UDP)	MM/DD/YYYY	HH:MM:SS,mmm	nnn.nn	nnn.nn	nnn.nn	X	nnn.nn
---------------------	------------	--------------	--------	--------	--------	---	--------

#### **Additional mark for TCP connection events**

Cnx #n (TCP) STARTIt indicates the connection #n starts (n: from 01 to 16). When this mark is included in the IP Generator traces, numerical values are set to 0.

Cnx #n (TCP) END It indicates the connection #n has stopped. Numerical values are latest values computed by "IP Traffic - Test & Measure".

## Additional mark for TCP or UDP disconnection events

Cnx #n (TCP) 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 IP Generator traces, numerical values are replaced by the error message returned by “IP Traffic – Test & Measure”.

## 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 IP Answering 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 'IP Generator' 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”.

## Export an IP Answering file sample

In this example, 3 connections have been selected with all parameters exported.

For each connection, the 'IP Answering' is operating with the echoer mode.

- Connection #01 is configured with the TCP protocol, and the remote 'IP Generator' includes the RTT information (so, “IP Traffic – Test & Measure” can check sequence errors at the 'IP Answering' level).
- Connection #02 is configured with the TCP protocol.
- Connection #03 is configured with the UDP protocol, and the remote 'IP Generator' includes the RTT information.

The “Refresh time” parameter is set to 2 seconds.

Starting session 04/02/2005 at 12:05:52.328									
IP Traffic - Test & Measure IP Answering									
Cnx#i (Protocol)	Date	Time	Tx Throughput (Kb/s)	Tx Volume (KB)	Rx Throughput (Kb/s)	Rx Volume (KB)	Data Not Echoed (KB)	Jitter (ms)	Seq. Num. Errors
Cnx#3 (UDP) START	04/02/2005	12:05:56.562	0.00	0.00	0.00	0.00	0	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:05:56.578	0.00	0.00	0.00	0.00	0	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:05:59.359	0.00	0.00	0.00	0.00	0	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:01.359	0.00	0.00	0.00	0.00	0	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:03.359	0.00	0.00	0.00	0.00	0	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:05.343	0.00	0.00	0.00	0.00	0	N/A	N/A
Cnx#3	04/02/2005	12:06:07.359	0.00	0.00	0.00	0.00	0	N/A	N/A

(UDP)									
Cnx#3 (UDP)	04/02/2005	12:06:09.359	0.00	0.00	0.00	0.00	0	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:11.359	0.00	0.00	0.00	0.00	0	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:13.359	0.00	0.00	0.00	0.00	0	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:15.343	0.00	0.00	0.00	0.00	0	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:17.359	0.00	0.00	0.00	0.00	0	N/A	N/A
Cnx#1 (TCP) START	04/02/2005	12:06:19.343	0.00	522.86	0.00	557.48	33992	0	0
Cnx#2 (TCP) START	04/02/2005	12:06:19.390	0.00	0.00	0.00	14.26	N/A	N/A	N/A
Cnx#1 (TCP)	04/02/2005	12:06:19.453	0.00	604.29	0.00	661.48	50376	0	0
Cnx#2 (TCP)	04/02/2005	12:06:19.453	0.00	0.00	0.00	19.96	N/A	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:19.453	31.94	32.79	31.94	32.79	0	0	1
Cnx#1 (TCP)	04/02/2005	12:06:21.406	9250.20	11887.52	9432.08	12070.66	180240	0	0
Cnx#2 (TCP)	04/02/2005	12:06:21.406	0.00	0.00	141.44	156.84	N/A	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:21.406	264.63	303.69	264.63	303.69	0	33	1
Cnx#1 (TCP)	04/02/2005	12:06:23.375	28277.21	24094.18	28719.79	24433.61	347576	0	0
Cnx#2 (TCP)	04/02/2005	12:06:23.375	0.00	0.00	371.84	297.99	N/A	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:23.375	720.88	586.00	720.88	586.00	0	42	1
Cnx#1 (TCP)	04/02/2005	12:06:25.359	46881.32	36029.09	47598.91	36568.44	552296	0	0
Cnx#2 (TCP)	04/02/2005	12:06:25.359	0.00	0.00	577.16	440.57	N/A	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:25.359	1140.63	865.45	1140.63	865.45	0	43	1
Cnx#1 (TCP)	04/02/2005	12:06:27.359	46094.04	46994.14	46856.10	47709.81	724656	0	0
Cnx#2 (TCP)	04/02/2005	12:06:27.359	0.00	0.00	570.31	584.57	N/A	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:27.359	1131.50	1150.61	1131.50	1150.61	0	42	1
Cnx#1 (TCP)	04/02/2005	12:06:29.359	45097.41	58641.58	45805.09	59512.11	889964	0	0
Cnx#2 (TCP)	04/02/2005	12:06:29.359	0.00	0.00	570.31	725.72	N/A	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:29.359	1129.22	1431.48	1129.22	1431.48	0	43	1
Cnx#1 (TCP)	04/02/2005	12:06:31.359	40478.24	67846.58	41069.34	68839.57	1008628	0	0
Cnx#2 (TCP)	04/02/2005	12:06:31.359	0.00	0.00	570.31	868.30	N/A	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:31.359	1131.50	1716.64	1131.50	1716.64	0	45	1
Cnx#1 (TCP)	04/02/2005	12:06:33.359	41607.71	78889.18	42226.82	80073.30	1204352	0	0
Cnx#2 (TCP)	04/02/2005	12:06:33.359	0.00	0.00	570.31	1010.88	N/A	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:33.359	1131.50	1993.24	1131.50	1993.24	0	40	2
Cnx#1 (TCP)	04/02/2005	12:06:35.359	36696.95	87350.39	37303.76	88657.93	1322532	0	0
Cnx#2 (TCP)	04/02/2005	12:06:35.359	0.00	0.00	568.03	1153.46	N/A	N/A	N/A
Cnx#3 (UDP)	04/02/2005	12:06:35.359	1120.09	2276.97	1122.38	2278.40	0	40	2
Cnx#1 (TCP)	04/02/2005	12:06:37.359	39717.18	98786.34	40323.89	100270.92	1503824	0	0
Cnx#2 (TCP)	04/02/2005	12:06:37.359	0.00	0.00	570.31	1294.61	N/A	N/A	N/A



Cnx#3 (UDP)	04/02/2005	12:06:37.359	1122.38	2556.43	1124.66	2557.85	0	40	2
Cnx#2 (TCP) ERROR	04/02/2005	12:06:38.968	IPTr:Ending on close for cnx 2						
Cnx#2 (TCP) END	04/02/2005	12:06:38.968	0.00	0.00	570.31	1395.84	N/A	N/A	N/A
Cnx#1 (TCP) ERROR	04/02/2005	12:06:39.031	IPTr:Ending on close for cnx 1						
Cnx#1 (TCP) END	04/02/2005	12:06:39.031	39717.18	106137.41	40323.89	107746.29	1631104	0	0
Cnx#3 (UDP)	04/02/2005	12:06:39.359	1126.94	2756.04	1129.22	2757.46	0	40	2
Cnx#3 (UDP)	04/02/2005	12:06:41.359	755.09	2756.04	755.09	2757.46	0	40	2
Cnx#3 (UDP)	04/02/2005	12:06:43.359	305.69	2756.04	305.69	2757.46	0	34	2
Cnx#3 (UDP)	04/02/2005	12:06:45.343	0.00	2756.04	0.00	2757.46	0	26	2
Cnx#3 (UDP)	04/02/2005	12:06:45.687	0.00	2756.04	0.00	2757.46	0	0	2

*The delimiter mark used between each field is the tabulation character.*

## 6.10 The 'Traffic Sniffer' tab

This tab is composed of three numbered areas:

1. **Step 1: Capture parameters:** traffic can be captured by "IP Traffic – Test & Measure" with 2 options: all IP traffic or IP traffic on connections specified by the user.
2. **Step 2: Capture sniffed traffic in a file:** once that capture parameters have been defined, captured traffic may be saved in a file.
3. **Step 3 (optional): Run analysis algorithm on a sniffed traffic file to generate data traffic files:** from an IP capture file, "IP Traffic – Test & Measure" uses an internal algorithm to produce two traffic files used by the Replay mode of the IP Generator and of IP Answering.

*Note: "IP Traffic – Test & Measure" allows capturing traffic in a file.*

*This is used in two cases:*

- *For off-line statistics (see tab 5: 'Traffic Observer'): in this case, step 3 is not necessary.*
- *In order to replay traffic via the 'IP Generator': in this case, step 3 must be done.*

The screenshot shows the 'Traffic Sniffer' tab with the following sections:

- Section 1: Capture Parameters**
  - Buttons: New filter, Edit filter, Delete filter
  - Table:

	Source IP addr.	Destination IP addr.	Source Port	Destination Port	Protocol
<input checked="" type="checkbox"/>	192.168.0.30	www.zti.fr	From any port	To any port	TCP & UDP
  - Radio button: ☐ All TCP and UDP packets (unicast and/or multicast)
  - Buttons: Help, Select adapters
- Section 2: Capture sniffed traffic in a file (used for statistics or traffic generator)**
  - File path: H:\Captures\HTTPTraffic.Trc (with Browse button)
  - Buttons: Start, Stop
  - Checkboxes:
    - ☒ Save only headers of the packets (Data are not registered)
    - ☒ Automatic refresh mode
    - ☒ Enable automatic start in 'Local operation'
  - Traffic overview during capture:

Capture started at 09:22:12 (UTC) - Only headers are saved into the file  
Capture stopped at 09:22:13 (UTC)
- Section 3: Run analysis algorithm on a sniffed traffic file to generate data traffic files (for use by the IP Traffic generator)**
  - Input traffic file: H:\Captures\Capture Netmeeting 1.T (with Browse button)
  - Output data traffic file 1 to replay after processing: H:\Captures\Netmeeting1 (with Browse button)
  - Output data traffic file 2 to replay after processing: H:\Captures\Netmeeting2 (with Browse button)
  - Synthesis after processing:

2830550 bytes written in file H:\Captures\Netmeeting1  
5642009 bytes written in file H:\Captures\Netmeeting2
  - Buttons: Start, Stop

Tab 4: "Traffic Sniffer"

## 6.10.1 Capture Parameters

**Step 1:** two options are available:

- ⇒ **All TCP and UDP unicast and/or multicast packets:** "IP Traffic – Test & Measure" will capture all TCP and UDP unicast packets seen by the 'Traffic Sniffer'. This option is selected by default.
- ⇒ **Use filter(s):** Traffic capture is made according to user defined filters as explained below.

### Note:

*With "Use filter(s)" option selected, at least one user defined filter should be selected in the list box to be allowed to start the traffic capture.*

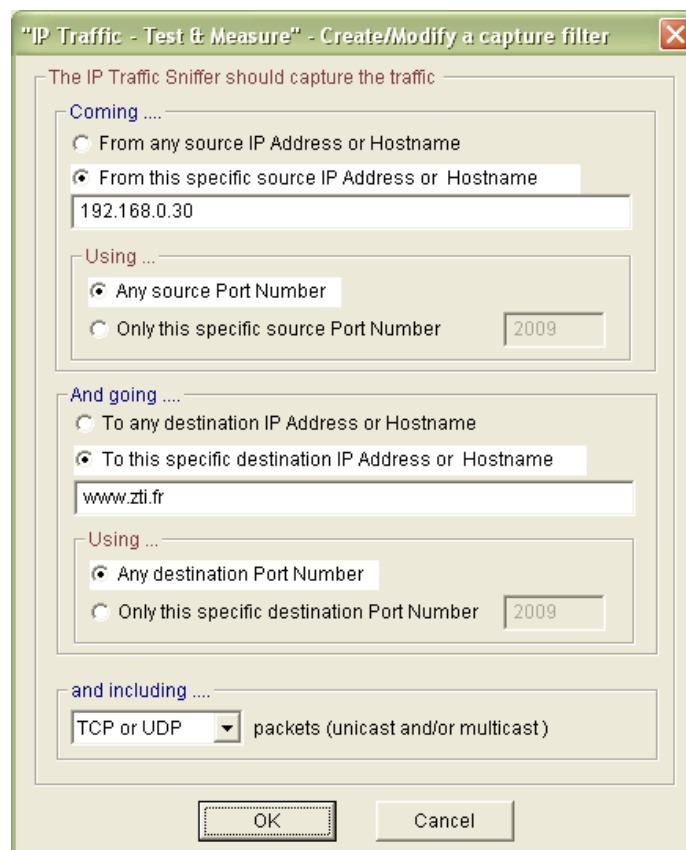


Step 1: Capture Parameters Specification

### 6.10.1.1 Create/Modify/Delete user defined filters

You can define many 'filters' composed of five parameters: Source IP address, Destination IP address, Source Port number, Destination Port number and Protocol.

The command buttons "Add filter", "Edit filter" and "Delete filter" allow adding, editing and removing the user-defined filters. By clicking on "Add filter", the window below appears:



Filter edition window

This window is composed by three main areas.

1. Specification of the "Coming ..." information
  - a. Specification of the source IP Address or Host Name of the traffic
  - b. Specification of a particular source port number
2. Specification of the "And going ..." information.
  - a. Specification of the destination IP Address or Host Name of the traffic
  - b. Specification of a particular destination port number
3. Specification of the protocol(s) :
  - a. Capture only TCP packets
  - b. Capture only UDP packets (including multicast traffic)
  - c. Capture TCP and UDP packets

Note:

*Each parameter is optional. It is not necessary to specify a value. In this case, this parameter is not used to filter packets.*

Warning:

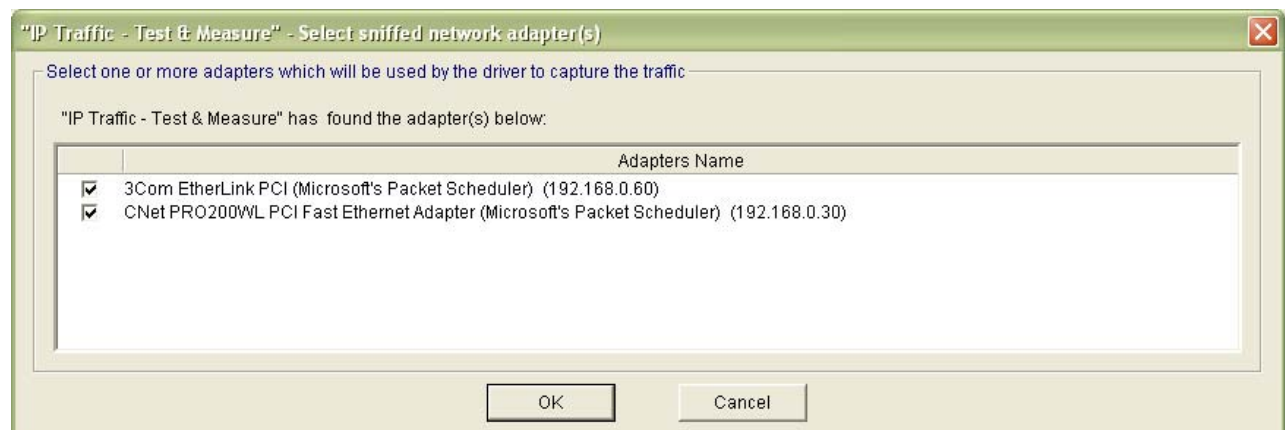
*You can input different filters, but "IP Traffic – Test & Measure" doesn't control the functional coherence between the filters.*

To edit a filter, select it in the list box and then press the 'Edit filter' button.

To delete a filter, select it in the list box and then press the 'Delete filter' button.

#### 6.10.1.2 Select Adapters (optional)

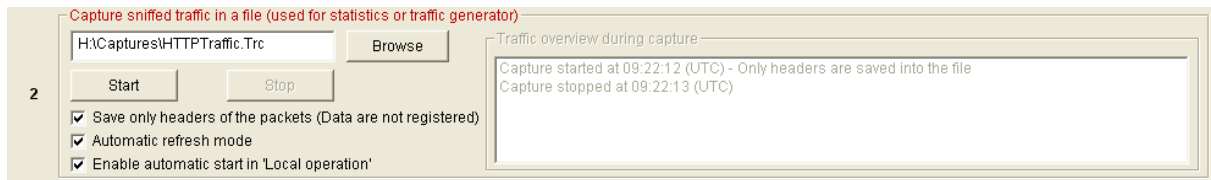
By clicking on the "Select Adapters" button, the window below opens. By default, if your machine contains more than one network card, IP Traffic Sniffer driver pools all of the network cards and captures all packets. This polling capacity can be greedy for resource. If it is not necessary, up to one network card could be specified.



*Adapters selection window*

## 6.10.2 Capture sniffed traffic into a file

**Step 2:** once that capture parameters have been defined in the previous area, you must define a capture file. The command buttons **“Start”** and **“Stop”** allow starting and stopping the traffic capture.



Step 2: Capture traffic control panel

During the capture process, information is displayed in the “Traffic overview during capture” object (statistics if available).

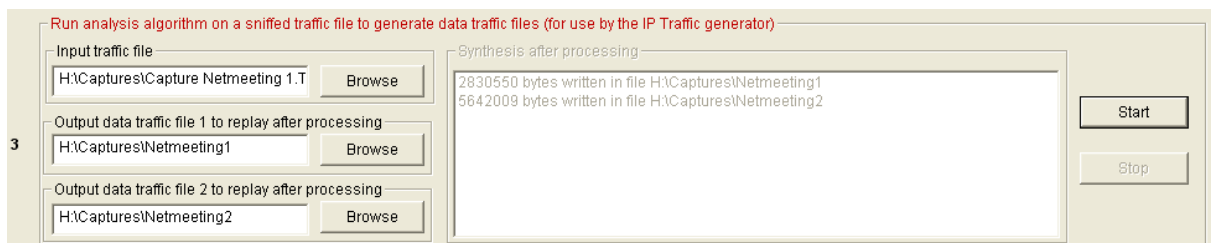
**“Save only the headers of the captured packets (Data are not saved)” check box:** if checked, only the packet headers are saved (thus significantly reducing the size of the capture file) but you will be not able to use this file for the step 3.

**“Automatic refresh mode” check box:** allows refreshing display in the “Traffic overview during capture” object.

**“Enable automatic start in ‘Local operation’ check box:** if checked, the “Start all processes” button of the “Local operation” will launch automatically the ‘Traffic Sniffer’.

## 6.10.3 Run analysis algorithm

**Step 3:** in step 2, the capture process has generated a capture traffic file.



Then if needed, you specify a capture traffic file name in the **“Input traffic file”** object and two output files.

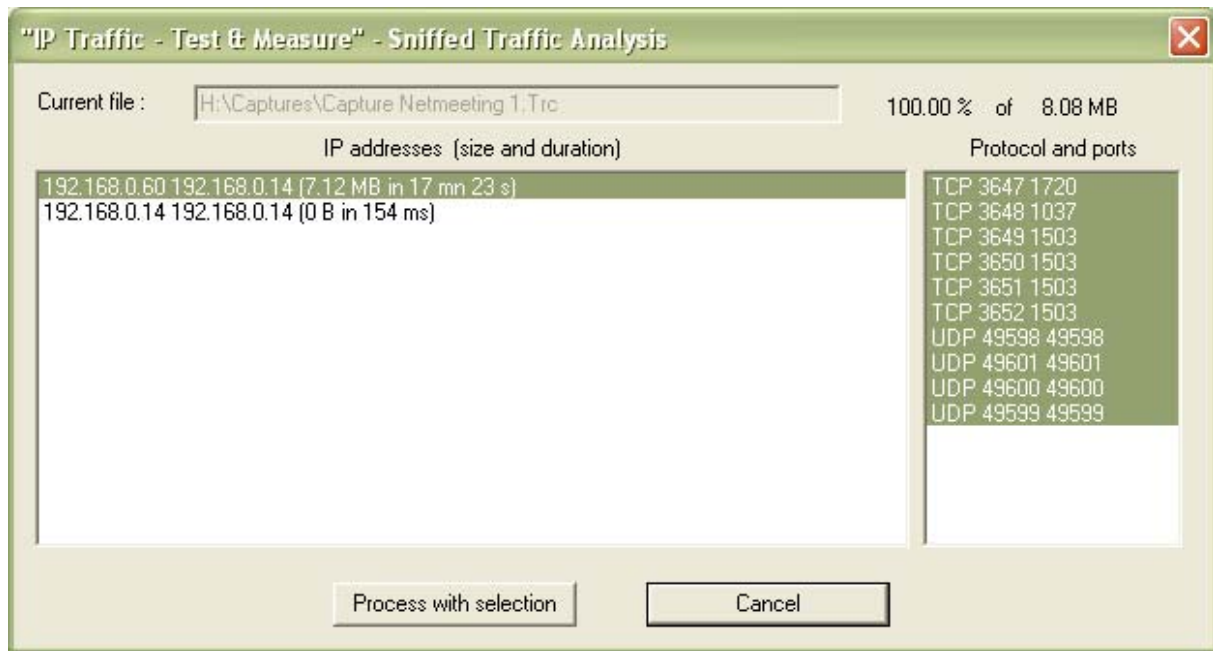
### Note:

The **“Input traffic file”** must contain data (see Step 2). Files containing only headers can’t be used by the Step 3.

This file contains IP frames with different IP source addresses and IP source destinations.

The goal is to find in the input traffic file the communication entities (IP Generator and IP Answering) and to produce two traffic files to replay. An internal “IP Traffic – Test & Measure” algorithm analyzes IP frames from the Input traffic file and produces the two traffic files named **“Output data traffic file1 to replay after processing”** and **“Output data traffic file2 to replay after processing”**.

When you press the "Start" button, the following window is displayed:



You can select connections to consider (addresses + protocol and ports) and then activate "Process with selection".

After processing, the object "**Synthesis after processing**" displays statistics information about generated files and connections.

## 6.11 The ‘Traffic Observer’ tab

This fifth tab allows to:

- Visualize statistics and graphs for different parameters: IP throughput, Inter packet delay, Packet Erasure Rate quality (PER quality) and Packet transit delay,
- Download remote statistics traffic files,
- Analyze off-line traffic,
- Export statistics in a file.

The tab is divided into three main areas:

- The central area displays graphs and values,
- The right area contains objects and command buttons to select parameters to display,
- The bottom area is composed of four blocks:
  - **Remote (statistics) traffic files:** to download statistics traffic files from the remote, in order to do off-line statistic analysis.
  - **Off-line traffic analysis:** to do off-line analysis. It is necessary to have a local statistic traffic file and a remote statistic traffic file (downloaded via the previous area).
  - **Index (on-line or off-line):** one index is a marker set by the user that is used during off-line analysis for graphics display.
  - **Export statistics:** you can define statistic parameters to export in a file and Start / Stop the export process.

The screenshot displays the 'Traffic Observer' tab of the IP Traffic software. The main window is divided into several sections:

- Top Tab Bar:** Includes 'IP Generator - Parameters', 'IP Generator - Traffic + Statistics', 'IP Answering - Parameters + Statistics', 'Traffic Sniffer', and the active 'Traffic Observer' tab.
- Statistical Values (based on Driver Statistics):** A large table with columns for 'IP Address/Host Name', 'Port', 'Prot.', 'IP Throughput Snapshot' (Tx, Rx), 'IP Throughput Average' (Tx, Rx), 'UDP or TCP Throughput' (Tx, Rx), 'Inter Packet Delay' (Tx, Rx), 'Packet Transit Delay' (Tx, Rx), and 'Packet Erasure Rate (PER)' (Tx, Rx). It lists 16 connections, all showing 0.00 b/s for throughput and 0 ms for delay.
- Right Panel:** Contains controls for 'IP Generator' and 'IP Answering'. Under 'Statistics Display', there are radio buttons for 'Values' (selected), 'Graphics', and 'Packet Statistics'. Below this are checkboxes for 'IP Throughput', 'Inter Packet Delay', 'Packet Transit Delay', and 'PER Quality'. At the bottom of the right panel are 'Reset Statistics' and 'Help' buttons.
- Bottom Panel:** Divided into four functional blocks:
  - Remote Traffic Files:** A 'Download...' button.
  - Off-Line Traffic Analysis:** Radio buttons for 'Yes' and 'No', followed by 'Process Files...', 'Play >', 'Play >>', 'Pause', and 'Stop' buttons.
  - Index (On-Line or Off-Line):** 'Next >', 'Add', a counter '00 / 00', 'Remove', and 'Remove all' buttons.
  - Export Statistics:** 'Parameters', 'Start', and 'Stop' buttons.

Tab 5: Traffic Observer (on-line mode)

**Note:**

Values and statistics displayed in this tab are calculated at the ‘time’ point of reference (see “IP Traffic – Test & Measure” architecture in Part 1) i.e. under the TCP/IP protocol stack.

### 6.11.1 “IP Traffic – Test & Measure”: On-line and Off-line modes for statistics

When “IP Traffic – Test & Measure” is operating (‘IP Generator’ is active and/or ‘IP Answering’ is active), this mode is named on-line. On-line statistics are displayed in the following tabs:

- ‘IP Generator – Traffic + statistics’: statistics area,
- ‘IP Answering – Parameters + statistics’: statistics area,
- ‘Traffic Observer’: statistics area, but all parameters are not displayed: PER (Packet Erasure Rate) and Packet transit delay need remote information to be computed.

By using the “Traffic Sniffer” tab, a capture traffic file can be defined (see step 2 in the Traffic Sniffer tab, Part 6-9) to save traffic that would be used in the off-line mode. Both file formats (With Data or Headers only) can be used for Off-line calculation.



You can switch between the off-line and on-line mode by using the Yes / No radio button.



Off-line mode is defined as a state where all “IP Traffic – Test & Measure” activity is stopped (‘IP Generator’, ‘IP Answering’ and ‘Traffic Sniffer’ are stopped). In this mode, only the “Traffic Observer” tab is available. All other tabs are inhibited.

In order to analyze traffic files and obtain all statistics, the user must first download a traffic file from the remote. “IP Traffic – Test & Measure” uses two traffic files to do off-line statistics analysis: a ‘local’ traffic file (generated by the ‘Traffic Sniffer’) and a downloaded ‘remote’ traffic file (generated by the remote ‘Traffic Sniffer’).

Note:

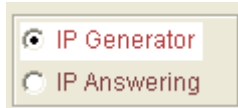
A red color for objects or command buttons in the ‘Traffic Observer’ tab means that these items are only available in the off-line mode.



## 6.11.2 Objects and command buttons

All objects and command buttons on the right and at the bottom of the 'Traffic Observer' tab are explained here.

### 6.11.2.1 On the right of the 'Traffic Observer' tab



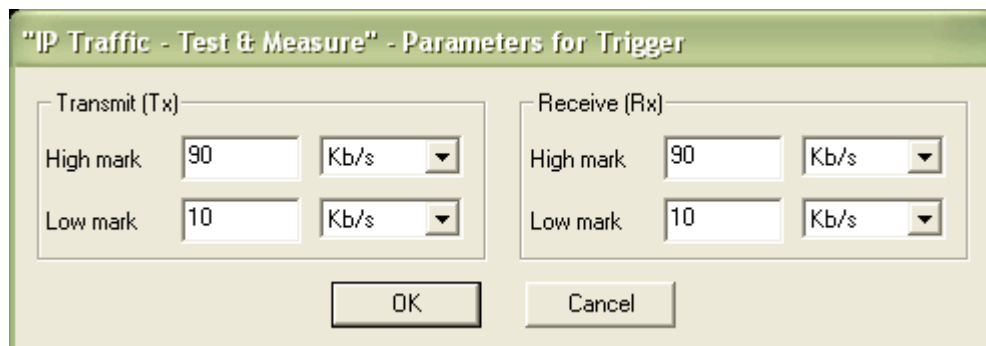
This choice allows selecting display connections for the 'IP Generator' or the "IP Answering" module. So, the user can switch simply to see statistics for the 16 'IP Generator' connections and the 16 'IP Answering' connections.

You can define different scale factors for the Transmit (Tx) and the Receive (Rx) graphs, and one value for the time scale.



Triggers are used for graphics displays (see statistics display below). The command button "**Triggers Parameters**" opens a dialog window where user defines 2 triggers (low and high) according to the parameters: IP throughput, Inter packet delay, PER and Packet transit delay. The command buttons "**Start Triggers**" and "**Stop Triggers**" allow enabling or disabling the defined triggers.

When a parameter is lower or upper than the threshold defined, counters are incremented in the graphic area. Triggers are displayed in red color.



*Parameters for the triggers*

The statistics display area allows choosing a display item:

*On-line mode*

*Off-line mode*



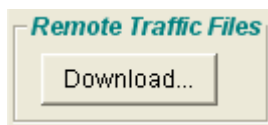
- **Values:** a values table (6 parameters for each connection with Tx and Rx values) is displayed (*on-line and off-line*),
- **Graphics:** select first 1 or all connections and then the parameter to display:
  - **IP Throughput** (*on-line and off-line*),
  - **Inter Packet Delay** (*on-line and off-line*),
  - **Packet Transit Delay** (*off-line only*),
  - **PER (Packet Erasure Rate) quality** (*off-line only*)
- **Packet Statistics:** *off-line only and when traffic files have been previously loaded and processed.*



The command button "**Reset statistics**" resets all statistics values displayed whatever the statistics display item is selected (see above).

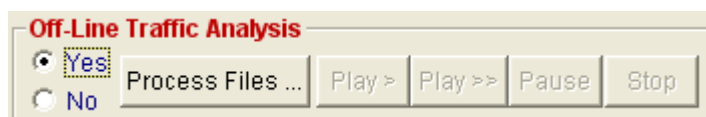
The command button "**Help**" displays a help window explaining all functionalities and commands for the 'Traffic Observer' tab.

#### 6.11.2.2 In the lower part of the 'Traffic Observer' tab



The command button "**Download...**" is used to download remote traffic files generated by "IP Traffic – Test & Measure" (via the 'Traffic Sniffer').

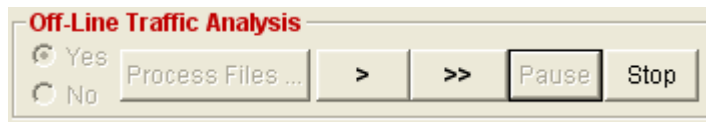
To calculate off-line statistics for all parameters, "IP Traffic – Test & Measure" uses 2 traffic files generated by the 'Traffic Sniffer' (see step 2 in the 'Traffic Sniffer' tab): a local traffic file and a remote traffic file.



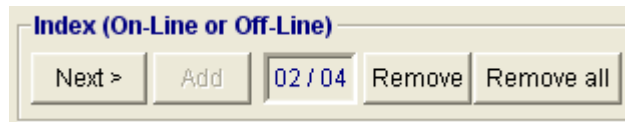
The command buttons of the "Off-line traffic analysis" area are used in off-line mode to display values and statistics from traffic files.

- "**Process files...**": to select two traffic files (a local traffic file and a remote traffic file downloaded via the previous "**Download...**" command button by example).
- "**Play >**": "IP Traffic – Test & Measure" replays the local traffic file at the beginning (selected via the previous "Process Files..." command) according to timing contained in the file.
- "**Play >>**": idem "Play >" with a quick replay speed.
- "**Pause**": traffic replay is halted. You can continue replay traffic with "Play >" or "Play >>".
- "**Stop**": ends traffic replay.

The "**Play >**", "**Play >>**" and "**Stop**" buttons are enabled once that traffic files have been analyzed via the "**Process files...**" button (see further in this paragraph).



The "**Play >**" or "**Play >>**" buttons are replaced by ">" and ">>" after the user has pressed "**Pause**" for the first time.



The command buttons of the "Index (On-line or Off-line)" area are used to manage display index (or markers) in graphic displays for the off-line mode. These buttons are used:

- To add and remove index,
- To help the user to navigate when displaying off-line traffic analysis.

- "**Next >**": the current position in the traffic file to analyze is set to the next display index set by the user.
- "**Add**": adds a display index at the current position.
- "**XX/YY**": displays the actual XX index number (YY is the total number of indexes set by the user).
- "**Remove**": removes the current displayed index.
- "**Remove all**": removes all displayed indexes.

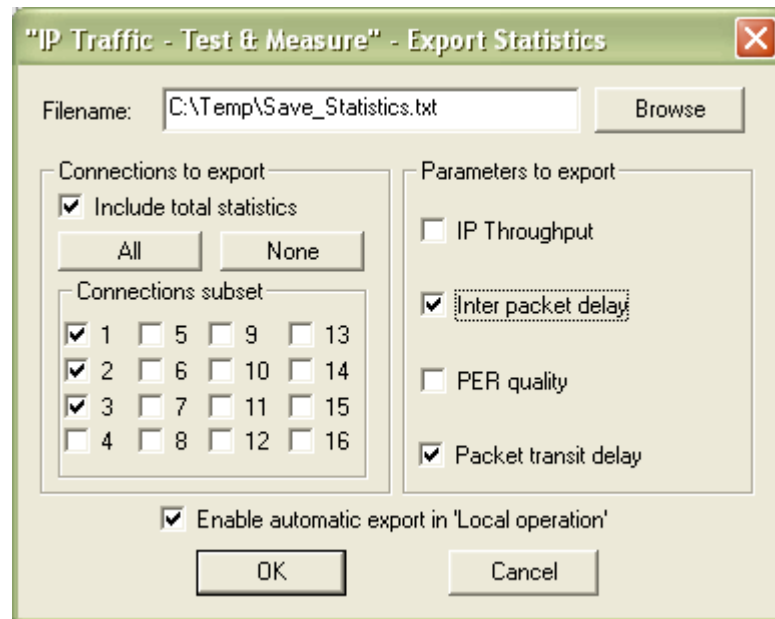


The "**Export statistics**" area allows exporting in a file statistics values calculated by "IP Traffic – Test & Measure" with filter parameters defined by the user.

You define first the export filters and filename by using the command button "**Parameters**". Export filters allow selecting: connection(s) and parameter(s).

The statistics export file is a text file with a format defined in the annex part.

The command buttons "**Start**" and "**Stop**" allow starting and stopping the export statistics process in the user-defined file.



*Parameters to export statistics*

### **Filename**

Statistics are saved in the specified file accordingly to parameters described below.

### **Connections to export:**

#### **Include total statistics**

If checked, the following parameters are saved in the file for the 'IP Generator' and the 'IP Answering' modules (see the file format explained in the next paragraph).

[Total Throughput Tx] [Total Throughput Rx] [Total Inter packet delay Tx] [Total Inter packet delay Rx] [Total PER Tx] [Total PER Rx] [Total Transit delay Tx] [Total Transit delay Rx]

where the term total is used as the sum of values for connections selected by user. Tx is used as Transmit and Rx as Receive.

#### **'All' or 'None'**

These buttons select all the connections or none.

#### **Connections subset**

Select the needed connections in order to save statistics for these connections.

### **Parameters to export:**

Select the parameter you want to save as statistics.

### **Enable automatic export in 'Local operation' check box**

If checked, the "Run all processes" button of the "Local operation" will launch automatically the export of statistics in the file according to parameters defined in the above window.

### Format of the statistics file

The general format is defined for one line in the file (with the tab character as delimiter) as:

<Location (if GPS operational)> <Date> <Time> [< Total statistics for the IP Generator>  
<Connections Statistics for the IP Generator> [< Total statistics for the IP Answering>  
<Connections Statistics for the IP Answering>

[< Total statistics for the IP Generator>] and [< Total statistics for the IP Answering>] are included if the 'Include total statistics' check box has been checked.

<Total statistics for the ...> is structured as follows:

[Total Throughput Tx] [Total Throughput Rx] [Total Inter packet delay Tx] [Total Inter packet delay Rx] [Total PER Tx] [Total PER Rx] [Total Transit delay Tx] [Total Transit delay Rx]

where the term total is used for the sum or the total of connections saved in the file, and Tx = Transmit, Rx= Receive.

<Connections Statistics for the IP Generator> or <Connections Statistics for the IP Answering> are structured as follows for a connection:

[#nn Throughput Tx] [#nn Throughput Rx] [#nn Inter packet delay Tx] [#nn Inter packet delay Rx] [#nn PER Tx] [#nn PER Rx] [#nn Transit delay Tx] [#nn Transit delay Rx]

These fields are present depending of the parameter(s) selected:

- IP Throughput
- Inter packet delay
- PER quality
- Packet transit delay

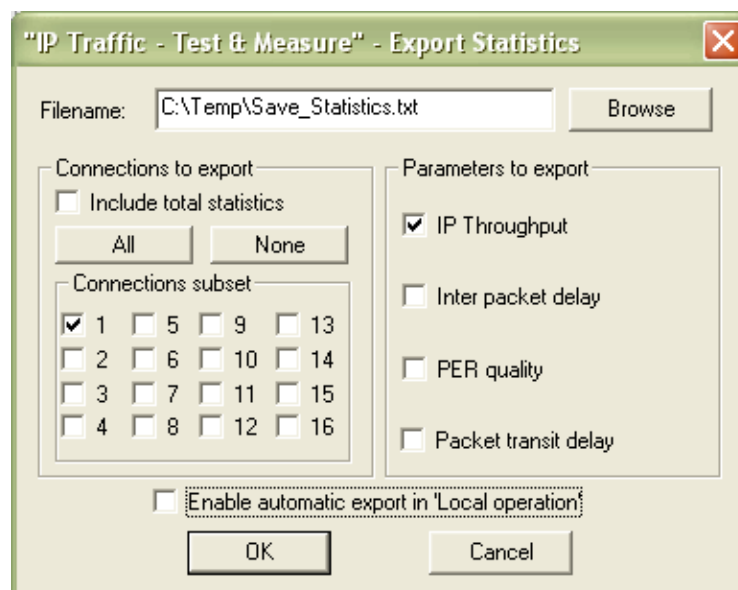
#### Note:

*It is recommended to define carefully the parameters to use; otherwise, the number of columns in the file can be high (and an application like Excel may have problems to import this file).*

*The 'Include total statistics' generate 16 columns per line (8 columns for the 'IP Generator' and '8 columns' for the IP Answering)*

*When you select the 4 parameters to export (IP Throughput, Inter packet delay, PER quality and packet transit delay), that generates 16 columns to export for each connection (2 columns Rx and Tx per parameter = 8 columns for the 'IP Generator' and 8 columns for the 'IP Answering'). When 16 connections are selected, that generates 16 x 16 = 256 columns.*

The following example has been generated for connection # 1 by using:

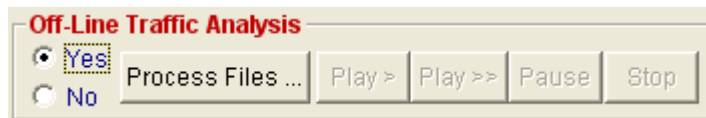


View of the generated file (by Excel):

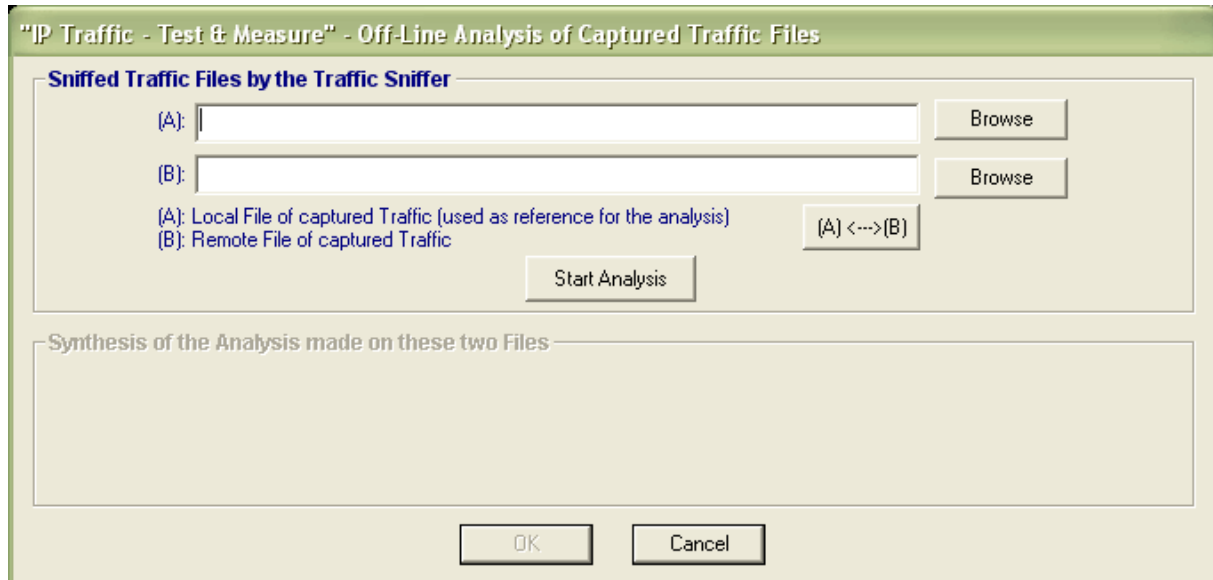
Starting session 04/02/2005 at 10:04:53,828						
IP generator then IP answering						
Location	Date	Time	#1 Throughput Tx (Kb/s)	#1 Throughput Rx (Kb/s)	#1 Throughput Tx (Kb/s)	#1 Throughput Rx (Kb/s)
	04/02/2005	10:05:32	585.37	7.80	7150.11	6724.68
	04/02/2005	10:05:33	585.37	7.80	34786.69	35534.52
	04/02/2005	10:05:34	575.34	7.83	47907.98	48467.63
	04/02/2005	10:05:35	585.94	7.50	38407.81	39074.06
	04/02/2005	10:05:36	573.66	7.80	47592.21	48103.96
	04/02/2005	10:05:37	585.94	7.81	38394.09	39121.09
	04/02/2005	10:05:38	573.66	7.80	43840.07	44810.15
	04/02/2005	10:05:39	575.34	7.51	38888.61	39524.54
	04/02/2005	10:05:40	574.22	7.81	45008.19	45548.91
	04/02/2005	10:05:41	585.94	7.81	39250.31	39998.91
	04/02/2005	10:05:42	573.66	7.80	47448.26	48630.01
	04/02/2005	10:05:43	574.78	7.51	40484.63	41211.65
	04/02/2005	10:05:44	585.37	7.80	46030.45	46680.51
	04/02/2005	10:05:45	574.78	7.82	38802.36	39085.05
	04/02/2005	10:05:46	585.94	7.81	43434.16	44418.28
	04/02/2005	10:05:47	562.50	7.81	45220.88	46275.47
	04/02/2005	10:05:48	562.50	7.50	47115.25	48163.28
	04/02/2005	10:05:49	561.95	7.80	47547.44	48164.68
	04/02/2005	10:05:50	585.94	7.81	44028.91	44662.66
	04/02/2005	10:05:51	574.78	7.51	40255.09	40881.64
	04/02/2005	10:05:52	573.66	7.80	46573.20	47739.16
	04/02/2005	10:05:53	574.22	7.50	37604.41	37977.81
	04/02/2005	10:05:54	586.51	7.82	49914.37	50371.54
	04/02/2005	10:05:55	573.66	7.80	37785.75	38784.15
	04/02/2005	10:05:56	574.22	7.81	46445.88	47119.38
	04/02/2005	10:05:57	574.22	7.50	44737.72	45502.97
	04/02/2005	10:05:58	574.78	7.82	46436.63	47073.00
	04/02/2005	10:05:59	539.06	7.19	42642.66	43495.94
	....	....	.... <i>Column 4</i>	.... <i>Column 5</i>	.... <i>Column 6</i>	.... <i>Column 7</i>

The columns 4 and 5 refer to the 'IP Generator' part and columns 6 and 7 to the 'IP Answering' part.

### **The "Process Files ..." command button**



This button is enabled only with the Off-line mode. It allows sniffed traffic files to replay. Once pressed, the following window is displayed:

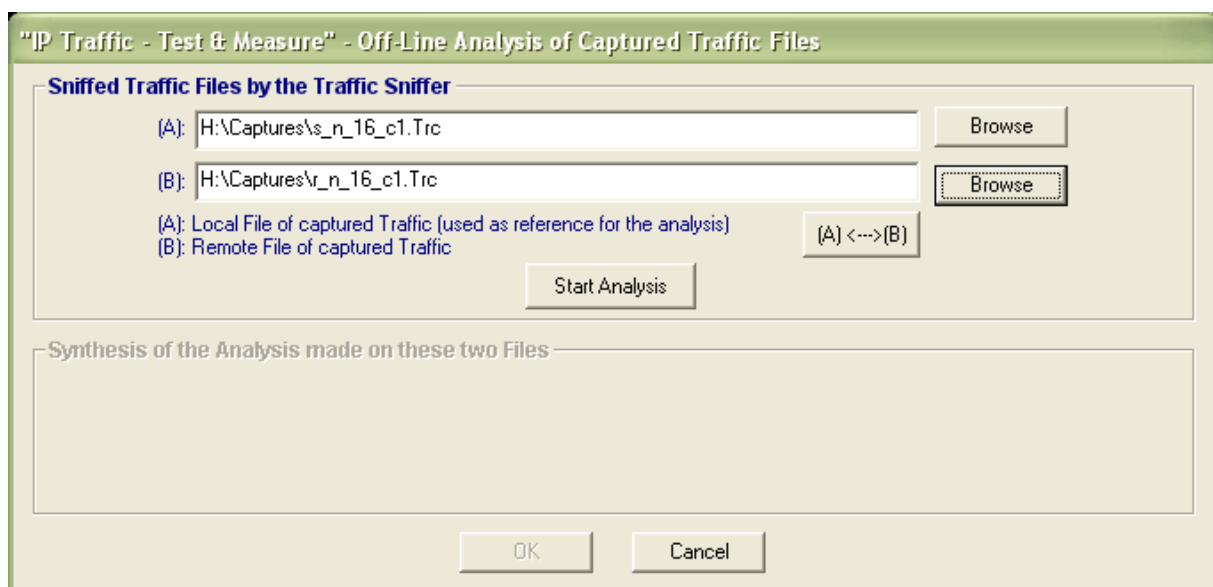


In order to proceed, you must input a local sniffed traffic file in (A) and a remote sniffed traffic file in (B).

The "(A) < --- > (B)" button inverts the (A) and (B) filenames.

#### **Note:**

*(A) will be used as reference to find the packet synchronization between these two files and to compute the statistics (for example, lost packets and the transit delay).*



Once files have been selected, then you can press the "Start Analysis" button and a new window is displayed:

**"IP Traffic - Test & Measure" - Processing of the Captured Traffic Files**

**Step 1: Files Overview**

(A):  (B):

(A) is used as reference for the analysis

When the scan is complete, please select in (A) a couple of IP addresses or connections for a couple of IP addresses. Then go to Step 2.  
Note: If you expect to replay connections, please select up to 16 connections.

**Step 2: Criteria to search the Synchronization between these two files**

Source: ☒ IP Address ☒ Port Number

Destination: ☒ IP Address ☒ Port Number

Others ...: ☒ Identification (IP header field)

Status:

You can now do the Step 3

**Step 3: Analysis to compute "Packets Statistics"**

Number of packets analysed:

Synthesis of the Analysis made on these two Files:

Processing of the sniffed traffic files is ended, you can now press "OK"

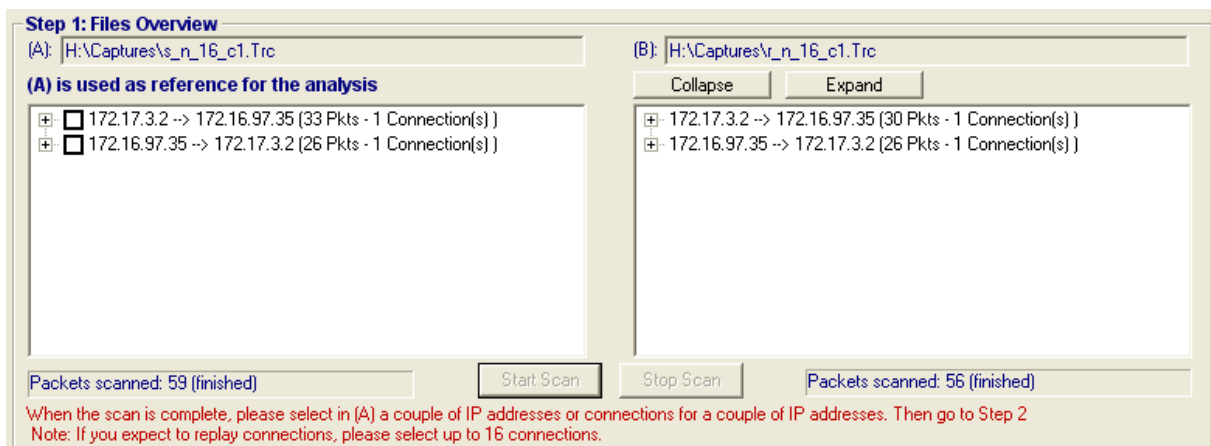
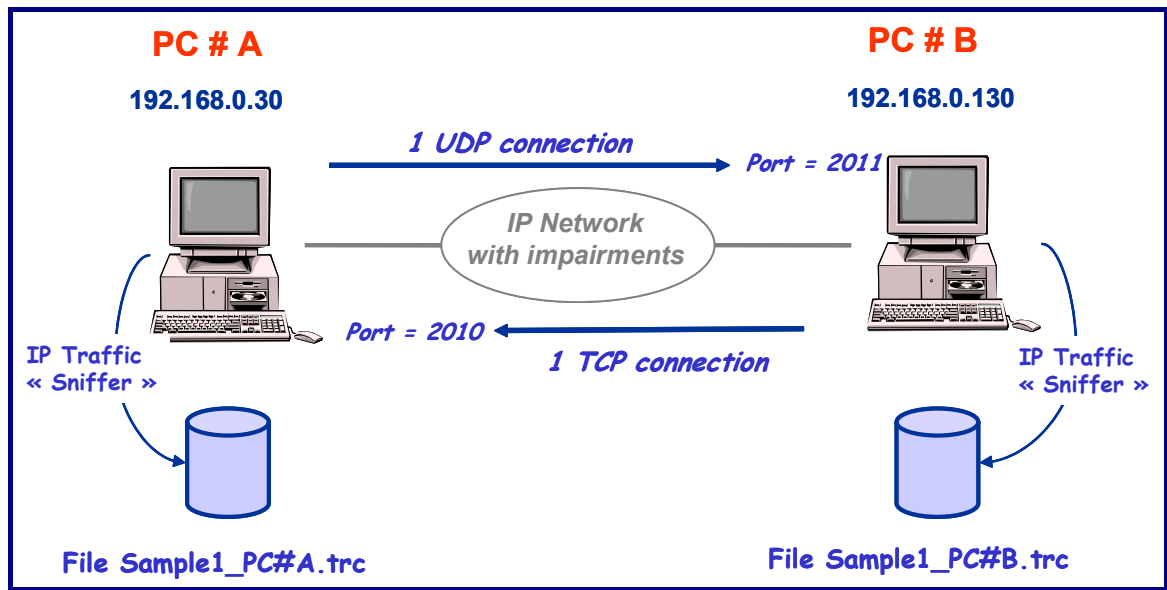
Three steps are defined in this window:

- **Step 1:** scanning of the selected files in order to display the TCP and UDP connections found.
- **Step 2:** once a couple of IP addresses or connections for a couple of IP addresses have been selected by using the step 1, you can specify one or more criteria in order to search the synchronization between these two files.
- **Step 3:** once the synchronization has been found in the step 2, you can now start the analysis in order to play these traffic files via the Traffic Observer off-line mode and compute the "Packet Statistics".

To proceed, you must first do the **Step 1** by pressing the "Start Scan" button. This scan allows display of couples of IP addresses found in these files and for each couple the number of connections and packets.



An example is given below by using two traffic files provided with the "IP Traffic – Test & Measure" software: These sniffed traffic files have been generated with the following configuration:



For each file, a descriptive is given with the following description when the scan is complete:

<Couple of IP addresses> (<Number of packets> – <Number of connections>)

where:

<Couple of IP addresses> = Source IP address → Destination IP address

<Number of packets> = number of packets found in the file for this couple of addresses

<Number of connections> = number of connections found in the file for this couple of addresses

So, you can examine easily the (A) and (B) file overviews in order to choose for analysis a specific couple of IP addresses or connection(s) for a couple of IP addresses.

For (B), two additional buttons are available 'Collapse' and 'Expand'.

As a sniffed traffic file may content a huge number of connections with for example IP address translation between the two files, you can examine the overview of these two files and decide which couple of IP addresses to consider or select one or more connections for a couple of IP addresses.

The selection can only be made on (A) which is used as reference.

Once selection is made, then the Step 2 is enabled.

**Step 1: Files Overview**

(A): H:\Captures\s\_n\_16\_c1.Trc

(B): H:\Captures\v\_n\_16\_c1.Trc

**(A) is used as reference for the analysis**

☐ 172.17.3.2 -> 172.16.97.35 (33 Pkts - 1 Connection(s))  
☒ 172.16.97.35 -> 172.17.3.2 (26 Pkts - 1 Connection(s))  
     ☒ Ports: 2009 -> 2690 (Protocol: TCP)

Packets scanned: 59 (finished)    Start Scan    Stop Scan    Packets scanned: 56 (finished)

When the scan is complete, please select in (A) a couple of IP addresses or connections for a couple of IP addresses. Then go to Step 2  
 Note: If you expect to replay connections, please select up to 16 connections.

**Step 2: Criteria to search the Synchronization between these two files**

Source: ☒ IP Address    ☒ Port Number  
 Destination: ☒ IP Address    ☒ Port Number  
 Others ...: ☒ Identification (IP header field)

Status: \_\_\_\_\_

Start Scan    Stop Scan

You can now do the Step 3

The **Step 2** is aimed to find the synchronization between the two files by using up to 5 criteria:

- Source IP address
- Source Port Number
- Destination IP address
- Destination Port Number
- Identification number (corresponding to the Identification field of the IP header)

**Note** at least one criterion must be selected.

Once you have defined one or more criteria, press the “Start Scan” button to run the search for synchronization.

During this process, the ‘Status’ field indicates statistics on the number of combinations analyzed. At the end, this field is updated with the result of the search synchronization (see examples below).

Synchronization found:	Status    Synchro Found (File A: Packet #1 <-> File B: Packet #1)
Synchronization not found:	Status    No Synchro Found

If the synchronization is not found, you can modify the search criteria and then retry.

*Remark: for example, if the receiving IP traffic system is behind a gateway that translates the source IP addresses, don’t use the ‘Source IP address’ criterion.*

With our example, we obtain the following results:

**Step 1: Files Overview**

(A): H:\Captures\s\_n\_16\_c1.Trc (B): H:\Captures\r\_n\_16\_c1.Trc

(A) is used as reference for the analysis

- ☐ 172.17.3.2 -> 172.16.97.35 (33 Pkts - 1 Connection(s))
- ☒ 172.16.97.35 -> 172.17.3.2 (26 Pkts - 1 Connection(s))
  - ☒ Ports: 2009 -> 2690 (Protocol: TCP)

Packets scanned: 59 (finished) Start Scan Stop Scan

When the scan is complete, please select in (A) a couple of IP addresses or connections for a couple of IP addresses. Then go to Step 2  
 Note: If you expect to replay connections, please select up to 16 connections.

**Step 2: Criteria to search the Synchronization between these two files**

Source: ☒ IP Address ☒ Port Number

Destination: ☒ IP Address ☒ Port Number

Others ... ☒ Identification (IP header field)

Status: Synchro Found (File A: Packet #1 <-> File B: Packet #1)

Start Scan Stop Scan

You can now do the Step 3

When the synchronization is found (for example the packet #2 of the file (A) has been founded in the file (B) as packet #2 for the search criteria defined), the Step 3 is enabled.

Note:  
 if needed you can modify the search criteria or change the selection made in step 1. In this case, you have to re-start the synchronization process

#### How does it work?

For packet #i in the file (A), a search is made in the whole file (B) by applying the user defined criteria. If success, the synchronization is found and computing is stopped, else the following packet #i+1 is considered for the next search up to the end of file (A) if necessary.

You can now run the **Step 3** by pressing the "Start Analysis" button in order to calculate the packet statistics (number of lost packets, transit delay for each packet and total statistics).

**Step 3: Analysis to compute "Packets Statistics"**

Number of packets analysed:

Start Analysis Stop Analysis

Synthesis of the Analysis made on these two Files

Processing of the sniffed traffic files is ended, you can now press "OK"

As soon as processing is started, the number of packets analyzed is displayed with the percentage already done.

#### How does it work?

For packet #i in the file (A), the search is made in the file (B) by applying the user defined criteria defined in the Step 2. As the packet #i can be received fragmented or desequenced, the search uses a depth parameter (**DEPTHFORPACKETANALYSIS**) in order to limit the processing time.

This process is applied to all packets contained in the two files in order to find the lost packets and to calculate the transit delay between the two endpoints (A) and (B).

**A packet is considered as LOST in a source file if the search on the target file has failed on a depth relative to the previous packet found in the target file.**

The depth is defined by the **DEPTHFORPACKETANALYSIS** parameter located in the Registry and valued by default to 500. To modify the DEPTHFORPACKETANALYSIS parameter located in the Registry, you must use the Registry Editor (run 'regedit').

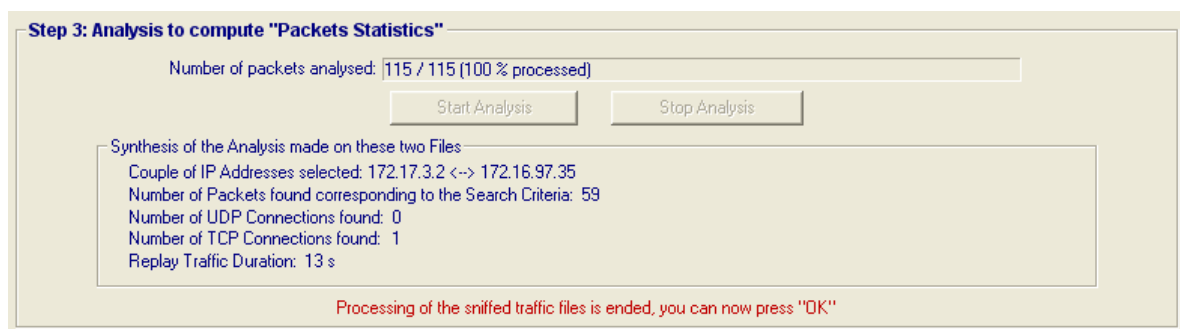
The based key to access this parameter is [\HKEY\\_LOCAL\\_MACHINE\Software\IPTraffic](#).

**Warning:**

*Once you have changed the value, you have to quit and re-start the "IP Traffic – Test & Measure" software in order "IP Traffic – Test & Measure" takes into account the new value.*

At the end of process, the number of packets analyzed is given and a synthesis is displayed:

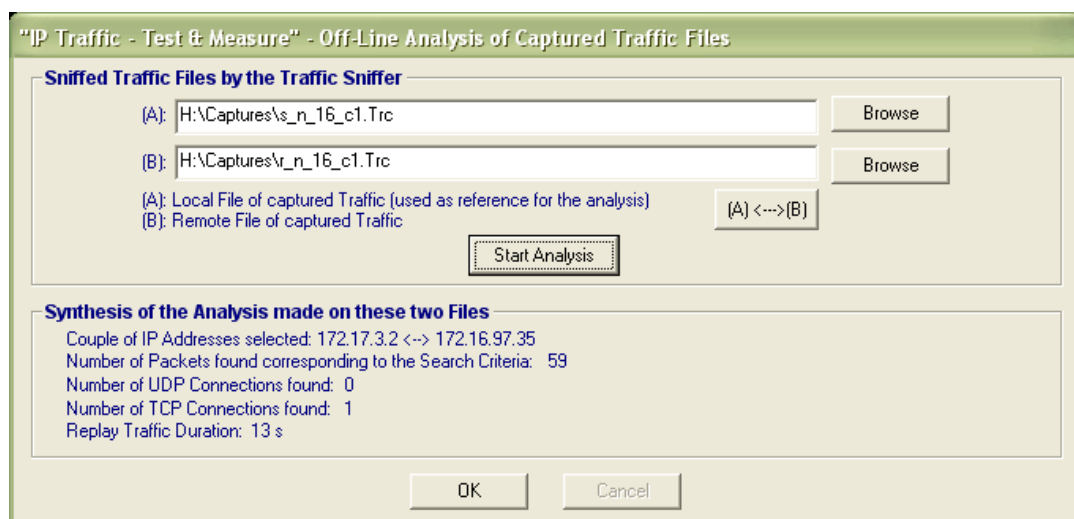
- Couple of IP addresses selected
- Number of packets found corresponding to the search criteria defined in the Step 2
- Number of UDP connections found
- Number of TDP connections found
- Replay traffic duration (useful if you want to play these sniffed traffic files via the Traffic Observer)



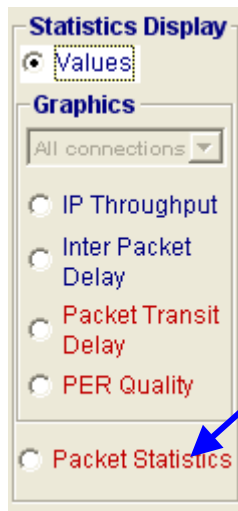
**Note:**

*In this example, 25,022 packets have been analyzed (in fact 12,511 for file (A) and 12,511 for file (B)) and 12,513 packets match the search criteria.*

You can then press OK to quit this window and come back to the previous window as shown below:



In this window, the synthesis is reminded. You can now press OK to quit the Off-line analysis.



The packet statistics can be viewed directly by using the Packet Statistics option of the Statistics display object.

With our example, we obtain the following results:

Offline Packet Statistics

Computer A ==> Computer B

IP address of A: 172.17.3.2

Save ...

Computer B ==> Computer A

IP address of B: 172.16.97.35

Time (UTC)	Sta...	Tra...	Port -> ...	IP size (pr...	Ident...
18:38:38.198	Sent	...	2690->2...	48 (TCP)	x67C3
PC 18:38:40.758	Sent	23...	2690->2...	44 (TCP)	x67C5
PC 18:38:40.760	Sent	21...	2690->2...	186 (TCP)	x67C6
PC 18:38:40.803	Sent	14...	2690->2...	576 (TCP)	x67C7
PC 18:38:40.803	Sent	14...	2690->2...	80 (TCP)	x67C8
PC 18:38:41.336	Sent	17...	2690->2...	576 (TCP)	x67D2
PC 18:38:42.555	Sent	16...	2690->2...	576 (TCP)	x67D3
PC 18:38:42.556	Sent	16...	2690->2...	576 (TCP)	x67D4
PC 18:38:42.556	Sent	15...	2690->2...	576 (TCP)	x67D5
PC 18:38:42.655	LO...	...	2690->2...	576 (TCP)	x67D6
PC 18:38:42.655	LO...	...	2690->2...	576 (TCP)	x67D7
PC 18:38:44.016	Sent	16...	2690->2...	576 (TCP)	x67D9
PC 18:38:44.016	Sent	15...	2690->2...	576 (TCP)	x67DA

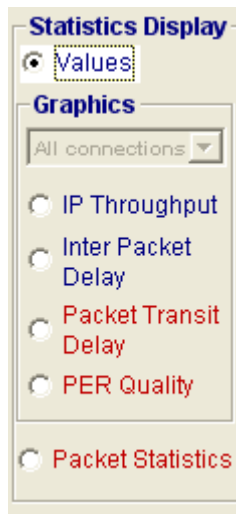
Port -> Port(Prot...	Packets	Lost	% L...	Delay	Jitter
Total Computer A	33	3	9%	1888 ...	230 ms
2690 -> 2009 (TCP)	33	3	9%	1888 ...	230 ms

Time (UTC)	Sta...	Tra...	Port -> ...	IP size (pr...	Ident...
18:38:40.141	Sent	...	2009->2...	52 (TCP)	x33F7
PC 18:38:40.578	Sent	14...	2009->2...	186 (TCP)	x33F8
PC 18:38:41.338	Sent	60...	2009->2...	576 (TCP)	x33F9
PC 18:38:41.520	Sent	51...	2009->2...	80 (TCP)	x33FA
PC 18:38:42.801	Sent	59...	2009->2...	576 (TCP)	x33FC
PC 18:38:42.880	Sent	12...	2009->2...	576 (TCP)	x33FD
PC 18:38:42.960	Sent	12...	2009->2...	576 (TCP)	x33FE
PC 18:38:44.280	Sent	7 (?)	2009->2...	56 (TCP)	x33FF
PC 18:38:44.280	Sent	39 ...	2009->2...	576 (TCP)	x3400
PC 18:38:44.380	Sent	7 (?)	2009->2...	56 (TCP)	x3401
PC 18:38:44.500	Sent	10 ...	2009->2...	56 (TCP)	x3402
PC 18:38:44.620	Sent	9 (?)	2009->2...	56 (TCP)	x3403
PC 18:38:44.720	Sent	7 (?)	2009->2...	56 (TCP)	x3404

Port -> Port(Prot...	Packets	Lost	% L...	Delay	Jitter
Total Computer B	26	0	0%	208 ms	128 ms
2009 -> 2690 (TCP)	26	0	0%	208 ms	128 ms

More information on the ‘Packet Statistics’ object is explained further in this chapter.

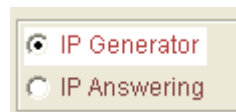
### 6.11.3 Values and statistics display



You can select six statistics displays via the "Statistics Display" object:

- Values
- 4 graphs:
  - IP Throughput
  - Inter Packet Delay
  - PER (Packet Erasure Rate) quality
  - Packet Transit Delay
- Packet Statistics

Before, you must select the 'IP Generator' or the 'IP Answering' part via:



*Note: switching between "IP Generator" and "IP Answering" can be done at any time.*

#### 6.11.3.1 Statistics display = Values

A value table is displayed as below (on-line example):

Statistical Values (based on Driver Statistics)															
	IP Address/Host Name	Port	Prot.	IP Throughput Snapshot		IP Throughput Average		UDP or TCP Throughput		Inter Packet Delay		Packet Transit Delay		Packet Erasure Rate (PER)	
				Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx
Connection #1	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #2	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #3	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #4	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #5	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #6	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #7	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #8	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #9	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #10	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #11	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #12	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #13	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #14	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #15	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A
Connection #16	NO_ADDRESS	2009	UDP	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0 ms	0 ms	N/A	N/A	N/A	N/A

For each connection (from 1 to 16), the following 6 parameters (and for each parameter, Tx = Transmit and Rx = Receive) are displayed in 3 distinct areas:

**Area 1** - IP address, Port number and protocol

**Area 2** - Four parameters (available on-line and off-line):

- ⇒ IP throughput snapshot (immediate value),
- ⇒ IP throughput average,
- ⇒ UDP or TCP throughput,
- ⇒ Inter packet delay.

**Area 3** - Two parameters (only available off-line):

- ⇒ **PER quality** (Packet Erasure Rate),
- ⇒ **Packet transit delay**.

In the Off-line mode, we have the following display, where a new object is defined: “Off-line duration information”. This object is used to indicate time of playing traffic files.

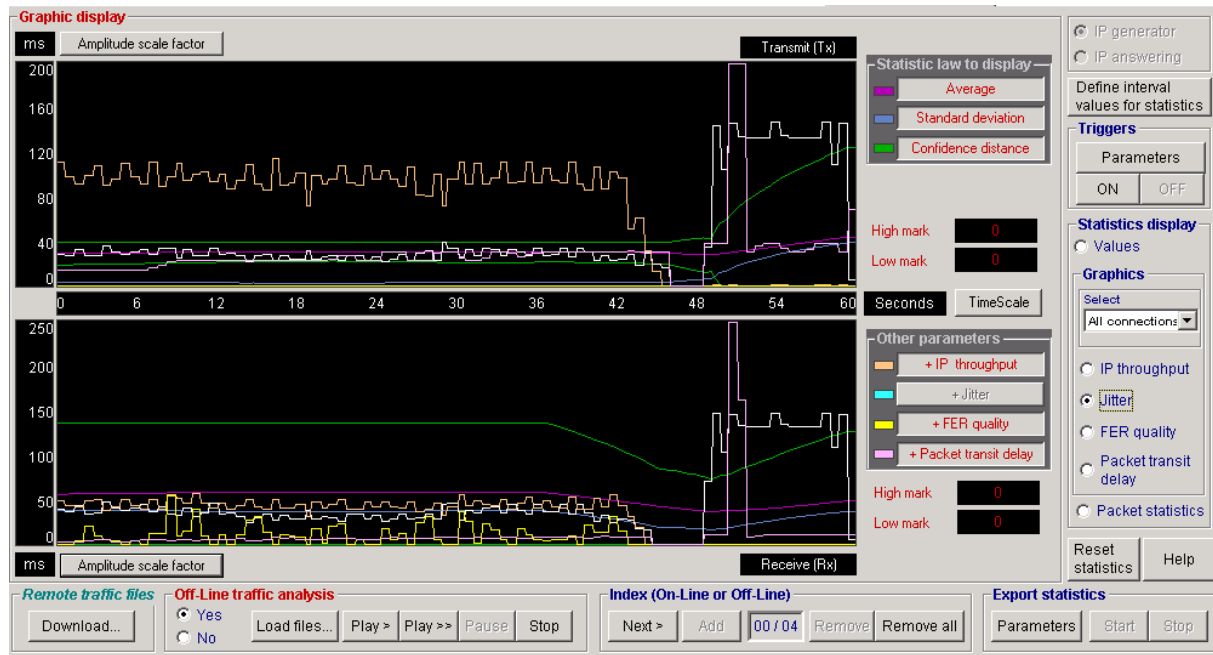
Statistical Values (based on Driver Statistics)															
	IP Address/Host Name	Port	Prot.	IP Throughput Snapshot		IP Throughput Average		UDP or TCP Throughput		Inter Packet Delay		Packet Transit Delay		Packet Erasure Rate (PER)	
				Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx
Connection #1															
Connection #2															
Connection #3															
Connection #4															
Connection #5															
Connection #6															
Connection #7															
Connection #8															
Connection #9															
Connection #10															
Connection #11															
Connection #12															
Connection #13															
Connection #14															
Connection #15															
Connection #16															
Off-Line duration information <input type="text"/>															

### 6.11.3.2 Statistics display = Graphics

"IP Traffic – Test & Measure" allows displaying four graphics for the following parameters:

- ⇒ IP throughput (immediate value): on-line and off-line,
- ⇒ Inter packet delay: on-line and off-line,
- ⇒ PER quality: only off-line,
- ⇒ Packet Transit Delay: only off-line.

When you select a graphic, the following view is displayed:



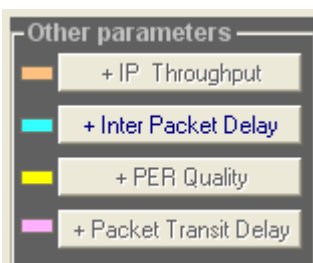
Example where all curves are displayed for all parameters

### On the right area of the graphic display: 'Statistical law to display' and 'Other parameters'



Select one or many statistic laws to display. The mechanism is based on an ON/OFF button command (the red color indicates that the curve is displayed):

- ⇒ Average (1 curve)
- ⇒ Standard deviation (1 curve)
- ⇒ Confidence distance (2 curves)



Select the other parameter(s) to display on the same graphic by pressing one or more buttons as shown on left.

These ON/OFF command buttons allow adding graphical display for the other parameters not currently displayed. Up to 3 parameters may be added to the current parameter. So, you can see on the same graphic simultaneous displays of the 4 parameters.

#### Notes:

PER (Packet Erasure Rate) quality and Packet Transit Delay are only available with the off-line mode.

Time base scale for additional parameter to display is identical to the time base scale of the current parameter.

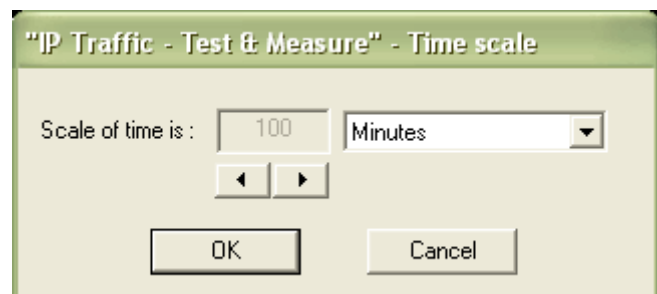
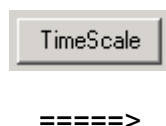
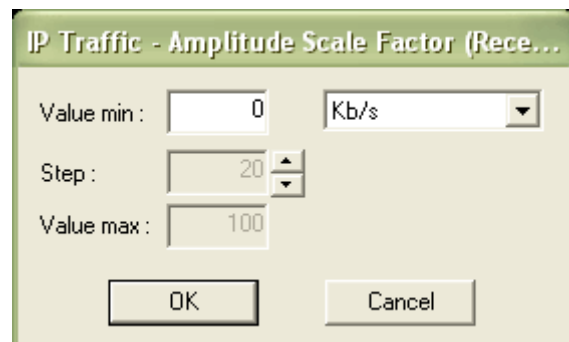
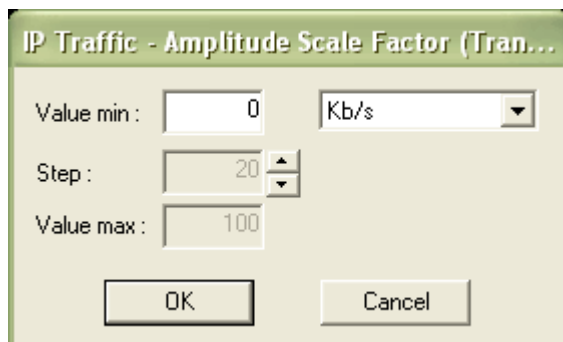
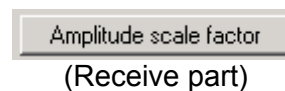
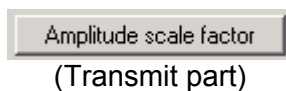
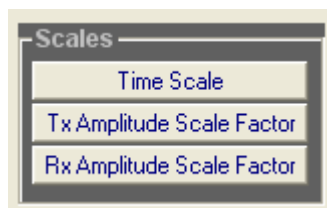


Formulas used for the statistical laws:

- Average  $m$ :  $m = \frac{\sum_{i=1}^n x_i}{n}$
- Standard deviation  $\sigma$ :  $\sigma = \sqrt{v}$  (with variance  $v$  defined as:  $v = \frac{\sum_{i=1}^n x_i^2}{n} - m^2$ )
- Confidence distance: 95.45 % of the values are between  $(m - 2\sigma)$  and  $(m + 2\sigma)$ .

In the graphic display area: amplitude and time scales

The following buttons allow entering values for the "Amplitude scale factor" and the "Time base scale" necessary to display the different curve(s).



When you change values during processing, the graphic is automatically updated with the new values.

### 6.11.3.3 *Statistics Display = Packet Statistics*

This display is only available off-line if sniffed traffic files have been already processed.

The two columns “Computer A ==> Computer B” and “Computer B ==> Computer A” display all IP packets exchanged and show if packets have been lost or received.

For each part, a synthesis is calculated and shown just under the packets list.

**Offline Packet Statistics**

Computer A ==> Computer B  
IP address of A: 192.168.0.30

Computer B ==> Computer A  
IP address of B: 192.168.0.130

Time (UTC)	Sta...	Transit...	Port -> Port	IP size (pr...	Ide...
22:00:43.428	Sent	...	2010->1055	48 (TCP)	xL
PC 22:00:43.451	Sent	0 (?)	2010->1055	40 (TCP)	xL
PC 22:00:43.490	Sent	0 (?)	2010->1055	40 (TCP)	xL
PC 22:00:43.530	Sent	0 (?)	2010->1055	40 (TCP)	xL
PC 22:00:43.570	Sent	0 (?)	2010->1055	40 (TCP)	xL
PC 22:00:43.611	Sent	0 (?)	2010->1055	40 (TCP)	xL
PC 22:00:43.651	Sent	0 (?)	2010->1055	40 (TCP)	xL
PC 22:00:43.691	Sent	0 (?)	2010->1055	40 (TCP)	xL
PC 22:00:43.731	Sent	0 (?)	2010->1055	40 (TCP)	xL
PC 22:00:43.771	Sent	0 (?)	2010->1055	40 (TCP)	xL
PC 22:00:43.810	Sent	0 (?)	2010->1055	40 (TCP)	xL
PC 22:00:43.850	Sent	0 (?)	2010->1055	40 (TCP)	xL
PC 22:00:43.890	Sent	0 (?)	2010->1055	40 (TCP)	xL

Port -> Port(Protoc...	Packets	Lost	% Lost	Delay
2010 -> 1055 (TCP)	2507	0	0%	6 ms
1066 -> 2011 (UDP)	5000	3	0%	178 ms
Total Computer A	7507	3	0%	120 ms

Time (UTC)	Sta...	Transit...	Port -> Port	IP size (pr...	Ide...
22:00:43.420	Sent	...	1055->2010	40 (TCP)	x6
PC 22:00:43.423	Sent	0 (?)	1055->2010	1500 (TCP)	x6
PC 22:00:43.442	Sent	0 (?)	1055->2010	1500 (TCP)	x6
PC 22:00:43.462	Sent	0 (?)	1055->2010	1500 (TCP)	x6
PC 22:00:43.481	Sent	0 (?)	1055->2010	1500 (TCP)	x6
PC 22:00:43.501	Sent	0 (?)	1055->2010	1500 (TCP)	x6
PC 22:00:43.521	Sent	0 (?)	1055->2010	1500 (TCP)	x6
PC 22:00:43.541	Sent	0 (?)	1055->2010	1500 (TCP)	x6
PC 22:00:43.561	Sent	0 (?)	1055->2010	1500 (TCP)	x6
PC 22:00:43.582	Sent	0 (?)	1055->2010	1500 (TCP)	x6
PC 22:00:43.602	Sent	1 (?)	1055->2010	1500 (TCP)	x6
PC 22:00:43.622	Sent	0 (?)	1055->2010	1500 (TCP)	x6
PC 22:00:43.642	Sent	0 (?)	1055->2010	1500 (TCP)	x6

Port -> Port(Protoc...	Packets	Lost	% Lost	Delay
1055 -> 2010 (TCP)	5006	3	0%	7 ms
Total Computer B	5006	3	0%	7 ms

#### *Description of the column headers for the packets list*

**Time (UTC):** in this column different symbols are used.

- the '🕒' (clock) symbol indicates that the absolute time reference is not available in one of the two traffic capture files used. In such case, “IP Traffic – Test & Measure” considers that the packet transit delay is valued to 0 for the first packet. For the following packets, the transit delay value is calculated by using the first packet as reference. Therefore, the calculated value for these packets corresponds to the time transit variation in relation to this first packet.
- the 'PC' symbol indicates that the PC clock has been used to timestamp the packet.
- the 'GPS' symbol is used when the GPS time was available to timestamp the packet.

**Status:** 2 states: **LOST**(\*) or **Sent** (meaning that the packet has been sent and received).

#### Note:

You can navigate from one **LOST** packet to another one in the (A) or (B) file by double-clicking the left button of your mouse.

**Transit in ms (accuracy):** time expressed in milliseconds for the packet transit delay and precision of the measure in brackets.

Three values can be displayed for the accuracy:

- (?) The question-mask means that the software cannot define the accuracy of the measurement because time stamping of packets in the source and the target files has not been done with an absolute time reference (use of the GPS) and a precise clock. This case is

encountered in particular when the PC clock has been used to timestamp the sent or received packets.

- **(±5)** More or less five means that the accuracy is less than or equal to **5 milliseconds**. This accuracy is obtained via the use of the GPS kit delivering an absolute time reference.
- **(±1)** More or less one means that the accuracy is less than or equal to **1 millisecond**. This accuracy is obtained via the use of the GPS kit delivering an absolute time reference and via the ZClock product delivering a very precise clock.

**Ports:** xxxx-yyyy with xxxx = source port number and yyyy= destination port number

**IP size (protocol):** **IP size** is the size of the IP packet (including the IP header) and **(protocol)** is the protocol used (TCP or UDP).

#### Description of the column headers for the synthesis

**Port → Port (Protocol):** indicates the Source Port number and the Destination Port number of the connection.

**Packets:** number of packets found for this connection.

**Lost:** number of LOST(\*) packets for this connection.

**%Lost:** percentage of LOST(\*) packets.

**Delay:** average of the transit delay calculated for all packets of the connection.

**Jitter:** average jitter calculated for all packets of the connection.

LOST(\*): see the "Process Files..." button description above for the definition of a lost packet.

All these results can be saved in a file by using the "Save..." button as shown in the following example in a text format.

This file is saved as a .txt file. Then it has been formatted using Excel (import is made with the tab as separator). Only a few lines have been selected to illustrate.

Reference time	SYN represents the synchronization point. PC indicates that the PC clock has been used to timestamp this packet.
Status	Indicates that this packet has been 'Sent' or 'LOST'.
Transit in ms (accuracy)	Packet transit delay expressed in milliseconds. (?) means that the accuracy of the measure cannot be defined.

**Computer A is: 192.168.0.30 - Computer B is: 192.168.0.130**

**Synthesis for Computer A**

Connection(Protocol)	Packets	Lost	% Lost	Delay	Jitter
Total Computer A	7507	3	0%	120 ms	1 ms
1066 -> 2011 (UDP)	5000	3	0%	178 ms	1 ms
2010 -> 1055 (TCP)	2507	0	0%	6 ms	0 ms

**Computer A ==> Computer B**

Reference time	Time (UTC)	Status	Transit in ms (accuracy)	Source Port	Destination Port	IP size	(protocol)
SYN	22:00:43.428	Sent	...	2010	1055	48	(TCP)
PC	22:00:43.451	Sent	0 (?)	2010	1055	40	(TCP)
PC	22:00:43.490	Sent	0 (?)	2010	1055	40	(TCP)
...	...	...	...	...	...	...	...
PC	22:00:46.730	Sent	184 (?)	1066	2011	1488	(UDP)
PC	22:00:46.733	Sent	0 (?)	2010	1055	40	(TCP)
PC	22:00:46.748	Sent	186 (?)	1066	2011	1488	(UDP)
PC	22:00:46.769	Sent	185 (?)	1066	2011	1488	(UDP)
PC	22:00:46.773	Sent	0 (?)	2010	1055	40	(TCP)
...	...	...	...	...	...	...	...
PC	22:02:35.847	Sent	170 (?)	1066	2011	1488	(UDP)
PC	22:02:35.867	Sent	170 (?)	1066	2011	1488	(UDP)
PC	22:02:35.888	Sent	169 (?)	1066	2011	1488	(UDP)
PC	22:02:35.908	Sent	169 (?)	1066	2011	1488	(UDP)
PC	22:02:35.929	Sent	168 (?)	1066	2011	1488	(UDP)
PC	22:02:40.433	Sent	15 (?)	2010	1055	40	(TCP)

**Synthesis for Computer B**

Connection(Protocol)	Packets	Lost	% Lost	Delay	Jitter
Total Computer B	5007	3	0%	8 ms	0 ms
1055 -> 2010 (TCP)	5007	3	0%	8 ms	0 ms

**Computer B ==> Computer A**

SYN	22:00:43.420	Sent	...	1055	2010	48	(TCP)
PC	22:00:43.420	Sent	0 (?)	1055	2010	40	(TCP)
PC	22:00:43.423	Sent	1 (?)	1055	2010	1500	(TCP)
PC	22:00:43.442	Sent	1 (?)	1055	2010	1500	(TCP)
...	...	...	...	...	...	...	...
PC	22:01:24.718	Sent	6 (?)	1055	2010	1500	(TCP)
PC	22:01:24.738	Sent	7 (?)	1055	2010	1500	(TCP)
PC	22:01:24.758	Sent	6 (?)	1055	2010	1500	(TCP)
PC	22:01:24.778	Sent	7 (?)	1055	2010	1500	(TCP)
PC	22:01:24.798	Sent	6 (?)	1055	2010	1500	(TCP)
PC	22:01:24.818	Sent	7 (?)	1055	2010	1500	(TCP)
...	...	...	...	...	...	...	...
PC	22:02:29.810	Sent	15 (?)	1055	2010	1500	(TCP)
PC	22:02:29.830	Sent	16 (?)	1055	2010	1500	(TCP)
PC	22:02:29.851	Sent	15 (?)	1055	2010	1500	(TCP)
PC	22:02:29.871	Sent	16 (?)	1055	2010	1500	(TCP)
PC	22:02:29.891	Sent	16 (?)	1055	2010	1500	(TCP)
PC	22:02:29.911	Sent	15 (?)	1055	2010	40	(TCP)
PC	22:02:40.409	Sent	16 (?)	1055	2010	40	(TCP)

Three examples are shown more precisely in the Part 9 "Examples of sniffed traffic files" at the end of this user guide.

## Part 7: Calculation Mode for the Statistics

### 7.1 Introduction

“IP Traffic – Test & Measure” allows calculating a set of statistics associated to every part of this tool:

- IP Generator
- IP Answering
- Traffic Sniffer
- Traffic Observer

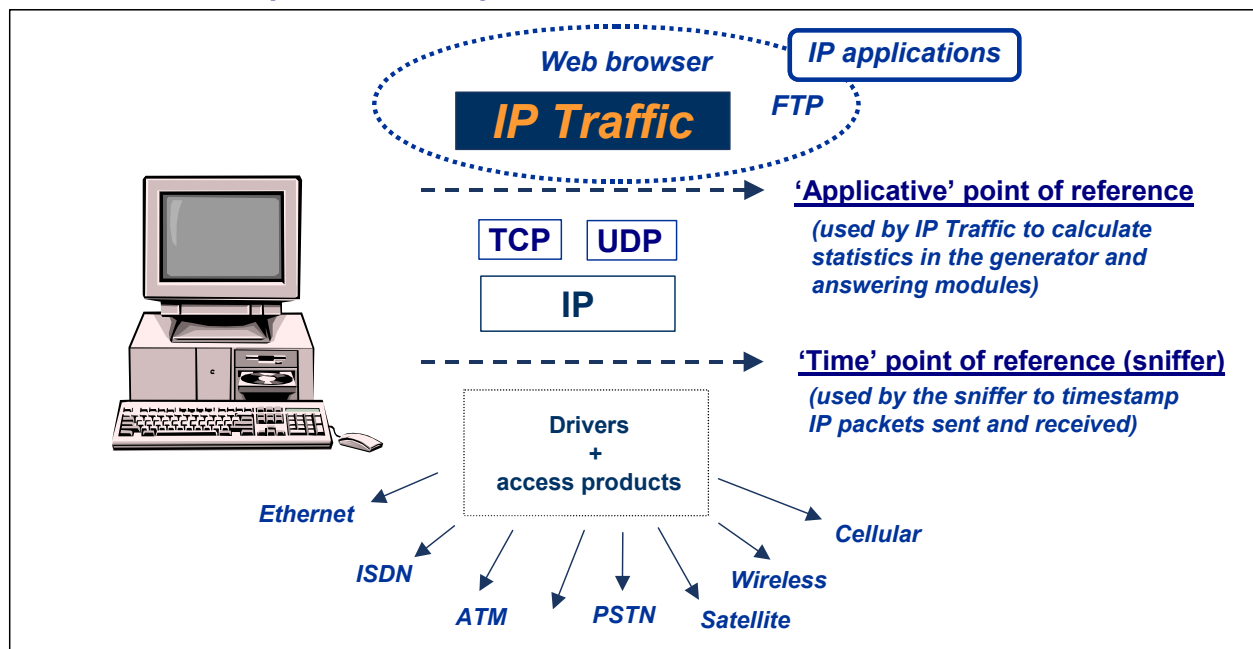
The statistics can be calculated on-line (real time mode) or off-line (differed time).

The off-line mode requires to have analyzed two sniffed traffic files (the local traffic file and the remote traffic file sent back on the local machine) and allows to calculate parameters such as the PER quality (Packet Erasure Rate) and the packet transit delay.

A sniffed traffic file is captured by the “Traffic Sniffer” module (with filters customizable by the user) which stores on hard disk and timestamps all the IP frames sent and received.

## 7.2 Statistics computed by “IP Traffic – Test & Measure”

### 7.2.1 Reference points to compute the statistics



Two points of reference are used by the “IP Traffic – Test & Measure” software.

- **‘Applicative’ point of reference**

In the ‘IP Generator’ and the ‘IP Answering’ modules, statistics (e.g. throughput, RTT,...) are calculated at the application level (above the TCP/IP stack). These statistics refer to data sent or received by the “IP Traffic – Test & Measure” application, and are independent of the protocol (TCP or UDP).

*Illustration:* the ‘Tx Throughput’ parameter displayed in the « IP Generator – Traffic + Statistics » tab for each active IP connection, is computed by using the following formula: data volume sent on the IP connection during the last seconds (defined by the ‘Throughput sampling period’ – this parameter is defined in the following paragraph and represents the sampling period of the throughput. The transmitted volume of data corresponds to the sum of the packet size sent at the WinSock2 interface (i.e. the ‘Applicative’ point of reference).

- **‘Time’ point of reference**

The Traffic Sniffer uses this point of reference in order to timestamp IP packets sent and received. Timestamp of packets is made at the nearest of the physical link (under the TCP/IP stack). Therefore, “IP Traffic – Test & Measure” can identify lost and retransmitted IP packets. Values and statistics of the ‘Traffic Observer’ tab use this point of reference.

*Illustration:* the ‘IP Throughput snapshot’ parameter presented in this tab and valued for each active IP connection, is calculated according to the following formula: volume of data sent on the connection during the last second. The volume of data sent corresponds to the sum of IP datagram with regard to the driver access except the IP header. At this level, one sees really the totality of the transmitted data whatever the protocol used (for example, TCP packets retransmission participate in the volume of data transmitted).

## 7.2.2 Statistics description

This paragraph lists all statistics calculated by “IP Traffic – Test & Measure” for the different parts. On-line statistics are blue colored and statistics only available off-line are red colored.

### 7.2.2.1 “IP Generator – Traffic + Statistics” tab

- Tx Throughput
- Rx Throughput
- Tx Packets Throughput
- Rx Packets Throughput
- Tx Packets
- Rx Packets
- Tx Volume
- Rx Volume
- Jitter
- Volume to send
- Remaining volume
- Seq. numb errors (sequence numbering errors)
- RTT (Round Trip Time)

### 7.2.2.2 “IP Answering – Parameters + Statistics” tab

- Tx Throughput
- Rx Throughput
- Tx Packets Throughput
- Rx Packets Throughput
- Tx Packets
- Rx Packets
- Tx Volume
- Rx Volume
- Jitter
- Volume to send
- Remaining volume
- Seq. numb errors (sequence numbering errors)
- Data not echoed

### 7.2.2.3 The 'Traffic Observer' tab

With the **on-line** mode, the following parameters are displayed by the 'Statistics display' object:

- ⇒ Table of values (if 'Statistics display' = values):
  - IP throughput snapshot
  - IP throughput average
  - UDP or TCP throughput
  - Inter packet delay
- ⇒ Graph: **IP Throughput** with the statistical laws **average**, **standard deviation** and **confidence distance**
- ⇒ Graph: **Inter packet delay** with the statistical laws **average**, **standard deviation** and **confidence distance**

With the **off-line** mode, the following parameters are displayed by the 'Statistics display' object:

- ⇒ Table of values (if 'Statistics display' = values):
  - IP throughput snapshot
  - IP throughput average
  - UDP or TCP throughput
  - Inter packet delay
  - **Packet Erasure Rate (PER)**
  - **Packet Transit Delay**
- ⇒ Graph: **IP Throughput** with the statistical laws **average**, **standard deviation** and **confidence distance**
- ⇒ Graph: **Inter packet delay** with the statistical laws **average**, **standard deviation** and **confidence distance**
- ⇒ Graph: **PER quality** with the statistical laws **average**, **standard deviation** and **confidence distance**
- ⇒ Graph: **Packet transit delay** with the statistical laws **average**, **standard deviation** and **confidence distance**
  - ⇒ Tables of packets sent and received (if 'Statistics display' = **Packet statistics** and sniffed traffic files have been previously processed)



### 7.3 General parameters used to calculate the statistics

The 'General parameters' item of the 'Configuration' menu contains parameters used for display and to calculate the statistics.

**"IP Traffic - Test & Measure" - General Parameters**

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

Refresh time (1 to 60 seconds)

Throughput sampling period (1 to 60 seconds)

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

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

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

**IP Traffic Buffer Size (SO\_RCVBUF and SO\_SNDBUF)**  
 The buffers used by "IP Traffic" 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 500,000 bytes)

Transmit buffer size (1,024 to 500,000 bytes)

**Acquisition period of statistics**  
 This parameter is used to define the polling driver time in order to get statistics by the "IP Traffic" application. This parameter defines the period to compute statistical average presented in the 'Traffic Observer' tab.

Acquisition period of statistics (10 to 60,000 ms)

**Refresh time:** this parameter defines the frequency to update the man machine interface. The different statistical values are updated all the xx seconds (for all tabs) where xx is the value defined by the user.

This parameter is also used to update the display of the following items:

- the 'GPS' state (if selected)
- the 'ZClock' state (if selected)
- the 'Activity' counter
- 'File size' and "Time before disk limit" for the 'Traffic Sniffer' activity

**Throughput sampling period:** this parameter specifies the last traffic seconds to use in order to calculate the throughput. More this value is high and more the average is smoothed. This parameter is also used to calculate the **IP throughput average** parameter of the 'Traffic Observer'.

**Acquisition period for statistics:** this parameter is used by the "Traffic Sniffer" module to define the frequency of data acquisition (i.e. the IP packets) at the driver level (under the TCP/IP stack). This parameter is also used to generate traffic when "IP Traffic – Test & Measure" is in replay mode.

The more the value is weak (without being lower than 10 ms) and the more one obtains samples for the calculation of the statistics. In return more and more records are saved in the statistics export file (if this option is selected) and the CPU load is increased by the number of statistical calculations to be realized.

#### Notes

*Every second, the following processes are realized:*

- + *Calculation of the CPU load ('Activity' counter),*
- + *Calculation of the statistics for activity ('IP Generator Activity' and 'IP Answering Activity' displayed at the bottom of the "IP Traffic – Test & Measure" main window).*

*Every 5 seconds, update of 'Activity Sniffer' is made (see 'Traffic Sniffer' - Traffic overview during capture).*

*These values of 1 and 5 seconds are not customizable and are fixed in the current version of the software.*

## 7.4 Detailed description for calculation of the statistics

### 7.4.1 The 'IP Generator – Traffic + Statistics' tab

The statistics in this tab are calculated at the 'Applicative' point of reference.

**Tx Throughput** = volume of data sent on the connection during the last seconds considered for calculation (see above description of the '*Throughput sampling period*' parameter).

**Rx Throughput** = volume of data received on the connection during the last seconds considered for calculation (see above description of the '*Throughput sampling period*' parameter).

**Tx Packets Throughput** = number of data packets sent on the connection during the last seconds considered for calculation (see above description of the '*Throughput sampling period*' parameter). This statistic is only available with the UDP connections.

**Rx Packets Throughput** = number of data packets received on the connection during the last seconds considered for calculation (see above description of the '*Throughput sampling period*' parameter). This statistic is only available with the UDP connections.

**Tx Packets** = It is the number of data packets sent on the connection. This statistic is only available with the UDP connections, because the TCP stack for the TCP connections cuts data to send in one or more TCP packets.

**Rx Packets** = It is the number of data packets received on the connection. This statistic is only available with the UDP connections, because the TCP stack for the TCP connections cuts data to send in one or more TCP packets.

**Tx Volume** = it's the number of data bytes sent on the connection.

**Rx Volume** = it's the number of data bytes received on the connection.

**Jitter** = Jitter is the mean variation of delays on packets received. This value is only available when the Timecode option is selected. This value corresponds to either the mean one-way variation (remote 'IP Answering' = Absorber Generator mode) or the mean two-ways variation (remote 'IP Answering' = Echoer mode).

**Volume to send** = Size of data (in bytes) to send on the connection. This information is displayed only if the 'IP Generator' can give this value, as by example for a file or for a mathematical law.

**Remaining volume** = size of data (in bytes) remaining to send on the connection. This information is available only if the '**Volume to send**' parameter has been calculated.

**Seq. numb errors (sequence numbering errors)** = it's the number of packets whose sequence number is not correct. This value is present only if the packets include the Timecode information. For each received packet, the process to find the Timecode information is applied. If the RTT identifier is found, "IP Traffic – Test & Measure" tests if the sequence number for the received packet follows the sequence number of the previous received packet. If an error is detected, the 'Sequence numbering errors' parameter is incremented. To calculate this parameter, the remote 'IP Answering' module must be configured in 'echoer' mode (each packet received is transmitted to the originator).

**RTT (Round Trip Time)** = average of the differences between the sending times and the receiving times (the multimedia timers of the OS are used, giving an accuracy of 1 ms – Microsoft information).

To calculate this parameter, the remote must be configured in echoer mode for the connection.

#### *Remark*

*The "IP Generator" builds data packets according to parameters defined by the user (contents, size and inter packet delay). The data packets are then provided to the Winsock 2 interface to be sent by the TCP/IP stack with the selected protocol (TCP or UDP). The volume of data sent or received does not include the encapsulated data added by the TCP/IP stack.*

## RTT information

The information necessary to calculate the RTT parameter is included in each data packet, at the beginning of the data.

Format of the RTT header (in little endian notation) is structured as follows:

- 4 bytes      magic number (always 0x54 0x87 0x54 0x41)
- 4 bytes      sequence number
- 16 bytes     time when sent
- 2 bytes      length (without the RTT header)

### 7.4.2 The 'IP Answering – Parameters + Statistics' tab

The statistics in this tab are calculated at the 'Applicative' point of reference.

**Tx Throughput** = see previous description above.

**Rx Throughput** = see previous description above.

**Tx Packets Throughput** = see previous description above.

**Rx Packets Throughput** = see previous description above.

**Tx Packets** = see previous description above.

**Rx Packets** = see previous description above.

**Tx Volume** = see previous description above.

**Rx Volume** = see previous description above.

**Jitter** = Jitter is the mean variation of delays on packets received. This value is only available when the Timecode option is selected (on the remote 'IP Generator'). This value corresponds to the mean one-way variation only.

**Volume to send** = see previous description above.

**Remaining volume** = see previous description above.

**Seq. numb errors (sequence numbering errors)** = see previous description above.

**Data not echoed** = this information is available only if the working mode of the connection is defined as 'Echoer' or 'Echoer file' and indicates that the "IP Answering" module has not been able to re-send data due to the TCP/IP stack performances.

For an UDP connection, it's the number of packets not re-sent.

For a TCP connection, it's the number of bytes not re-sent.

### 7.4.3 The 'Traffic Observer' tab

The statistics in this tab are calculated at the driver level (under the TCP/IP stack).

The parameters described in this paragraph are calculated for each active connection. As a connection can send and receive simultaneously data, the two values Tx (Transmit) and Rx (Receive) are calculated for each parameter.

Calculation is made simultaneously for the 32 connections (16 for the 'IP Generator' module and 16 for the 'IP Answering' module).

Definition of terms used in this paragraph:

- the term 'IP data' does not include the IP header.
- the term 'protocol data' does not include the IP header and the specific header of the protocol. In this way for a TCP connection, the ACKnowledge packet does not contain data.
- Most values displayed in the 'Traffic Observer' tab are 'snapshot' values.

#### 7.4.3.1 Calculation of instantaneous values

The coherence between the numerical values "Statistical values" and their graphical display is respected by using the following rules:

- The scale unit defined by the 'Time scale' parameter for the graph allows calculating the number of milliseconds of traffic for 1 pixel.
- For each data acquisition (see description of the 'Acquisition period for statistics' parameter in general parameters used for statistics), "IP Traffic – Test & Measure" updates the statistics with the following manner:

⇒ **Example 1:** a pixel is valued to 30 ms and 'Acquisition period for statistics' is valued to 100 (ms).

- First data acquisition: data associated to the pixels number 1, 2 and 3 correspond to 90% of the acquisition. The rest of 10% is used with the next acquisition.
- Second data acquisition: the previous rest (10%) added to the 20% of the new acquisition are associated to the pixel number 4, then 30 % for pixel #5 and 30% for pixel #6. The rest of 20% will be used with the next acquisition.

⇒ **Example 2:** a pixel is valued to 200 ms and 'Acquisition period for statistics' is valued to 80 (ms).

- First data acquisition: there is not enough data to associate to one pixel. Data is put aside (the rest for the next acquisition is 80 ms).
- Second data acquisition: the rest and the new data are not sufficient to correspond to 1 pixel. The new rest is then 160 ms.
- Third data acquisition: the rest and new data can be associated to pixel #1 (this pixel represents the two first acquisitions and 50% of the third). Then the rest is 50% that will be used with the next acquisition.

The 'snapshot' value is the last calculated value allocated to a pixel.

#### 7.4.3.2 Triggers update

Each time a value is allocated to a pixel, the comparison is made with the trigger values. Then the min or max trigger value is updated if the value exceeds the threshold.

### 7.4.3.3 Calculation of parameters displayed in the "Statistical values" table

**IP throughput snapshot** = instantaneous throughput calculated by using the IP data volume received on the connection.

**IP throughput average** = average of the IP throughput by using the IP data volume received on the connection during the last seconds used for calculation (see the 'Throughput sampling period' parameter)

**UDP or TCP throughput** = instantaneous throughput calculated by using the protocol data volume received on the connection.

**Inter packet delay** = instantaneous average distance from time between two successive received IP packets, calculated by dividing the sum of the distances by the number of received packets.

**Packet Erasure Rate (PER)** = instantaneous rate of loss packets, expressed in percentage of the number of packets not received with regard to the number of packets sent.

**Packet transit delay** = instantaneous delay for the transfer of packets. It's the average of the transfer delays for all packets exchanged between two "IP Traffic – Test & Measure" machines. The transfer delay (named 'transit delay') for a packet is the difference of time between the time when the packet has been sent and the time when the packet has been received.

Both times – sent and received time - are stored in the record of the capture file made by the 'Traffic Sniffer'.

### 7.4.3.4 Statistical laws for the graphs

"IP Traffic – Test & Measure" allows displaying four graphs for the following parameters:

**IP Throughput** = corresponds to the '**IP throughput snapshot**' parameter (see above)

**Inter packet delay** = corresponds to the '**Inter packet delay**' parameter (see above)

**PER quality** = corresponds to the '**Packet Erasure Rate (PER)**' parameter (see above)

**Packet transit delay** = corresponds to the '**Packet transit delay**' parameter (see above)

For these parameters, three statistical laws are calculated and can be displayed:

- **Average**
- **Standard deviation**
- **Confidence distance**

Formulas used to calculate these variables:

- **Average**  $m$ :  $m = \frac{\sum_{i=1}^n x_i}{n}$
- **Standard deviation**  $\sigma$ :  $\sigma = \sqrt{v}$  (with variance  $v$  defined as:  $v = \frac{\sum_{i=1}^n x_i^2}{n} - m^2$ )
- **Confidence distance** : 95.45 % of the values are between  $(m - 2\sigma)$  and  $(m + 2\sigma)$ .

#### Notes:

-  $n$  is the minimum between the number of calculated pixels and the number of displayed pixels.

- the confidence distance is calculated only at the time of display.

## Part 8: Annexes

### 8.1 Description of the Mathematical Laws used by “IP Traffic – Test & Measure”

“IP Traffic – Test & Measure” is based on the use of random number generation laws to determine the starting time connection and data volume to send, and for the inter packet delay in the ‘IP Generator’ module. Four mathematical laws are offered. **Uniform**, **Exponential** and **Gauss** laws are used for starting time connection and data volume. **Pareto**’s law is only used for data volume. The mathematical laws are used:

⇒ For the unitary mode when the mathematical law data source is selected. In this case, only data volume laws are available.

⇒ For the automatic mode: starting time connection generation and data volumes laws are required parameters.

Hereafter is a detailed description of each mathematical law.

#### 8.1.1 Uniform Law

##### ❖ Presentation:

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

With the Uniform law, the units used are millisecond for the starting time connection generation laws and byte for the data volume to send laws.

##### ❖ Mathematical function:

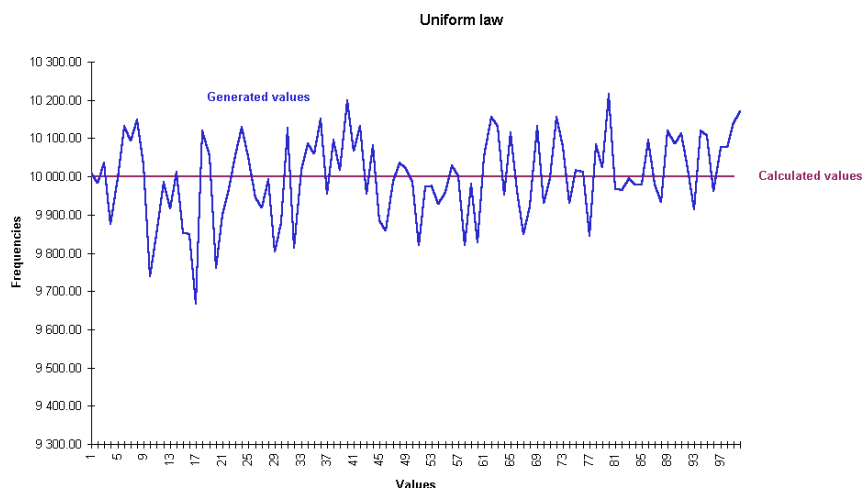
Uniform law on  $(\alpha, \beta)$  range

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

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

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

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



## 8.1.2 Exponential Law

### ❖ Presentation

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

The unit is the millisecond for the starting time connections generation laws and byte for the data volume laws.

### ❖ Mathematical function:

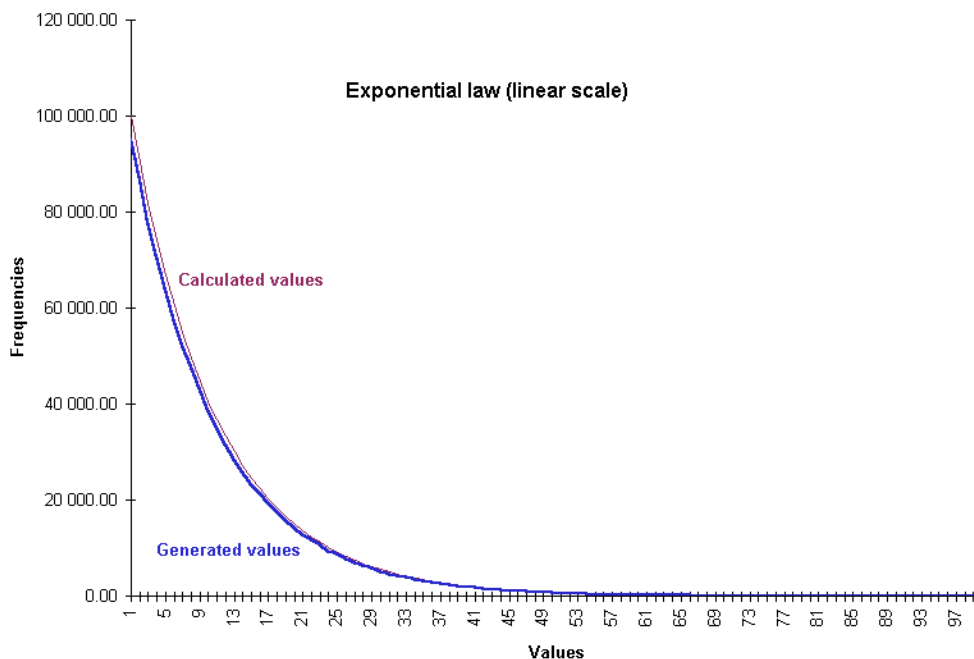
Exponential law ( $\lambda > 0$ )

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

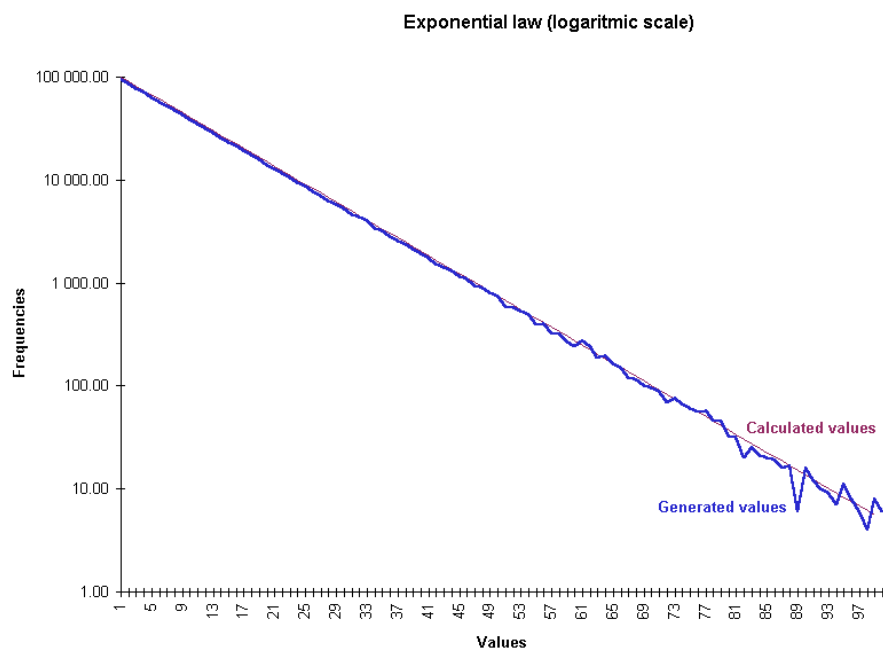
$$f(x) = 0 \quad \text{if } x < 0$$

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

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







❖ *Exponential law- Table of generated values:*

Values	Starting time laws results	Data volume laws results
$\lambda = 1$	10 ms	10 bytes
$\lambda = 0,1$	100 ms	100 bytes
$\lambda = 0,01$	1s	1 Kbytes
$\lambda = 0,001$	10s	10 Kbytes
$\lambda = 0,0001$	1mn43	100 Kbytes
$\lambda = 0,00001$	17mn19	1 Mbytes
$\lambda = 0,000001$	2h53	10 Mbytes
Precision limit for $\lambda$		

### 8.1.3 Law of Pareto

#### ❖ Presentation:

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

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

The following values have been noticed:

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

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

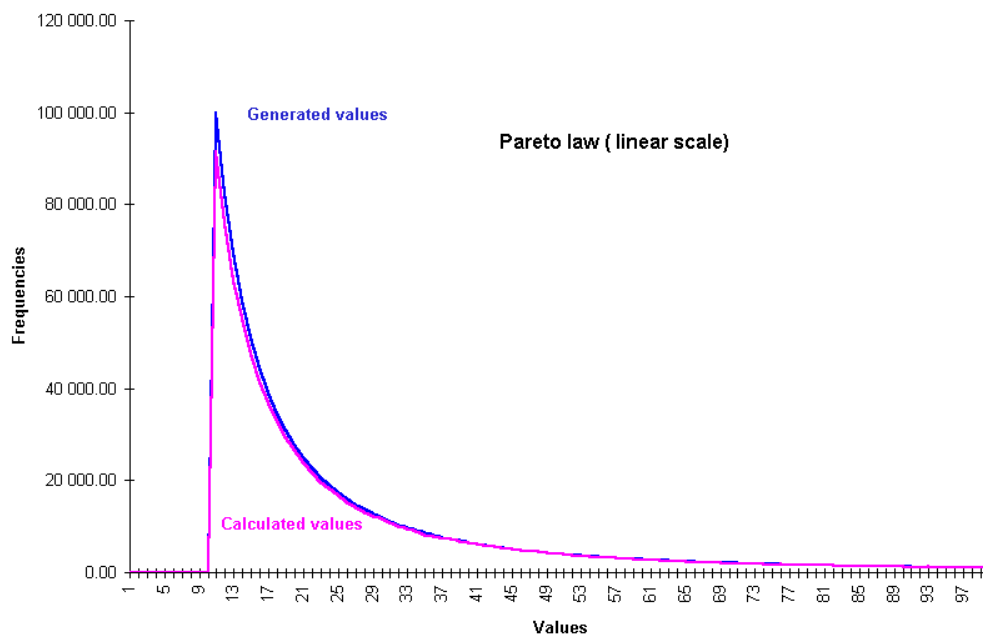
#### ❖ Mathematical function:

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 $\beta = 1$ .



### 8.1.4 Gauss law

#### ❖ Presentation:

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

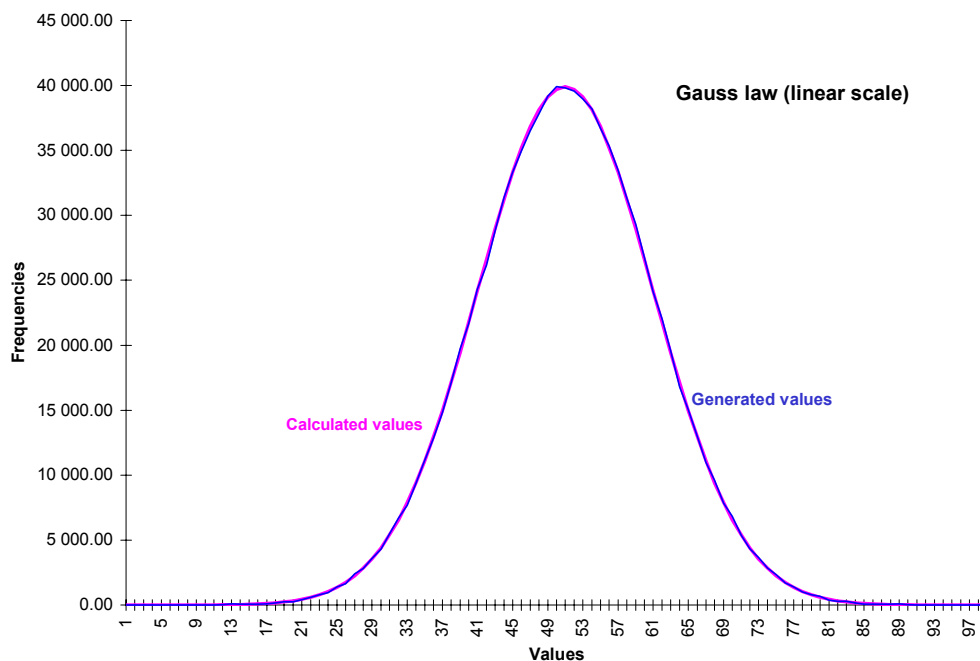
With this law, the unit used is the millisecond for the starting time connection generation laws and byte for the data volume to send laws.

#### ❖ Mathematical function:

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

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

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



## 8.2 “IP Traffic – Test & Measure” Traces

In case of problem when using “IP Traffic – Test & Measure”, the trace functionality allows to retrieve in a file or in a debug window, information regarding Winsock exchanges made by “IP Traffic – Test & Measure”.

Traces activation is done by modifying directly in the registry database of Windows, the value of DebugLevel in the key `\\HKEY_LOCAL_MACHINE\\SOFTWARE\\IPTraffic`.

*TraceFile* parameter defines the name for the file receiving traces (by default DEBUG.LOG).

The user shall reset the content of this file manually to avoid disk space wasting. If the *TraceFile* parameter is not selected (empty chain), traces are sent to the debug standard output -via OutputDebugString- in external tools trace (e.g. ‘Softlce’ from Compuware, the Microsoft Development environment).

“IP Traffic – Test & Measure” must be restarted after  
“DebugLevel” or “TraceFile” parameter modification.

## 8.3 Configuration parameters saved in the Registry database

The based key to access these parameters is `\\HKEY_LOCAL_MACHINE\\Software\\IPTraffic`.

Key name	Type	Default value (dec)	Description
<b>DEBUGLEVEL</b>	REG_DWORD	0	0x00000000 No trace. 0x00000001 Add errors in the trace. 0x00000002 Important information for the ZTI support. 0x00000010 Add verbose information used by the ZTI support. 0x00000080 Save debug information into a file specified by the DEBUGFILENAME key. 0x00000100 Add the current time to each trace message. 0x00000400 Add intermediate value computed during the statistics process providing information to the Observer Tab. 0x00001000 Detail the operation of the Sniffer Analyzer when splitting a captured file into data files replay. 0x00002000 Detail operations of the IP Answering (Receiver verbose mode). 0x00004000 Provide information via the GPS. 0x00008000 Detail operations of the Sender (Sender verbose mode). 0x00010000 Detail operations when the Replay mode is used (Replay verbose mode). 0x00020000 Detail operations for the Off-line mode. 0x00040000 Provide information for the Remote control mode. 0x00080000 Specific flag for statistics generated at the 'IP Generator' and 'IP Answering' levels. 0x00100000 IP Traffic-API specific traces which details exchanges between the external application and IP Traffic
<b>DEBUGFILENAME</b>	REG_SZ	DEBUG.LOG	Filename to save the traces.
<b>DEPTHFORPACKETANALYSIS</b>	REG_DWORD	500	Parameter used in the search algorithm of the 'Traffic Observer' to calculate the packets statistics. <b>Use a higher value if needed.</b>
<b>UDPINACTIVITY</b>	REG_DWORD	10	For UDP connections, timer (expressed in seconds) used in the Absorber/Generator mode to identify a connection has stopped (10 seconds by default). In such a case, the generator stops too.
<b>TCPINACTIVITY</b>	REG_DWORD	10	For TCP connections, timer (expressed in seconds) to detect the 'IP Generator' has stopped the connection (10 seconds by default). The TCP connection is closed by "IP Traffic".

Key name	Type	Default value (dec)	Description
<b>SENDTIMEOUT</b>	REG_DWORD	500	Maximal period (expressed in milliseconds) allocated to send/receive data (default is 500 milliseconds). <i>Use a higher value for IP network with low throughput or with high latency (for example: 10000)</i>
<b>TCPCONNECTRETRYCOUNTER</b>	REG_DWORD	0x1	Number of retry to establish a TCP connection
<b>TCPNODELAY</b>	REG_DWORD	0x0	0x0 : Nagle algorithm enabled Other value: Nagle algorithm disabled
<b>TCPRECEIVERPACKETSIZE</b>	REG_DWORD	8192	Buffer size (expressed in bytes) used by "IP Traffic" to get TCP data from the Winsock2 interface. It is not the MTU. If the size is big then the performances are better because Winsock 2 is called less often. Max value = 65,535
<b>FILETRANSFERINACTIVITY</b>	REG_DWORD	5	When the file downloading is active, this timer (expressed in seconds) is used to detect the sender has stopped the connection (5 seconds by default). The file transfer connection is closed by "IP Traffic" when the timer is reached.
<b>FILETRANSFERPACKETSIZE</b>	REG_DWORD	1460	Maximum size of a packet used during a file transfer. (Expressed in bytes. Default value = 1460. Max value = 65,535).

***Warning: "IP Traffic – Test & Measure" must be restarted after each modification of these parameters.***

**The following registry values list is given for information ONLY.**

Key name	Type	Default value (dec)	Description
<b>ACROREADINFO</b>	REG_SZ	20050412	Date (YYYYMMDD) of the "IP Traffic" help file in PDF format
<b>ACROREADTIMER</b>	REG_DWORD	30	When a command is sent to Acrobat, it should answer within this timeout value, otherwise an error message will be generated (Expressed in second)
<b>HELP-GENERAL</b>	REG_DWORD	8	Page number where general help is located
<b>HELP-OBSERVER</b>	REG_DWORD	119	Page number where the 'Traffic Observer' tab help is located
<b>HELP-AUTOMATICMODE</b>	REG_DWORD	82	Page number where 'Generator Automatic' help is located
<b>HELP-UNITARYMODE</b>	REG_DWORD	72	Page number where 'Generator Unitary' help is located
<b>HELP-SNIFFER</b>	REG_DWORD	114	Page number where 'Traffic Sniffer' tab help is located
<b>HELP-GPS</b>	REG_DWORD	53	Page number where GPS configuration help is located
<b>HELP-REPLAYMODE</b>	REG_DWORD	86	Page number where Replay operation help is located
<b>HELP-REPLAYMODE-RCV</b>	REG_DWORD	106	Page number where Replay operation for the 'IP Answering' tab help is located
<b>HELP-FILEMANAGER</b>	REG_DWORD	52	Page number where File Operating modes help is located
<b>HELP-EXPORTSTATS-SENDER</b>	REG_DWORD	90	Page number where Export IP Generator statistics help is located
<b>HELP-EXPORTSTATS-RECEIVER</b>	REG_DWORD	109	Page number where Export IP Answering statistics help is located
<b>HELP-PARAMCNX-SENDER</b>	REG_DWORD	68	Page number where IP Generator network interface help is located
<b>HELP-FILEDOWNLOADING</b>	REG_DWORD	58	Page number where File Downloading help is located
<b>HELP-PARAMCNX-RECEIVER</b>	REG_DWORD	100	Page number where IP Answering network interface help is located
<b>AUTOMATION PATH</b>	REG_SZ		Full path name to Aut_IPTraff .exe ("Automation Tool for IP Traffic" binary file.
<b>IPTRAFFICPATH</b>	REG_SZ		Full path name to the "IP Traffic - Test & Measure" binary file.
<b>CURRENTVERSION</b>	REG_SZ	V 2.3.0	Current version installed.
<b>INSTALLATIONPATH</b>	REG_SZ		Selected installation path ('[Your Windows Drive]\Program Files\IP Traffic' by default.

## 8.4 Default Value of a Context

The default values when opening a new context are:

### ♦ IP Generator parameters

<b>IP address</b>	NO_ADDRESS		
<b>Port Number</b>	2009		
<b>Protocol</b>	TCP		
<b>Testing mode</b>	Unitary mode	<b>Data source</b>	Packet generator (number of packets: infinite, packet contents: fix = 5A)
		<b>Packets size</b>	Fix = 1460 bytes
		<b>Inter Packet Delay</b>	Fix = 20 ms
		<b>RTT option</b>	No

### ♦ IP Answering parameters

<b>IP address</b>	ANY_ADDRESS
<b>Port number</b>	2009
<b>Protocol</b>	TCP
<b>Receiving working mode</b>	Absorber

### ♦ Configuration

#### TCP stack parameters

TCP Buffer size		
	<b>S0_RCVBUF</b>	8192
	<b>S0_SNDBUF</b>	8192
TCP Windows size		
	<b>TCPWindowSize</b>	Windows configuration dependant
	<b>SACKS Options</b>	Windows configuration dependant

#### Display parameters

<b>Refresh time</b>	2 s
<b>Throughput sampling period</b>	5 s

#### Connection parameters

<b>Timeout for TCP packets echoed</b>	500 ms
<b>Timeout for UDP packets echoed</b>	700 ms
<b>Acquisition period for statistics</b>	1000 ms

#### File Operating Modes parameter

<b>File Operating Mode</b>	Overwrite
----------------------------	-----------

◆ **File transfer**

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

◆ **Remote port**

<b>Port number</b>	2600
--------------------	------

◆ **GPS parameter**

<b>Port number</b>	COM1
<b>Speed</b>	9600
<b>Data</b>	8 bytes
<b>Stop</b>	1 bit
<b>Parity</b>	Odd

◆ **Traffic Observer**

<b>Mode</b>	Generator
<b>Statistics display</b>	Values

◆ **Graphical units**

UNIT	Value	Trigger
<b>IP throughput</b>	0-100 Kb/s	10-90 Kb/s
<b>Inter packet delay</b>	0-50 ms	10-90 ms
<b>PER quality</b>	0-100	10-90
<b>Packet transit delay</b>	0-1000 ms	100-900 ms

◆ **Driver polling interval**

<b>Period</b>	1000 ms
---------------	---------

◆ **Sniffer**

<b>Auto refresh period</b>	5 s
----------------------------	-----

## 8.5 External File for the ‘IP Generator’ module

The IP Generator module can use an external file defined by the user. Information of this file is used to send data packets on an IP connection. This file is independent of the specified protocol (UDP or TCP).

The file is composed of two sections: [HEADER] and [DATA].

Section [HEADER] : Code, Parameters

Section [DATA] : data size, delay (in milliseconds) before sending of next packet

*Example of external data file [generation of random characters comprised between 32(decimal value) and 48 (decimal value)]*

```

;
;   Sample DataFile for «IP Traffic» generator
;
;   Section [HEADER] defines the content
;       1, char           = fix character
;       2, cmin, cmax      = random character
;       3, c1, c2          = alternate character
;       4, FileName        = Content is based on a file
;
[HEADER]
    2, 32, 48

[DATA]
    100, 20
    200, 10
    300, 30
    400, 40
    500, 5
    600, 50
    700, 60
    800, 70
    10, 80
    20, 10
    30, 20
    40, 30
    50, 50
    60, 60
    70, 100
    80, 200
    
```

*Section [HEADER] : Code, Parameters*

Code	Meaning	Parameters	Example
1	Fix character	Char to use	1, 'Z'
2	Random character	Char 1 (min), Char 2 (max)	2, 32,48
3	Alternate character	Char 1, Char 2	3, x32,x48
4	File	Filename	4, C:\Temp\test.bin

Coding of characters:

- character between quotes, e.g. 'Z'
- decimal value, e.g. 32
- hexadecimal value, e.g. X32

## 8.6 External DLL for the ‘IP Generator’ module

This external DLL is loaded by the 'IP Generator' module. This DLL must offer three entry points described in the following paragraphs:



- **TrafficInit**
- **PacketDelay**
- **PacketData**

An example of external DLL is available. See the directory IPTraffic\SAMPLES\User-DLL with all files to compile and generate the DLL (DllSample.dll).

### 8.6.1 TrafficInit

**BOOL CALLBACK TrafficInit( int CnxID, unsigned long IPAddr, unsigned char protocol, unsigned port)**

To init a new connection identified by par CnxID.

Parameters:

<b>CnxID</b>	Connection identifier
<b>IPAddr</b>	Remote IP address
<b>Protocol</b>	Protocol to use (UDP or TCP)
<b>Port</b>	Port number

Return codes:

<b>True</b>	The DLL is ready to provide data to the IP Generator.
<b>False</b>	The DLL can't provide data. The complementary error code is handled by the DLL and the DLL must warn the user directly.

Remark:

When a connection must use an external DLL, the IP Generator module verifies that the DLL is present (via LoadLibrary). Then it looks for the 3 required entry points. **TrafficInit()** is called when a connection is established with the remote.

### 8.6.2 PacketDelay

**BOOL CALLBACK PacketDelay( int CnxID, unsigned long \*pulDelay)**

Parameters:

<b>CnxID</b>	Connection identifier
<b>pulDelay</b>	Address for delay expressed in milliseconds

Return codes:

<b>True</b>	The DLL has provided the delay for the next packet. If this delay equals 0, the IP Generator calls immediately <b>PacketData()</b> .
<b>False</b>	The DLL has not provided a delay. The connection is stopped by the IP generator.

Remark:

The **PacketDelay()** function is used to get the delay before a new packet contents.

### 8.6.3 PacketData

BOOL CALLBACK PacketData( int CnxID, unsigned short usBufferSize, unsigned char \*pBuffer, unsigned short \*pusUsedSize)

Parameters:

**CnxID** Connection identifier

**usBufferSize** Max size of the buffer (pBuffer)

**pBuffer** Address of data to send

**pusUsedSize** Address of the data size to send. If size equals 0, a new delay is asked.  
To avoid a 'deadlock', it is not authorized to provide more than 2 data packets with a zero size.

Return codes:

**True** The DLL has provided data to send immediately.

**False** The DLL has not provided data. Connection is stopped by the IP Generator.

Remark:

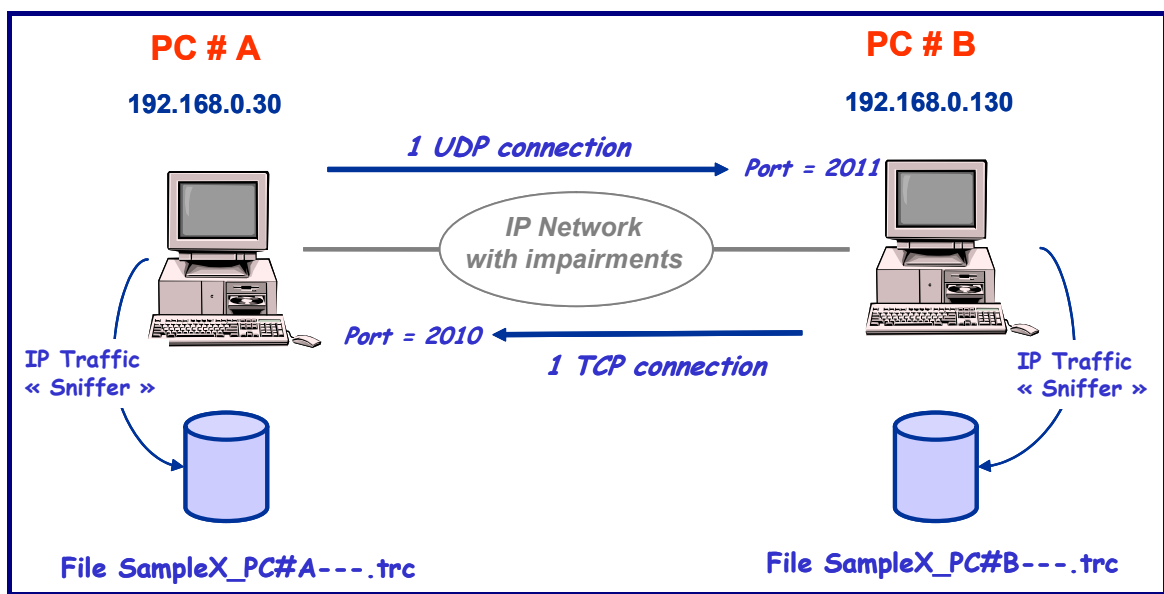
Before calling the **PacketData()** function, the buffer pointed by pBuffer is initialized with zeros. The used length is initialized with zeros. The maximum size is 1460 in the sample.

## Part 9: Examples of sniffed traffic files

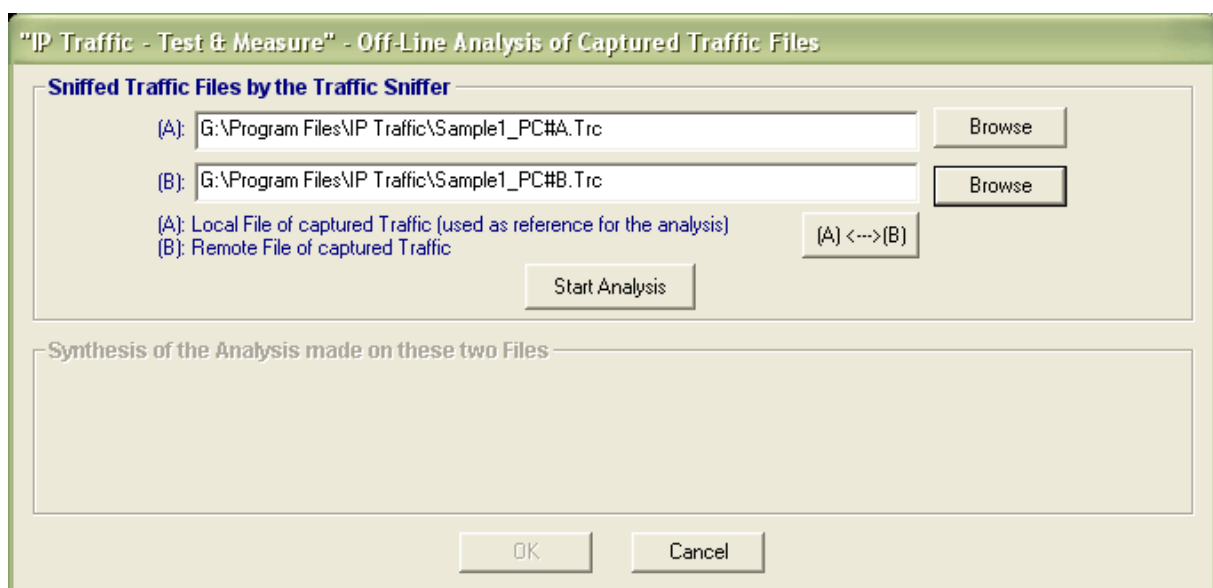
Six traffic captured files are provided to illustrate the off-line analysis:

- Example 1: two files without use of the GPS Kit and the ZClock module  
([Sample1\\_PC#A.Trc](#) and [Sample1\\_PC#B.Trc](#))
- Example 2: two files with use of the GPS Kit  
([Sample2\\_PC#A\\_with\\_GPS.Trc](#) and [Sample2\\_PC#B\\_with\\_GPS.Trc](#))
- Example 3: two files with use of the GPS Kit and the ZClock module  
([Sample3\\_PC#A\\_with\\_GPS&ZClock.Trc](#) and [Sample3\\_PC#B\\_with\\_GPS&ZClock.Trc](#))

The test configuration used to generate these traffic files is defined as below:



### Example 1: no GPS kit and no ZClock module



By pressing the « Start Analysis » button, the following window is displayed.

**"IP Traffic - Test & Measure" - Processing of the Captured Traffic Files**

**Step 1: Files Overview**

(A): G:\Program Files\IP Traffic\Sample1\_PC#A.Trc  
**(A) is used as reference for the analysis**

- ☐ 192.168.0.130 -> 192.168.0.30 (5004 Pkts - 1 Connection(s) )
- ☒ 192.168.0.30 -> 192.168.0.130 (7507 Pkts - 2 Connection(s) )
  - ☒ Ports: 2010 -> 1055 (Protocol: TCP)
  - ☒ Ports: 1066 -> 2011 (Protocol: UDP)

Packets scanned: 12511 (finished) [Start Scan] [Stop Scan] Packets scanned: 12511 (finished)

When the scan is complete, please select in (A) a couple of IP addresses or connections for a couple of IP addresses. Then go to Step 2  
 Note: If you expect to replay connections, please select up to 16 connections.

**Step 2: Criteria to search the Synchronization between these two files**

Source: ☒ IP Address ☒ Port Number  
 Destination: ☒ IP Address ☒ Port Number  
 Others ...: ☒ Identification (IP header field)

Status: Synchro Found (File A: Packet #1 <-> File B: Packet #1)  
 [Start Scan] [Stop Scan]  
 You can now do the Step 3

**Step 3: Analysis to compute "Packets Statistics"**

Number of packets analysed: 25022 / 25022 (100 % processed)  
 [Start Analysis] [Stop Analysis]

Synthesis of the Analysis made on these two Files

- Couple of IP Addresses selected: 192.168.0.30 <-> 192.168.0.130
- Number of Packets found corresponding to the Search Criteria: 12514
- Number of UDP Connections found: 1
- Number of TCP Connections found: 1
- Replay Traffic Duration: 1 mn 57 s

Processing of the sniffed traffic files is ended, you can now press "OK"

[OK] [Cancel]

In the Step 1 the couple of IP addresses 192.168.0.30 ➔ 192.168.0.130 is selected. Then the synchronization between these two files is founded for the step 2. After running the step 3, the synthesis is displayed showing 1 TCP and 1 UDP connections.

By using the "Packet Statistics" option, the following results are displayed.

Offline Packet Statistics

Computer A ==> Computer B

IP address of A: 192.168.0.30

Save ...

Computer B ==> Computer A

IP address of B: 192.168.0.130

Time (UTC)	Sta...	Tra...	Port -> ...	IP size (pro...	Identi...
22:00:43.428	Sent	...	2010->1...	48 (TCP)	xD013
PC 22:00:43.451	Sent	0 (?)	2010->1...	40 (TCP)	xD014
PC 22:00:43.490	Sent	0 (?)	2010->1...	40 (TCP)	xD015
PC 22:00:43.530	Sent	0 (?)	2010->1...	40 (TCP)	xD016
PC 22:00:43.570	Sent	0 (?)	2010->1...	40 (TCP)	xD017
PC 22:00:43.611	Sent	0 (?)	2010->1...	40 (TCP)	xD018
PC 22:00:43.651	Sent	0 (?)	2010->1...	40 (TCP)	xD019
PC 22:00:43.691	Sent	0 (?)	2010->1...	40 (TCP)	xD01A
PC 22:00:43.731	Sent	0 (?)	2010->1...	40 (TCP)	xD01B
PC 22:00:43.771	Sent	0 (?)	2010->1...	40 (TCP)	xD01C
PC 22:00:43.810	Sent	0 (?)	2010->1...	40 (TCP)	xD01D
PC 22:00:43.850	Sent	0 (?)	2010->1...	40 (TCP)	xD01E
PC 22:00:43.890	Sent	0 (?)	2010->1...	40 (TCP)	xD01F

Port -> Port(Prot...	Packets	Lost	% L...	Delay	Jitter
Total Computer A	7507	3	0%	120 ms	1 ms
1066 -> 2011 (UDP)	5000	3	0%	178 ms	1 ms
2010 -> 1055 (TCP)	2507	0	0%	6 ms	0 ms

Time (UTC)	Sta...	Tra...	Port -> ...	IP size (pro...	Identi...
22:00:43.420	Sent	...	1055->2...	48 (TCP)	x6441
PC 22:00:43.420	Sent	0 (?)	1055->2...	40 (TCP)	x6442
PC 22:00:43.423	Sent	1 (?)	1055->2...	1500 (TCP)	x6443
PC 22:00:43.442	Sent	1 (?)	1055->2...	1500 (TCP)	x6444
PC 22:00:43.462	Sent	1 (?)	1055->2...	1500 (TCP)	x6445
PC 22:00:43.481	Sent	1 (?)	1055->2...	1500 (TCP)	x6446
PC 22:00:43.501	Sent	1 (?)	1055->2...	1500 (TCP)	x6447
PC 22:00:43.521	Sent	1 (?)	1055->2...	1500 (TCP)	x6448
PC 22:00:43.541	Sent	1 (?)	1055->2...	1500 (TCP)	x6449
PC 22:00:43.561	Sent	1 (?)	1055->2...	1500 (TCP)	x644A
PC 22:00:43.582	Sent	1 (?)	1055->2...	1500 (TCP)	x644B
PC 22:00:43.602	Sent	2 (?)	1055->2...	1500 (TCP)	x644C
PC 22:00:43.622	Sent	1 (?)	1055->2...	1500 (TCP)	x644D

Port -> Port(Prot...	Packets	Lost	% L...	Delay	Jitter
Total Computer B	5007	3	0%	8 ms	0 ms
1055 -> 2010 (TCP)	5007	3	0%	8 ms	0 ms

In this example, 3 UDP packets have been lost and the transit delay has an average of 178 ms for the UDP connection. 3 TCP packets sent by the PC #B have been lost and the average for the transit delay is 7 ms.

**Note:**

The ‘Transit ...’ column contains the symbols (?) to indicate that the accuracy for measurement cannot be defined (no common clock reference between the PCs and the PC clock is used for packet time stamping by the IP Traffic Sniffer when capturing the packets).

**Example 2: use of the GPS kit and no ZClock module**

“IP Traffic - Test & Measure” - Off-Line Analysis of Captured Traffic Files

**Sniffed Traffic Files by the Traffic Sniffer**

(A): G:\Program Files\IP Traffic\Sample2\_PC#A\_with\_GPS.Trc

(B): G:\Program Files\IP Traffic\Sample2\_PC#B\_with\_GPS.Trc

(A): Local File of captured Traffic (used as reference for the analysis)  
 (B): Remote File of captured Traffic

By pressing the « Start Analysis » button, the following window is displayed.

**"IP Traffic - Test & Measure" - Processing of the Captured Traffic Files**

**Step 1: Files Overview**

(A): G:\Program Files\IP Traffic\Sample2\_PC#A\_with\_GPS.Trc

(B): G:\Program Files\IP Traffic\Sample2\_PC#B\_with\_GPS.Trc

**(A) is used as reference for the analysis**

☒ 192.168.0.30 -> 192.168.0.130 (7508 Pkts - 2 Connection(s))

☒ Ports: 1064 -> 2011 (Protocol: UDP)

☒ Ports: 2010 -> 1053 (Protocol: TCP)

☐ 192.168.0.130 -> 192.168.0.30 (5007 Pkts - 1 Connection(s))

☐ 192.168.0.30 -> 192.168.0.130 (7503 Pkts - 2 Connection(s))

☐ 192.168.0.130 -> 192.168.0.30 (5007 Pkts - 1 Connection(s))

Packets scanned: 12511 (finished) Start Scan Stop Scan Packets scanned: 12510 (finished)

When the scan is complete, please select in (A) a couple of IP addresses or connections for a couple of IP addresses. Then go to Step 2  
Note: If you expect to replay connections, please select up to 16 connections.

**Step 2: Criteria to search the Synchronization between these two files**

Source: ☒ IP Address ☒ Port Number

Destination: ☒ IP Address ☒ Port Number

Others ... ☒ Identification (IP header field)

Status: Synchro Found (File A: Packet #1 <-> File B: Packet #1)

Start Scan Stop Scan

You can now do the Step 3

**Step 3: Analysis to compute "Packets Statistics"**

Number of packets analysed: 25021 / 25021 (100 % processed)

Start Analysis Stop Analysis

Synthesis of the Analysis made on these two Files

Couple of IP Addresses selected: 192.168.0.30 <-> 192.168.0.130

Number of Packets found corresponding to the Search Criteria: 12515

Number of UDP Connections found: 1

Number of TCP Connections found: 1

Replay Traffic Duration: 2 mn 04 s

Processing of the sniffed traffic files is ended, you can now press "OK"

OK Cancel

In Step 1, the couple of IP addresses 192.168.0.30 → 192.168.0.130 is selected. Then the synchronization between these two files is founded for the step 2. After running the step 3, the synthesis is displayed showing 1 TCP and 1 UDP connections.

By using the "Packet Statistics" option, the following results are displayed.

Offline Packet Statistics											
Computer A ==> Computer B						Computer B ==> Computer A					
IP address of A: 192.168.0.30						IP address of B: 192.168.0.130					
Time (UTC)	Sta...	Tra...	Port -> ...	IP size (pro...	Identi...	Time (UTC)	Sta...	Tra...	Port -> ...	IP size (pro...	Identi...
21:55:03.559	Sent	180...	1064->2...	1488 (UDP)	x9567	21:55:20.725	Sent	1 (...)	1053->2...	48 (TCP)	x3D21
21:55:03.579	Sent	180...	1064->2...	1488 (UDP)	x9568	21:55:20.726	Sent	1 (...)	1053->2...	40 (TCP)	x3D22
21:55:03.598	Sent	171...	1064->2...	1488 (UDP)	x9569	21:55:20.728	Sent	3 (...)	1053->2...	1500 (TCP)	x3D23
21:55:03.620	Sent	179...	1064->2...	1488 (UDP)	x956A	21:55:20.747	Sent	1 (...)	1053->2...	1500 (TCP)	x3D24
21:55:03.639	Sent	179...	1064->2...	1488 (UDP)	x956B	21:55:20.767	Sent	2 (...)	1053->2...	1500 (TCP)	x3D25
21:55:03.661	Sent	178...	1064->2...	1488 (UDP)	x956C	21:55:20.787	Sent	1 (...)	1053->2...	1500 (TCP)	x3D26
21:55:03.685	Sent	173...	1064->2...	1488 (UDP)	x956D	21:55:20.807	Sent	1 (...)	1053->2...	1500 (TCP)	x3D27
21:55:03.717	Sent	171...	1064->2...	1488 (UDP)	x956E	21:55:20.827	Sent	1 (...)	1053->2...	1500 (TCP)	x3D28
21:55:03.739	Sent	180...	1064->2...	1488 (UDP)	x956F	21:55:20.847	Sent	1 (...)	1053->2...	1500 (TCP)	x3D29
21:55:03.758	Sent	170...	1064->2...	1488 (UDP)	x9570	21:55:20.866	Sent	2 (...)	1053->2...	1500 (TCP)	x3D2A
21:55:03.780	Sent	179...	1064->2...	1488 (UDP)	x9571	21:55:20.886	Sent	1 (...)	1053->2...	1500 (TCP)	x3D2B
21:55:03.799	Sent	179...	1064->2...	1488 (UDP)	x9572	21:55:20.906	Sent	2 (...)	1053->2...	1500 (TCP)	x3D2C
21:55:03.821	Sent	178...	1064->2...	1488 (UDP)	x9573	21:55:20.926	Sent	1 (...)	1053->2...	1500 (TCP)	x3D2D
Port -> Port(Prot...	Packets	Lost	% L...	Delay	Jitter	Port -> Port(Prot...	Packets	Lost	% L...	Delay	Jitter
Total Computer A	7508	5	0%	122 ms	1 ms	Total Computer B	5007	4	0%	1 ms	0 ms
2010 -> 1053 (TCP)	2508	0	0%	0 ms	0 ms	1053 -> 2010 (TCP)	5007	4	0%	1 ms	0 ms
1064 -> 2011 (UDP)	5000	5	0%	184 ms	1 ms						

In this example, 5 UDP packets have been lost and the transit delay has an average of 184 ms for the UDP connection. 4 TCP packets sent by the PC #B have been lost and the average for the transit delay is 1 ms.

*Note: the ‘Transit ...’ column indicates the symbols ( $\pm 5$ ) in order to precise that the accuracy for measurement is less than or equal to 5 ms (due to use of the GPS Kit that delivers a precise time reference used for packet time stamping by the IP Traffic Sniffer when capturing the packets).*

### Example 3: use of the GPS kit and the ZClock module

“IP Traffic - Test & Measure” - Off-Line Analysis of Captured Traffic Files

**Sniffed Traffic Files by the Traffic Sniffer**

(A): G:\Program Files\IP Traffic\Sample3\_PC#A\_with\_GPS&ZClock.Trac

(B): G:\Program Files\IP Traffic\Sample3\_PC#B\_with\_GPS&ZClock.Trac

(A): Local File of captured Traffic (used as reference for the analysis)  
 (B): Remote File of captured Traffic

(A) <--> (B)

Synthesis of the Analysis made on these two Files

By pressing the « Start Analysis » button, the following window is displayed.



**"IP Traffic - Test & Measure" - Processing of the Captured Traffic Files**

**Step 1: Files Overview**

(A): G:\Program Files\IP Traffic\Sample3\_PC#A\_with\_GPS&ZClock.Trc  
 (B): G:\Program Files\IP Traffic\Sample3\_PC#B\_with\_GPS&ZClock.Trc

**(A) is used as reference for the analysis**

☒ 192.168.0.30 -> 192.168.0.130 (7508 Pkts - 2 Connection(s))  
   ☒ Ports: 1065 -> 2011 (Protocol: UDP)  
   ☒ Ports: 2010 -> 1054 (Protocol: TCP)  
☐ 192.168.0.130 -> 192.168.0.30 (5007 Pkts - 1 Connection(s))

☐ 192.168.0.30 -> 192.168.0.130 (7502 Pkts - 2 Connection(s))  
☐ 192.168.0.130 -> 192.168.0.30 (5007 Pkts - 1 Connection(s))

Packets scanned: 12511 (finished)   Packets scanned: 12509 (finished)

When the scan is complete, please select in (A) a couple of IP addresses or connections for a couple of IP addresses. Then go to Step 2  
 Note: If you expect to replay connections, please select up to 16 connections.

**Step 2: Criteria to search the Synchronization between these two files**

Source: ☒ IP Address ☒ Port Number  
 Destination: ☒ IP Address ☒ Port Number  
 Others ... ☒ Identification (IP header field)

Status: Synchro Found (File A: Packet #1 <-> File B: Packet #1)

You can now do the Step 3

**Step 3: Analysis to compute "Packets Statistics"**

Number of packets analysed: 25020 / 25020 (100 % processed)

Synthesis of the Analysis made on these two Files

Couple of IP Addresses selected: 192.168.0.30 <-> 192.168.0.130  
 Number of Packets found corresponding to the Search Criteria: 12515  
 Number of UDP Connections found: 1  
 Number of TCP Connections found: 1  
 Replay Traffic Duration: 1 mn 53 s

Processing of the sniffed traffic files is ended, you can now press "OK"

In Step 1, the couple of IP addresses 192.168.0.30 → 192.168.0.130 is selected. Then the synchronization between these two files is founded for the step 2. After running the step 3, the synthesis is displayed showing 1 TCP and 1 UDP connections.

By using the "Packet Statistics" option, the following results are displayed.



Offline Packet Statistics

Computer A ==> Computer B

Save ...

Computer B ==> Computer A

IP address of A: 192.168.0.30

IP address of B: 192.168.0.130

Time (UTC)	Sta...	Tra...	Port -> ...	IP size (pro...	Identi...
21:58:02.199	Sent	0 (...	2010->1...	40 (TCP)	xB454
21:58:02.203	Sent	187...	1065->2...	1488 (UDP)	xB455
21:58:02.225	Sent	185...	1065->2...	1488 (UDP)	xB456
21:58:02.239	Sent	0 (...	2010->1...	40 (TCP)	xB457
21:58:02.244	Sent	186...	1065->2...	1488 (UDP)	xB458
21:58:02.266	Sent	184...	1065->2...	1488 (UDP)	xB459
21:58:02.279	Sent	0 (...	2010->1...	40 (TCP)	xB45A
21:58:02.285	Sent	185...	1065->2...	1488 (UDP)	xB45B
21:58:02.307	Sent	183...	1065->2...	1488 (UDP)	xB45C
21:58:02.320	Sent	0 (...	2010->1...	40 (TCP)	xB45D
21:58:02.326	Sent	184...	1065->2...	1488 (UDP)	xB45E
21:58:02.348	LOST	...	1065->2...	1488 (UDP)	xB45F
21:58:02.359	Sent	0 (...	2010->1...	40 (TCP)	xB460

Port -> Port(Prot...	Packets	Lost	% L...	Delay	Jitter
Total Computer A	7508	6	0%	123 ms	1 ms
2010 -> 1054 (TCP)	2508	0	0%	0 ms	0 ms
1065 -> 2011 (UDP)	5000	6	0%	186 ms	1 ms

Time (UTC)	Sta...	Tra...	Port -> ...	IP size (pro...	Identi...
21:58:00.793	Sent	0 (...	1054->2...	48 (TCP)	x50B1
21:58:00.794	Sent	0 (...	1054->2...	40 (TCP)	x50B2
21:58:00.796	Sent	1 (...	1054->2...	1500 (TCP)	x50B3
21:58:00.815	Sent	1 (...	1054->2...	1500 (TCP)	x50B4
21:58:00.835	Sent	1 (...	1054->2...	1500 (TCP)	x50B5
21:58:00.855	Sent	1 (...	1054->2...	1500 (TCP)	x50B6
21:58:00.875	Sent	1 (...	1054->2...	1500 (TCP)	x50B7
21:58:00.895	Sent	1 (...	1054->2...	1500 (TCP)	x50B8
21:58:00.915	Sent	1 (...	1054->2...	1500 (TCP)	x50B9
21:58:00.935	Sent	1 (...	1054->2...	1500 (TCP)	x50BA
21:58:00.955	Sent	1 (...	1054->2...	1500 (TCP)	x50BB
21:58:00.975	Sent	1 (...	1054->2...	1500 (TCP)	x50BC
21:58:01.046	Sent	1 (...	1054->2...	1500 (TCP)	x50BD

Port -> Port(Prot...	Packets	Lost	% L...	Delay	Jitter
Total Computer B	5007	4	0%	1 ms	0 ms
1054 -> 2010 (TCP)	5007	4	0%	1 ms	0 ms

In this example, 6 UDP packets have been lost and the transit delay has an average of 186 ms for the UDP connection. 4 TCP packets sent by the PC #B have been lost and the average for the transit delay is 1 ms.

*Note: the ‘Transit ...’ column indicates the symbols ( $\pm 1$ ) in order to precise that the accuracy for measurement is less than or equal to 1 ms (due to use of the GPS Kit that delivers a precise time reference and the ZClock module used for packet time stamping by the ‘Traffic Sniffer’ when capturing the packets).*