



"IP Traffic – Test & Measure"

Version 2.4

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

"IP Traffic - Test & Measure"

File Edit Configuration Tools File Downloading Automation Tool Help Operating mode

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

Destination Parameters

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

Unitary Mode

| Type | Parameters | Enabled |
|------------------|----------------|---------|
| Packet generator | Parameters #1 | Enabled |
| Packet generator | Parameters #2 | Enabled |
| Packet generator | Parameters #3 | Enabled |
| Packet generator | Parameters #4 | Enabled |
| Packet generator | Parameters #5 | Enabled |
| Packet generator | Parameters #6 | Enabled |
| Packet generator | Parameters #7 | Enabled |
| Packet generator | Parameters #8 | Enabled |
| Packet generator | Parameters #9 | Enabled |
| Packet generator | Parameters #10 | Enabled |
| Packet generator | Parameters #11 | Enabled |
| Packet generator | Parameters #12 | Enabled |
| Packet generator | Parameters #13 | Enabled |
| Packet generator | Parameters #14 | Enabled |
| Packet generator | Parameters #15 | Enabled |
| Packet generator | Parameters #16 | Enabled |

Automatic Mode

Replay Mode

GPS ZClock Activity

Active connections: 0 Throughput: 0.00 b/s

IP Generator Activity (based on application data)

Active connections: 0 Throughput: 0.00 b/s

IP Answering Activity (based on application data)

Active connections: 0 Throughput: 0.00 b/s

Sniffer Activity

File size: Time before disk limit:

Remote Control of an IP Traffic - Test & Measure system

Remote file context: Remote IP address or Host Name: NO_ADDRESS Port: 2600

Remote Operation

Run all processes Stop

Local Operation

Start All Local Processes Stop All Local Processes

User Guide

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

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

Email: contact@zti-telecom.com / Web: www.zti-telecom.com

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

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

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

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

To contact us:

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

Phone: +33 2 96 48 43 43
Fax: +33 2 96 48 14 85
Web: <http://www.zti-telecom.com> or <http://www.zti.fr>
Email: contact@zti-telecom.com (marketing & sales)
support@zti-telecom.com (technical support)

Copyrights

Copyright ZTI 2000-2006. All rights reserved.
France Telecom licensed product.

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

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

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

Software License Agreement

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

- **COPYRIGHT**

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

French copyright laws and international treaties protect the products. ZTI grants you the right to use the products according to the following:

- **USE OF THE SOFTWARE**

You may:

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

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

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

- **SOFTWARE PROTECTION**

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

- **LIMITED WARRANTY**

The software is supplied without any express or implied warranty regarding the performances or results obtained by the use of the Products.

ZTI warrants that the software media (i.e. CD-ROM) will be free of material defects for a ninety (90) days period following purchase. The limited warranty applies to the media and not the information contained on it. If the media does not comply with this limited warranty, the only remedy is the replacement of the media software. In no event, ZTI will be liable for any kind of direct or indirect damages caused by the Products.

- **JURISDICTION**

French laws will govern this agreement.

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

FOR FURTHER INFORMATION, PLEASE CONTACT: ZTI CUSTOMER SUPPORT DEPARTMENT.

ZTI
1 boulevard d'Armor
BP 20254
22302 Lannion Cedex
France
Phone: +33 2 96 48 43 43
Fax: +33 2 96 48 14 85
Email: support@zti-telecom.com or support@zti.fr
Web: <http://www.zti-telecom.com> or <http://www.zti.fr>

Table of contents

| | | |
|----------------|---|-----------|
| PART 0 | PREFACE | 7 |
| 0.1 | ORGANIZATION OF THIS MANUAL | 7 |
| 0.2 | MINIMUM SYSTEM REQUIREMENTS | 8 |
| 0.3 | REFERENCES | 8 |
| 0.4 | TERMS USED IN THIS DOCUMENT | 9 |
| 0.5 | TECHNICAL SUPPORT | 9 |
| PART 1 | OVERVIEW | 10 |
| 1.1 | GENERAL DESCRIPTION | 10 |
| 1.2 | ARCHITECTURE | 13 |
| 1.3 | HARDWARE OPTIONS AVAILABLE | 14 |
| 1.4 | "IP TRAFFIC – TEST & MEASURE" KEY FEATURES | 15 |
| 1.5 | THE AUTOMATION TOOL FOR "IP TRAFFIC – TEST & MEASURE" | 22 |
| PART 2 | WHAT'S NEW IN "IP TRAFFIC – TEST & MEASURE" VERSION 2.4 | 23 |
| 2.1 | NEW FEATURES AND IMPROVEMENTS INCLUDED IN THE VERSION 2.4 | 23 |
| 2.2 | UPGRADING FROM "IP TRAFFIC – TEST & MEASURE" VERSION 2.3 | 24 |
| 2.3 | UPGRADING FROM "IP TRAFFIC – TEST & MEASURE" VERSION 2.2 | 24 |
| 2.4 | UPGRADING FROM "IP TRAFFIC – TEST & MEASURE" VERSION 2.1 | 25 |
| 2.5 | UPGRADING FROM "IP TRAFFIC – TEST & MEASURE" VERSION 2.0 | 25 |
| 2.6 | UPGRADING FROM VERSIONS 1 (INCLUDING VERSION 1.3) | 26 |
| 2.7 | ACROBAT READER VERSION COMPATIBILITY | 26 |
| PART 3 | INSTALL "IP TRAFFIC – TEST & MEASURE" | 27 |
| 3.1 | HOW TO INSTALL THE SOFTWARE DOWNLOADED FROM THE INTERNET | 27 |
| 3.2 | HOW TO INSTALL THE SOFTWARE FROM THE CD-ROM | 31 |
| PART 4 | SOFTWARE LICENSE CONFIGURATION | 34 |
| 4.1 | HOW TO CONFIGURE THE LICENSE | 34 |
| 4.2 | LICENSE TRANSFERS | 37 |
| 4.2.1 | <i>Direct Transfer: move the license from one local directory to another</i> | <i>37</i> |
| 4.2.1 | <i>Transfer by media (floppy disk or USB key) from a source PC to a target PC</i> | <i>38</i> |
| 4.3 | HOW TO KILL A LICENSE | 44 |
| PART 5 | UNINSTALL "IP TRAFFIC – TEST & MEASURE" | 45 |
| PART 6 | "IP TRAFFIC – TEST & MEASURE" GETTING STARTED | 46 |
| PART 7 | RUN "IP TRAFFIC – TEST & MEASURE" | 51 |
| PART 8 | "IP TRAFFIC – TEST & MEASURE" / WINDOWS FIREWALL | 52 |
| 8.1 | CONFIGURATION FOR UDP, TCP CONNECTIONS AND ICMP IPv4 | 52 |
| 8.2 | CONFIGURATION FOR ICMP IPv6 CONNECTIONS | 55 |
| 8.3 | HOW TO CONFIGURE A FIREWALL (LIST OF THE PORTS USED) | 56 |
| PART 9 | HARDWARE INSTALLATION (GPS KIT AND ZCLOCK) | 57 |
| 9.1 | CONFIGURATION 1: "IP TRAFFIC – TEST & MEASURE" + GPS KIT | 57 |
| 9.2 | CONFIGURATION 2: "IP TRAFFIC – TEST & MEASURE" + ZCLOCK | 58 |
| 9.3 | CONFIGURATION 3: "IP TRAFFIC – TEST & MEASURE" + GPS KIT + ZCLOCK | 59 |
| PART 10 | GRAPHICAL USER INTERFACE | 60 |
| 10.1 | MAIN WINDOW | 60 |
| 10.2 | DISPLAY GENERAL RULES OF THE "IP TRAFFIC – TEST & MEASURE" GUI | 61 |
| 10.3 | USED UNITS IN INFORMATION DISPLAY | 62 |
| 10.3.1 | <i>Volume units</i> | <i>62</i> |
| 10.3.2 | <i>Throughput units</i> | <i>62</i> |

| | | |
|----------------|---|------------|
| 10.3.3 | Duration units..... | 62 |
| PART 11 | USING "IP TRAFFIC – TEST & MEASURE" | 63 |
| 11.1 | MAIN STEPS | 63 |
| 11.2 | LAUNCH "IP TRAFFIC – TEST & MEASURE" | 64 |
| 11.3 | MENU DESCRIPTION..... | 65 |
| 11.3.1 | File Menu..... | 65 |
| 11.3.2 | Edit menu..... | 66 |
| 11.3.3 | Configuration menu..... | 68 |
| 11.3.4 | Tools menu..... | 75 |
| 11.3.5 | File downloading menu | 76 |
| 11.3.6 | Automation Tool menu | 79 |
| 11.3.7 | Help Menu | 79 |
| 11.3.8 | Operating mode menu | 82 |
| 11.4 | MAIN WINDOW: THE FIVE TABS | 83 |
| 11.5 | MAIN WINDOW: THE ACTIVITY DISPLAY | 83 |
| 11.6 | MAIN WINDOW: THE GENERAL COMMANDS | 84 |
| 11.7 | THE 'IP GENERATOR – PARAMETERS' TAB..... | 85 |
| 11.7.1 | Destination Parameters | 86 |
| 11.7.2 | Configure the unitary mode..... | 92 |
| 11.7.3 | Configure the automatic mode | 102 |
| 11.7.4 | Configure the replay sniffed traffic mode..... | 106 |
| 11.8 | THE 'IP GENERATOR – TRAFFIC + STATISTICS' TAB | 108 |
| 11.8.1 | Destination Parameters area..... | 108 |
| 11.8.2 | Statistics (Application Level)..... | 109 |
| 11.8.3 | Run an unitary testing session..... | 115 |
| 11.8.4 | Run an automatic testing session..... | 116 |
| 11.8.5 | Run a replay traffic session | 117 |
| 11.8.6 | Using ICMP capacity of the Traffic Generator..... | 118 |
| 11.9 | THE 'IP ANSWERING' TAB..... | 119 |
| 11.9.1 | Duplicate parameters of a connection onto others..... | 119 |
| 11.9.2 | Listening To | 120 |
| 11.9.3 | Coming From | 124 |
| 11.9.4 | Receiving working mode..... | 125 |
| 11.9.5 | 'IP Answering' Statistics | 128 |
| 11.9.6 | "Export IP Answering statistics into a file" parameters..... | 130 |
| 11.10 | THE 'TRAFFIC SNIFFER' TAB | 134 |
| 11.10.1 | Capture Parameters (Step 1)..... | 135 |
| 11.10.2 | Capture sniffed traffic into a file (Step 2)..... | 137 |
| 11.10.3 | Run analysis algorithm (Step 3) | 138 |
| 11.11 | THE 'TRAFFIC OBSERVER' TAB..... | 139 |
| 11.11.1 | "IP Traffic – Test & Measure": On-line and Off-line modes for statistics..... | 140 |
| 11.11.2 | Objects and command buttons..... | 141 |
| 11.11.3 | Values and statistics display..... | 154 |
| PART 12 | CALCULATION MODE FOR THE STATISTICS | 162 |
| 12.1 | INTRODUCTION | 162 |
| 12.2 | STATISTICS COMPUTED BY "IP TRAFFIC – TEST & MEASURE" | 163 |
| 12.2.1 | Reference points to compute the statistics | 163 |
| 12.2.2 | Statistics description..... | 164 |
| 12.3 | GENERAL PARAMETERS USED TO CALCULATE THE STATISTICS | 166 |
| 12.4 | THE CALCULATION METHOD IS USED BY "IP TRAFFIC – TEST & MEASURE" TO COMPUTE STATISTICS..... | 168 |
| 12.4.1 | The two calculation methods..... | 168 |
| 12.4.2 | IP Traffic - IP Generator statistics..... | 168 |
| 12.4.3 | IP Traffic - IP Answering statistics | 169 |
| 12.4.4 | IP Traffic – Traffic Observer statistics..... | 169 |

| | | |
|----------------|--|------------|
| 12.4.5 | <i>IP Traffic –Packets Statistics Synthesis</i> | 169 |
| 12.5 | DETAILED DESCRIPTION FOR CALCULATION OF THE STATISTICS | 170 |
| 12.5.1 | <i>The 'IP Generator – Traffic + Statistics' tab</i> | 170 |
| 12.5.2 | <i>The 'IP Answering – Parameters + Statistics' tab</i> | 172 |
| 12.5.3 | <i>The 'Traffic Observer' tab</i> | 173 |
| PART 13 | ANNEXES | 175 |
| 13.1 | DESCRIPTION OF THE MATHEMATICAL LAWS USED BY "IP TRAFFIC – TEST & MEASURE" | 175 |
| 13.1.1 | <i>Uniform Law</i> | 175 |
| 13.1.2 | <i>Exponential Law</i> | 176 |
| 13.1.3 | <i>Law of Pareto</i> | 178 |
| 13.1.4 | <i>Gauss law</i> | 179 |
| 13.2 | "IP TRAFFIC – TEST & MEASURE" TRACES | 179 |
| 13.3 | CONFIGURATION PARAMETERS SAVED IN THE REGISTRY DATABASE..... | 180 |
| 13.4 | DEFAULT VALUES OF A CONTEXT..... | 182 |
| 13.5 | EXTERNAL FILE FOR THE 'IP GENERATOR' MODULE..... | 184 |
| 13.6 | EXTERNAL DLL FOR THE 'IP GENERATOR' MODULE | 185 |
| 13.6.1 | <i>TrafficInit</i> | 185 |
| 13.6.2 | <i>PacketDelay</i> | 185 |
| 13.6.3 | <i>PacketData</i> | 186 |
| PART 14 | EXAMPLES OF SNIFFED TRAFFIC FILES | 187 |

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**

This part briefly describes the key features of the **"IP Traffic – Test & Measure» and Automation Tool for "IP Traffic – Test & Measure"**.

- **Part 2: What's new in "IP Traffic – Test & Measure" version 2.4**

This part is a general overview of new features, main improvements provided with **"IP Traffic – Test & Measure"** version 2.4 and important information to upgrade from previous versions.

- **Part 3: Install "IP Traffic – Test & Measure"**

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

- **Part 4: Software License Configuration**

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

- **Part 5: Uninstall "IP Traffic – Test & Measure"**

How to uninstall the software.

- **Part 6: "IP Traffic – Test & Measure" Getting Started**

New users can use this help as an introduction to **"IP Traffic – Test & Measure"** and generate or receive traffic with the IPv4 protocol in a few clicks.

- **Part 7: Run "IP Traffic – Test & Measure"**

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

- **Part 8: "IP Traffic – Test & Measure" / Windows Firewall**

How to configure the Windows firewall to authorize the use of **"IP Traffic – Test & Measure"**.

- **Part 9: Hardware Installation (GPS Kit and ZClock)**

How to connect the GPS Kit via a serial cable and ZClock via a parallel cable to the PC.

- **Part 10: Graphical User Interface**

Presents the **"IP Traffic – Test & Measure"** Graphical User's Interface, i.e. the main rules and principles of representation and display.

- **Part 11: Using "IP Traffic – Test & Measure"**

How to use **"IP Traffic – Test & Measure"**. This part includes the menu and functionalities description. It is based on windows and tabs description. Each tab is presented separately.

- **Part 12: Calculation Mode for the Statistics**

This part describes the rules and methods used to calculate statistics displayed by **"IP Traffic – Test & Measure"**.

- **Part 13: Annex**

Provides 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 14: Examples of sniffed traffic files**

Eight sample files (containing IP packets captured with the 'Traffic Sniffer') are provided with **"IP Traffic – Test & Measure"**. These files can be used with the off-line mode of the 'Traffic Observer'.

0.2 Minimum System Requirements

To appropriately operate **"IP Traffic – Test & Measure"** you need the following minimum system requirements:

- Windows 98 (SE recommended), 2000 (SP 3 or earlier recommended), XP or Server 2003
- Pentium processor with 128 MB memory
- 1024 x 768 display
- 25 MB free hard disk space



To use IPv6, Windows XP or Server 2003 is required.



*Acrobat Reader is needed to display the **"IP Traffic – Test & Measure"** Help. If Acrobat reader hasn't been installed, a warning message is displayed to inform that **"IP Traffic – Test & Measure"** is available but without the help file.*

0.3 References

- [WINSOCK2] « Windows Socket 2 - Application Programming Interface » Revision 2.2.0 - May 10, 1996
- [RFC2460] "Internet Protocol, Version 6 (IPv6) - Specification"
- [RFC2373] "IP Version 6 Addressing Architecture"

0.4 Terms used in this document

| | |
|------------|--|
| Interface | Generic term used to reference a NIC (LAN adapter), a connected RAS connection (ISDN, ADSL, Modem) or a tunneling path. |
| Tooltip | A tooltip is a popup window displayed when you move the mouse over a sensitive area. "IP Traffic – Test & Measure" displays the tooltip during 5 seconds. |
| Automation | Automation is an add-on scripting tool used to pilot automatically "IP Traffic – Test & Measure" . |

0.5 Technical Support

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

Before contacting our Technical Support, please read the relevant sections of the product documentation and the "Read Me First" file.

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

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

You can contact the technical support by:

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

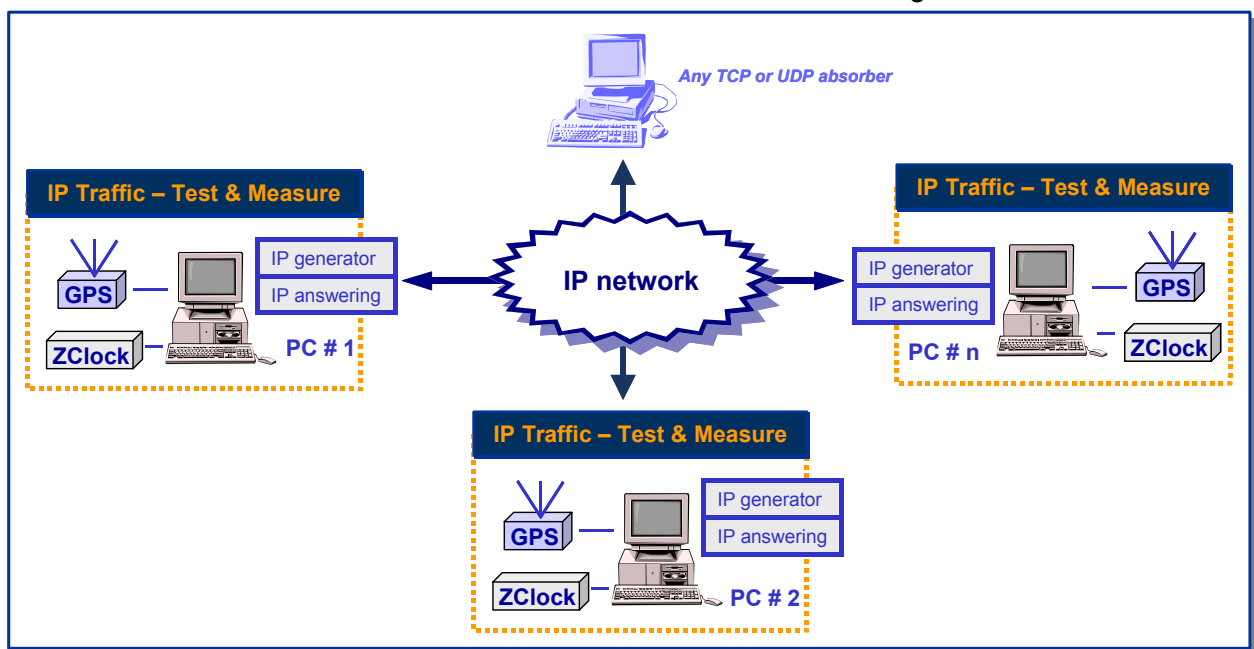
PART 1 Overview

1.1 General Description

"IP Traffic – Test & Measure" 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, XP or Server 2003. 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.

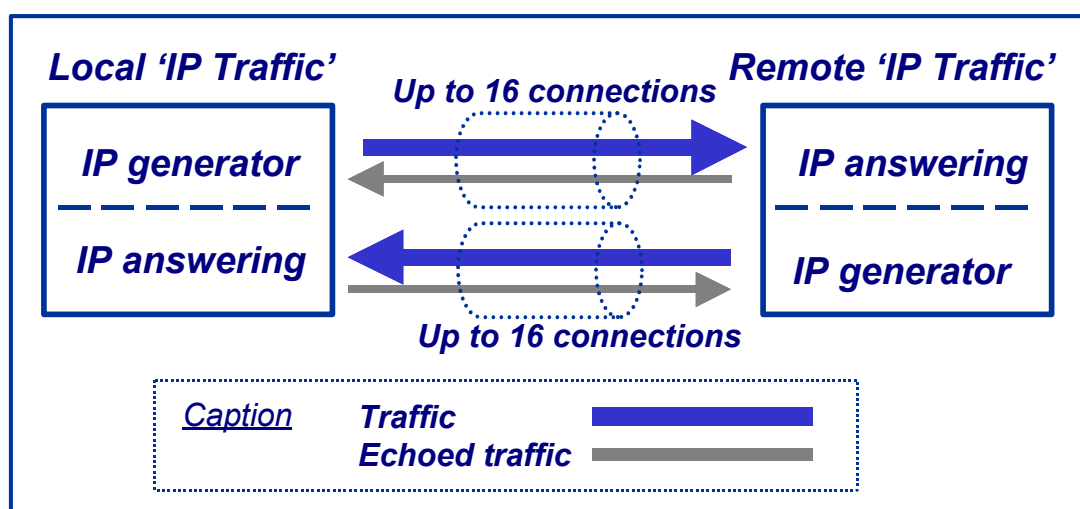


"IP Traffic – Test & Measure" is an IP software testing tool using the Microsoft Windows TCP/IP stack (Winsock2 interface). So, "IP Traffic – Test & Measure" is independent of any transmission or telecom link and can use any transmission link managed by the Windows operating system: LAN (Ethernet, Token-ring, 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 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).

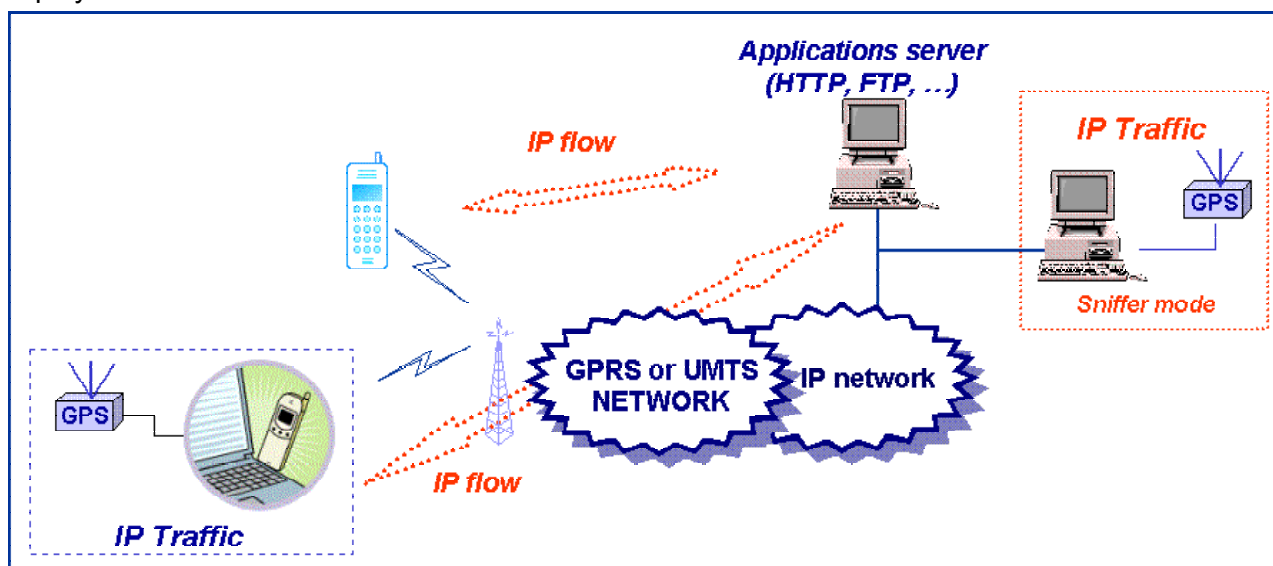
"IP Traffic – Test & Measure" is composed of four modules: 'IP Generator', 'IP Answering', 'Traffic Sniffer' and 'Traffic Observer'.

- **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. The 'IP Generator' module can replay these traffic files.



"IP Traffic – Test & Measure": sniffer mode

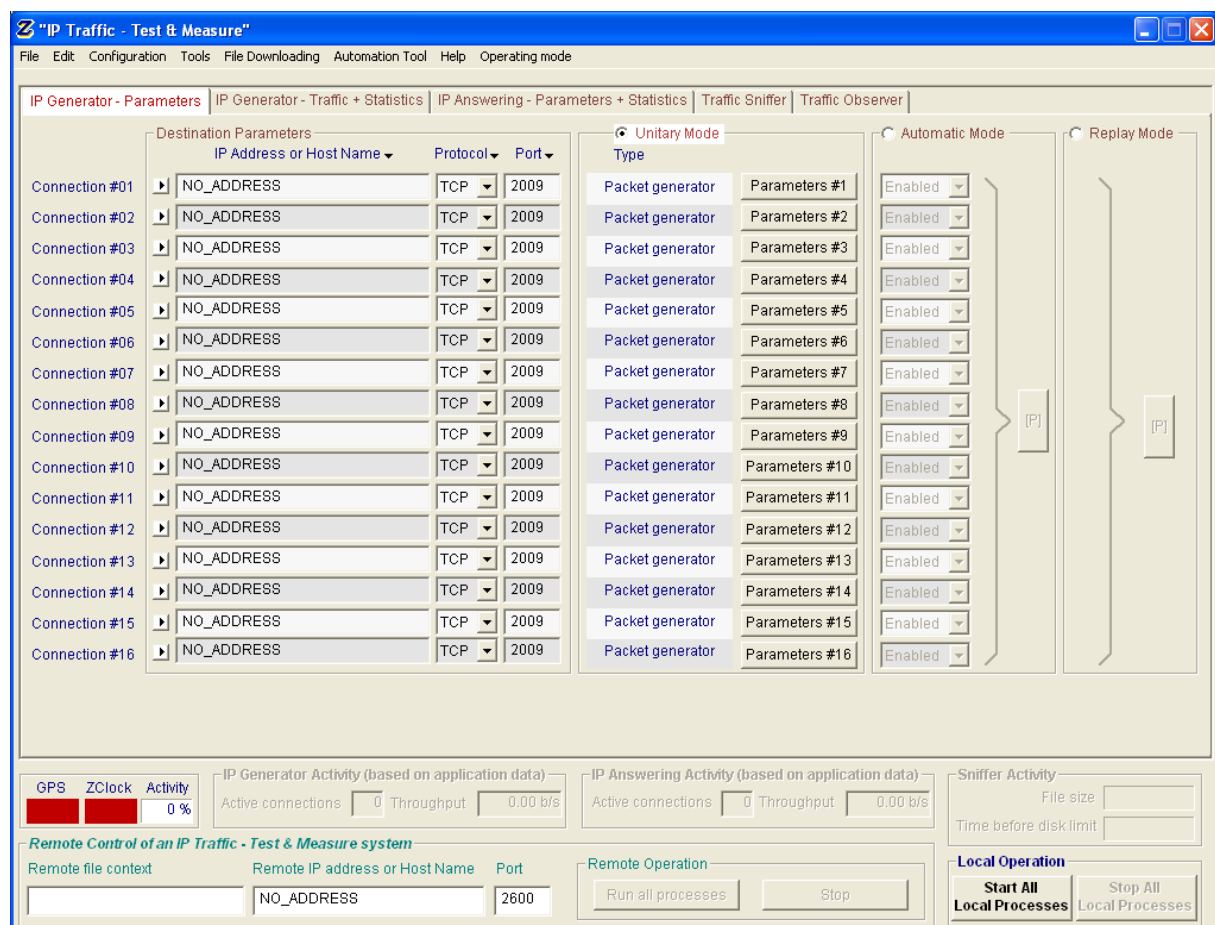
"IP Traffic – Test & Measure" can be used to capture IP traffic with the 'Traffic Sniffer': for example, the IP flows between a mobile and an application server (web, video telephony...) can be captured and saved in a file. IP packets are time stamped, to replay IP traffic with the same timing as for 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 – Test & Measure" generator as source traffic.

- **Module 4: the 'Traffic Observer'** is a powerful **graphic tool** to display and visualize traffic statistics of 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 – Test & Measure" can be operated with two main modes:

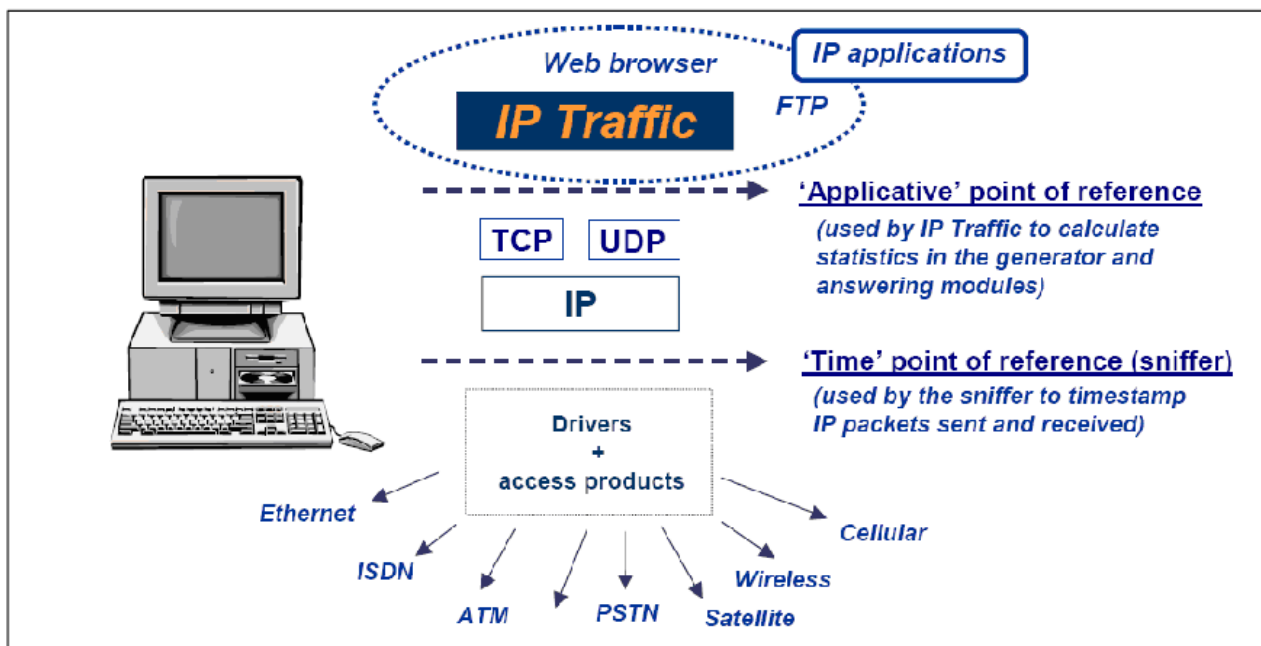
- The **normal** mode: the user can access all commands and functionalities
- The **remote control** mode: the user can't access locally commands of **"IP Traffic – Test & Measure"**. It's mainly used for control by a remote **"IP Traffic – Test & Measure"** system. It's very useful for example to use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

'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 "IP Traffic – Test & Measure", and are independent of the protocol (TCP or UDP).

'Time' point of reference

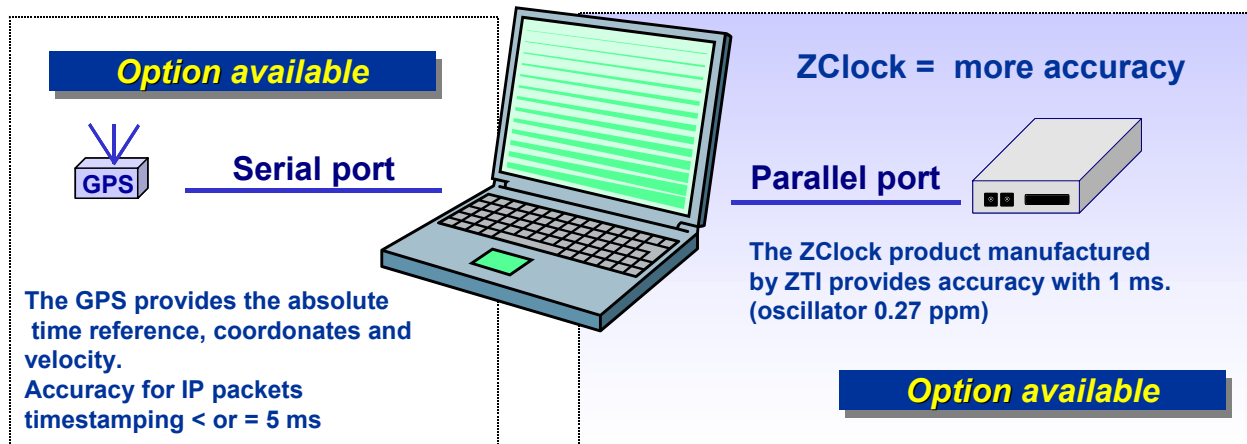
The 'Traffic Sniffer' uses this point of reference in order to timestamp IP packets sent and received. Timestamp of packets is made at the nearest of the physical link (under the TCP/IP stack). Therefore, "IP Traffic – Test & Measure" can identify lost and retransmitted IP packets. Values and statistics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

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

To free "IP Traffic – Test & Measure" 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 "IP Traffic – Test & Measure":

| 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). This is a relative reference. | 1 millisecond |
| 3 | "IP Traffic – Test & Measure" + GPS + ZClock | GPS (ZClock is initialized with the GPS time). This is an absolute reference. | 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. ZClock provides a very precise clock time reference (by the use of a high stability quartz oscillator $< \pm 1.10^{-9}$ 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. When the ZClock and GPS work together, the GPS provides the reference time to the ZClock. Then the ZClock time is used to timestamp the packets.

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 $< \text{or} = 5$ milliseconds.

ZClock 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 connections
- 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).

- **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)
 - Min RTT

- Max RTT
- Jitter

A RTT summary is also available. This summary shows the minimum, maximum and Mean RTT values for all connections of the 'IP Generator' part.

These statistics can be saved in a CSV 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 using only one testing mode:

⇒ **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.
- Mean Packet Throughput for the connection in p/s (packets per second)

- **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)
- Min RTT
- Max RTT

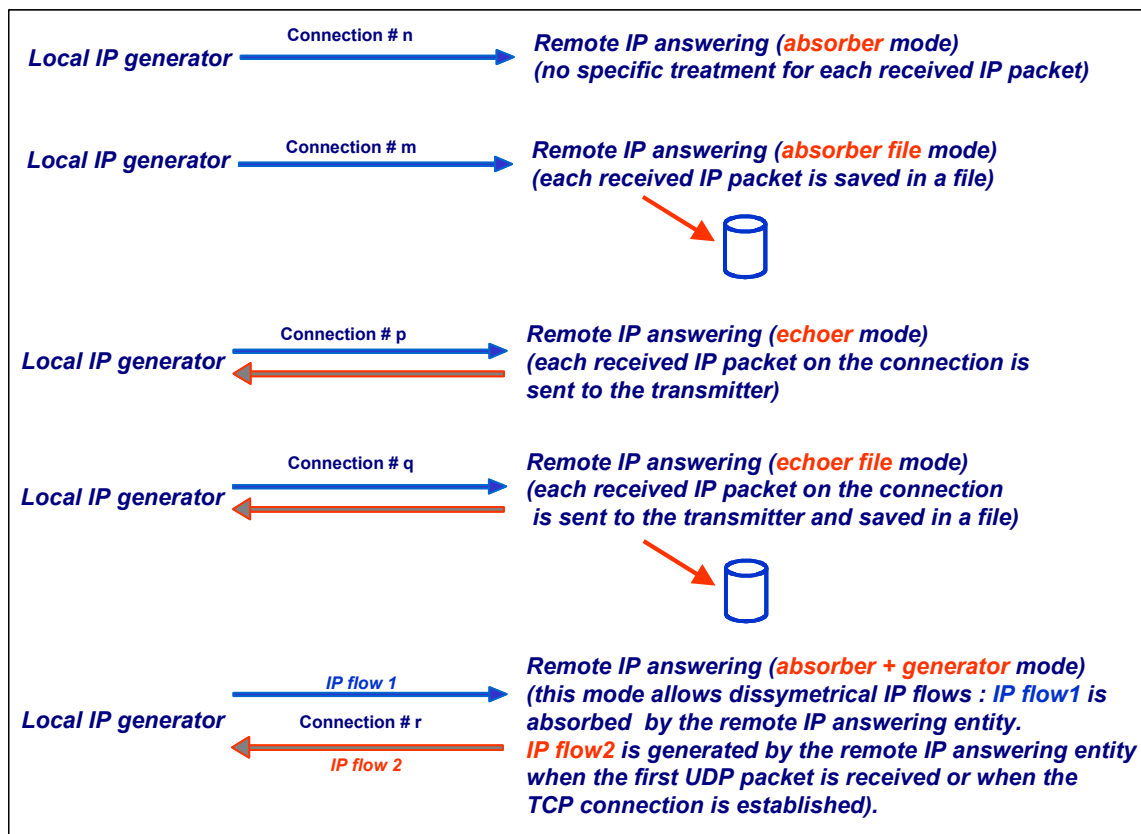
A RTT summary is also available. This summary shows the minimum, maximum and Mean RTT values for all connections of the 'IP Generator' part.

These statistics can be saved in a CSV 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

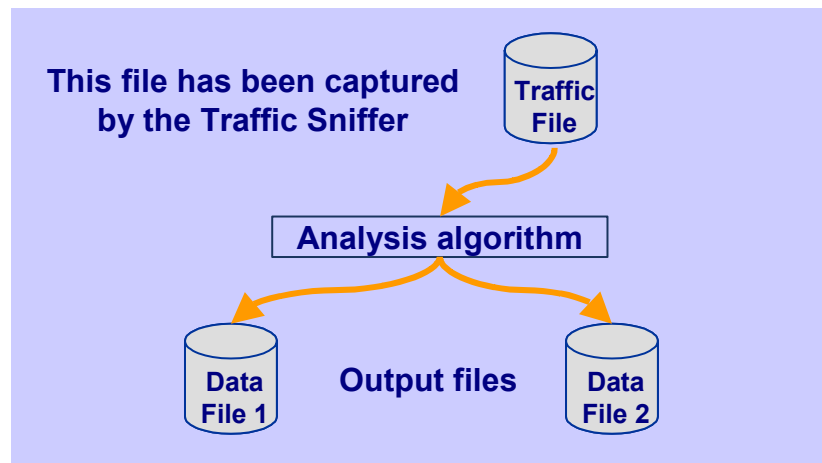
These statistics can be saved in a CSV file defined by the user.

Module 3: 'Traffic Sniffer' Overview

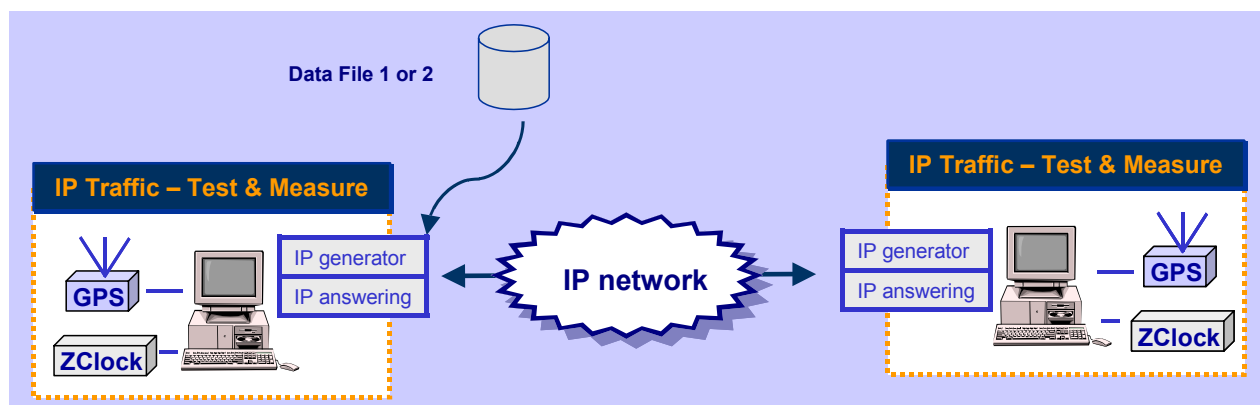
Sent and received IP packets are time stamped by the '**Traffic Sniffer**' and then saved in a file to generate capture traffic files.

The user can define IP filters to capture IP traffic in a file.

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):



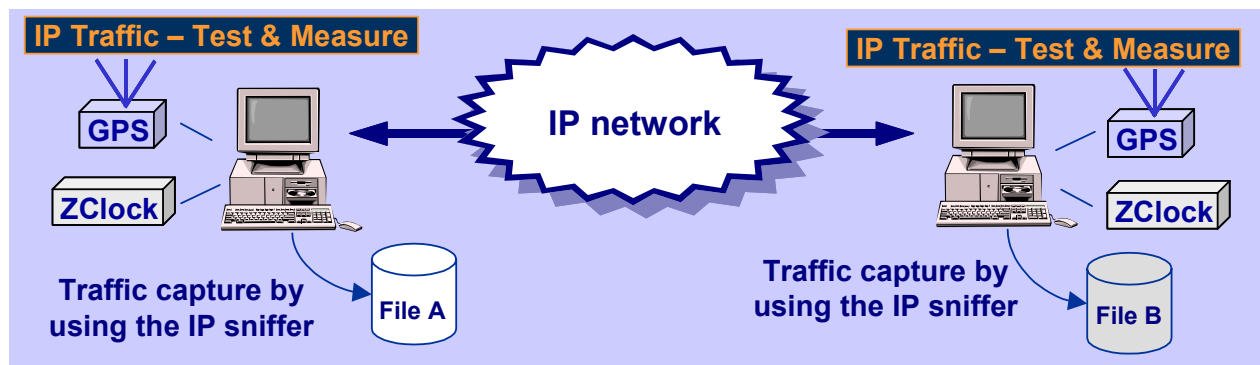
Then it is possible to use a data file generated in order to replay traffic via the '**IP Generator**' module:



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). In the example shown below, the '**Traffic Sniffer**' is activated on each system to generate a traffic file. Two traffic files are produced: File A and File B. The '**Traffic Observer**' can then use these traffic files A and B in order to calculate off-line statistics.

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**'. The statistics in red are only available with the offline mode. The green values are available with both offline and online modes.

□ 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 CSV file with filters defined by user
- ⇒ Reset statistics
- ⇒ Help window

□ Features available with the off-line mode

- ⇒ 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

For each packet:

- Packet Status: Lost or Sent
- Transit Delay
- Packet transit delay
- IP size
- IP Identification (available for each packet with IPv4 and only on fragment packets in IPv6)

For each connection (TCP or UDP) and for each side:

- Number of sent packets
- Mean Transit Delay
- Mean Jitter
- Number (and percentage) of lost packets
- Number of TCP packets which have been retransmitted (only for TCP connection)

- ⇒ Export statistics in a CSV file with filters defined by user (the GPS location is also exported in this CSV file).
- ⇒ Reset statistics
- ⇒ Help window

Multicast feature



"IP Traffic – Test & Measure" is able to generate and receive Unicast and Multicast IP traffic (IPv4 and IPv6). The multicast feature is used for the UDP protocol only.

- Multicast & IPV4:** IPv4 addresses from 224.0.0.0 to 239.255.255.255 are MULTICAST IP addresses. These addresses can be used to generate multicast IP traffic (define the multicast IP address in the Sender part) or to receive multicast IP traffic (define the multicast IP address in the Receiver part).
For information: these IPv4 addresses 224.0.0.0 to 224.255.255.255 do not generate IGMP JOIN /LEAVE messages.
- Multicast & IPv6:** IPv6 multicast addresses are defined in "IP Version 6 Addressing Architecture" [RFC2373].
This defines fixed and variable scope multicast addresses.
IPv6 multicast addresses are distinguished from unicast addresses by the value of the high-order octet of the addresses: a value of 0xFF (binary 11111111) identifies an address as a multicast address; any other value identifies an address as a unicast address (FE80::/10 are Link local addresses, FEC0::/10 are Site Local addresses where FF00::/8 are Multicast addresses).
Multicast addresses from FF01:: through FF0F:: are reserved.
The complete list of Reserved IPv6 multicast addresses can be found in "IPv6 Multicast Address Assignments" [RFC 2375].
The ICMPv6 messages are used to convey IPv6 Multicast addresses resolution.

IP version selection (Windows XP and later)

Please note that **"IP Traffic – Test & Measure"** supports IPv6 for Windows XP and later versions (i.e. Server 2003) but doesn't support IPv6 for Windows 2000.

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

"IP Traffic – Test & Measure" supports the IPv6 numerical address format (128 bits long) as well as canonical addresses. The IPv6 multicast is available with **"IP Traffic – Test & Measure"** in accordance to RFC 2373 where a multicast IPv6 address starts with FF.

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

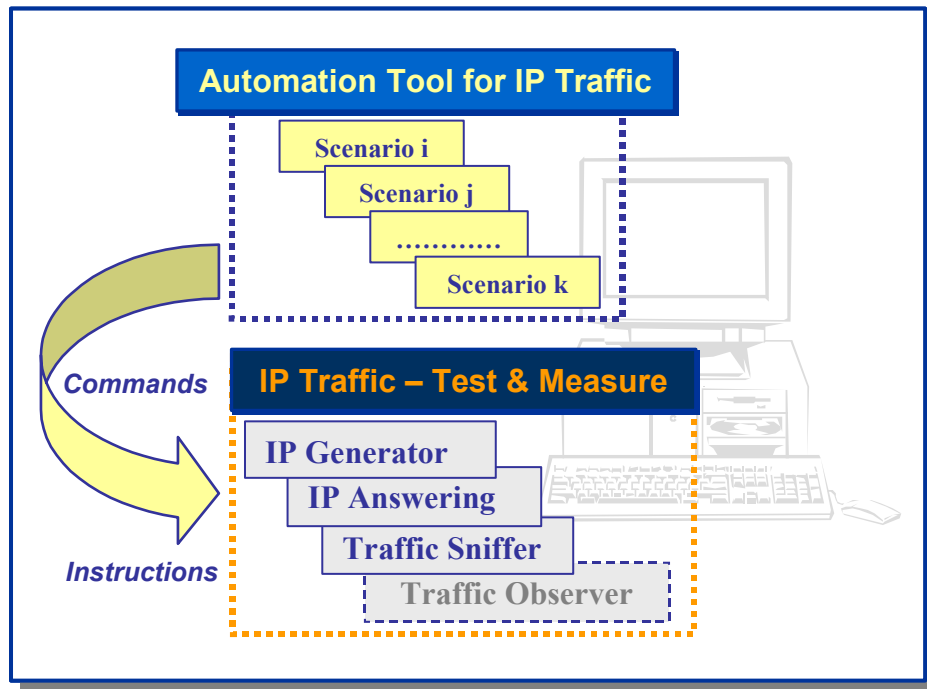
Interface selection

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

"IP Traffic – Test & Measure" is able to generate and receive Unicast and Multicast IP traffic on a selected interface, giving the user a deeper control where data are exchanged and makes multiple routes definition easily.

1.5 The Automation Tool for "IP Traffic – Test & Measure"

The add-on software **Automation Tool for "IP Traffic – Test & Measure"** allows you to edit scenarios, carry out scenarios, set the **"IP Traffic – Test & Measure"** parameters and pilot **"IP Traffic – Test & Measure"** automatically on the same PC.



A scenario is a succession of **commands** and **instructions**.

A **command** is used to set parameters and/or activate a function of **"IP Traffic – Test & Measure"**.

For example the **Set and Start connection(s)** command helps to set parameters for IP connections and to start the traffic on these connections. With such command you specify the IP address, port number, protocol, packet size, inter packet delay, duration, etc. and you start the traffic generation for these connections.

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

By using the **Automation Tool for "IP Traffic – Test & Measure"** you can:

- Set automatically the parameters of the **"IP Traffic – Test & Measure"** software,
- Start and stop IP connections based on timers,
- Execute the scheduled operations in accordance with your own timing,
- Make repetitive tests operations automatically,
- Simplify the tests reproduction,
- And more...

PART 2 What's new in "IP Traffic – Test & Measure" Version 2.4

This part is a general overview of new features and main improvements of "IP Traffic – Test & Measure" version 2.4. You will find some important information on how to upgrade your software from previous versions. Details regarding features and corrections included in the different versions of "IP Traffic – Test & Measure" can be found in the version.txt file located in the installation directory (by default: C:\Program Files\IP Traffic).

To upgrade your software from 1.3, 2.0, 2.1, 2.2 or 2.3 to 2.4 version, please refer to paragraphs below.

2.1 New features and improvements included in the version 2.4

⇒ "IP Traffic – Test & Measure" (Version 2.4)

- IPv6 ready (generation, capture, replay and conversion)
- First time users: Getting Started information
- Min/Max/Mean RTT values are available for each connection (a synthesis of all values is also available).
- RTT, Sequence numbers errors and jitter values calculation for each connection are now based on a sampling period
- The statistics are saved in CSV files
- By double-clicking on a context file, IP Traffic starts and opens the context file.
- The RPC port number used by the Automation Tool and IP Traffic to dialog can be changed using the key sited into the registry (more details in the "IP Traffic – Test & Measure" User Guide).

The contexts created with versions 2.0 and higher are reused automatically. When saved, they become the new 2.4 context file format.

⇒ Automation Tool for "IP Traffic – Test & Measure" (Version 1.4)

- By double-clicking on a .scn file, the Automation Tool starts and opens the scenario file.
- The RPC port number used by the Automation Tool and IP Traffic to dialog can be changed using the key sited into the registry (more details in the "IP Traffic – Test & Measure" User Guide).
- During a wait command execution, the elapsed and the remaining time are displayed
- The number of iteration passed when using a repeat command is shown on the execution result area
- Start and stop the Automation Tool using command lines

The scenarios created with older versions are reused automatically. When saved, they become the new 1.4 scenario file format.

2.2 Upgrading from "IP Traffic – Test & Measure" version 2.3

There is no need to uninstall **"IP Traffic – Test & Measure"** version 2.3 before upgrading to version 2.4. The installation procedure checks if a previous version of **"IP Traffic – Test & Measure"** was installed. When the version 2.3 is found, it updates automatically the **"IP Traffic – Test & Measure"** components.

Installation of the **"IP Traffic – Test & Measure"** version 2.4 over the **"IP Traffic – Test & Measure"** version 2.3 replaces the IPTraff.exe application and the old znpf.sys driver by the new znpf.sys driver where they have been installed. The old help file named 'User Guide IP Traffic V2.3.pdf' is replaced by the 'IP Traffic V2.4 User Guide.pdf' file. The registry content is extended with new parameters needed by the help mechanism and the "Automation Tool for IP Traffic". Finally, the DLL file "packet.dll" is replaced by a new version including ZTI extensions (only for Windows 2000/XP/Server 2003 systems).

The license scheme is retained during the upgrade process. If an unlimited license was available, the **"IP Traffic – Test & Measure"** version 2.4 is ready to be used unlimited. If the trial version was used, the number of remaining days isn't changed: it will continue to decrease up to the final date.

Acrobat Reader is needed with **"IP Traffic – Test & Measure"** version 2.4: see 'paragraph 2.7 Acrobat Reader version compatibility' for more details.

2.3 Upgrading from "IP Traffic – Test & Measure" version 2.2

There is no need to uninstall **"IP Traffic – Test & Measure"** version 2.2 before upgrading to version 2.4. The installation procedure checks if a previous version of **"IP Traffic – Test & Measure"** was installed. When the version 2.2 is found, it updates automatically the **"IP Traffic – Test & Measure"** components.

Installation of the **"IP Traffic – Test & Measure"** version 2.4 over the **"IP Traffic – Test & Measure"** version 2.2 replaces the IPTraff.exe application and the ltsnif.sys driver by the znpf.sys driver where they have been installed. The old help file named 'User Guide IP Traffic V2.2.pdf' is replaced by the 'IP Traffic V2.4 User Guide.pdf' file. The registry content is extended with new parameters needed by the help mechanism and the "Automation Tool for IP Traffic". Finally, the DLL file "packet.dll" is replaced by a new version including ZTI extensions (only for Windows 2000/XP/Server 2003 systems).

The license scheme is retained during the upgrade process. If an unlimited license was available, the **"IP Traffic – Test & Measure"** version 2.4 is ready to be used unlimited. If the trial version was used, the number of remaining days isn't changed: it will continue to decrease up to the final date.

Acrobat Reader is needed with **"IP Traffic – Test & Measure"** version 2.4: see 'paragraph 2.7 Acrobat Reader version compatibility' for more details.

2.4 Upgrading from "IP Traffic – Test & Measure" version 2.1

There is no need to uninstall **"IP Traffic – Test & Measure"** version 2.1 before upgrading to version 2.4. The installation procedure checks if a previous version of **"IP Traffic – Test & Measure"** was installed. When the version 2.1 is found, it updates automatically the **"IP Traffic – Test & Measure"** components.

Installation of the **"IP Traffic – Test & Measure"** version 2.4 over the **"IP Traffic – Test & Measure"** version 2.1 replaces the IPTraff.exe application and the Itsnif.sys driver by the znpf.sys driver where they have been installed. The old help file named 'User Guide IP Traffic V2.1.pdf' is replaced by the 'IP Traffic V2.4 User Guide.pdf' file. The registry content is extended with new parameters needed by the help mechanism and the "Automation Tool for IP Traffic". Finally, the DLL file "packet.dll" is replaced by a new version including ZTI extensions (only for Windows 2000/XP/Server 2003 systems).

The license scheme is retained during the upgrade process. If an unlimited license was available, the **"IP Traffic – Test & Measure"** version 2.4 is ready to be used unlimited. If the trial version was used, the number of remaining days isn't changed: it will continue to decrease up to the final date.

Acrobat Reader is needed with **"IP Traffic – Test & Measure"** version 2.4: see 'paragraph 2.7 Acrobat Reader version compatibility' for more details.

2.5 Upgrading from "IP Traffic – Test & Measure" version 2.0

There is no need to uninstall **"IP Traffic – Test & Measure"** version 2.0 before upgrading to version 2.4. The installation procedure checks if a previous version of **"IP Traffic – Test & Measure"** was installed. When the version 2.0 is found, it updates automatically the **"IP Traffic – Test & Measure"** components.

Installation of the **"IP Traffic – Test & Measure"** version 2.4 over the **"IP Traffic – Test & Measure"** version 2.0 replaces the IPTraff.exe application and the Itsnif.sys driver by the znpf.sys driver where they have been installed. The old help file named IPTraffic.chm is replaced by the 'IP Traffic V2.4 User Guide.pdf' file. The registry content is extended with new parameters needed by the help mechanism. Finally, the DLL file "packet.dll" is replaced by a new version including ZTI extensions (only for Windows 2000/XP/Server 2003 systems).

The license scheme is retained during the upgrade process. If an unlimited license was available, the **"IP Traffic – Test & Measure"** version 2.4 is ready to be used unlimited. If the trial version was used, the number of remaining days isn't changed: it will continue to decrease up to the final date.

Acrobat Reader is needed with **"IP Traffic – Test & Measure"** version 2.4: see 'paragraph 2.7 Acrobat Reader version compatibility' for more details.

2.6 Upgrading from versions 1 (including version 1.3)

An upgrade from **"IP Traffic – Test & Measure"** versions earlier than version 2.0 needs to uninstall the current version before upgrading to **"IP Traffic – Test & Measure"** version 2.4. Due to the changes in the license scheme introduced with version 2.0, the reinstallation will not keep the unlimited license information. You should contact ZTI (contact@zti-telecom.com) to get back a new unlimited license number when upgrading to version 2.4 with the new site code. Finally, the DLL file "packet.dll" is replaced by a new version including ZTI extensions (only for Windows 2000/XP/Server 2003 systems).

Context files from version 1.3 and earlier are not compatible with the version 2.4. There is no converter tool to translate versions 1's context files into version 2.4.

Acrobat Reader is needed with **"IP Traffic – Test & Measure"** version 2.4: see 'paragraph [2.7 Acrobat Reader version compatibility](#)' for more details.

2.7 Acrobat Reader version compatibility

To access the **"IP Traffic – Test & Measure"**'s help file, Acrobat Reader is required.

"IP Traffic – Test & Measure" supports Acrobat Reader version from 4.01 to 7.0 that have been tested successfully.

If the Acrobat reader version you are using is too old, you can find the latest version on the **"IP Traffic – Test & Measure"**'s CD-ROM or download it straight from the Acrobat reader's website: www.adobe.com.

PART 3 Install "IP Traffic – Test & Measure"

"IP Traffic – Test & Measure" requires less than 25 MB of free disk-space. The default settings folder is C:\Program files\IP Traffic.

The **Automation Tool for "IP Traffic – Test & Measure"** add-on software is automatically installed with "IP Traffic – Test & Measure".



** To run "IP Traffic – Test & Measure" your computer screen resolution must be at least 1024 X 768 and the DPI setting should be set up with the "Normal size (96 DPI)" value.*

** To install "IP Traffic – Test & Measure" for Windows 2000, XP and Server 2003, you must log on with your administrators rights.*



We recommend that you shutdown first your anti-virus application before installing "IP Traffic – Test & Measure".

Please note that you should mask the task bar in a 1024x768 screen resolution, so you get an optimal view of the software interface.

The default settings of "IP Traffic – Test & Measure" come with a 15-day limited license. When it reaches the deadline, "IP Traffic – Test & Measure" stops running. Go to PART 4 for more information about the license program.

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

3.1 How to install the software downloaded from the Internet



To install "IP Traffic – Test & Measure" for Windows 2000, XP and Server 2003, you must log on with your administrators rights.

If you have downloaded "IP Traffic – Test & Measure" trial version from our website, you have downloaded the "IPTraffic.zip" file including the software and the related documentation.

You must first unzip this file in a temporary directory.

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

The default settings install "IP Traffic – Test & Measure" in the following directory: C:\Program Files\IP Traffic.

The "IP Traffic – Test & Measure" installation procedure installs the following files on your hard disk:

- IP Traff.exe: program file
- "IP Traffic – Test & Measure" User Guide: PDF file (use the free version of Adobe® Acrobat® Reader® software. Available on www.adobe.com).
- Aut_IPTraff.exe: program file (Automation tool)
- Automation Tool for "IP Traffic – Test & Measure" User Guide: PDF file
- IP Traffic license help file

- Version.txt: text file that contains information about the versions and the Registry parameters.



All files created by "IP Traffic – Test & Measure" are saved in the folder where "IP Traffic – Test & Measure" has been installed.

- The following step of the installation procedure depends on the target Operating System (Windows 98 or Windows 2000/XP/Server 2003). Follow the instructions relating to your Operating System in the table below:

| Windows 98 install | Windows 2000/XP/Server 2003 install |
|--|--|
| <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 & 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 & Measure" installation procedure.</p> <p>You must then reboot 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 need to reboot your computer to consider changes.</p> |

Start Menu shortcuts created:

Start > Programs > **IP Traffic – Test & Measure**

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



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

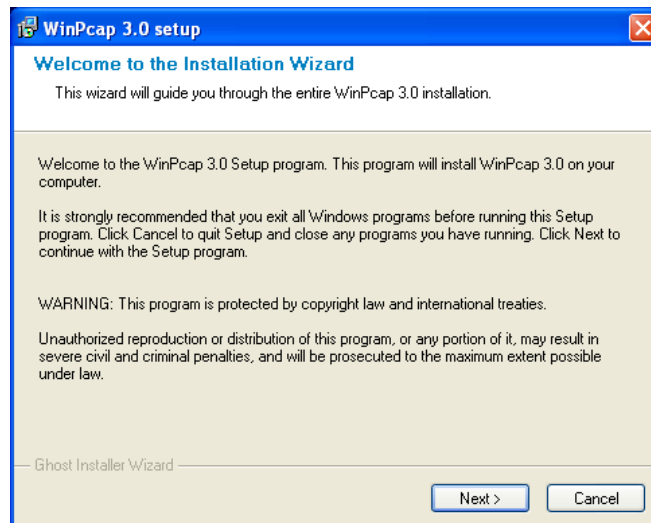
When launching a **"IP Traffic – Test & Measure"** trial version for the first time, a message is displayed showing the remaining days of use (for example, 15 days left out of 15 in the following example):



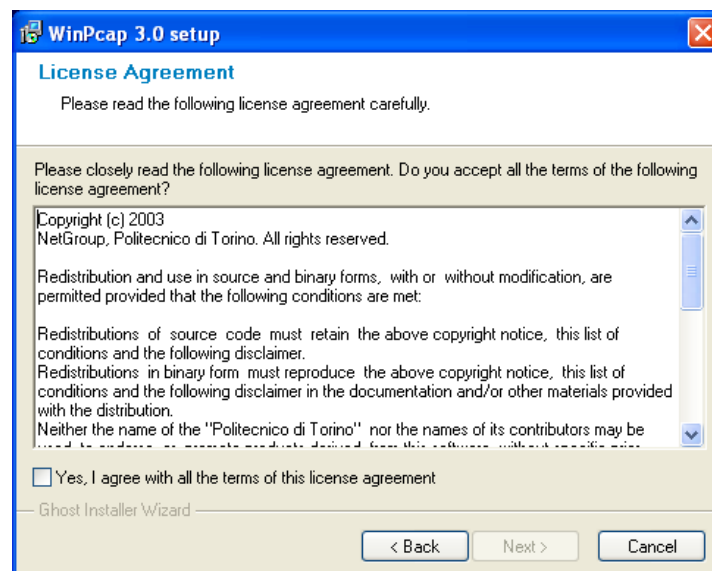
Please refer to PART 4 (Software License Configuration) to configure your unlimited license.

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

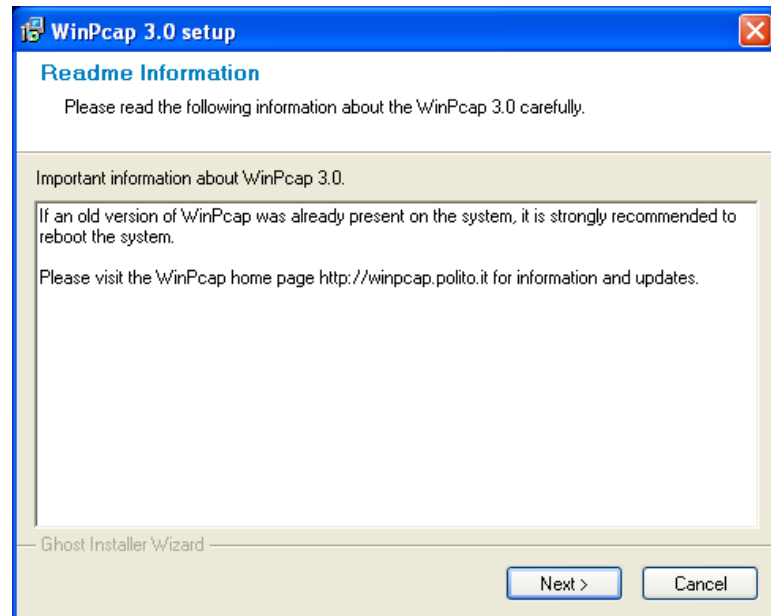
Note: The WinPcap program includes software developed by the Politecnico di Torino and its contributors.



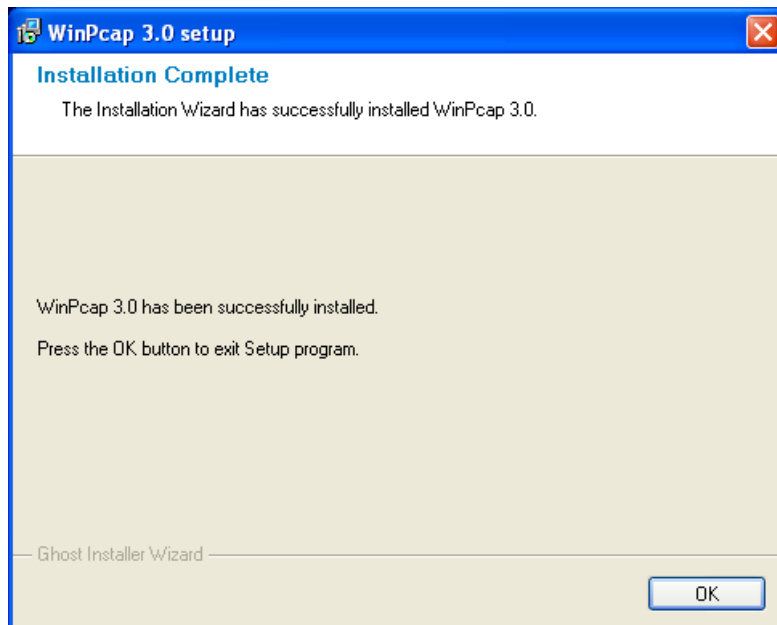
Then press Next to continue and display the License Agreement.



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



Press Next to continue.



3.2 How to install the software from the CD-ROM

The installation procedure is a standard installation program.



To install "IP Traffic – Test & Measure" for Windows 2000, XP or Server 2003, you must log on with your administrators rights.

- First, insert the **"IP Traffic – Test & Measure"** CD-ROM in your CD-ROM drive.
- Click on "Start", "Execute" and type "CD unit>: \Setup_IPTrafficBundle.exe". Follow the **"IP Traffic – Test & Measure"** setup instructions to proceed with the installation.
"IP Traffic – Test & Measure" default settings install files in the following directory:
C:\Program Files\IP Traffic.
- The following step of the installation procedure depends on the target Operating System (Windows 98 or Windows 2000/XP/Server 2003). Follow the instructions relating to your Operating System in the table below:

| Windows 98 install | Windows 2000/XP/Server 2003 install |
|--|--|
| <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 & 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 & Measure" installation procedure.</p> <p>You must then reboot 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 need to reboot your computer to consider changes.</p> |

Start Menu shortcuts created:

Start > Programs > **IP Traffic – Test & Measure**

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



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

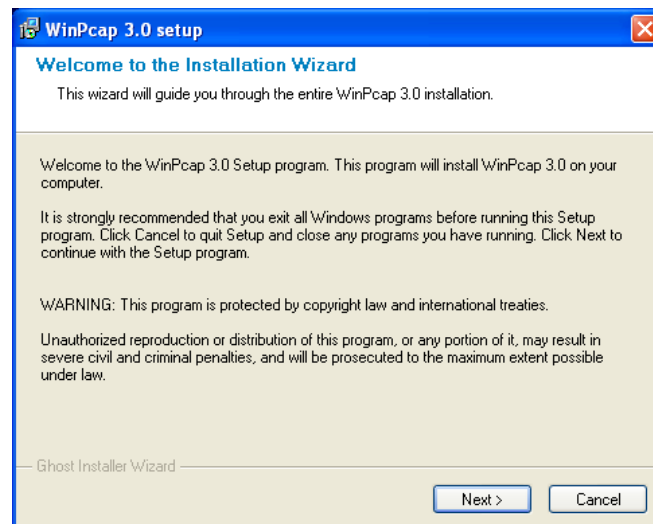
When launching **"IP Traffic – Test & Measure"** for the first time, a message is displayed showing the remaining days of use, even if you have bought an unlimited license (for example, 15 days left out of 15 in the following window):



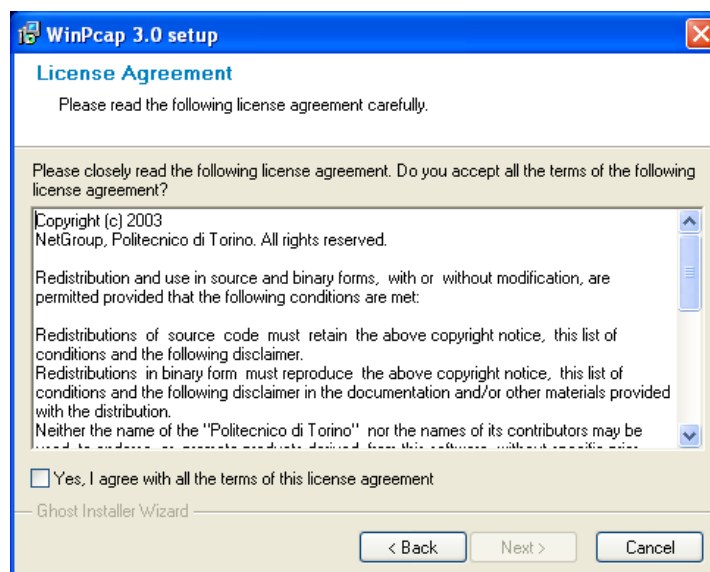
Please refer to PART 4 (Software License Configuration) to configure your unlimited license.

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

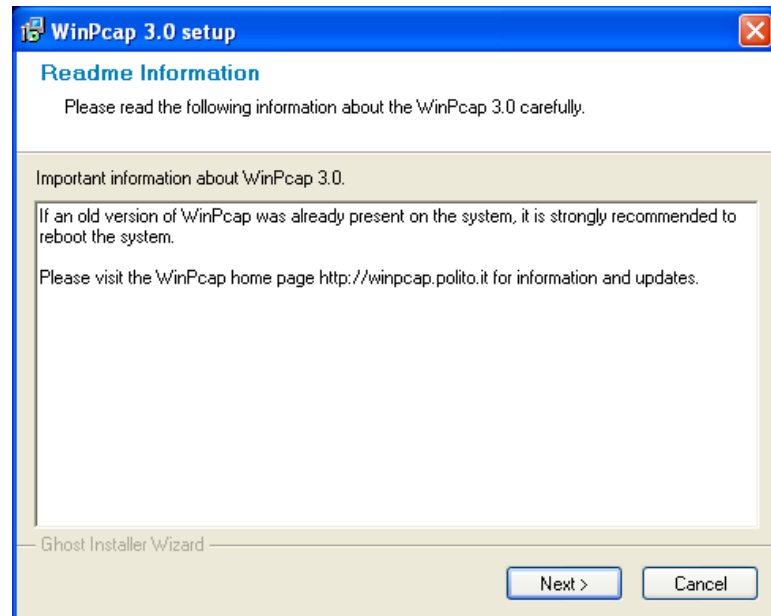
Note: The WinPcap program includes software developed by the Polytecnico di Torino and its contributors.



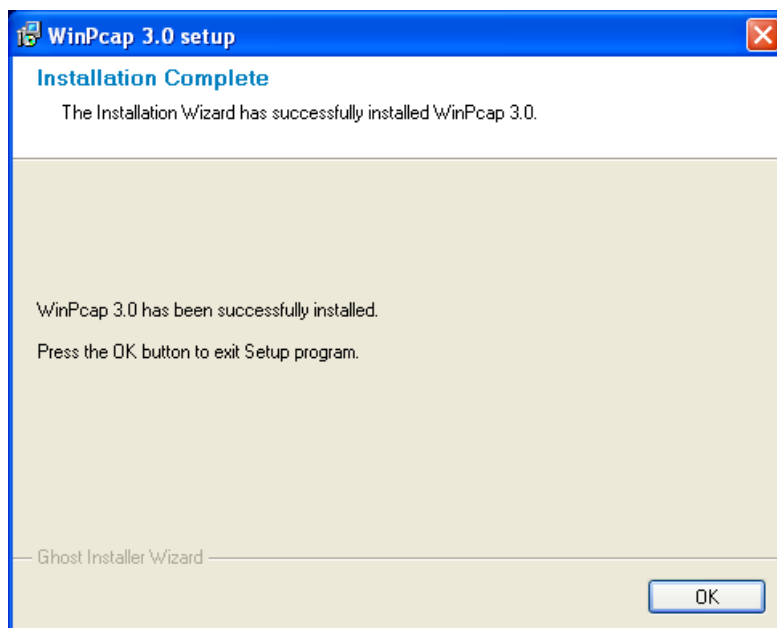
Then press Next to continue and display the License Agreement.



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



Press Next to continue.

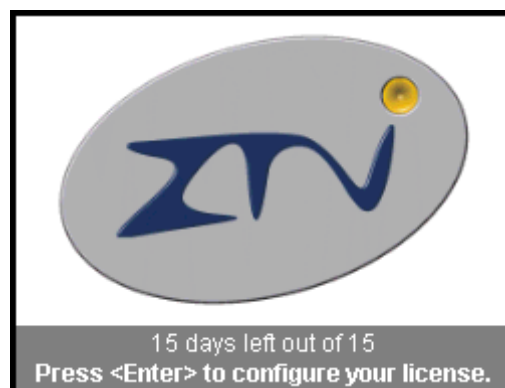


PART 4 Software License Configuration

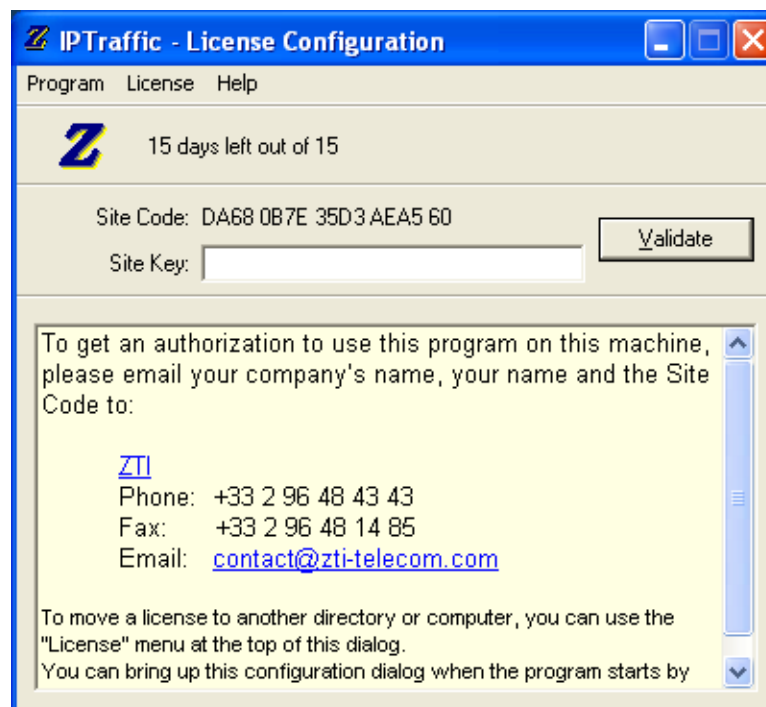
4.1 How to configure the license

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

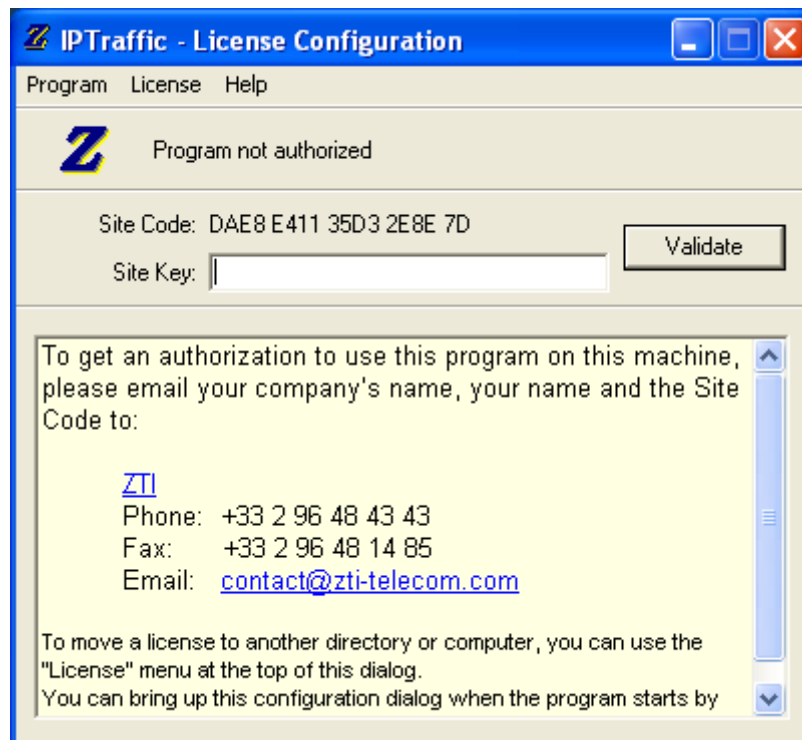
If you wish to configure your license before the trial period ends, press **Enter** just after launching the software when the following message is displayed:



You will then see the following license configuration window:



At the end of the trial period when you launch **"IP Traffic – Test & Measure"**, the same license configuration window appears, but says, "Program not authorized" instead of showing the remaining days of use.



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

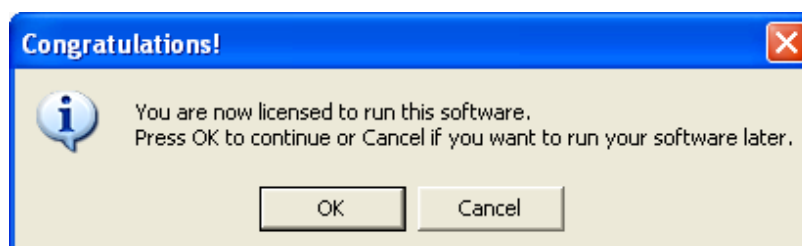
- The **Site Code** (you can copy and paste the Site Code displayed in the license window)
- The name of the software, for example: "**IP Traffic – Test & Measure**" or the "**IP Traffic – Test & Measure**" software bundle (including the **Automation Tool for "IP Traffic – Test & Measure"**)
- The OS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

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

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

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

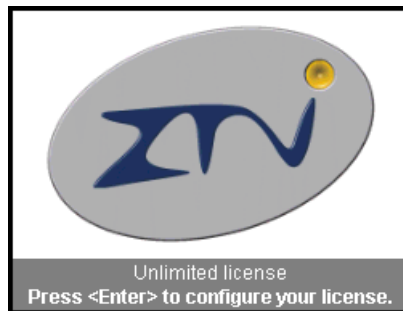
After validation of the Site Key, you will get the following message:



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



When you launch "**IP Traffic – Test & Measure**" with an unlimited license, you will see the following window:



4.2 License Transfers



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

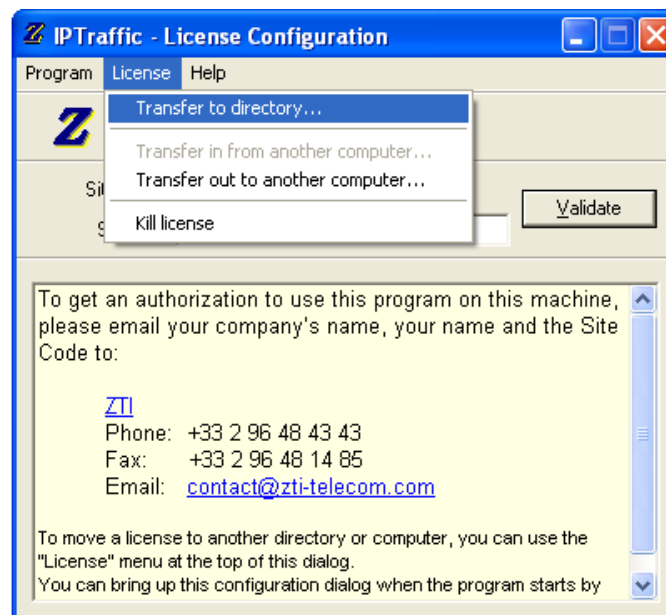
Licenses can be transferred using one of the following methods:

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

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

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

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



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

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



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

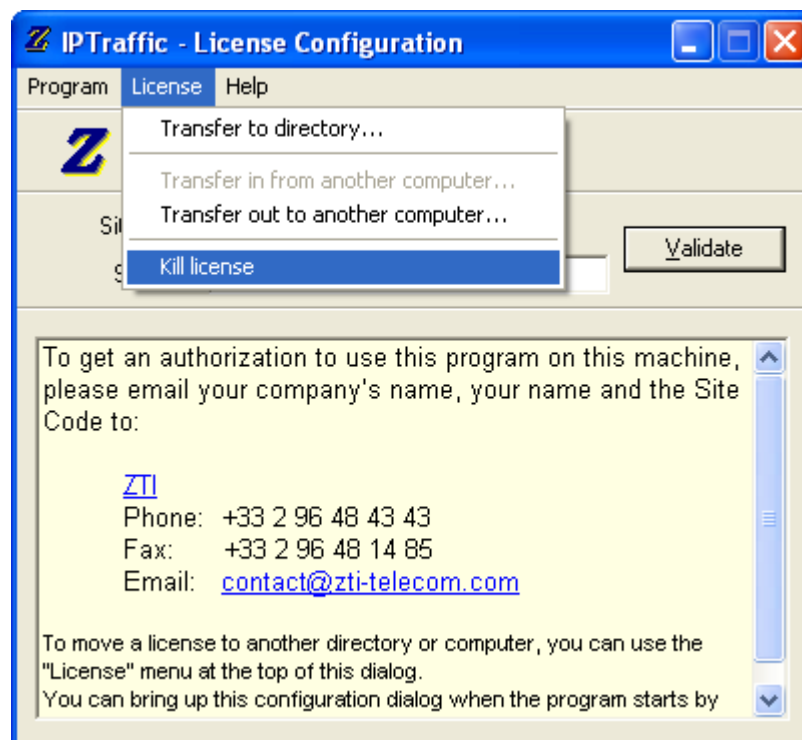
To transfer the license from the source PC (PC #1) to the target PC (PC #2), proceed as described in the following order:

- 1) First install the program on the target PC (PC # 2).
- 2) Run the software on PC # 2 and delete the trial license in order to get an unauthorized license on this PC.

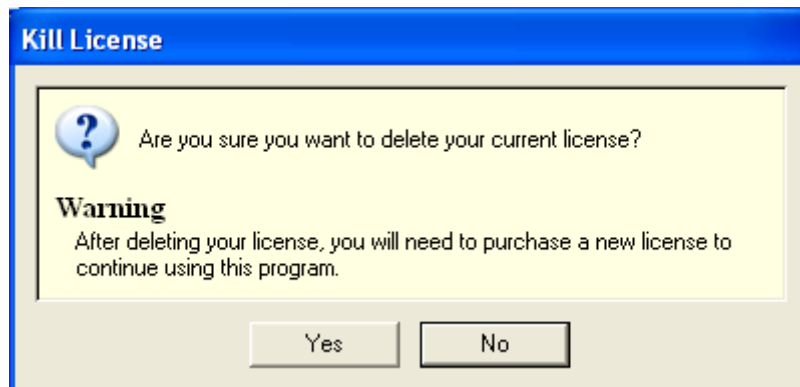
If the "Transfer in from another computer ..." item of the license menu is disabled, you must kill the license.

How to kill a license?

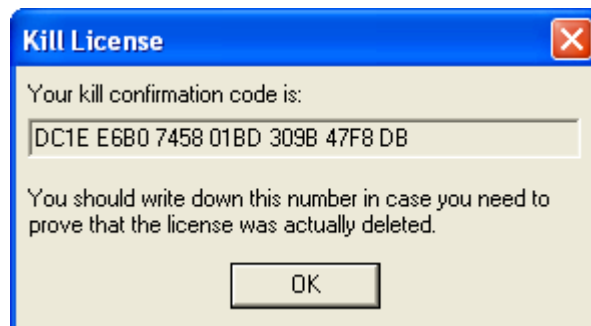
When the license configuration window appears, press **Enter** and select "License > Kill license" in the license menu.



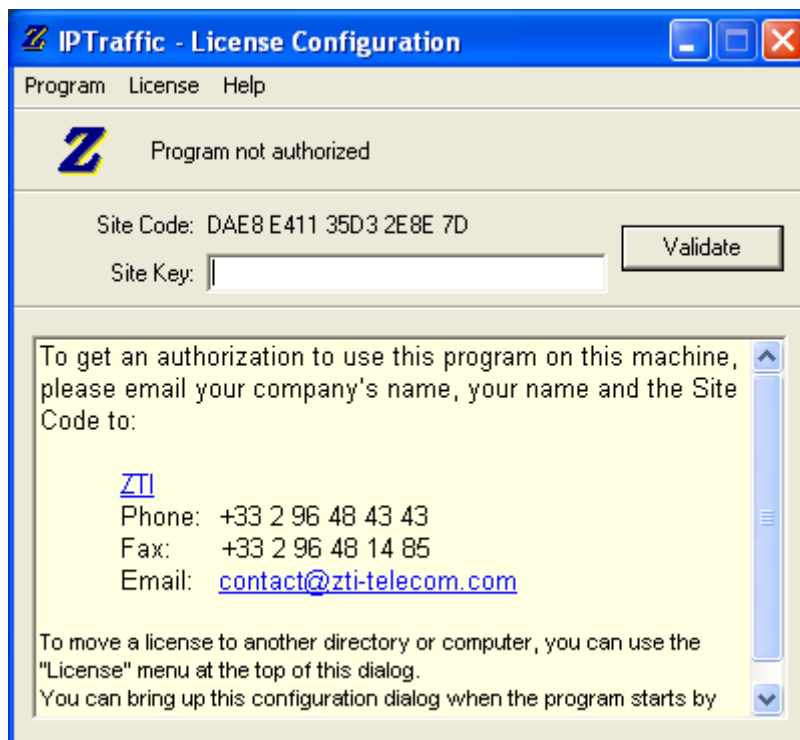
A message box will appear:



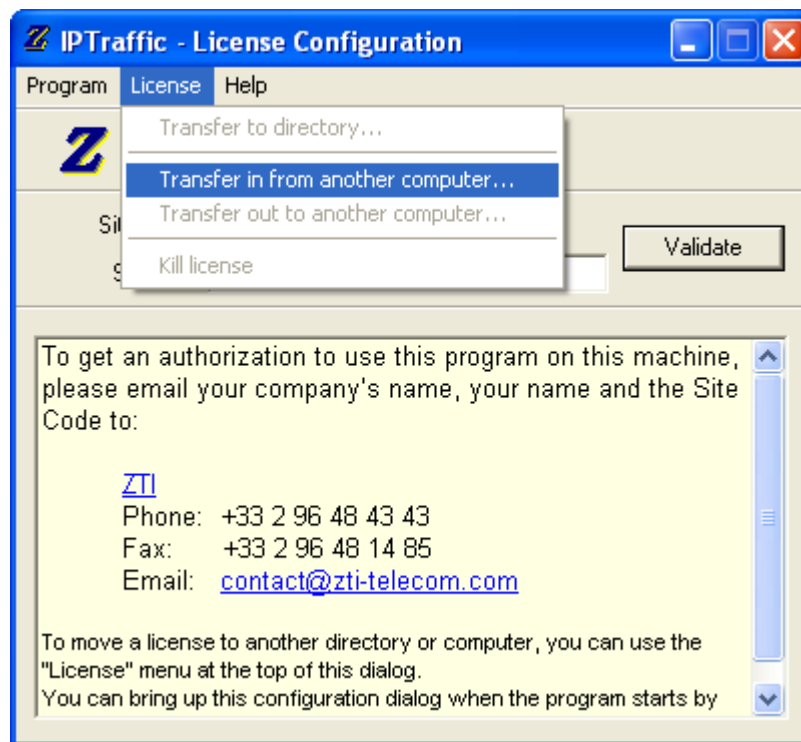
Press 'Yes' to kill the license and a confirmation code is displayed:



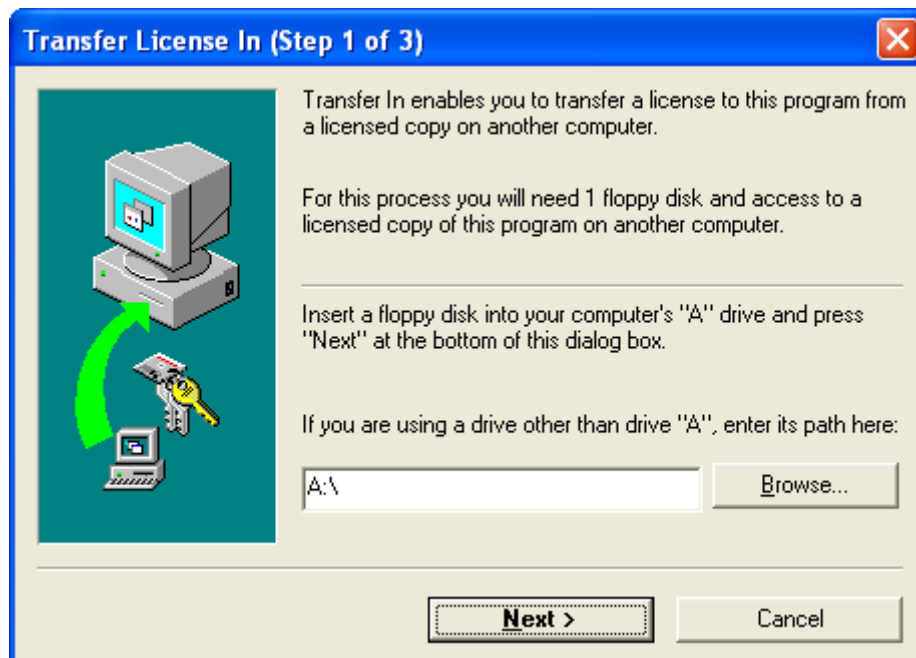
Click 'OK' and the license window displays now "Program not authorized":



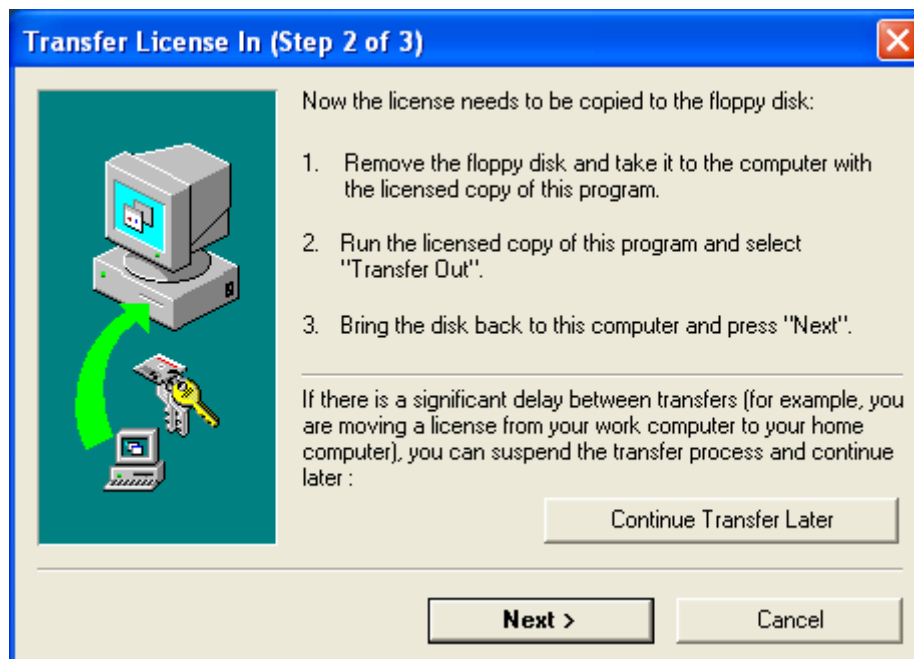
3) Select "License > Transfer in from another computer ..." from the license menu:



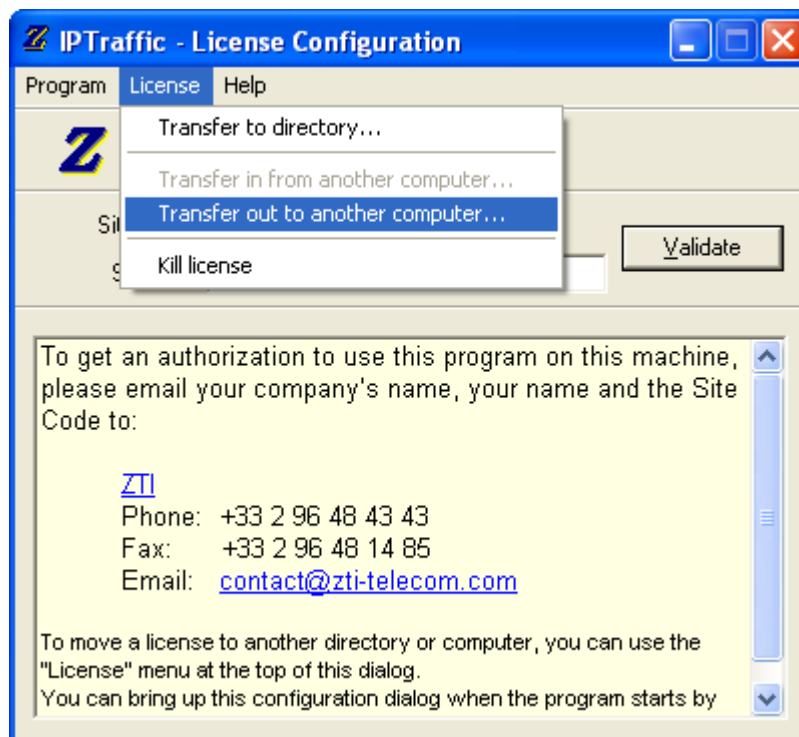
The "Transfer License In (Step 1 of 3)" window is displayed:



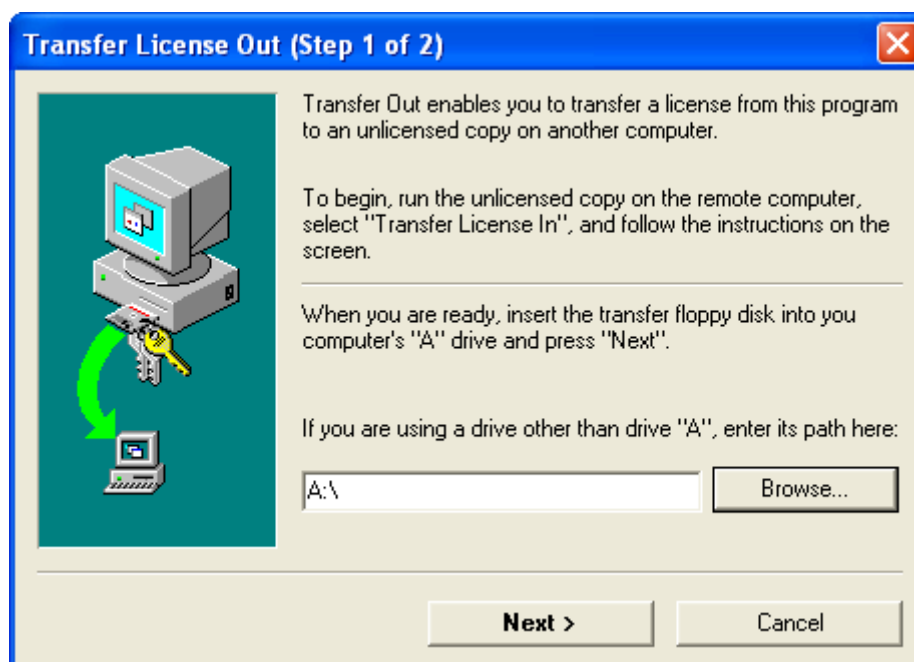
4) Insert a floppy disk or use a USB key as requested in step 1 of 3 and specify the path. Then press "Next >": the "Transfer License In (Step 2 of 3)" window is displayed:



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

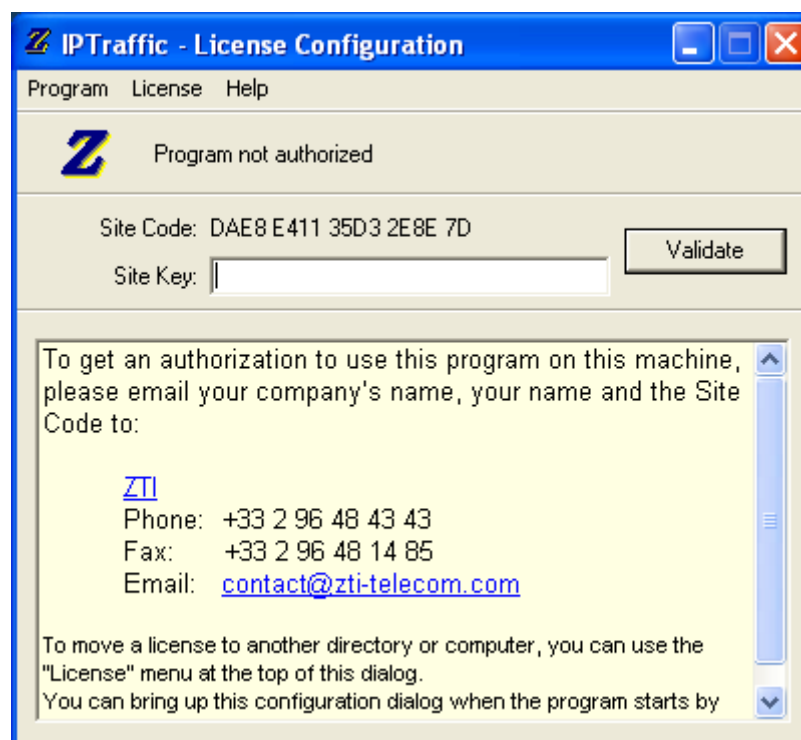


The following window is displayed:



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

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



You can check that the license is not available anymore on the source PC since the "IP Traffic – Test & Measure" software license is on a workstation basis.

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

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

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

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



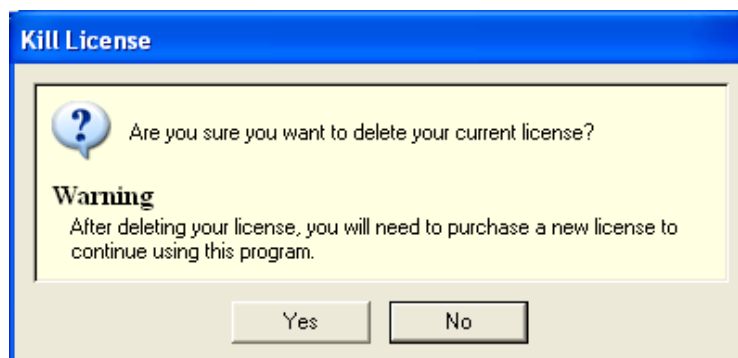
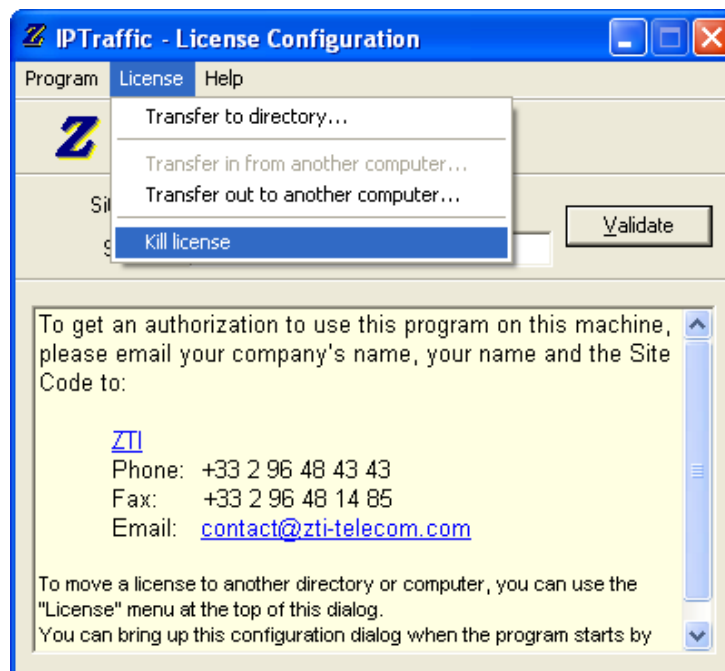
Click Finish to continue.

4.3 How to kill a license

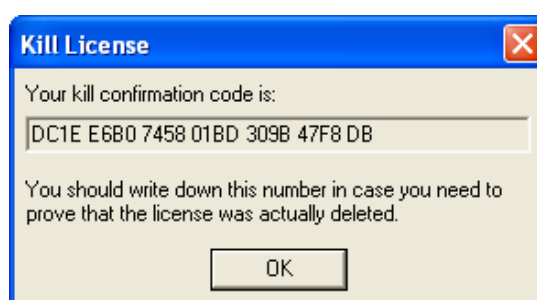
If you would like to transfer an unlimited license key onto a PC where a trial period is still active, you should first delete the active trial period. If you don't delete the active trial period, you will not be able to transfer an unlimited license.

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

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



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



PART 5 Uninstall "IP Traffic – Test & Measure"

The uninstall procedure is a standard uninstall program.

To uninstall **"IP Traffic – Test & Measure"** select "Uninstall IP Traffic – Test & Measure" in the "Start > Programs > IP Traffic – Test & Measure" menu.

| <i>Windows 98 uninstall</i> | <i>Windows 2000/XP/Server 2003 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>Then reboot your PC.</p> | <p>Then delete all remaining files in the directory "C:\Program Files\IP Traffic".</p> |

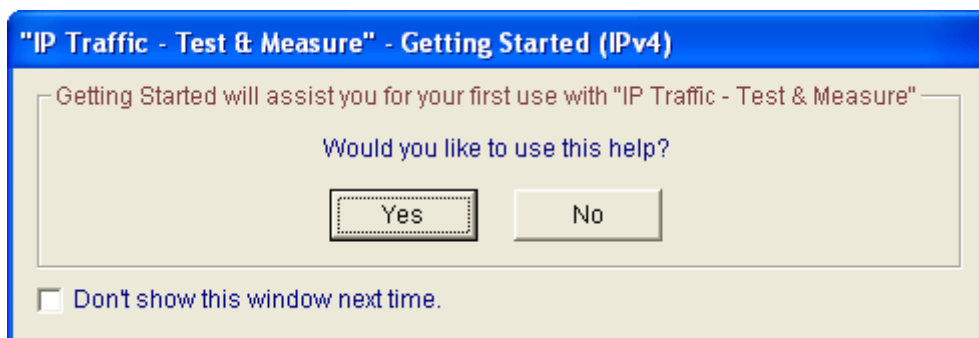
PART 6 "IP Traffic – Test & Measure" Getting Started



Anti-virus or firewall applications may disrupt **"IP Traffic – Test & Measure"** when sending or receiving data.
Please set up your security software before using **"IP Traffic – Test & Measure"** (see PART 7 and PART 8).

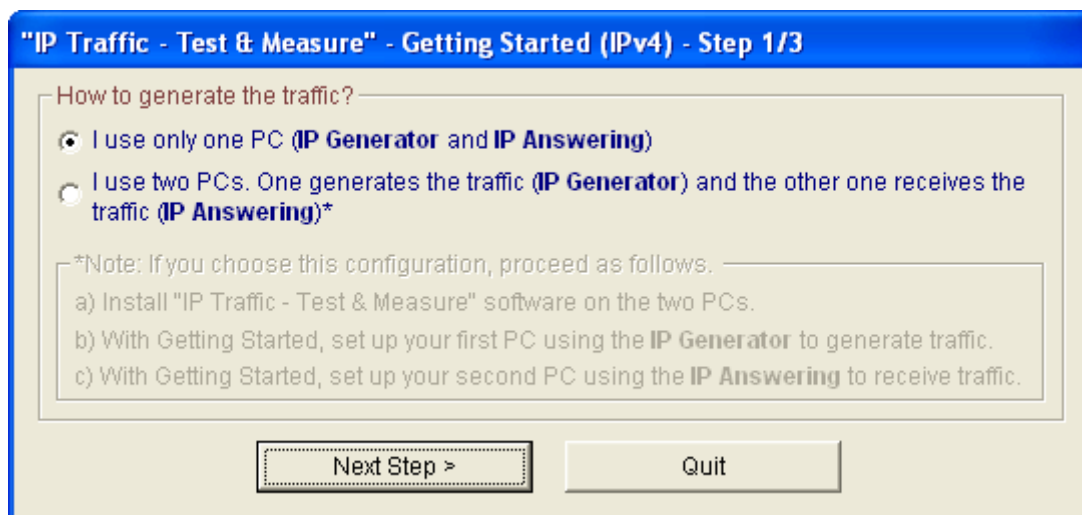
New users can use this help as an introduction to **"IP Traffic – Test & Measure"** and generate or receive traffic with the IPv4 protocol in a few clicks.

Just after launching **"IP Traffic – Test & Measure"**, the Getting Started Window is displayed:

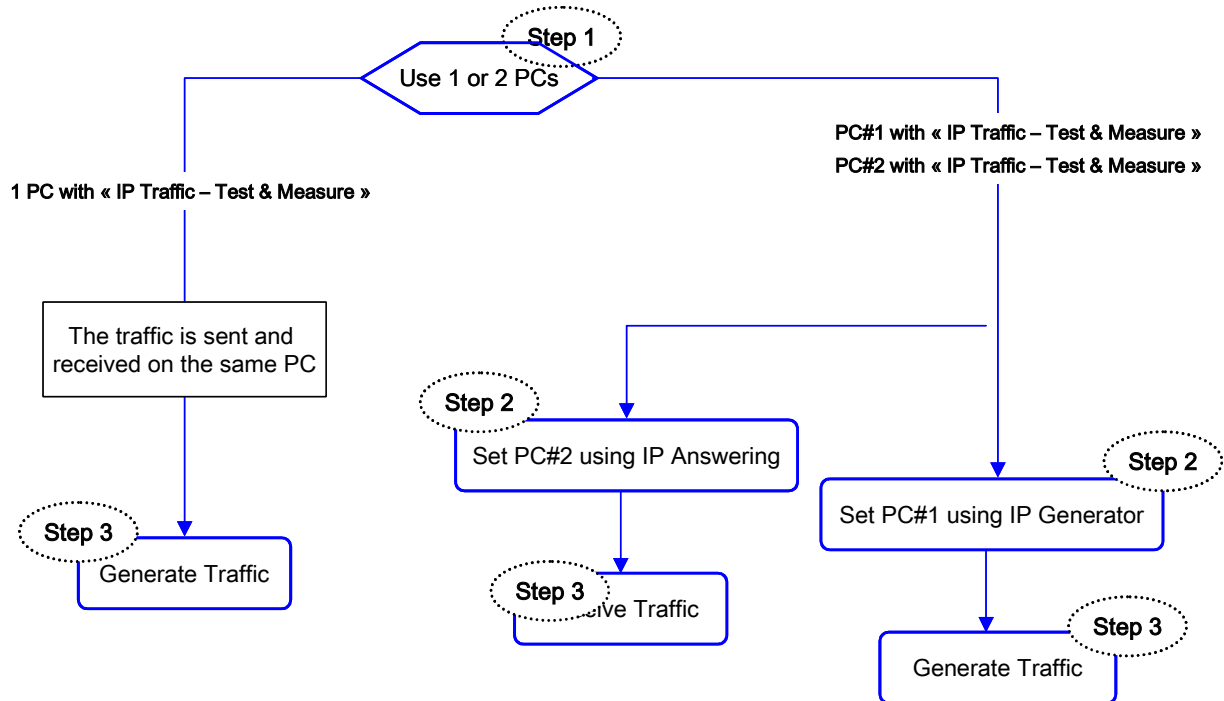


Press **No** if you don't want to use this help.

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

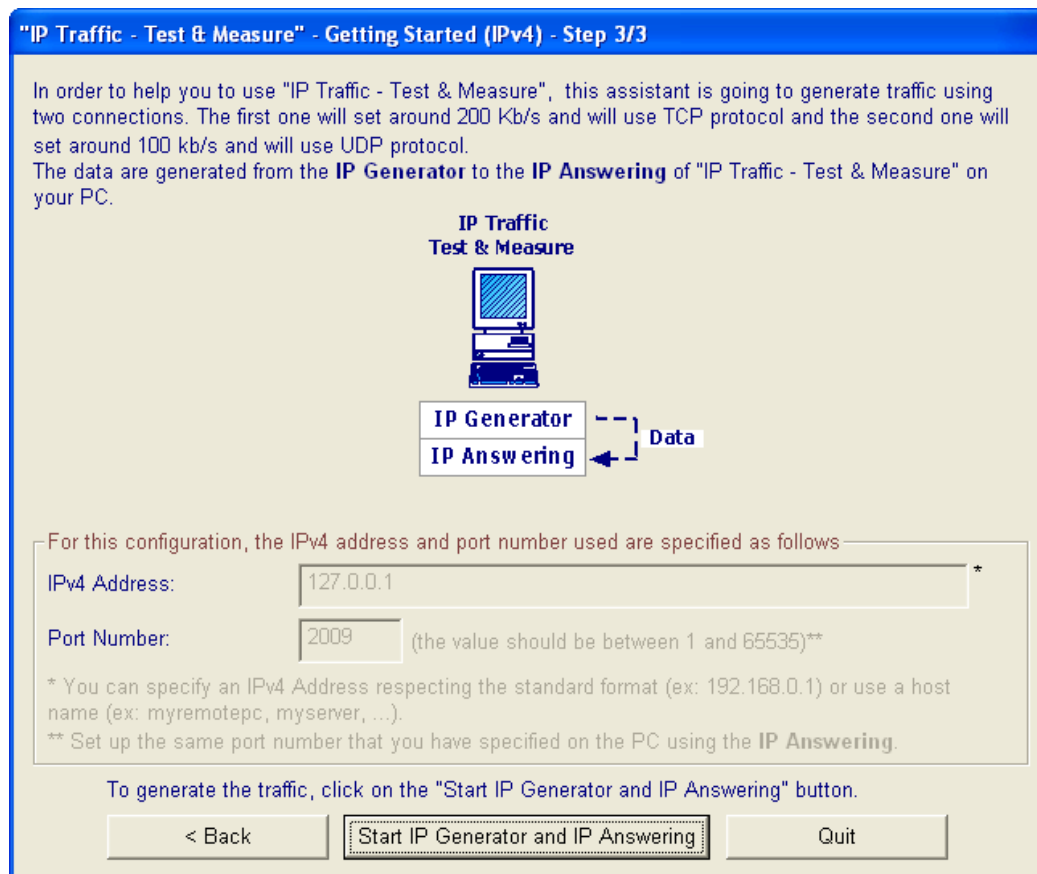


Depending on your choice to use 1 or 2 PCs, the plan below shows the steps:

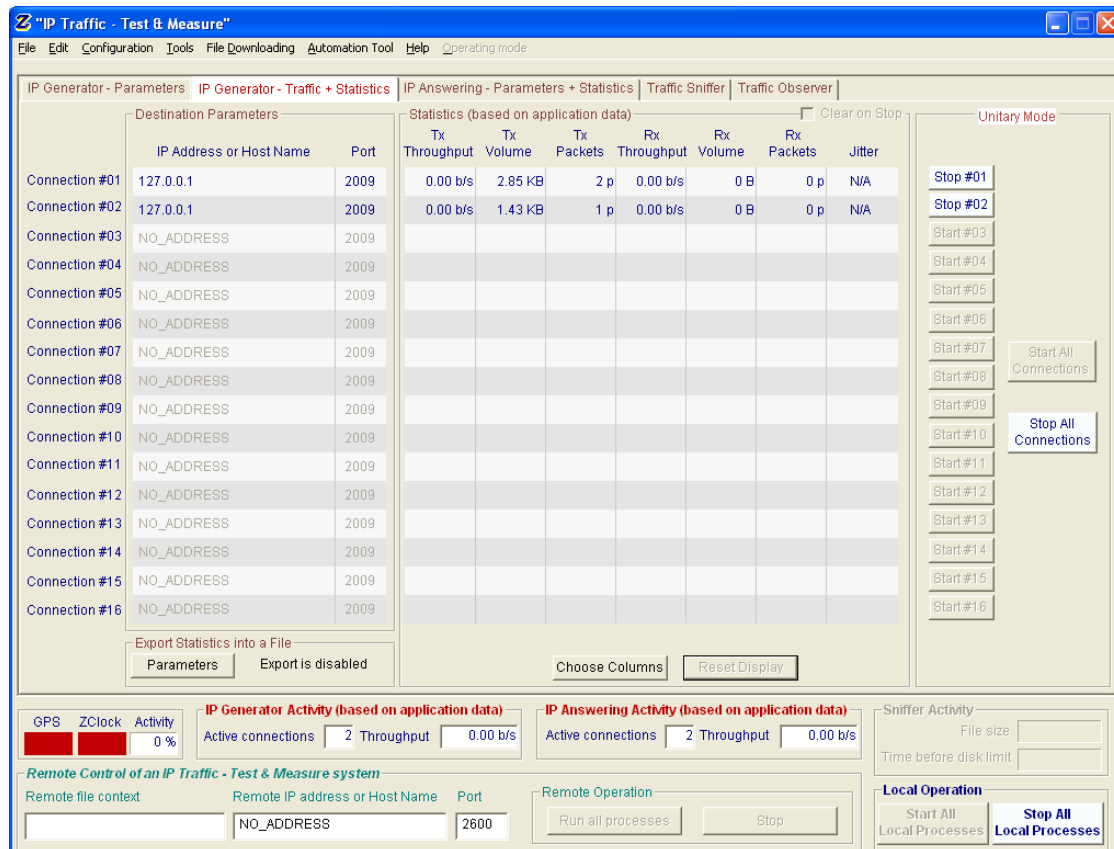


For the use of 1 PC

The following windows are displayed.



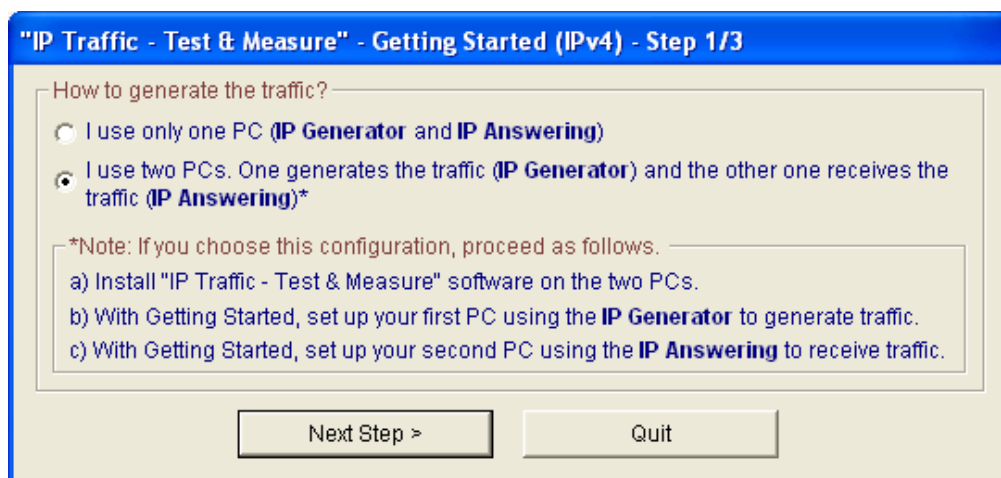
Then press the "Start IP Generator and IP Answering" button to continue. The "IP Generator – Traffic + Statistics" tab of **"IP Traffic – Test & Measure"** will display the two first active connections as shown on the following window:



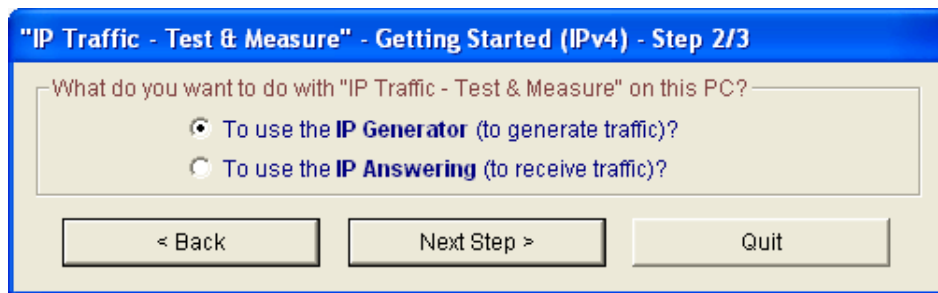
For the use of 2 PCs

If you select the option: **I use two PCs**, read the following instructions.

"IP Traffic – Test & Measure" must be installed on the two PCs.

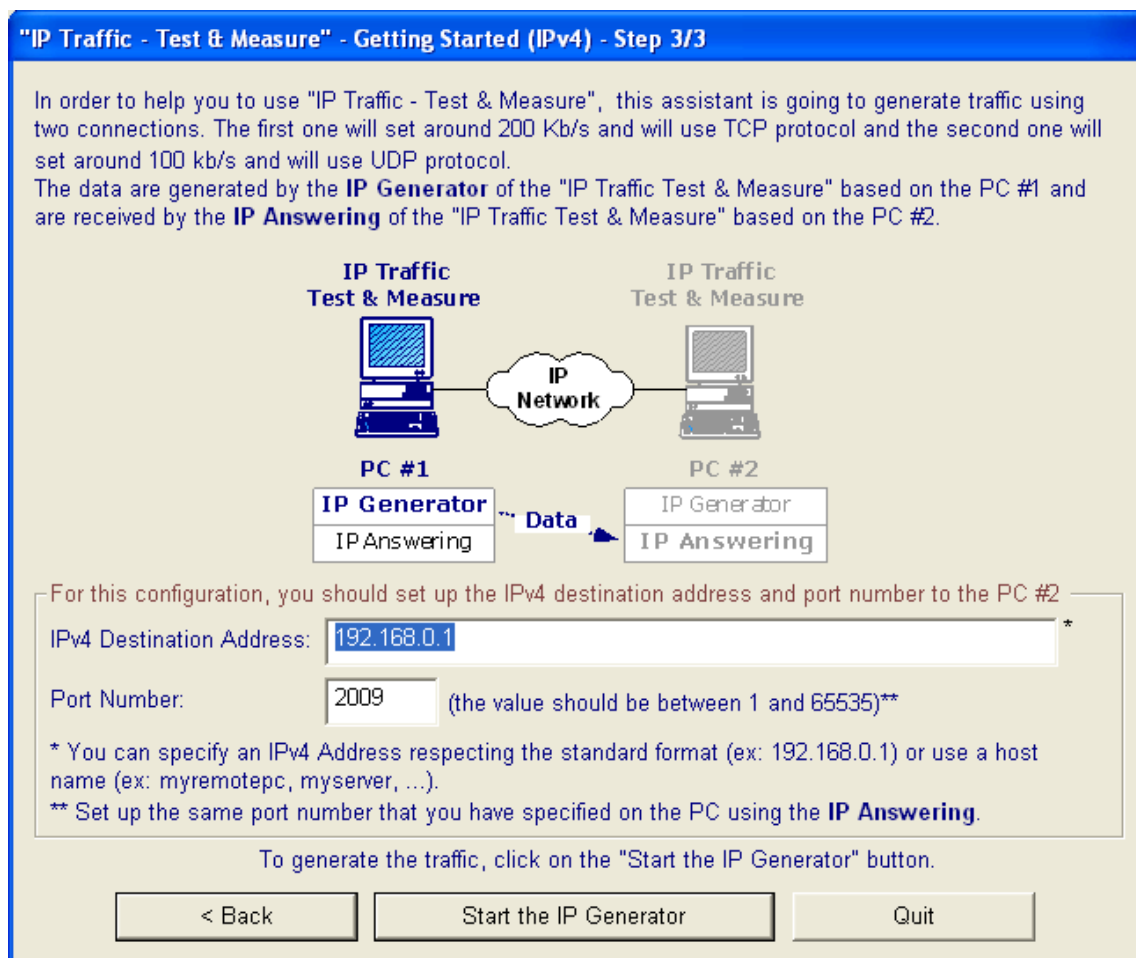


Press "Next Step >" to continue.



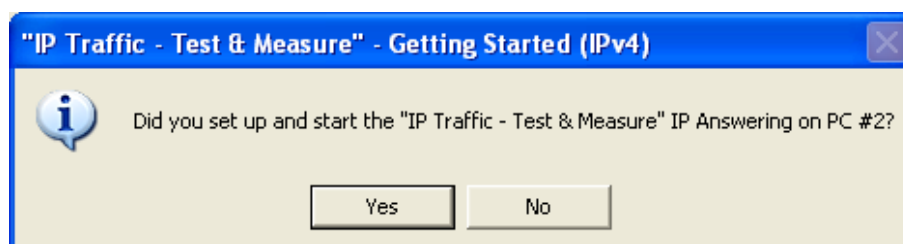
Then choose if you want to generate or receive the traffic on this PC.

If you select "Use the IP Generator" the following window will appear:

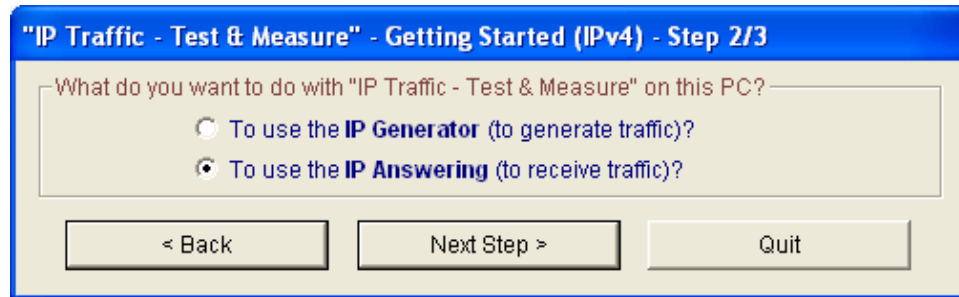


Define the IPv4 address and port number to use.

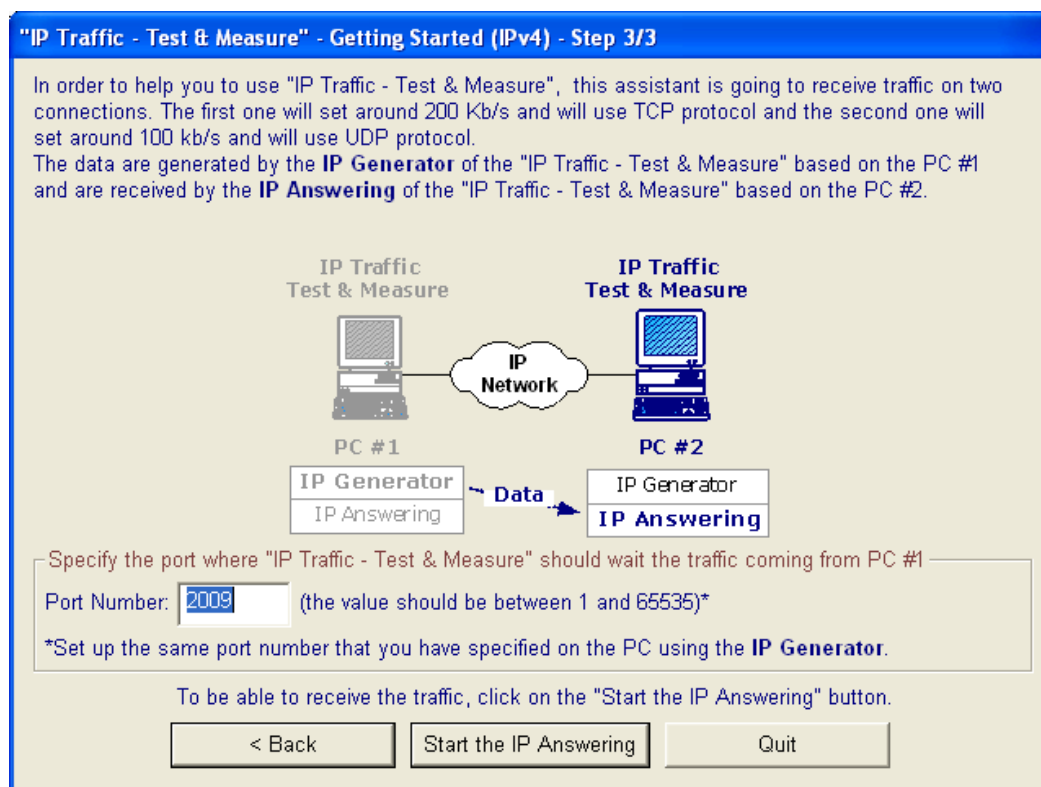
Then press the "Start the IP Generator" button and a warning dialog is displayed:



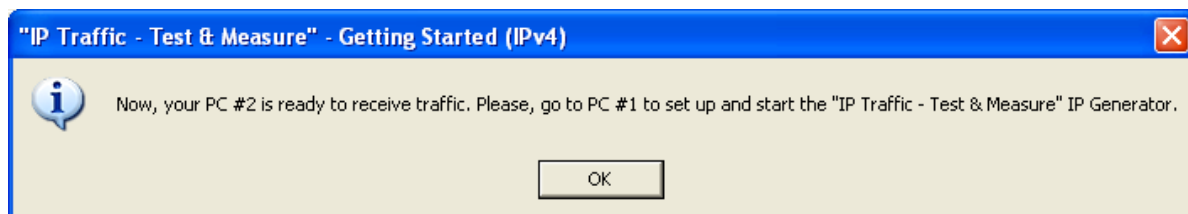
Before generating traffic towards PC # 2, the PC # 2 must be configured as IP Answering.



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



After pressing the "Start the IP Answering" button, a warning message will appear:



Press "OK" and the "IP Answering – Parameters + Statistics" tab of **"IP Traffic – Test & Measure"** is displayed on PC # 2.

Then go to PC # 1 and start the **"IP Traffic – Test & Measure"** IP Generator. The "IP Generator–Traffic + Statistics" tab of **"IP Traffic – Test & Measure"** displays now the two first active connections.

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

PART 7 Run "IP Traffic – Test & Measure"

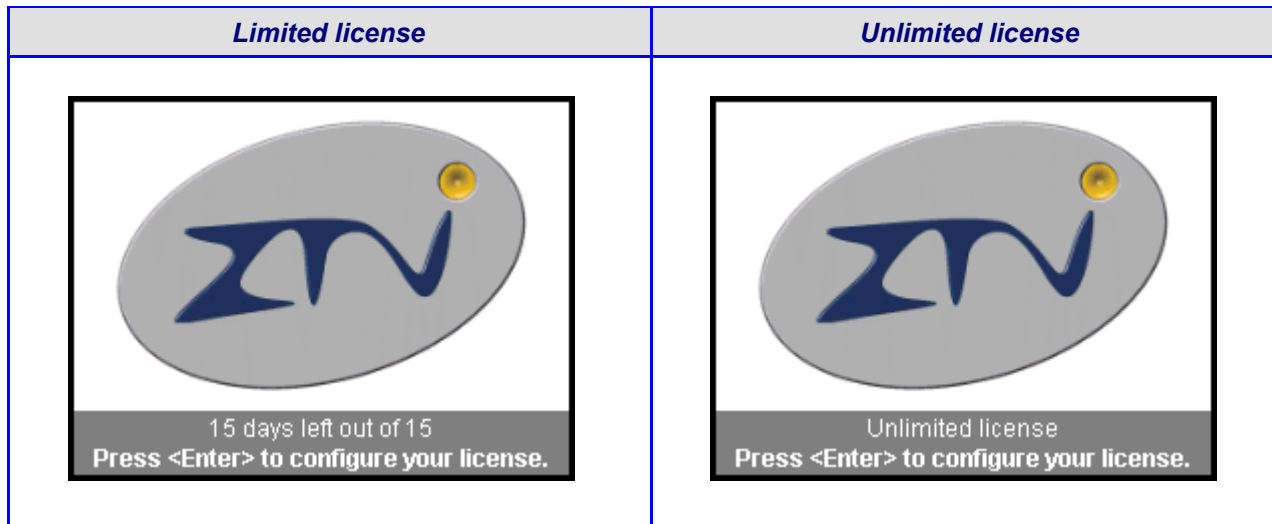
Use the Windows start menu:

Start ► All Programs ► IP Traffic –
Test & Measure ►



Click
here.

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



Press **Enter** only if you need to configure your license.

If you don't, allow a few seconds for the main window of **"IP Traffic – Test & Measure"** to open.

With Windows XP Service Pack 2, the window below may appear.

This window allows configuring the Windows Firewall settings for **"IP Traffic – Test & Measure"**. Click on the "Unblock" button to add **"IP Traffic – Test & Measure"** into the authorized programs list.



PART 8 "IP Traffic – Test & Measure" / Windows Firewall



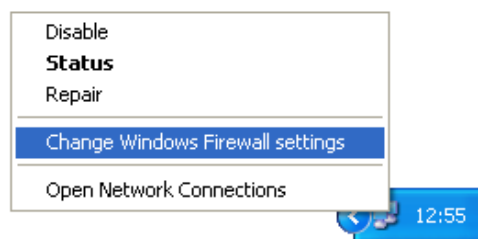
Anti-virus or firewall applications may disrupt **"IP Traffic – Test & Measure"** from sending or receiving data. Please set up your security software before using **"IP Traffic – Test & Measure"**.

Some anti-virus configurations can stop **"IP Traffic – Test & Measure"** working because of their security settings. For commercial anti-virus, please refer to the related documentation to authorize **"IP Traffic – Test & Measure"**.

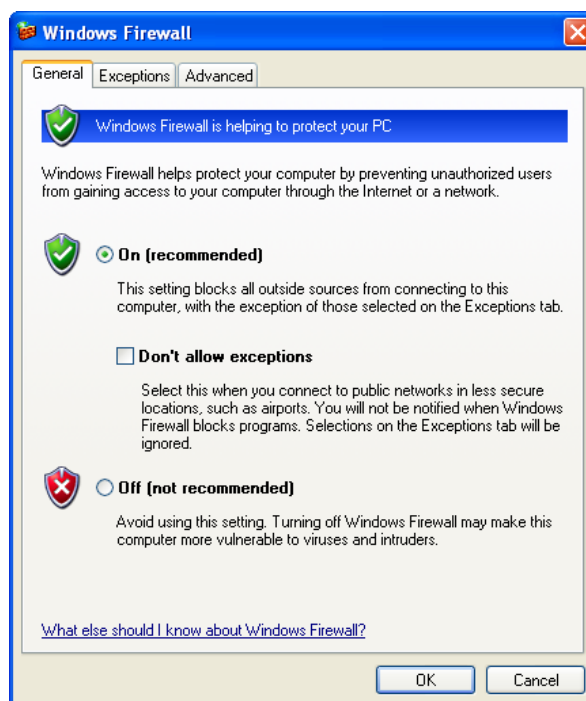
8.1 Configuration for UDP, TCP connections and ICMP IPv4

See below how to configure the Windows Firewall included in Windows XP Service Pack 2 or in Windows Server 2003 to use UDP & TCP connections for IPv4 and IPv6, and the ICMP (IPv4) connections.

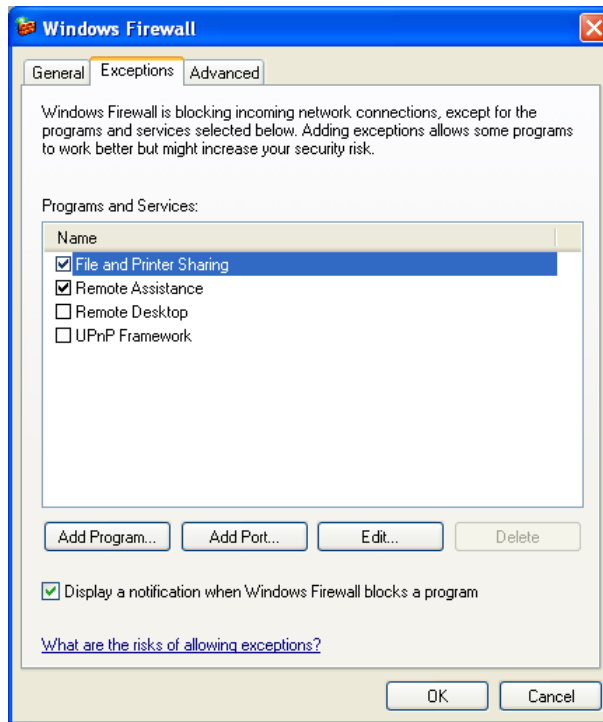
1. Open the Windows Firewall settings window by right clicking on the two computers representing the network interface that **"IP Traffic – Test & Measure"** will use.



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

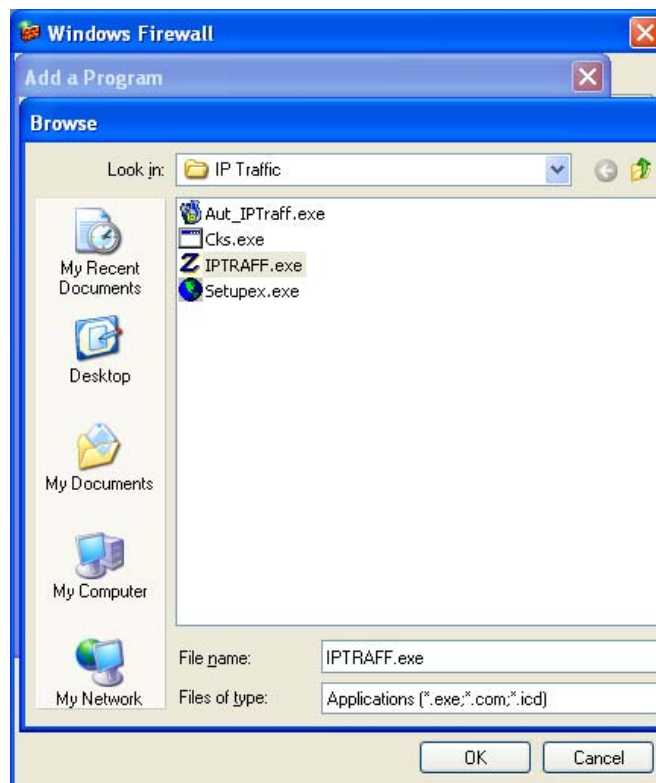


3. First switch on the "Exceptions" tab.

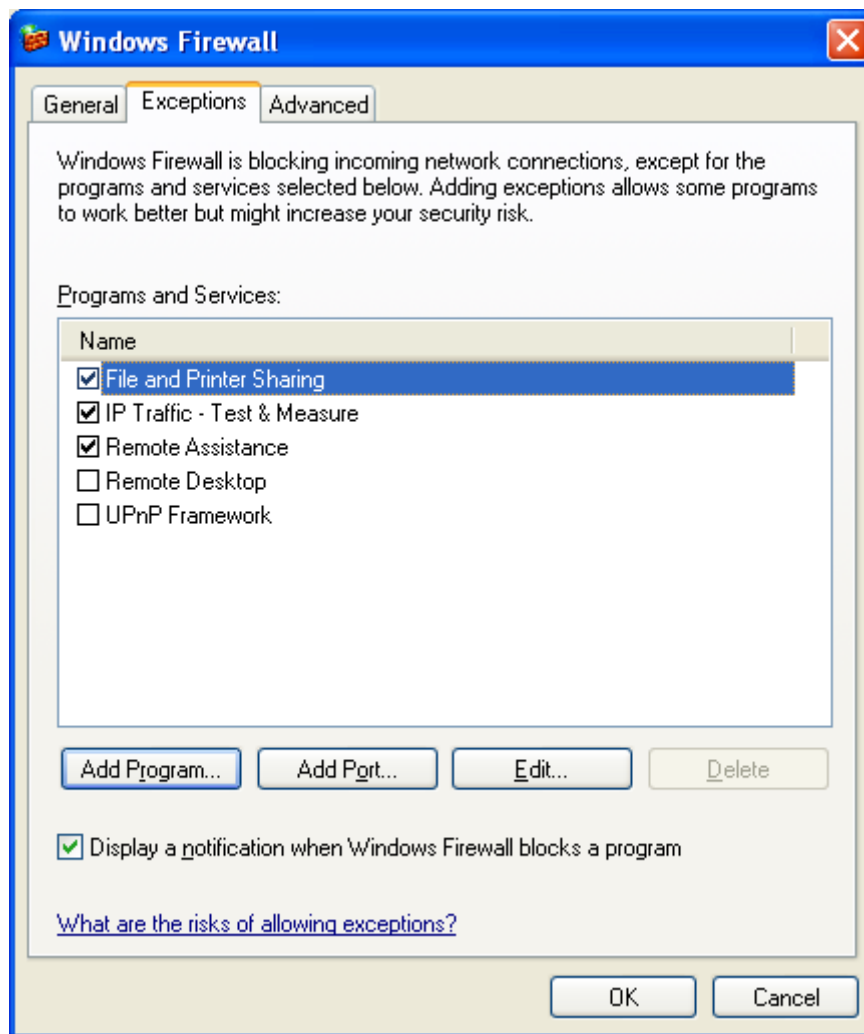


If **"IP Traffic – Test & Measure"** is already in the list, just select it by checking the box and press "OK".

If **"IP Traffic – Test & Measure"** is not in the list, click on the "Add Program ..." button. Then click on the "Browse" button and add it by selecting the IPTraff.exe file placed in the installation directory (default settings: "[Drive]:\Program Files\IP Traffic\").



4. Then select **"IP Traffic – Test & Measure"** into the program list and press "OK".



Now **"IP Traffic – Test & Measure"** is allowed to use ports, generate and receive TCP and UDP IPv4 and IPv6 traffic, including ICMP (IPv4). Click "OK" to save the new settings.

8.2 Configuration for ICMP IPv6 connections

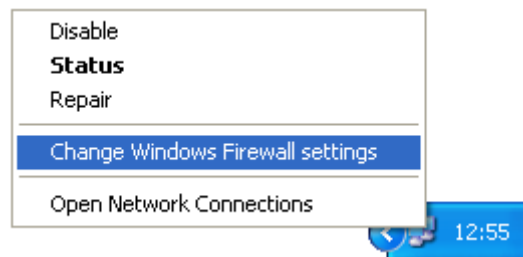


The use of the ICMP IPv6 connection requires disabling the Windows Firewall before using "IP Traffic – Test & Measure".

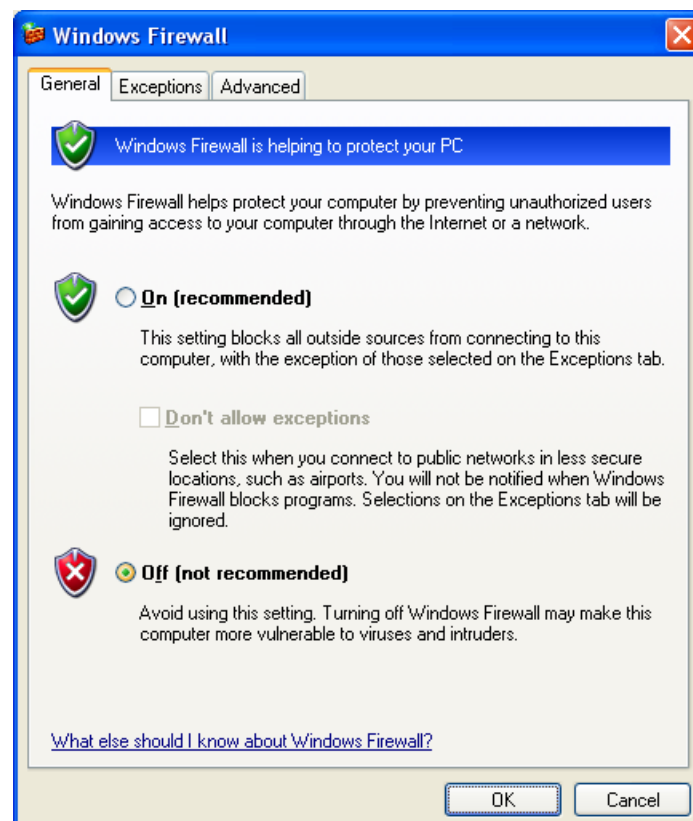
By disabling the Windows Firewall, you enable the TCP, UDP and ICMP (IPv4) connections as described in the paragraph 8.1 .

See below how to disable the Windows Firewall included in Windows XP Service Pack 2 or in Windows Server 2003 to use ICMP IPv6 connections, as well as TCP, UDP and ICMP (IPv4) connections.

1. Open the Windows Firewall settings window by right clicking on the two computers representing the network interface that **"IP Traffic – Test & Measure"** will use.



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



8.3 How to configure a firewall (list of the ports used)

To be able to quickly configure a firewall, a list of the port number and protocols used by **"IP Traffic – Test & Measure"** is shown hereafter. Note also the user can redefined all ports used by **"IP Traffic – Test & Measure"**.

| Functionality | Port Number | Protocol | IP Version |
|---|-------------|------------|--------------|
| Remote Mode* | 2600 | TCP | IPv4 & IPv6 |
| File Downloading* | 2500 | TCP | IPv4 & IPv6 |
| RPC Server (used to dialog with the Automation Tool)* | 1001 | TCP | IPv4 |
| Source port number (IP Generator) | 1 to 65535 | TCP or UDP | IPv4 or IPv6 |
| Destination port Number (IP Generator) | 1 to 65535 | TCP or UDP | IPv4 or IPv6 |
| Listening to ... (IP Answering) | 1 to 65535 | TCP or UDP | IPv4 or IPv6 |
| Ping Mode(IP Generator) | - | ICMP | IPv4 or IPv6 |

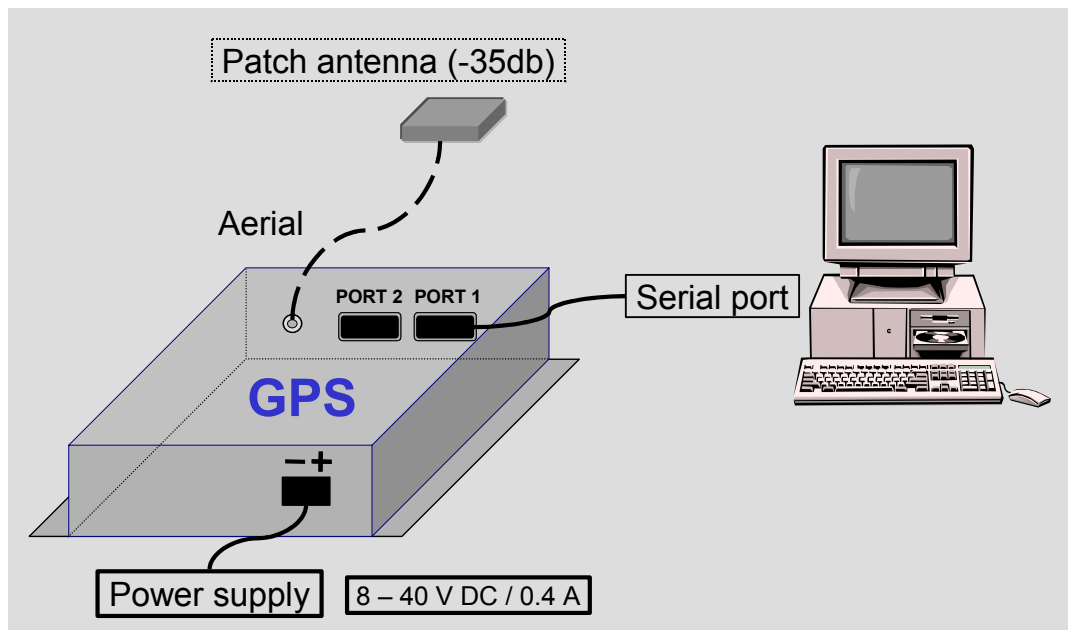
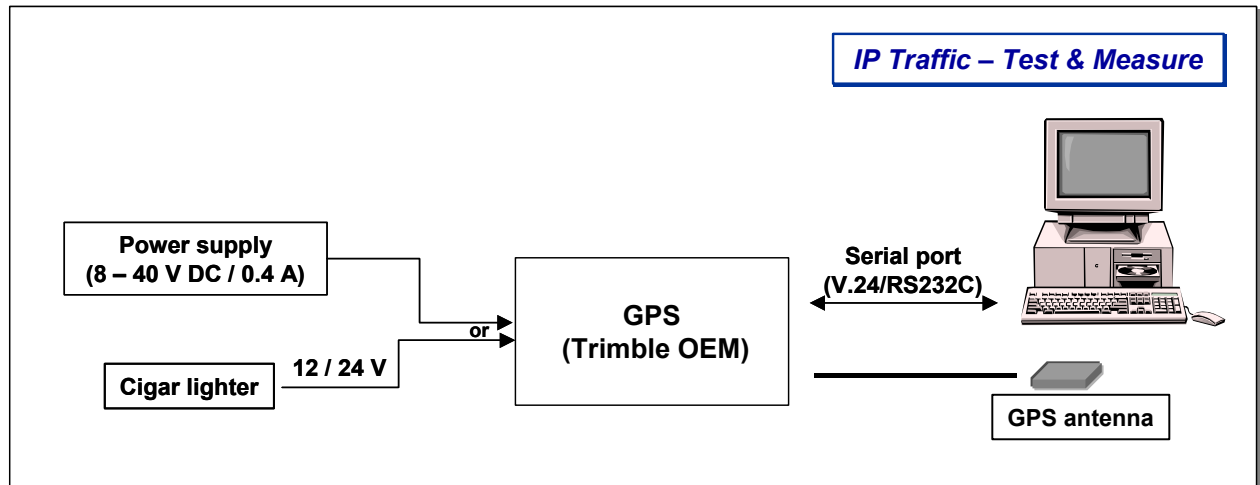
* These ports are opened when the software starts. For the functionalities using IPv4 and IPv6, two ports are opened (one using IPv4 and one using IPv6).

PART 9 Hardware Installation (GPS Kit and ZClock)

9.1 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: ± 500 nanoseconds).

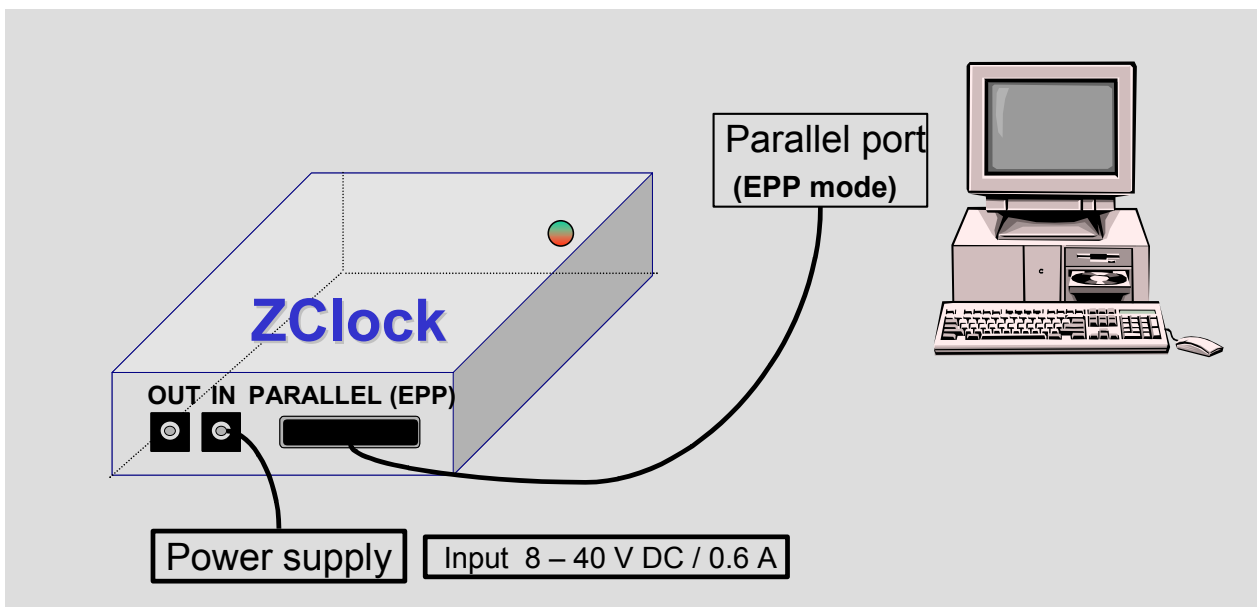
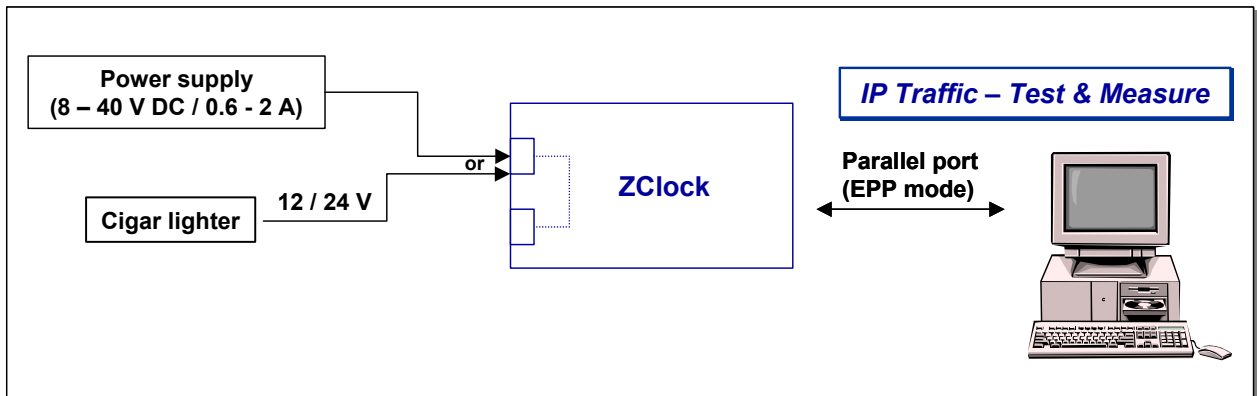
By using this GPS kit (Trimble OEM), the accuracy for IP packets time stamping is ≤ 5 milliseconds.



9.2 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, but a relative time. The user can use an external system in order to provide an absolute 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 ± 1 millisecond.

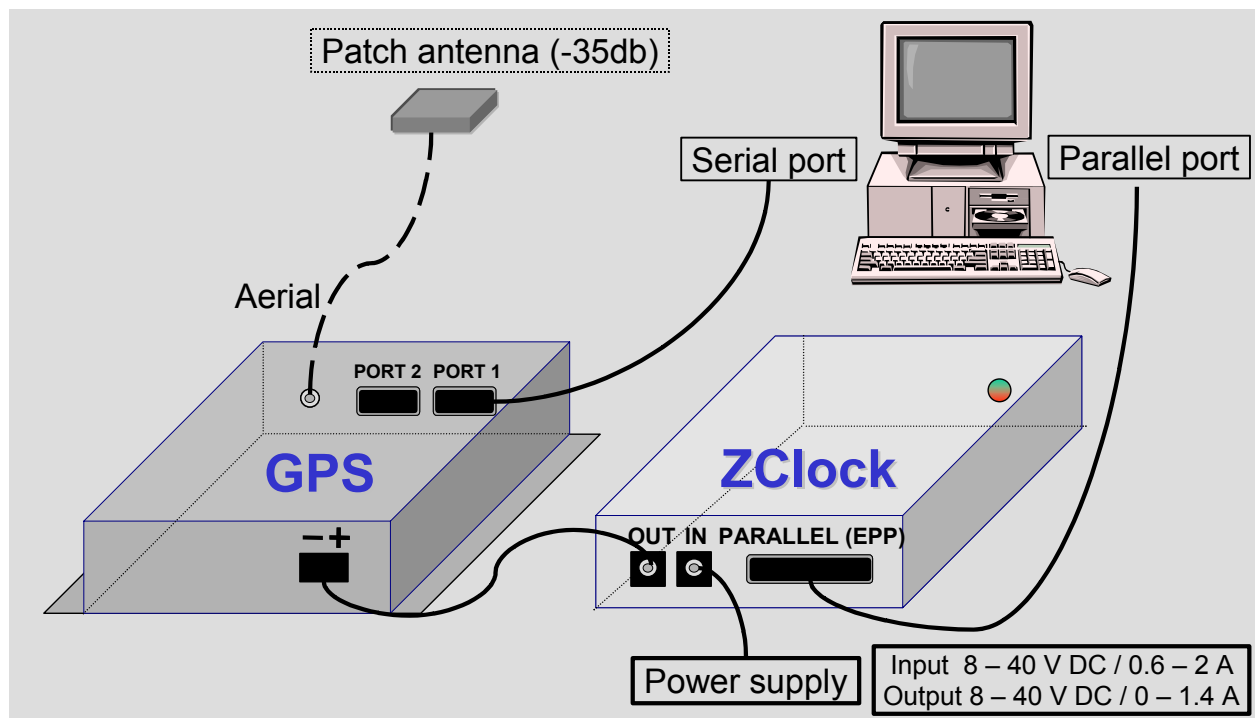
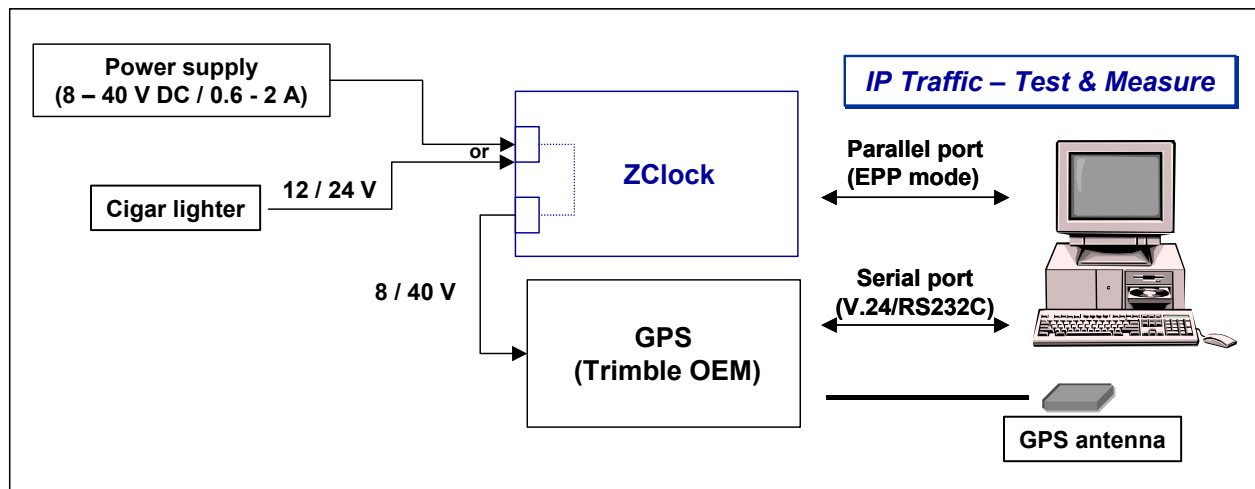


9.3 Configuration 3: "IP Traffic – Test & Measure" + GPS Kit + ZClock

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: ± 500 nanoseconds).

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

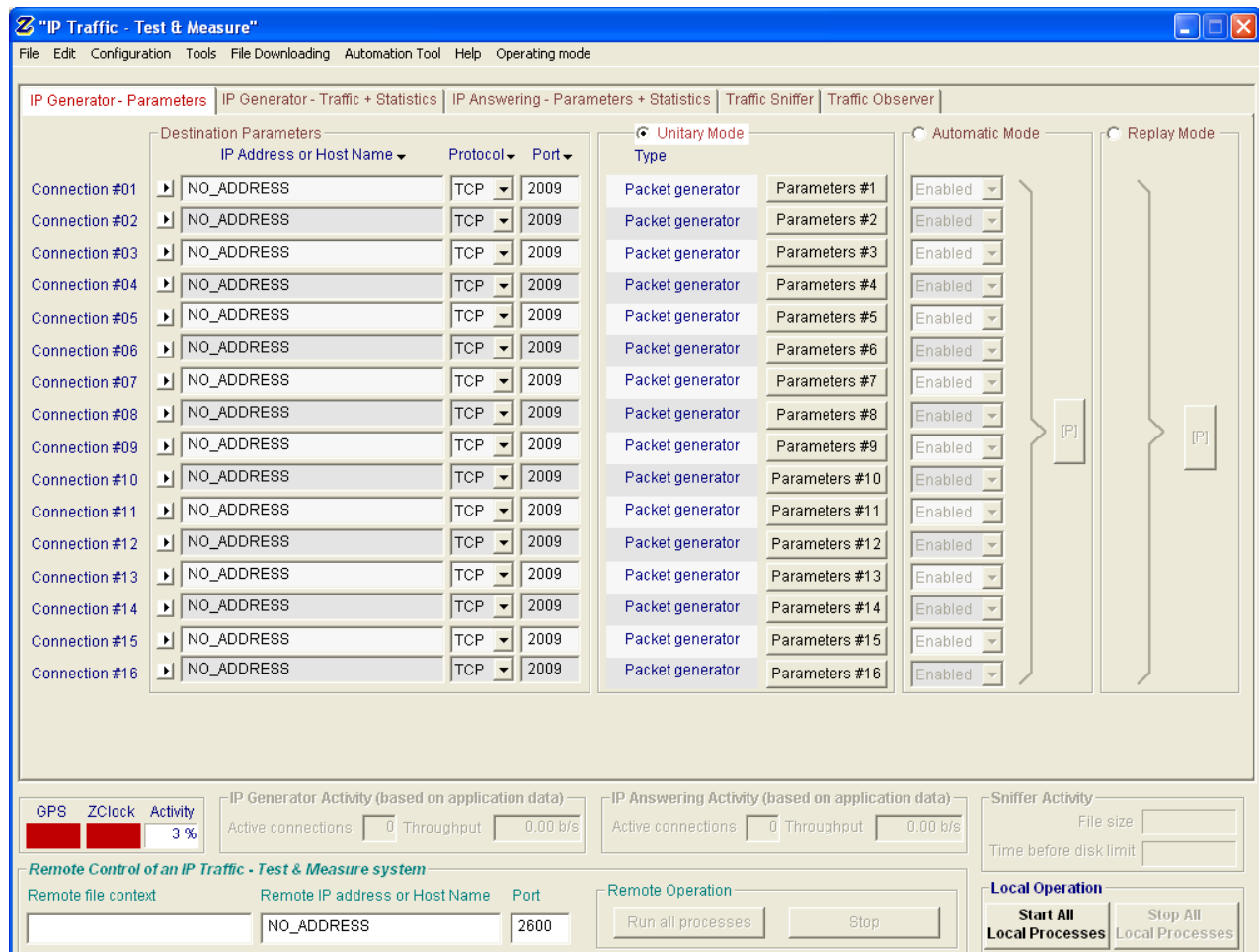
The GPS time reference is used to initialize ZClock. By using the GPS and ZClock, time stamping of IP packets by the Traffic Sniffer is made with an accuracy of ± 1 millisecond.



PART 10 Graphical User Interface

10.1 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 see a tab, click on the tab title you want to display.
- **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.

10.2 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 you can enter values

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

- Statistics fields

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

When a statistic value cannot be computed, "N/A" for Not Applicable is displayed in the field.

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

These fields are filled automatically by **"IP Traffic – Test & Measure"** further to use enter or parameters selection. They are displayed as reminder and will be modified by another user action.

These fields are recognizable by black writing on gray background.

- Fields turned out of reach further to user action

User actions and parameters selection may turn some **"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. You must stop the connection in order to change the parameters of the connection.
- When a testing mode (unitary or automatic) is selected, it is impossible to change parameters of the unselected testing mode.

If you enter a non valid value in a field, the connection could be disabled or actions button in the configuration's window could become out of reach.

10.3 Used Units in Information Display

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

10.3.1 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 ⁶⁵ | 1.23 x 10 ⁶⁵ Bytes |
| 1 p | 1 packet |

10.3.2 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 ⁶⁵ | 1.23 x 10 ⁶⁵ bits per second |
| 1 p/s | Packet per second |



Throughput computing

The "IP Traffic – Test & Measure" displayed throughputs correspond to payload data on the sampling period (defined in the "IP Traffic – Test & Measure" configuration menu) and bring back to a bits/second number. The displayed throughput is an "application" throughput. At some instant, it could be different from the physical network throughput because data can be split and buffered at various system levels.

10.3.3 Duration units

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



Unit changing

To change, a volume value in KB to a volume value in MB, "IP Traffic – Test & Measure" divides the first value per 1024. Ex: 1000 KB = 0.98 MB. The same rule is applied with throughput values. In order to have a throughput in Mb/s coming from a throughput in Kb/s, "IP Traffic – Test & Measure" divides the first value per 1024. Ex: 2048 Kb/s = 2.00 Mb/s.

PART 11 Using "IP Traffic – Test & Measure"

11.1 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.



About the context file



In order to avoid entering again all parameters for a new testing session, or to create again mathematical laws, all **"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.

11.2 Launch "IP Traffic – Test & Measure"

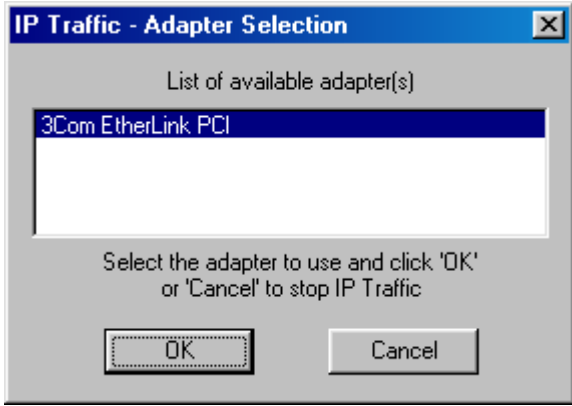
In the 'Start > programs > IP Traffic – Test & Measure' Menu, select **"IP Traffic – Test & Measure"** and click. The software is launched.

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

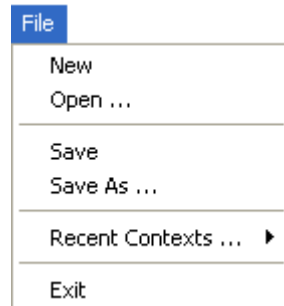
| Windows 98 | Windows 2000, XP or Server 2003 |
|--|--|
| <p>The user must first select the adapter needed to send and receive IP traffic.</p>  <p>For example, select the 3Com Ethernet adapter in this desktop configuration and then press OK.</p> <p>After a while due to initializations, the "IP Traffic – Test & Measure" main window is displayed.</p> | <p>After a while due to initializations, the "IP Traffic – Test & Measure" main window is displayed.</p> |

11.3 Menu description

The menu's bar is made of 8 items:

File Edit Configuration Tools File Downloading Automation Tool Help Operating mode

11.3.1 File Menu



11.3.1.1 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.

11.3.1.2 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.

11.3.1.3 File/Save

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

11.3.1.4 File/Save as

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

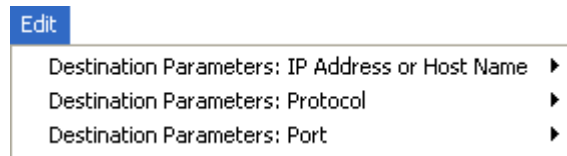
11.3.1.5 File/Recent Contexts

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

11.3.1.6 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.

11.3.2 Edit menu



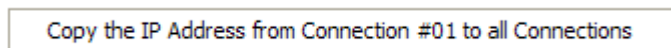
Active tab: "IP Generator – Parameters"



Active tab: "IP Answering – Parameters + Statistics"

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

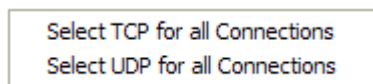
One option is available:



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

11.3.2.2 Edit/Destination Parameters: Protocol (for IP Generator)

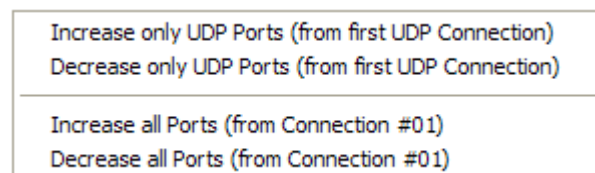
Two options are available:



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

11.3.2.3 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 considering the protocol in use.

11.3.2.4 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 considering the protocol in use.

11.3.2.5 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.

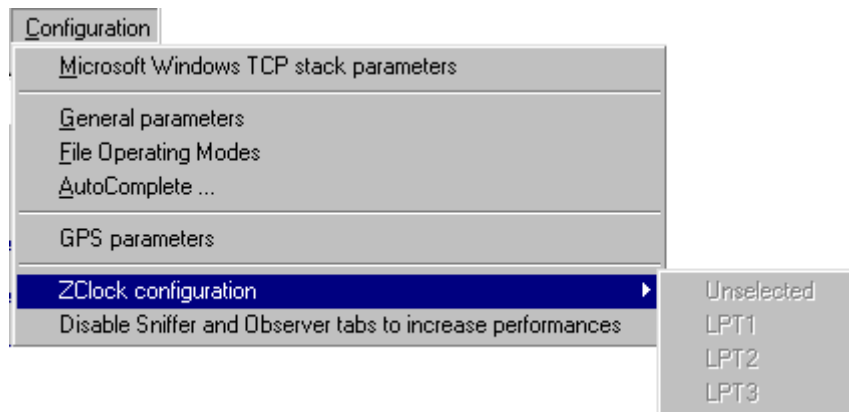
11.3.2.6 Edit/Coming From: Remote IP Address or Host Name (for IP Answering)

One option is available:

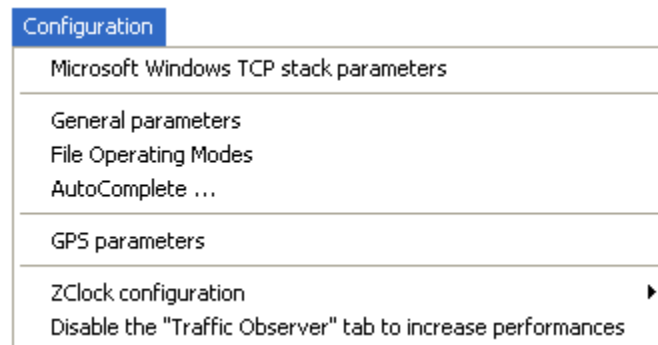
| |
|--|
| Copy the IP Address from Connection #01 to all Connections |
|--|

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

11.3.3 Configuration menu



Windows 98

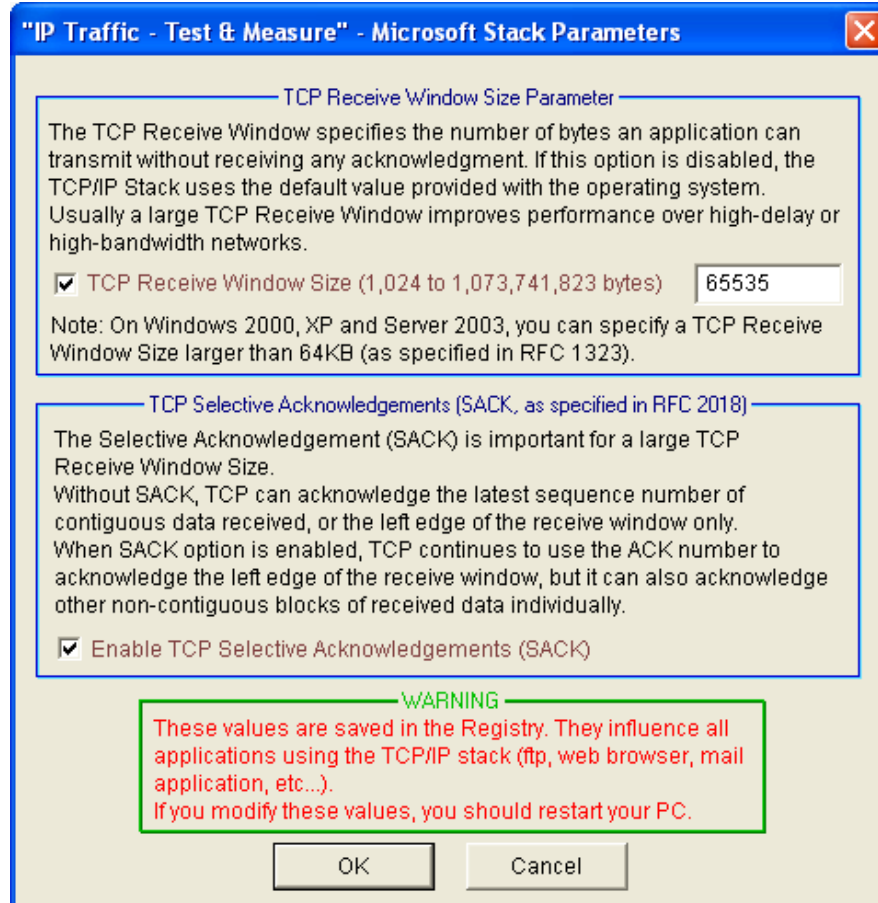


Windows 2000, XP or Server 2003


The ZClock module is not available with Windows 98. That is why, the parallel ports are grayed on Windows 98 computer.

11.3.3.1 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, XP or Server 2003 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).

11.3.3.2 General parameters

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

"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 - Test & Measure". This parameter also applies to statistics exportation. The throughput sampling period defines the number of seconds of traffic needed to calculate the throughput.

Refresh Time (1 to 60 seconds)

Throughput Sampling Period (1 to 60 seconds)

TCP and UDP received Data Timeout

These parameters are for the IP Generator Part only. When there is no more data to be sent, "IP Traffic - Test & Measure" continues to receive data until the timeout expires. Then the connection is released. When the timeout is 0, the connection is stopped as soon as there is no more data to be sent.

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

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

"IP Traffic - Test & Measure" Buffer Size (SO_RCVBUF and SO_SNDBUF)

The buffers used by "IP Traffic - Test & Measure" to dialog with the Winsock API influence the throughput performance for high speed network. The best performance can be reached with a high buffer size. Change in one of these sizes concerns the new connections only.

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

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

General parameters window

Parameters applying to the GUI display

Refresh time: 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 except if this value equals zero.

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. except if this value equals zero.

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.

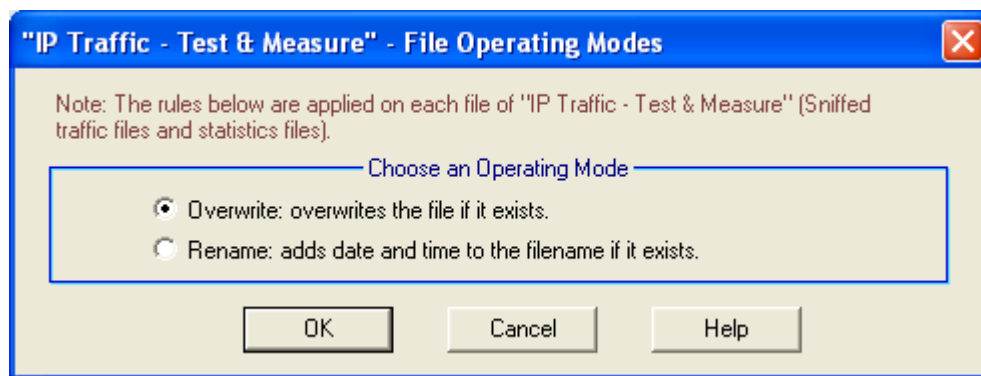
Transmit buffer size: this value is saved in the current context only and is used when sending data to the Microsoft Winsock2 interface.

Acquisition period for statistics

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

11.3.3.3 File Operating Modes

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



File Operating Modes window

Overwrite

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

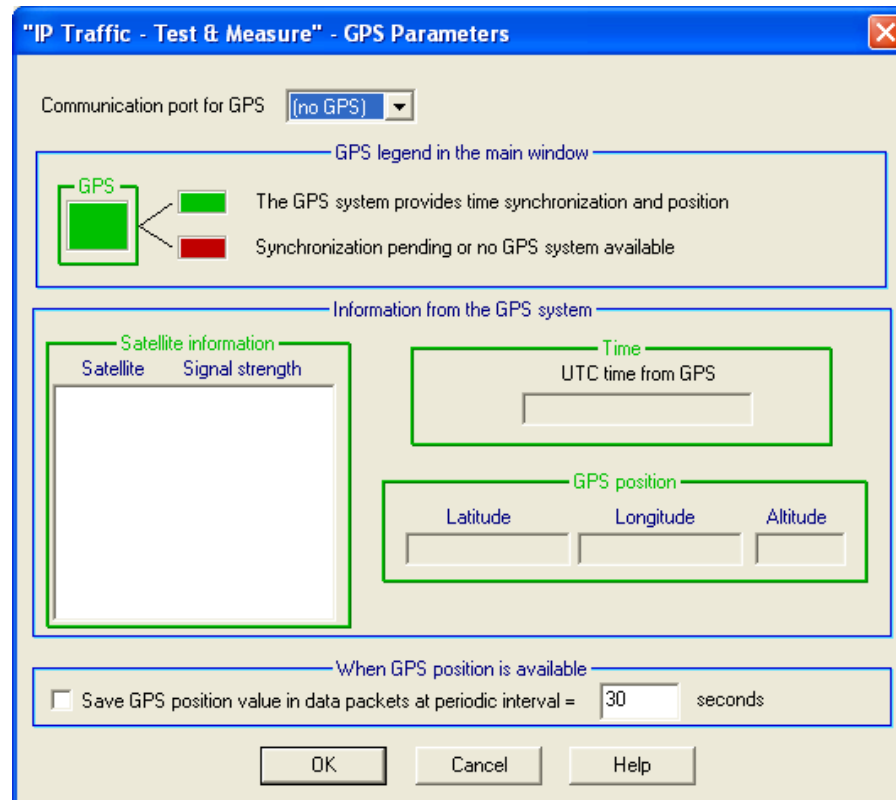
Rename

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.

11.3.3.4 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 three 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 |
| 10 | 12.20 |
| 13 | 3.80 |
| 2 | 7.80 |
| (23) | 0.00 |
| (24) | 0.00 |
| (27) | 0.00 |
| (4) | 0.00 |
| (8) | --- |

In this example, 8 satellites are displayed, and only the satellites number 10, 13 and 2 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**: the 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 a specific record of the Traffic sniffed file and it is not included in the data packets. By saving the GPS position, IP Traffic is able to provide the location of the computers when they receive or send a packet. (see 11.11.3.3 Statistics Display = Packet Statistics).

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, three satellites have a significant level, and GPS position is available.

"IP Traffic - Test & Measure" - GPS Parameters

Communication port for GPS: COM1

GPS legend in the main window

 The GPS system provides time synchronization and position
 Synchronization pending or no GPS system available

Information from the GPS system

| Satellite | Signal strength |
|-----------|-----------------|
| 10 | 12.20 |
| 13 | 3.80 |
| 2 | 7.80 |
| (23) | 0.00 |
| (24) | 0.00 |
| (27) | 0.00 |
| (4) | 0.00 |
| (8) | --- |

Time

UTC time from GPS

2006/04/19 15:54:21

GPS position

| Latitude | Longitude | Altitude |
|-----------------|----------------|----------|
| +48° 44' 37.96" | -3° 28' 21.94" | 143 |

When GPS position is available

☐ Save GPS position value in data packets at periodic interval = 30 seconds

OK Cancel Help



When loading a context having the GPS enabled, IP Traffic checks each COM Port to find the GPS unit.



Moreover, if a GPS is already active when loading a context having the GPS enabled, IP Traffic doesn't resynchronize itself with the GPS unit.

11.3.3.5 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 5 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 31st entry is typed, the 1st entry is deleted: the historical record is handled like a FIFO list.

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

- **NO_ADDRESS:** this is the default 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.

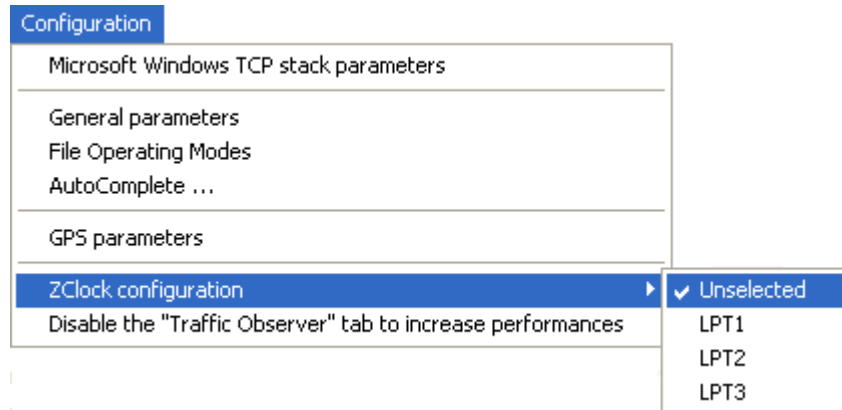
When AutoComplete is disabled, the historical record doesn't continue to be filled. User entries available - before AutoComplete deactivation - remain when AutoComplete is activated again.

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.

11.3.3.6 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"**.

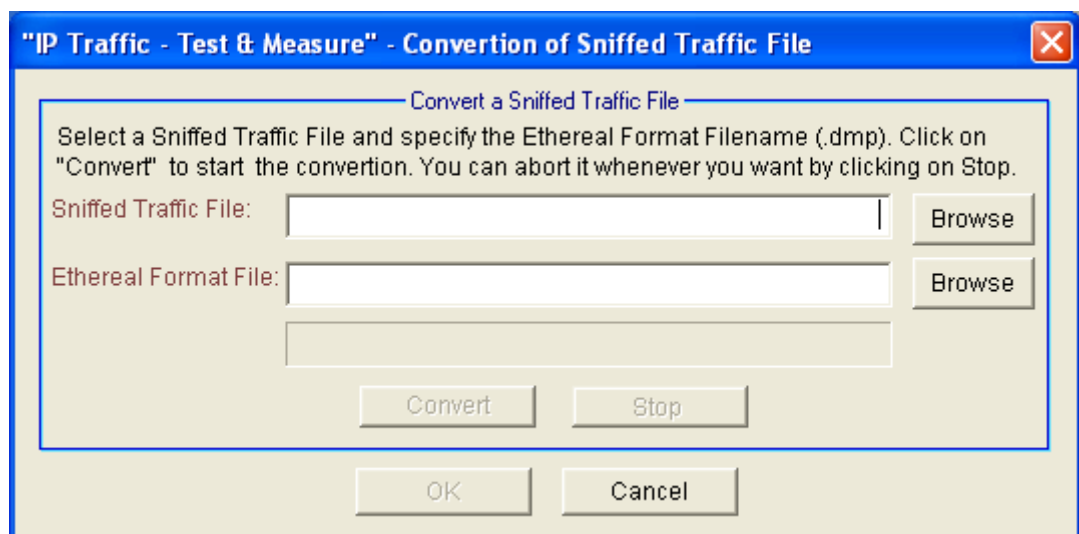
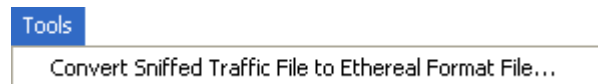


11.3.3.7 Disable the 'Traffic Observer' tabs to increase performances

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

When this option is selected, IP level statistics (and graphics) are not available any more.

11.3.4 Tools menu



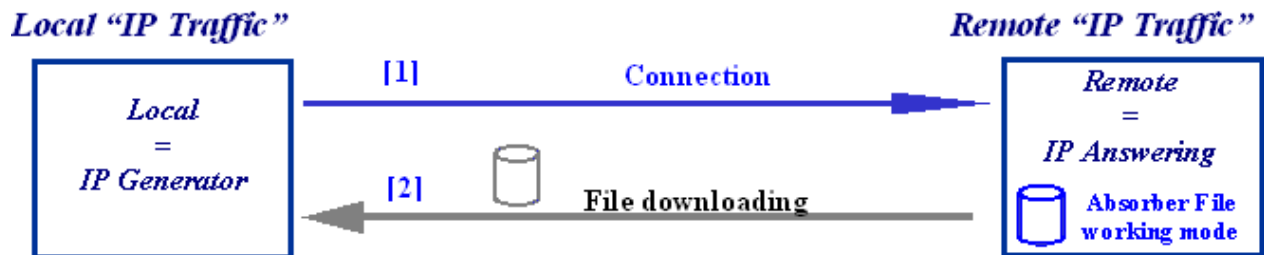
This tool allows converting the Sniffed Traffic files by **"IP Traffic – Test & Measure"** format to Ethereal standard format. By realizing this operation, the result file (dmp) can be opened by a Network Analyzer software such as Ethereal or Network Instruments Observer. This tool can convert capture traffic files containing IPv4 and IPv6 packets.

11.3.5 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 appears:

"IP Traffic - Test & Measure" - File downloading Parameters

This function allows file downloading from a remote "IP Traffic - Test & Measure" PC to the local "IP Traffic - Test & Measure" by using a specific TCP port number. The remote and the local PCs must have the same port number.

File downloading Port Number

1 Local port number (1 to 65,535) 2500

File downloading from a Remote

2 Remote source filename G:\Program Files\IP Traffic\logs\Capture.trc

3 IP Address or Host Name 192.168.0.35

4 Local destination filename C:\Program Files\IP Traffic\logs\CaptureFromRemote.trc Browse

5 ☒ Delete the remote file at the end of the downloading

0 100

6 Start Stop

OK Cancel Help

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. Can be an IPv4 or an IPv6 address.

[4] Give local name of the destination file.

[5] If necessary, the remote file can be deleted after the downloading

[6] 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:

"IP Traffic - Test & Measure" - File downloading in Progress from a Remote

Remote IP Address: 192.168.0.51

Port Number: 2500

Local Filename downloaded by the Remote: C:\Program Files\IP Traffic\logs\Capture.trc

Data volume to send (Bytes): 289602904

Volume of Data remaining (Bytes): 278871384

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

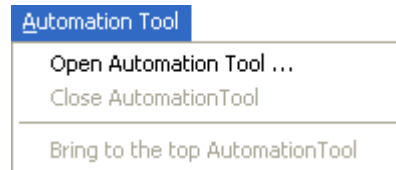
- Remote IP address is the IP address or host name of the machine from which you want to download the file. Can be an IPv4 or an IPv6 address.
- Port number is the port number for the file downloading process (it must be the same for remote and local machines).
- Local filename downloaded by remote is 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:

- The Local requests the file that is sent by the Remote machine.
- The Local establishes the connection.
- When the Remote receives the connection demand, it stops all of its running processes.
- The Remote accepts the connection and waits for the filename (with a timeout - default 10 s. This value can be customized. For more information, see the parameter TCP_INACTIVITY at 13.3 Configuration parameters saved in the Registry database).
- When connected, the Local sends the filename.
- When the Remote receives the filename, it checks if the file exists and sends the size (0 means no file or file access error) and data.
- When the Local wants to stop the reception of the file, it disconnects.
- When the 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, the Local sends an ACK.
- When the Remote receives an ACK, it waits for the deletion order
- If the Local receives the whole file, it sends the deletion order (the order can be: "delete" or "do not delete" the file).
- If the file should not be deleted:
 - When the Remote receives the deletion order, it disconnects (no more operation to do).
- If the file should be deleted:
 - When the Remote receives the deletion order, it deletes the file and sends back the result of the deletion (succeeded or not). Then, it disconnects.
- When the Remote receives an expiration of the Timeout, it disconnects.

11.3.6 Automation Tool menu



11.3.6.1 Open

The Open command launches the **Automation Tool for "IP Traffic – Test & Measure"**.

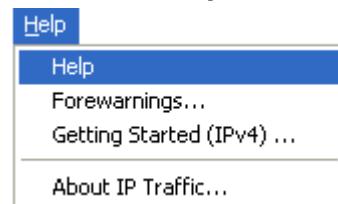
11.3.6.2 Close

The Close command stops the **Automation Tool for "IP Traffic – Test & Measure"**.

11.3.6.3 Bring to the top

The Bring to the top command displays the **Automation Tool for "IP Traffic – Test & Measure"** on the top of other windows.

11.3.7 Help Menu



11.3.7.1 Help

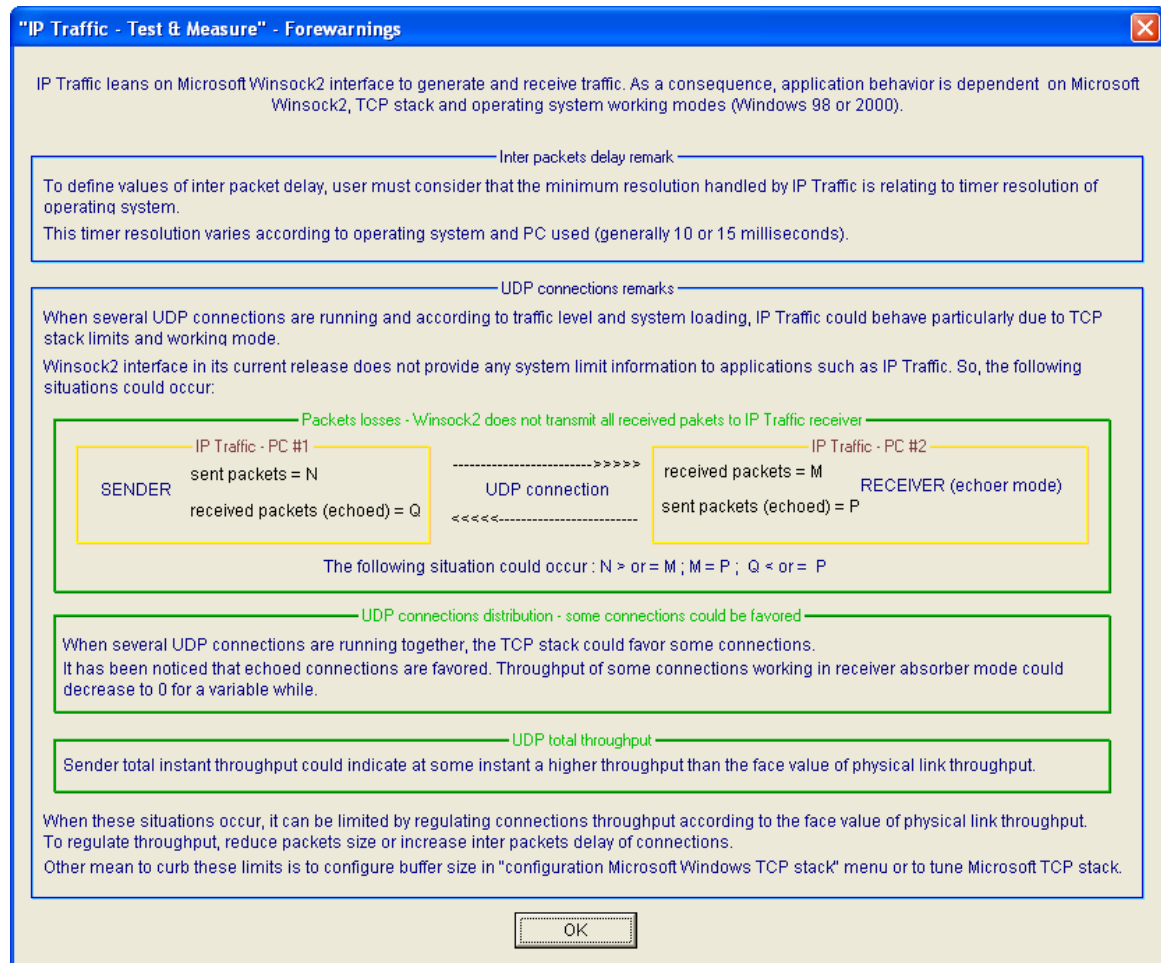
Help command displays help on **"IP Traffic – Test & Measure"**. Pressing the **F1** key can also activate help. To display the **"IP Traffic – Test & Measure"** Help, Acrobat Reader should be installed. If Acrobat reader is not installed, a warning message is displayed.

You can download the latest version from <http://www.adobe.com>, or use the version of Acrobat Reader provided with the **"IP Traffic – Test & Measure» CD ROM**.



***"IP Traffic – Test & Measure"** doesn't support other PDF readers than Acrobat Reader.*

11.3.7.2 Forewarnings menu



This menu is aimed to inform you of **"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"**'s behavior, as any Winsock 2 application, is dependent on Winsock 2 Interface, Microsoft TCP Stack and operating system working modes.

11.3.7.2.1 Inter packets Delay

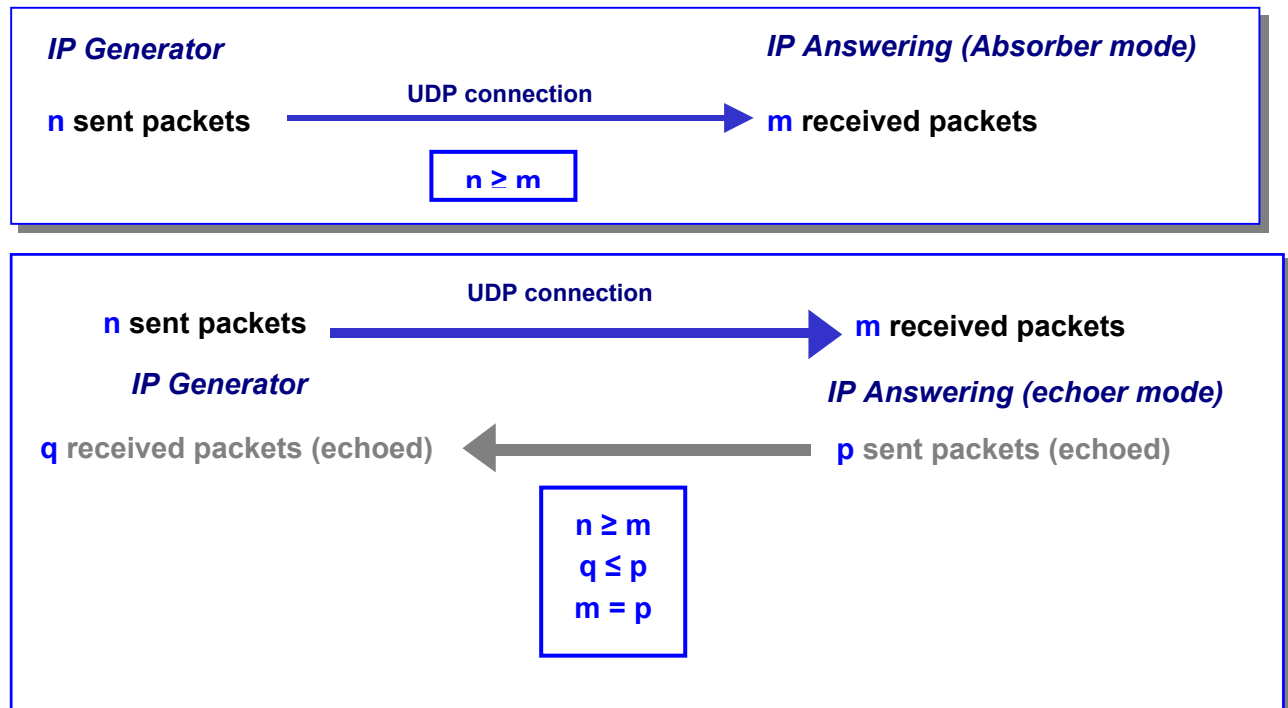
When defining Inter packet delay, the user must consider that minimum resolution handled by **"IP Traffic – Test & Measure"** is related to timer resolution of operating system. This timer resolution varies according to the used operating system and PC. Usually, timer resolution is 10 or 15 ms.

11.3.7.2.2 UDP connections

When several UDP connections are running and according to traffic level and system loading, **"IP Traffic – Test & Measure"** can have strange behavior 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.



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

In this case, the 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/IP stack may be favor echoed connections.

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

▪ **UDP total throughput**

IP Generator total instant throughput could indicates 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.

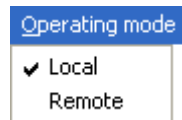
11.3.7.3 Help/Getting Started (IPv4)

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

11.3.7.4 About "IP Traffic – Test & Measure"...

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

11.3.8 Operating mode menu



11.3.8.1 Local mode

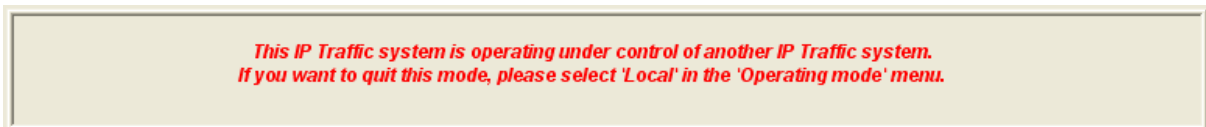
By selecting this mode, all **"IP Traffic – Test & Measure"** functionalities and commands are available.

11.3.8.2 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. A port is opened with IPv4 and another port with IPv6.

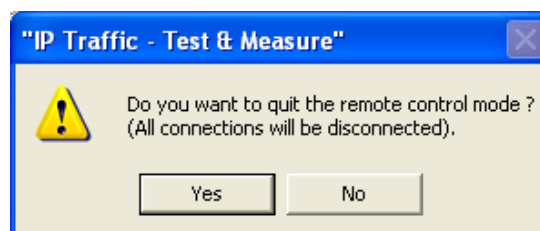


When the remote control mode is selected, a message is displayed at the bottom of the **"IP Traffic – Test & Measure"** main window as described below, and all button commands and tabs are inhibited.



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 or host name (**IPv4 or IPv6**) and the 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.

11.4 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.

11.5 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> <div>Active connections</div> <div>16</div> <div>Throughput</div> <div>7.25 Mb/s</div> </div> | <div>IP Answering Activity (based on application data)</div> <div> <div>Active connections</div> <div>16</div> <div>Throughput</div> <div>7.25 Mb/s</div> </div> | <div>Sniffer Activity</div> <div> <div>File size</div> <div>8 B</div> <div>Time before disk limit</div> <div>>24 h</div> </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. This throughput shows Rx **and** Tx activities for the IP Generator part.
- **IP Answering Activity** with the total number of active connections and the total throughput for these connections. This throughput shows Rx **and** Tx activities for the IP Answering part.
- **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.

11.6 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 located on the remote
- ⇒ The remote IP address or host name (IPv4 or IPv6)
- ⇒ 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. Moreover, if the option is selected, the Traffic Sniffer and the statistics export process of the Traffic Observer can be handle by this button.
- ⇒ **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"). For the Traffic Sniffer and the Traffic Observer tabs, read the note below.

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 the check boxes in the 'Traffic Sniffer' (Enable automatic start and stop in local operation) in the paragraph 11.10.2 Capture sniffed traffic into a file and in the parameters button of 'Export statistics' in the 'Traffic Observer' (Enable automatic export in local operation) in the paragraph 11.11 The 'Traffic Observer' tab.

11.7 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:

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

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

| Destination Parameters | | | |
|------------------------|-------------------------|----------|------|
| | IP Address or Host Name | Protocol | Port |
| Connection #1 | 192.168.0.30 | UDP | 2009 |
| Connection #2 | 192.168.0.30 | UDP | 2010 |
| Connection #3 | 192.168.0.30 | UDP | 2011 |
| Connection #4 | 192.168.0.30 | UDP | 2012 |
| Connection #5 | 192.168.0.30 | UDP | 2013 |
| Connection #6 | NO_ADDRESS | TCP | 2014 |
| Connection #7 | 192.168.0.30 | TCP | 2015 |
| Connection #8 | 192.168.0.30 | TCP | 2016 |
| Connection #9 | 192.168.0.30 | TCP | 2017 |
| Connection #10 | 192.168.0.30 | TCP | 2018 |
| Connection #11 | 192.168.0.30 | TCP | 2019 |
| Connection #12 | 192.168.0.30 | TCP | 2020 |
| Connection #13 | 192.168.0.30 | TCP | 2021 |
| Connection #14 | 192.168.0.30 | TCP | 2022 |
| Connection #15 | 192.168.0.30 | UDP | 2023 |
| Connection #16 | 192.168.0.30 | TCP | 2024 |

| 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 |
| Packet generator | Parameters #9 |
| Packet generator | Parameters #10 |
| Packet generator | Parameters #11 |
| Packet generator | Parameters #12 |
| Packet generator | Parameters #13 |
| Packet generator | Parameters #14 |
| Packet generator | Parameters #15 |
| Packet generator | Parameters #16 |

| Automatic Mode | Replay Mode |
|----------------|-------------|
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |
| Enabled | |

IP Generator – Parameters tab

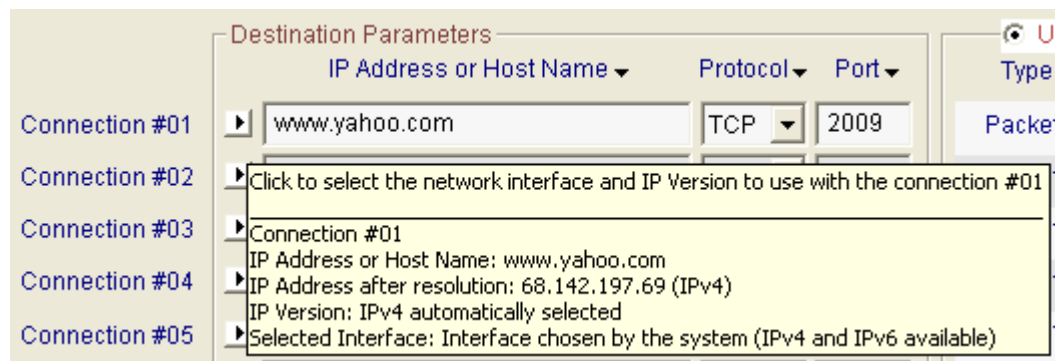
11.7.1 Destination Parameters

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

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

11.7.1.1 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:

- The first item is the connection number the tooltip refers to.
- The next item is the IP address or host name defined by the user.
- The next item is the IP address translated when IP Translation address has succeeded (e.g. the address is not NO_ADDRESS nor 0.0.0.0).
- The next item is the IP version currently selected.
- The last item is the interface's 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").

11.7.1.2 Select the network interface, source IP address and source port number

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

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

- (1) The **network interface** selection is optional with IPv4. It is used to constrain connections to be established using a specific interface.
- By default:
 - The IP version is automatically selected by **"IP Traffic – Test & Measure"** regarding the destination address or host name specified on the "IP Generator - Parameters" tab (see below).
 - The IP stack resolves the interface selection to send packets to the remote. The IP stack uses the destination IP address to select the correct interface. The IP address and the netmask related to each interface are checked against the remote IP address to reach. When an interface that matches the remote IP address is found, it is used. To understand how the IP stack selects the interface, you may enter 'route print' console command to list the interface order, the IP address and the network address mask.
 - You can select one interface from the list of the connected interfaces. **"IP Traffic – Test & Measure"** will only use the selected interface to translate IP address and to make a connection. You must select the interface compatible with the remote IP address you want to reach. When the IP address translation failed, the current connection parameters area is updated as follows:

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

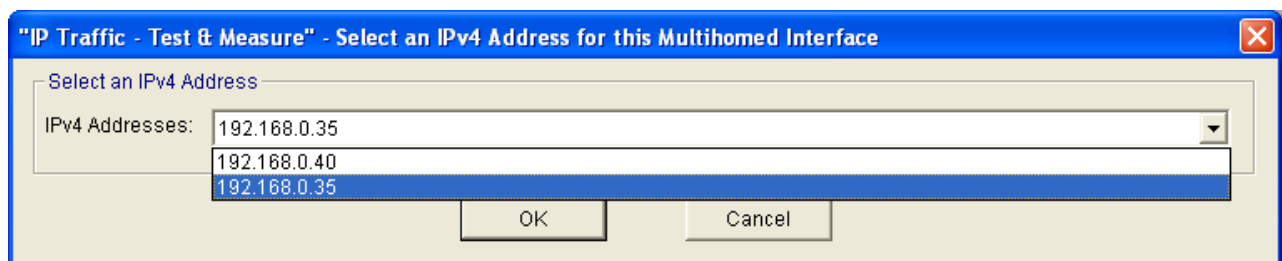
(2) The IP version selection is available:

- with Windows XP or Windows Server 2003
- If IPv6 features are installed on the target machine. Please refer to the Windows XP or Server 2003 documentation to install the IPv6 stack.
- You can allow **"IP Traffic – Test & Measure"** to choose automatically the good IP version regarding the address or host name resolution result. If a canonical name corresponds at the same time to an IPv4 and IPv6 address, **"IP Traffic – Test & Measure"** chooses the IPv4 address. In that case, to use the IPv6 address, you should leave the automatic selection mode and specify the use of IPv6.

If you have selected an IP version, the IP address translation (see 11.7.1.3) uses the current selected IP version to get the IP address numerical form.

(3) Select IP address is available when multiple IP addresses are attached to the network interface. This interface configuration is also known as 'multihomed' interface. The selection of a Source IP address is generally not required: **"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.

Example of an IP address selection for a multihomed interface:



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

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

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

- The source port used is dynamically updated with the user selection.
- IP addresses are static. The IP address translation process occurs after you click on OK.
- IP version field is dynamically updated with the user selection.
- Current interface is dynamically updated with the user selection.



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

11.7.1.3 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 Interface parameters changes, when you move from 'IP Address or Host Name' field to another field, or to another tab, when the Enter key is pressed or when the Interface parameters change, all of these actions start the IP address translation function.

Because the IP address translation mechanism is time consuming, you should be carefully when using IP canonical addresses. The time consumption depends on the DNS answer speed, the number of DNS configured and the network load when the DNS request is sent.

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



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



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

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



If no IP version has been selected, the IP address translation mechanism chooses the good IP version regarding the IP version returned by the resolution process. If for example, a canonical name represents at the same time an IPv4 and an IPv6 addresses, the IP Address Translation mechanism chooses the IPv4 address. If you want to use the IPv6 address, you should select IPv6 version (see 11.7.1.2 Select the network interface, source IP address and source port number).

11.7.1.4 Duplicate parameters of a connection onto others

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


Duplication of connection'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 (for 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 function allows copying parameters from one connection (source) to another one (target). Repeat this process for others connections if needed.

11.7.1.5 Description of the floating menu mechanism

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



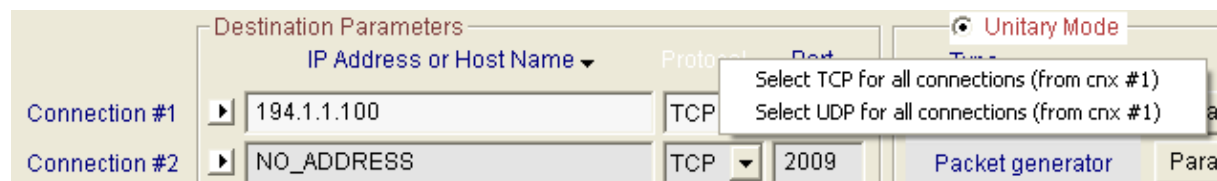
When the mouse is located on the 'IP Address or Host Name' text area for example, the text color changes to white. Then click left your mouse to display the associated menu.

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



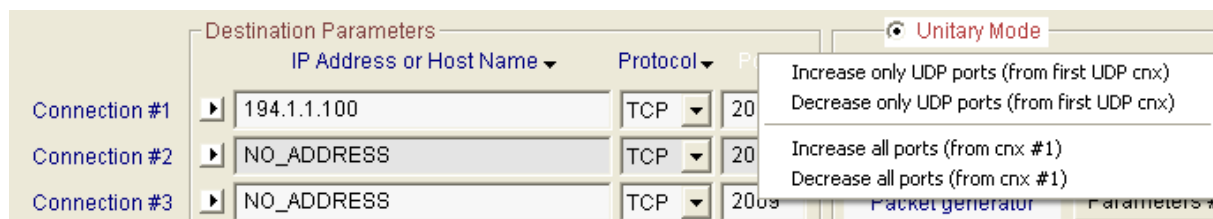
With this function, you can duplicate the IP address or the Host name from the first connection to the others fifteen connections.

Floating menu for the 'Protocol' label



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

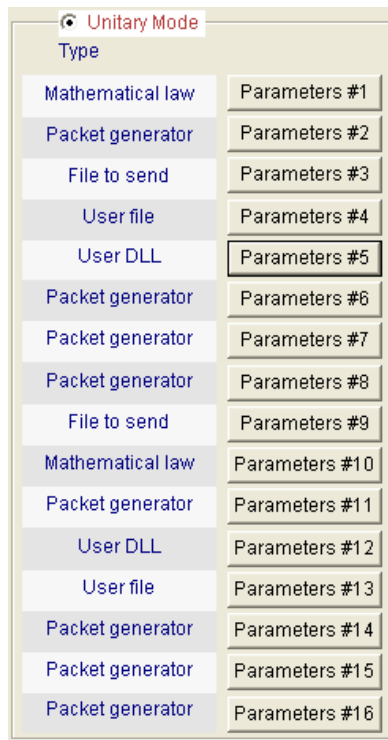
Floating menu for the 'Port' label



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.

11.7.2 Configure the unitary mode



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.

"IP Traffic - Test & Measure" - Parameters in unitary testing mode

Mode 1: Using the Internal Data Generator

Step1: 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

Mathematical law
 Law : data volume to send

 Uniform law
 Range : [9.77 KB , 2.38 MB]

File to send
 Filename:
 Loop counter (1 to 99) Idle time between each loop (0 to 99 s)

Step2: Specify Data size and packets parameters
 In this step, define Data Size and packets parameters as well as the delay between each sent packet.

TCP Data Size (1 to 65535 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.

☐ 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 (except for TCP 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 the RTT is enabled, IP Traffic adds 14 bytes to the "Data Size" defined by the Mode 1 or Mode 2 settings. ☐ 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 and the external data source generator.

11.7.2.1 Mode 1: Using the Internal data generator

Mode 1: Using the Internal Data Generator

Step1: 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

Mathematical law
 Law: data volume to send
 Edit...
 Uniform law
 Range : [9.77 KB , 2.38 MB]

File to send
 Filename: Browse
 Loop counter (1 to 99) Idle time between each loop (0 to 99 s)

Step2: Specify Data size and packets parameters
In this step, define Data Size and packets parameters as well as the delay between each sent packet.

TCP Data Size (1 to 65535 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 Edit...

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 (except for TCP 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)

11.7.2.1.1 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)

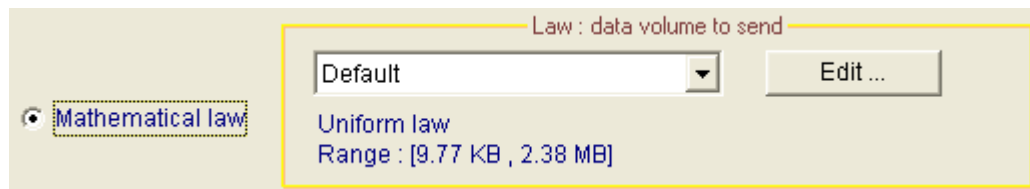
11.7.2.1.1.1 Mathematical law

In the unitary mode, the offered mathematical law is a data volume to send law. Volume will modify 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

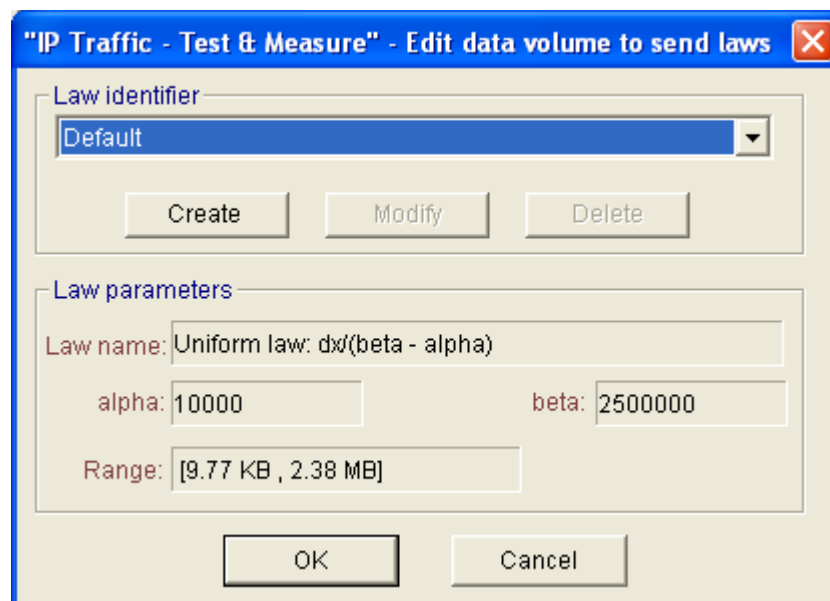
These laws are presented in details in the [Annex Part](#).



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 operations 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.

11.7.2.1.1.2 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.

11.7.2.1.1.3 File to send

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

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. Notice that the remote IP Answering should be configured accordingly to accept an idle time greater than the 'Idle time between each loop value'.

11.7.2.1.2 Step 2: Specify Data size and packets parameters

11.7.2.1.2.1 Data Size

This parameter defines the size of transmitted packets.

The maximum accepted value is 65 535 for TCP connections and 65507 for UDP connections. 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:

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 13.3 Configuration parameters saved in the Registry database for more details).

In addition, if the time code option is selected, the real TCP or UDP data size adds the size of the time code option. (see 11.7.2.3.1 Time code option).

11.7.2.1.2.2 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.

11.7.2.1.3 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.

11.7.2.2 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:

Mode 2: Using the External Data Source Generator - (User file or User DLL)

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

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 13.5 External File for the 'IP Generator' module). 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 13.6 External DLL for the 'IP Generator' module 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.

11.7.2.3 Options

11.7.2.3.1 Time code option

Timecode (RTT) option

If the RTT is enabled, IP Traffic adds 14 bytes to the "Data Size" defined by the Mode 1 or Mode 2 settings. ☐ Yes ☒ No

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:

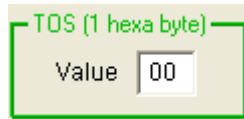
- 4 bytes magic number
- 4 bytes sequence number
- 4 bytes time when sent
- 2 bytes length (without the RTT header)

This information is used in conjunction with connections running in the echoer mode on the Remote IP Answering module. The Local 'IP Generator' module analyzes each echoed packet. 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.

11.7.2.3.2 The TOS byte

The TOS field is available only if IPv4 is selected for the connection. This option is not available in the IPv6 header.



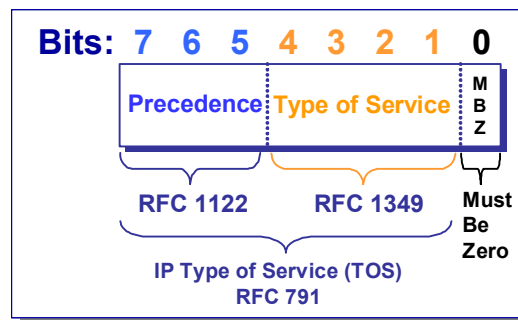
TOS (1 hexa byte)
Value: 00

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

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

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

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



IPv4 Type of Service byte

The TOS value entered is included without modification in the IP header i.e. "IP Traffic – Test & Measure" doesn't change what you set in the TOS byte.

Use of DSCP (Differentiated Services Code Point)

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

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

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

The DSCP totally overlaps the Precedence field.

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

This leads the notion of "class", each class being a group of the DSCPs with the same *Precedence* value.

Values within a class offer similar network services but with slight differences (different levels of service such as "gold", "silver" and "bronze").

From the initial definition of the RFC 2474, RFC 2697 added the "assured forwarding" service and RFC 2598 defined the "expedited forwarding" service.

The DSCPs are defined as following:

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



A new registry key must be added on Windows 2000/XP/Server 2003. It is necessary to edit the Registry and modify this key in order to use the TOS byte with **"IP Traffic – Test & Measure"**.



Using Registry Editor inaccurately can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. For information about how to edit the registry, view the "Changing Keys and Values" Help topic in Registry Editor (regedit.exe) or the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in regedit.exe. Note that you should back up the registry before you edit it. If you are running Windows 2000, XP or Server 2003 you should also update your Emergency Repair Disk (ERD).

Follow these steps to enable the IP_TOS option for the Winsock setsockopt function and the -v option for the ping utility on Windows 2000/XP/Server 2003:

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

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

NOTE: The registry key is one path.

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

11.7.2.3.3 The TTL field

| | |
|--|--|
| <div style="border: 1px solid green; padding: 5px;"> <p style="color: green; margin: 0;">Time To Live (TTL)</p> <p>Value <input style="width: 50px;" type="text" value="00"/></p> </div> | <p>The user can input the TTL/Hop Limit value (hexadecimal) used for each packet sent on the connection.</p> <p>Default value = 00</p> |
|--|--|

The TTL field is only considering with the UDP connections.

11.7.2.3.4 Save incoming data traffic or generated traffic into a file

Save incoming data traffic (needs remote in echo mode)

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:

Save generated traffic into file (only data are saved)

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

11.7.3 Configure the automatic mode

Automatic Mode

Enabled

Enabled

Enabled

Enabled

Enabled

Enabled

Enabled

Enabled

Enabled

Enabled

Enabled

Enabled

Enabled

Enabled

Enabled

Enabled

[P]

The 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.

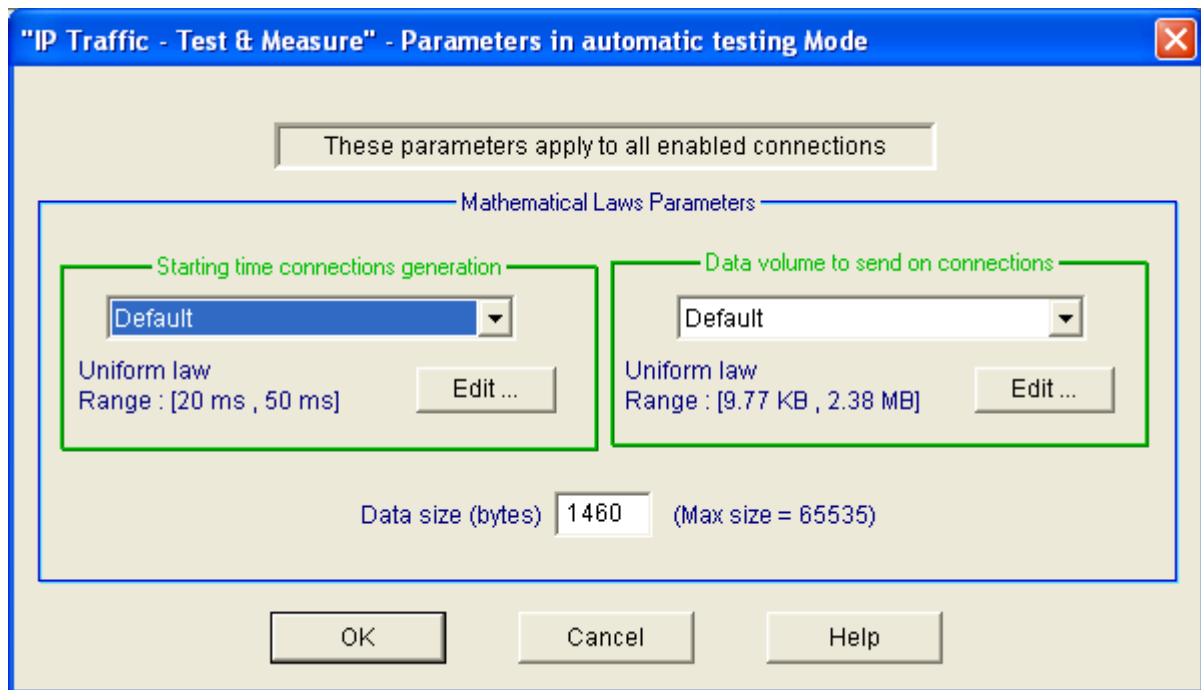
As the unitary mode, the automatic mode is configured in Tab 1 "IP Generator – Parameters" and is run in Tab 2 "IP Generator – Traffic +Statistics".

Once the 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:

© ZTI, 2000-2006

Page 102/195

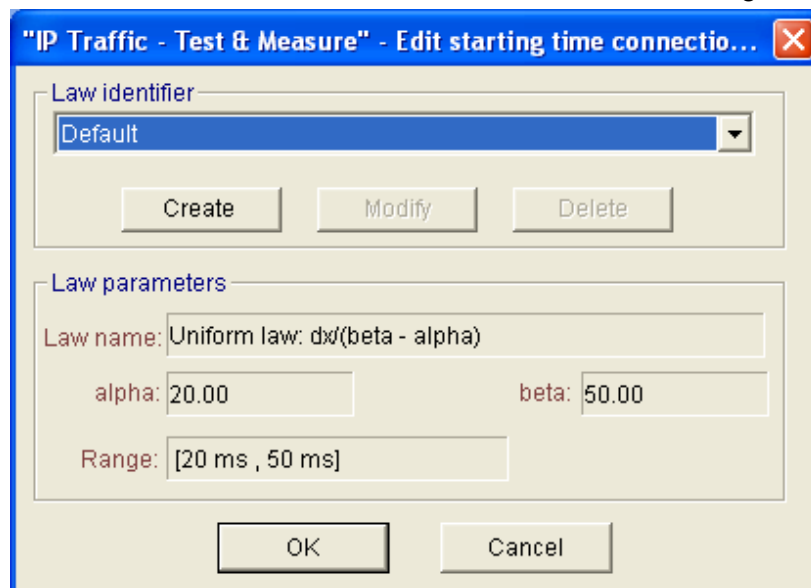


Automatic testing parameters window

3.1 Starting time connections generation laws

Starting time connection laws regulates the timing between the beginnings 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 operations 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 the "OK" button.
5. Your new law is selected in the parent window
6. Repeat operations 1 to 5 to create other laws

Note:

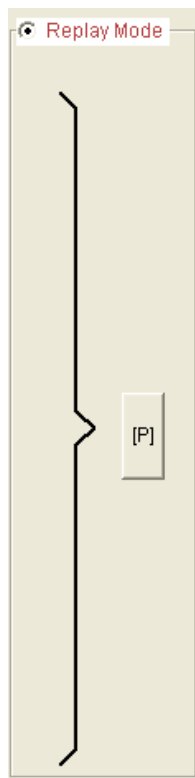
Up to the used OS (Windows 98, 2000, XP or Server 2003), WinSock 2 Interface could present number-limits of the incoming simultaneous calls. Consequence for "IP Traffic – Test & Measure" is the presence of "connection failed", particularly when connections frequency is very near (inferior to 150 ms), 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 for TCP connections and to 65507 bytes for UDP connections.

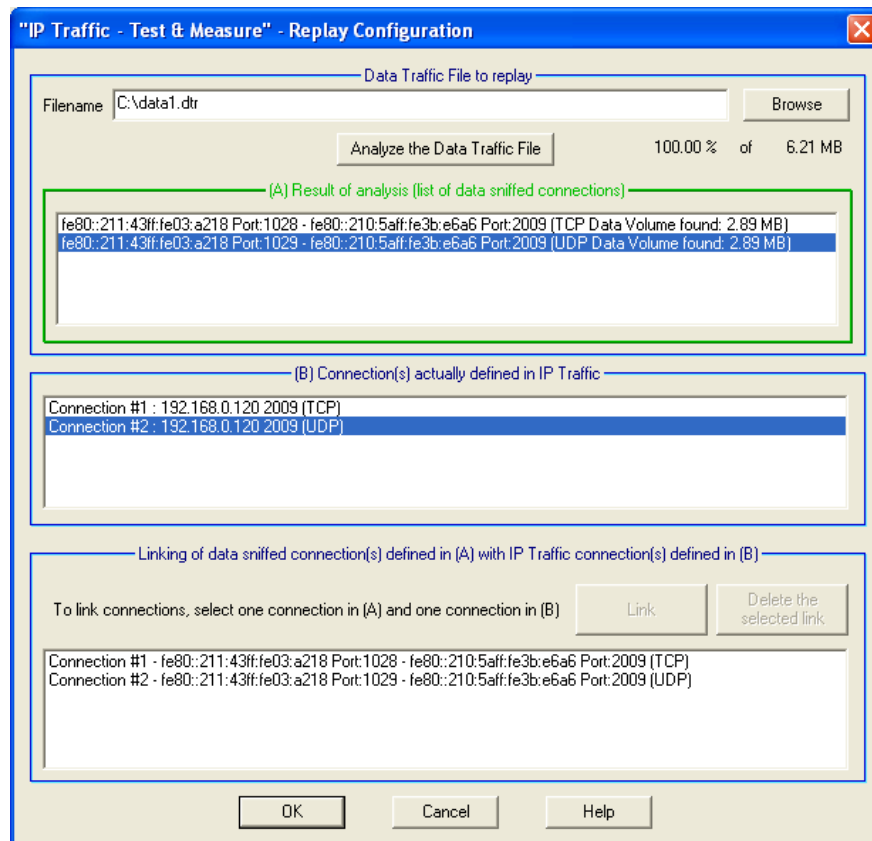
11.7.4 Configure the replay sniffed traffic mode



In this mode, **"IP Traffic – Test & Measure"** uses traffic files captured by the "Traffic Sniffer" (see 11.10 The 'Traffic Sniffer' tab).

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 MB" (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.

11.7.4.1 How does "IP Traffic – Test & Measure" replay the traffic ?

The first step, as explained before, is to link a connection #A from the « .dtr » file to a connection #B defined on the IP Generator.

When the replay is started, **"IP Traffic – Test & Measure"** reads the ".dtr" file to get the packets of the connection #A. Two data are necessary for the replay mode : the timestamp of the packet and the data payload. **"IP Traffic – Test & Measure"** is not be concerned by the IP version (IPv4 or IPv6), the protocol or the IP addresses used by the connection #A. The replay process, in relation with the link done between the connection #A and the connection #B, reuses the data payload respecting the timestamp of each packet some is the protocol or the IP version used to replay the data. For example a UDP connection using IPv4 can be replayed on a TCP connection using IPv6.

Note: the ".dtr" file contains only one-way packets. More details about how creating ".dtr" files are available in the paragraph 11.10.3 Run analysis algorithm

11.8 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 CSV 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.

| Destination Parameters | | | Statistics (based on application data) | | | | | | | | Unitary Mode | |
|------------------------|-------------------------|------|--|------------|-----------|---------------|-----------|------------|------|-----------|--------------|--|
| | IP Address or Host Name | Port | Tx Throughput | Tx Packets | Tx Volume | Rx Throughput | Rx Volume | Rx Packets | RTT | | | |
| Connection #01 | 192.168.0.120 | 9 | 570 Kb/s | 559 p | 797 KB | 0.00 b/s | 0 B | 0 p | N/A | Stop #01 | | |
| Connection #02 | 192.168.0.120 | 7 | 570 Kb/s | 559 p | 797 KB | 570 Kb/s | 797 KB | 558 p | 6 ms | Stop #02 | | |
| Connection #03 | 192.168.0.120 | 9 | 570 Kb/s | 559 p | 797 KB | 0.00 b/s | 0 B | 0 p | N/A | Stop #03 | | |
| Connection #04 | 192.168.0.120 | 9 | 570 Kb/s | 559 p | 797 KB | 0.00 b/s | 0 B | 0 p | N/A | Stop #04 | | |
| Connection #05 | 192.168.0.120 | 7 | 570 Kb/s | 559 p | 797 KB | 570 Kb/s | 797 KB | 559 p | 5 ms | Stop #05 | | |
| Connection #06 | NO_ADDRESS | 2009 | | | | | | | | Start #06 | | |
| Connection #07 | NO_ADDRESS | 2009 | | | | | | | | Start #07 | | |
| Connection #08 | NO_ADDRESS | 2009 | | | | | | | | Start #08 | | |
| Connection #09 | NO_ADDRESS | 2009 | | | | | | | | Start #09 | | |
| Connection #10 | NO_ADDRESS | 2009 | | | | | | | | Start #10 | | |
| Connection #11 | NO_ADDRESS | 2009 | | | | | | | | Start #11 | | |
| Connection #12 | NO_ADDRESS | 2009 | | | | | | | | Start #12 | | |
| Connection #13 | NO_ADDRESS | 2009 | | | | | | | | Start #13 | | |
| Connection #14 | NO_ADDRESS | 2009 | | | | | | | | Start #14 | | |
| Connection #15 | NO_ADDRESS | 2009 | | | | | | | | Start #15 | | |
| Connection #16 | NO_ADDRESS | 2009 | | | | | | | | Start #16 | | |

Export Statistics into a File
Parameters Export is running

RTT summary of all connections - Min: 0 ms - Max: 63 ms - Mean: 6 ms
Choose Columns Reset Display

Unitary Mode
Start All Connections
Stop All Connections

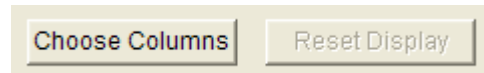
Tab 2: "IP Generator - Traffic + Statistics"

11.8.1 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.

11.8.2 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 the 15 parameters described later in this paragraph, and at least one parameter must be selected.

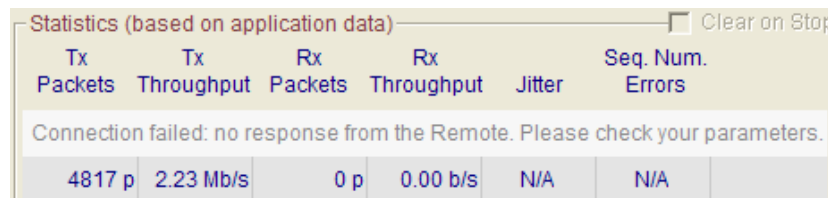
These statistics are computed at the application level (and based on application data sent or received). No MAC, IP and TCP/UDP headers and trailers are taken into account.

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).

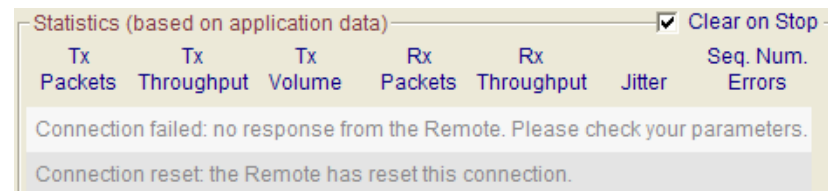


The "**N/A**" (Not Applicable) mention can be displayed instead of a value in the cell of the statistics table if the parameter cannot be calculated.



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.



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

11.8.2.1 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. |

11.8.2.2 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. |

11.8.2.3 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. |
| ◆ Mean RTT | 'Mean RTT' is the Round Trip Time of a packet that 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. |
| ◆ Min RTT | "Min RTT" is the minimum value of the Round Trip Time calculated by "IP Traffic – Test & Measure" . For more information, please see the "Mean RTT" column information. |
| ◆ Max RTT | "Max RTT" is the maximum value of the Round Trip Time calculated by "IP Traffic – Test & Measure" . For more information, please see the "Mean RTT" column information. |
| ◆ 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. |

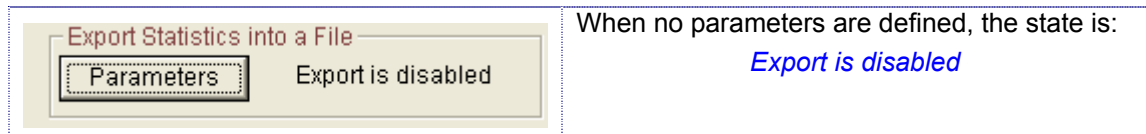
A RTT summary for all connections is also available. This summary displays the minimum, maximum and Mean RTT values of all connections (for connections having RTT (Timecode) option selected (see 11.7.2.3.1 Time code option for more information)).

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.

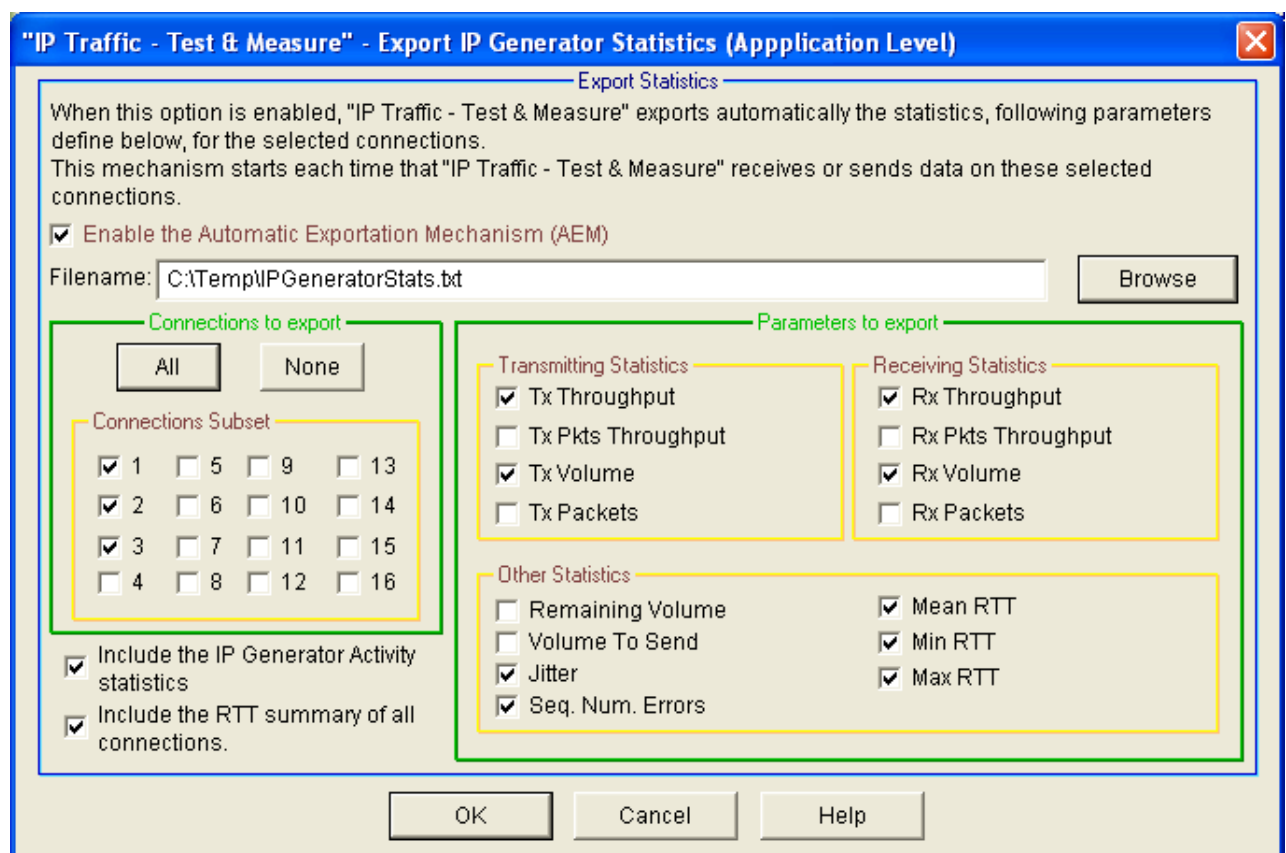
11.8.2.4 Export statistics into a file

To export all or part of **statistics** into a CSV file, click on the 'Parameters' button when enabled (i.e. when no connection of the IP Generator is active):



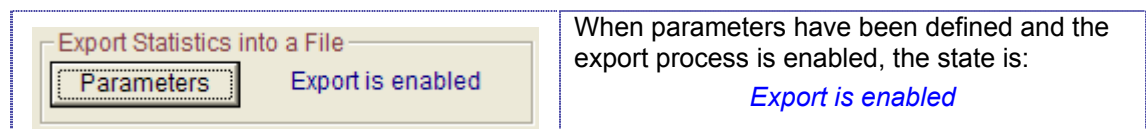
Then a window allows defining parameters for the export process:

- Enable or disable the export process,
- The filename (.csv extension) of the export file,
- The identification of the needed connections,
- The parameters to export (up to 15).
- Include or not the RTT summary or the IP Generator activity into the statistics file.



"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. If you do so, a warning message is displayed.

Note: The maximum number of columns handled by Excel is 255. If the number of statistics and connections you have selected exceeds this limit of Excel, you have to restrict to the most important statistics that you need, or to reduce the number of connections.

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 CSV file as soon as one connection of the IP Generator is started and the 'Export is running' state is displayed:



When all the 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 also the statistics which are not displayed) in a file, you can use the parameters connection and statistics dialog.

The RTT summary is exported even if the selected connections don't use the RTT option.

11.8.2.4.1 The IP Generator statistics CSV file format

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

First line: (All types of statistics are represented here. The general statistics (RTT summary, IP Generator activity, Date/Time, etc ...) and the statistics available for each connection. The statistics headers can be up to fifteen for each connection)

| | | | | | | | |
|--|---|---|-------------------------------------|--|---|---|-------------------------------------|
| IP Generator Date/Time | RTT Summary: Mean RTT (ms) | RTT Summary: Min RTT (ms) | RTT Summary: Max RTT (ms) | State Connection #xx | Tx Throughput Connection #xx (Kb/s) | Tx Pkts Throughput Connection #xx (Pkts/s) | Tx Volume Connection #xx (KB) |
| Tx Packets Connection #xx (Pkts) | Rx Throughput Connection #xx (Kb/s) | Rx Pkts Throughput Connection #xx (Pkts/s) | Rx Volume Connection #xx (KB) | Rx Packets Connection #xx (Pkts) | Remaining Volume Connection #xx (KB) | Volume To Send Connection #xx (KB) | Mean RTT Connection #xx (ms) |
| Jitter Connection #xx (ms) | Seq. Num. Errors Connection #xx | Min RTT Connection #xx (ms) | Max RTT Connection #xx (ms) | | | | |

Next lines:

| | | | | | | | |
|----------------------------|--------|--------|-----|-----------------------|--------|--------|-----|
| MM/DD/YYYY HH:MM:SS.mmm | mmm | mmm | mmm | TCP or UDP or ICMP | nnn.nn | nnn.nn | mmm |
| mmm | nnn.nn | nnn.nn | mmm | mmm | mmm | mmm | mmm |
| mmm | mmm | mmm | mmm | | | | |

Additional mark for TCP, UDP or ICMP connection events

| | |
|-----------------|---|
| TCP START | This mark indicates the connection starts. When this mark is included in the IP Generator traces, the numerical values are set to 0. |
| TCP END | This mark indicates the corresponding connection has stopped. The numerical values are the latest values computed by "IP Traffic – Test & Measure" . Moreover, for IP Generator part, the line containing the END flag shows a synthesis of all statistics. The averages are calculated from the START flag time to the END flag time. |
| TCP PENDING | This mark indicates the connection is launched but that no data packet has been sent for the moment (for example in TCP, time to realize the "Three-ways Handshake"). |
| TCP WAITING END | This mark indicates the connection has sent all of its packets but still waiting for the echoed packets until the timeout is reached (see 11.3.3.2 General parameters). |

Additional mark for TCP or UDP disconnection events

| | |
|-----------|---|
| TCP ERROR | This mark indicates the reason of the disconnection if this one is not produced by the click on the stop button or the scheduled end of the traffic generation (due to the generator parameters, for example: Number packets to send = 1000) When this mark is included in the IP Generator traces, the error message returned by "IP Traffic – Test & Measure" is placed after the "ERROR" mark. |
|-----------|---|

Idle connections

When the connection is idle, no numerical value is set into the file. The field is empty.

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", "Mean RTT", "Min RTT" and "Max 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 "Mean RTT", "Min RTT" and "Max RTT", "Seq. Num. Errors", "Tx Packets" and "Rx Packets".

Then for the RTT summary, "Mean RTT", "Min RTT" and "Max RTT" are filled with the "N/A" symbol until one "RTT" header is found in the received data by the 'IP Generator' part (at least for one connection).

When "Mean RTT", "Min RTT" or "Max RTT" is filled with the value 0, this means that the result is less than 1 millisecond.

How to open this CSV file with Excel ?

To open this file with Microsoft Excel, the comma should be defined as "list separator" (this is the default value with English regional settings). In case of problem, click on "Start > Control Panel" and click on "Regional and Language Options", select an item in the list or click Customize to define your own parameters.

How to change the date/time format ?

To change the format of the date/time column, select the whole column and right click on the column. Choose "Format Cells ...", then, in the Category list, choose "Custom". In the "Type" area, enter the following string: mm/dd/yyyy hh:mm:ss.000. Using this string, the date/time format will be changed to : 04/20/2006 09:45:50.840.

Export an IP Generator file sample

In this example, 2 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 (with RTT activated).
- Connection #02 is configured with the UDP protocol and uses the internal data generator (with RTT activated).

The "Refresh time" parameter is set to 2 seconds.

| IP Generator Date/Time | State Connection #01 | Tx Throughput Connection #01 (Kb/s) | Rx Throughput Connection #01 (Kb/s) | Mean RTT Connection #01 (ms) | State Connection #02 | Tx Throughput Connection #02 (Kb/s) | Rx Throughput Connection #02 (Kb/s) | Mean RTT Connection #02 (ms) |
|-------------------------|----------------------|-------------------------------------|-------------------------------------|------------------------------|----------------------|-------------------------------------|-------------------------------------|------------------------------|
| 04/20/2006 13:25:40.421 | | | | | UDP PENDING | 0 | 0 | N/A |
| 04/20/2006 13:25:40.421 | | | | | UDP START | 0 | 0 | N/A |
| 04/20/2006 13:25:40.437 | | | | | UDP | 0 | 0 | N/A |
| 04/20/2006 13:25:40.453 | TCP START | 0 | 0 | N/A | UDP | 0 | 0 | N/A |
| 04/20/2006 13:25:41.859 | TCP | 98.09 | 98.09 | 2 | UDP | 98.09 | 98.09 | 1 |
| 04/20/2006 13:25:43.843 | TCP | 326.22 | 326.22 | 1 | UDP | 326.22 | 326.22 | 1 |
| 04/20/2006 13:25:45.843 | TCP | 554.34 | 554.34 | 1 | UDP | 554.34 | 554.34 | 1 |
| 04/20/2006 13:25:47.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:25:49.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:25:51.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:25:53.843 | TCP | 570.31 | 574.88 | 1 | UDP | 570.31 | 572.59 | 2 |
| 04/20/2006 13:25:55.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:25:57.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:25:59.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:01.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:03.843 | TCP | 570.31 | 574.88 | 1 | UDP | 570.31 | 574.88 | 2 |
| 04/20/2006 13:26:05.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:07.843 | TCP | 570.31 | 570.31 | 0 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:09.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:11.859 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:13.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:15.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:17.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:19.843 | TCP | 570.31 | 570.31 | 1 | UDP | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:20.453 | TCP WAITING END | 570.31 | 570.31 | 1 | UDP WAITING END | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:20.453 | TCP WAITING END | 570.31 | 570.31 | 1 | UDP WAITING END | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:20.968 | TCP END | 563.1 | 563.1 | 1 | UDP WAITING END | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:21.046 | | | | | UDP WAITING END | 570.31 | 570.31 | 1 |
| 04/20/2006 13:26:21.156 | | | | | UDP END | 559.93 | 559.93 | 1 |

The delimiter mark used between each field is the comma character (in conformance with the CSV file format). In this example, the lines containing the END flag have a synthesis of all statistics exported. The throughputs showed are the mean throughputs calculated from the START flag time to the END flag time.

11.8.3 Run an unitary testing session

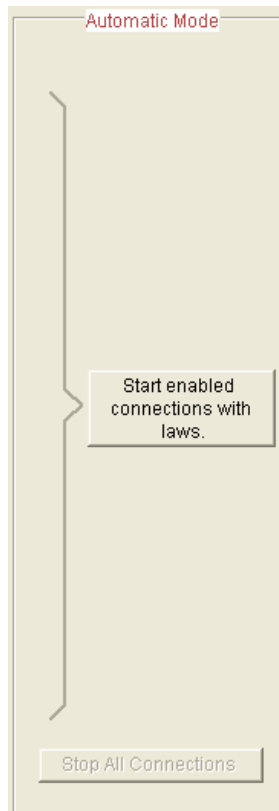


The unitary testing session can be started from the "Unitary mode" area in Tab 2 "IP Generator - Traffic + Statistics". From this area, you can start or stop connections in unitary testing separately or all together.

To run an unitary mode session:

1. *In Tab 2 "IP Generator - Traffic + Statistics":*
→ If the 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 unitary testing mode.
3. *In Tab 1 "IP Generator - Parameters":*
→ If necessary configure the 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.

11.8.4 Run an automatic testing session

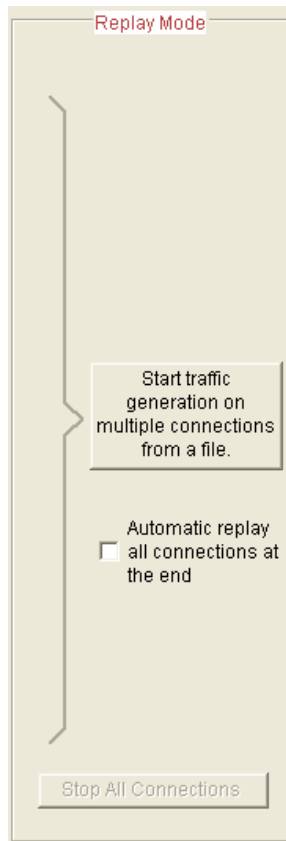


An automatic testing session is launched from the "Automatic Mode" area in Tab 2 "IP Generator - Traffic + Statistics". In this area, there is only one button to start and to stop all enabled connections in the automatic mode.

To carry out the automatic mode session:

- 1 *In Tab 2 "IP Generator - Traffic + Statistics":*
 - If the 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 automatic testing mode.
- 3 *In Tab 1 "IP Generator - Parameters":*
 - If necessary, configure the 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.

11.8.5 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 the 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.*

11.8.6 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) which can use IPv4 or IPv6 IP version.

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 specified.
- In the upper part of the Step 2, the ICMP Echo Request data size can be defined.
- The lower part of Step 2 allows the definition of the replies timeout.
- In Step 3 you can define the mean packet throughput.

Note: more information about these three areas is available in paragraph 11.7.2.1 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.
- Mean RTT: this value shows the average Round Trip Time.
- Min RTT: this value is the minimum Round Trip Time calculated
- Max RTT: this value is the maximum Round Trip Time calculated
- Seq. Num. Errors: this value represents the number of replies that "IP Traffic – Test & Measure" does not receive.

11.9 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"


11.9.1 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 0).

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

11.9.2 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:

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

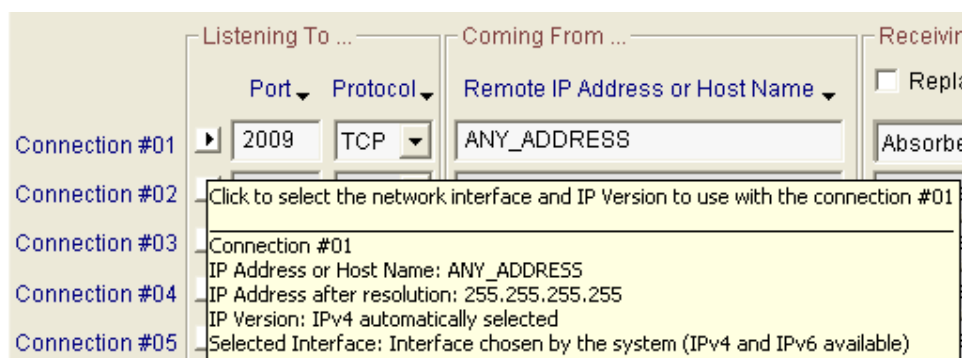
11.9.2.1 Specific Rules to receive TCP or UDP traffic

| Rules | TCP | UDP |
|---|-----|------|
| The same port number can be used by several IPv4 or IPv6 connections | YES | NO |
| The same port number can be used by two connections using either IPv4 or IPv6 | YES | YES |
| The same port number can be used by connections using different NICs | YES | YES* |
| The same port number can be used by connections using the same multihomed NIC but by selecting different IP Addresses | YES | YES* |

* If a UDP connection uses the "default interface", this connection is disabled in favor of the connection using an interface.

11.9.2.2 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 five items:

- The first item is the connection number the tooltip refers to.
- The next item is the IP address defined by the user.
- The next item is the IP address translated when IP Translation address has succeeded (e.g. the address is not NO_ADDRESS or 0.0.0.0).
- The next item is the IP version currently selected.

- The last item is the interface name selected. The name displayed is the name of the connection presented in the "Settings/Network and Dial-up Connections" Start menu of the operating system (Default is "Interface chosen by the system").

11.9.2.3 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 connection

- (1) The **network interface** selection is optional. It is used to constrain connections to be established using a specific interface.

- By default:
 - The IP version is automatically selected by "IP Traffic – Test & Measure" regarding the destination address or host name specified on the "IP Answering – Traffic + Statistics" tab (see below). By default, NO_ADDRESS is an IPv4 address.
 - The IP stack resolves the interface selection to send packets to the remote. The IP stack uses the destination IP address to select the correct interface. The IP address and the netmask related to each interface are checked against the remote IP address to reach. When an interface that matches the remote IP address is found, it is used. To understand how the IP stack selects the interface, you may enter 'route print' console command to list the interface order, the IP address and the network address mask.
- You can select one interface from the list of connected interfaces. "IP Traffic – Test & Measure" will only use the selected interface to translate the IP address and to make a connection. You must select the interface compatible with the remote IP address you want to reach. When the IP address translation failed, current connection parameters area is updated as follows:

- 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.

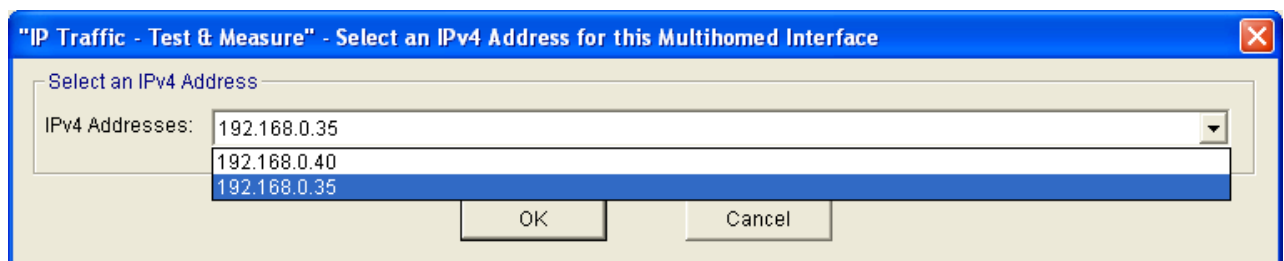
(2) The **IP version** selection is available:

- with Windows XP (or later)
- If IPv6 features are installed on the target machine. Please refer to the Windows XP or Windows Server 2003 documentation to install the IPv6 stack.
- You can allow **"IP Traffic – Test & Measure"** to choose automatically the good IP version regarding the address or host name resolution result. If a canonical name corresponds at the same time to an IPv4 and IPv6 addresses, **"IP Traffic – Test & Measure"** chooses the IPv4 address. In that case, to use the IPv6 address, you should select the use of IPv6 only (Use IPv6 only).

If you have selected an IP version, the IP address translation (see 11.7.1.3) uses the current selected IP version to get the IP address numerical form.

(3) **Select IP address** is available when multiple IP addresses are attached to the network interface. This interface configuration is also known as 'multihomed' interface. The selection of a Source IP address is generally not required: **"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. Example of an IP address selection for a multihomed interface:



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

(4) **Specification of the local source port number** is disabled in the receiver Interface configuration because the source port number and the destination port number are generated by the remote as the originator of the connection.

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

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



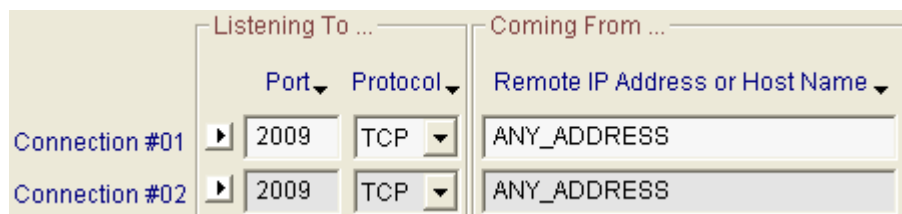
When you click on the OK button, if the interface selected or IP version has changed, the IP address translation is automatically started. It may be time consuming.

So, you can configure various incoming connection criteria:

- **Interface:** you limit a connection to a specific Interface or let the Operating System to return connections from any interfaces.
- **IP version:** when an Interface offers the two IP versions, you can select the IP version expected or not. By default, the automatic selection is activated.
- **When multiple IP addresses are attached to one interface,** you should select the destination IP address the incoming connection should refer to. By default, the first IP address returned by the system is selected.

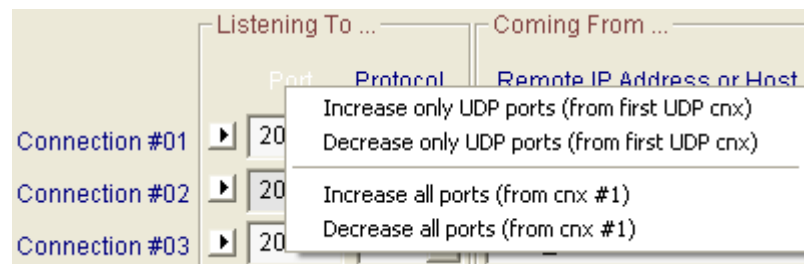
11.9.2.4 Description of the floating menu mechanism

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.

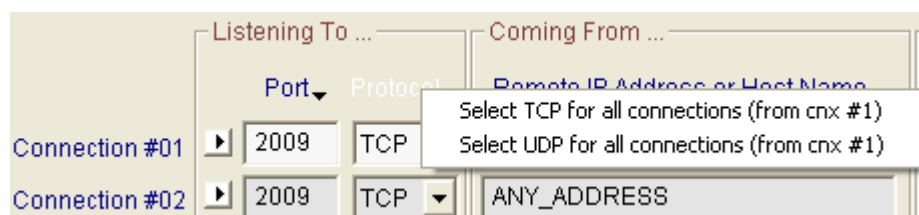
11.9.2.4.1 Floating menu for the 'Port' label



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.

11.9.2.4.2 Floating menu for the 'Protocol' label



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

11.9.3 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).

With a TCP connection, the incoming connection is rejected if "IP Traffic – Test & Measure" can't correlate this IP Address or host name with the source IP Address of the incoming packet.

With a UDP connection, the incoming packets are received but if "IP Traffic – Test & Measure" can't correlate this IP Address or host name with the source IP Address of the incoming packets, "IP Traffic – Test & Measure" doesn't take them into account in the statistics.

11.9.3.1 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 out to all connections from #02 to #16.

11.9.3.2 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 the Interface parameters change, all of these actions start the IP address translation function.

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

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



When the IP address translation failed, the IP address is written in red on a white background. This connection cannot be started.



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

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

11.9.4 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.

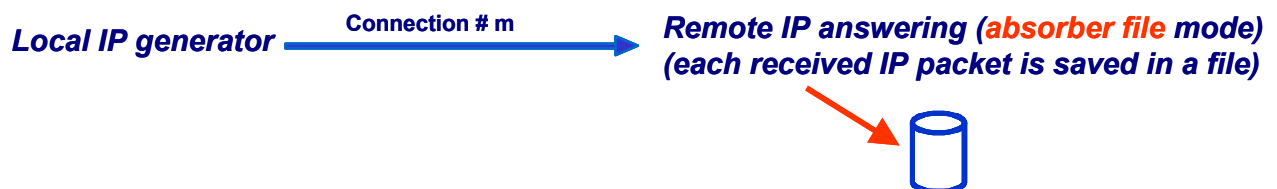
11.9.4.1 Absorber mode

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



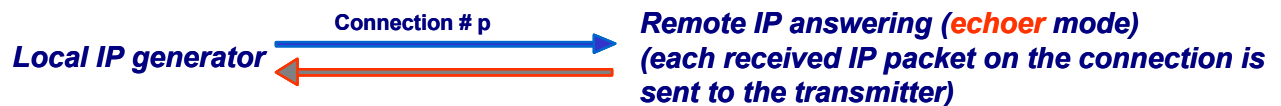
11.9.4.2 Absorber File mode

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



11.9.4.3 Echoer mode

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



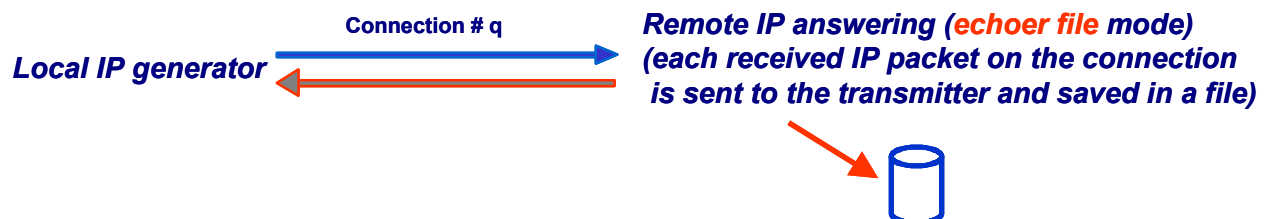
With UDP protocol, the 'Echoer' mode is available if a connected 'IP Generator' address is specified only.

Remind:

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

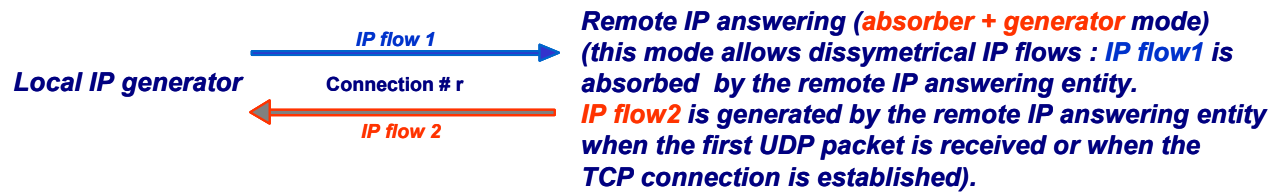
11.9.4.4 Echoer File mode

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.

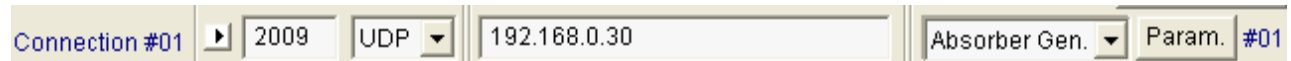


11.9.4.5 Absorber + Generator mode

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 used to compute statistics only.



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. The IP flow 2 is stopped when the FIN or RESET flag is received or when the user stops the IP Answering. The IP flow 2 is also stop is no data are received during *TCPINACTIVITY* seconds. (see 13.3 Configuration parameters saved in the Registry database)

For an UDP connection, *IP flow 2* is generated as soon as the remote 'IP Answering' module will receive the first UDP packet. The IP flow 2 is stopped when the RESET flag is received or when the user stops the IP Answering. The IP flow 2 is also stop is no data are received during *UDPINACTIVITY* seconds. (see 13.3 Configuration parameters saved in the Registry database)

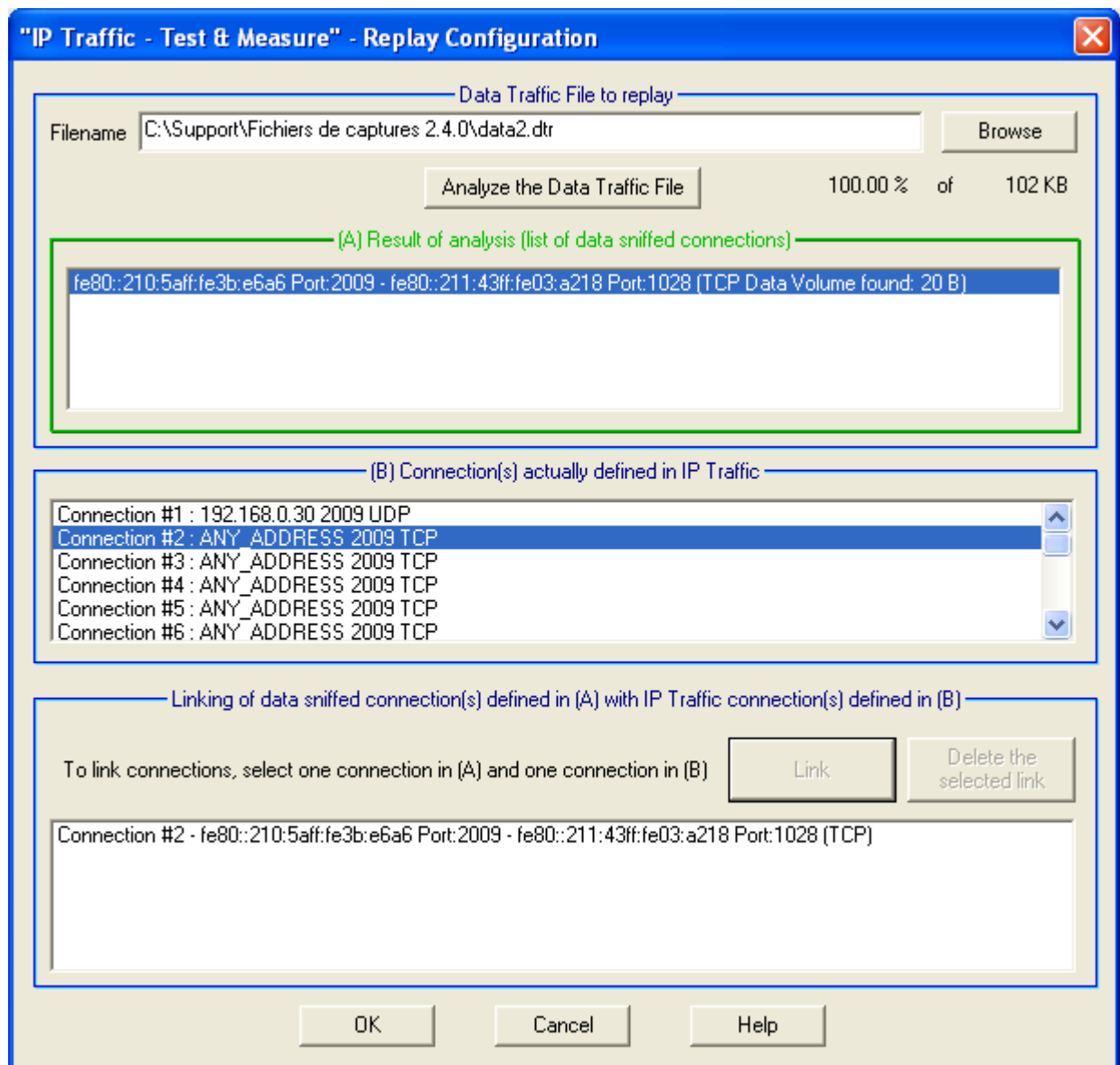
11.9.4.6 Disable mode

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.

11.9.4.7 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).

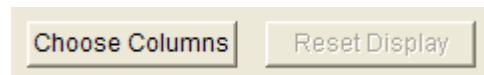
After the analysis of the data traffic file, all IP connections found in the sniffed traffic file are then displayed in the "(A) Result of analysis (list of data sniffed connections)" object.

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.

11.9.5 '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). | | | | |

11.9.5.1 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 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. |

11.9.5.2 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. |

11.9.5.3 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 bellow)

When pressing the “Stop receiving traffic” button:

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

11.9.6 "Export IP Answering statistics into a file" parameters

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

| | |
|--|--|
| <div>Export Statistics into a File</div> <div>Parameters Export is disabled</div> | When no parameters are defined, the state is: <i>Export is disabled</i> |
|--|--|

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

- Enable or disable the export process,
- The filename (.csv extension) 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:

| | |
|---|--|
| <div>Export Statistics into a File</div> <div>Parameters Export is enabled</div> | When parameters have been defined and the export process is enabled, the state is: <i>Export is enabled</i> |
|---|--|

Note:

Do not specify the same filename to save statistics for the 'IP Generator' and the 'IP Answering' parts. If you do so, a warning message is displayed.

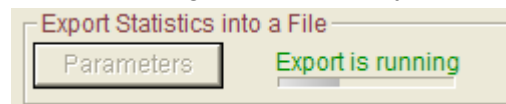
Note: The maximum number of columns handled by Excel is 255. If the number of statistics and connections you have selected exceeds this limit of Excel, you have to restrict to the most important statistics that you need, or to reduce the number of connections.

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:



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:



11.9.6.1 The 'IP Answering' statistics file format

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

First line: (All types of statistics available for each connection are represented here. The statistics headers can be up to fifteen for each connection)

| IP Answering Date/Time | State Connection #xx | Tx Throughput Connection #xx (Kb/s) | Tx Pkts Throughput Connection #xx (Pkts/s) | Tx Volume Connection #xx (KB) | Tx Packets Connection #xx (Pkts) | Rx Throughput Connection #xx (Kb/s) | Rx Pkts Throughput Connection #xx (Pkts/s) |
|---------------------------|----------------------------|---|---|-------------------------------------|--|---|---|
|---------------------------|----------------------------|---|---|-------------------------------------|--|---|---|

| Rx Volume Connection #xx (KB) | Rx Packets Connection #xx (Pkts) | Remaining Volume Connection #xx (KB) | Volume To Send Connection #xx (KB) | Data Not Echoed Connection #xx (KB) | Jitter Connection #xx (ms) | Seq. Num. Errors Connection #xx |
|-------------------------------------|--|---|---|--|----------------------------------|--|
|-------------------------------------|--|---|---|--|----------------------------------|--|

Next lines:

| | | | | | | | |
|----------------------------|-----------------------|--------|--------|-----|-----|--------|--------|
| MM/DD/YYYY HH:MM:SS.mmm | TCP or UDP or ICMP | nnn.nn | nnn.nn | mmm | mmm | nnn.nn | nnn.nn |
| mmm | mmm | mmm | mmm | mmm | mmm | mmm | |

Additional mark for TCP or UDP connection events

TCP START It indicates the corresponding connection starts. When this mark is included in the IP Answering traces, the numerical values are set to 0.

TCP END It indicates the corresponding connection has stopped. The numerical values are the latest values computed by "IP Traffic – Test & Measure".

Additional mark for TCP or UDP disconnection events

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 i.e. when the number of packets to send has been reached.

When this mark is included in the IP Answering traces, the error message returned by **"IP Traffic – Test & Measure"** is placed after the "ERROR" mark.

Idle connections

When the connection is idle, no numerical values are set. The fields are empty.

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.

How to open this CSV file with Excel ?

To open this file with Microsoft Excel, the comma should be defined as list separator (this is the default value with English regional settings). In case of problem, click on "Start > Control Panel" and click on "Regional and Language Options", select an item in the list or click Customize to define your own parameters.

How to change the date/time format ?

To change the format of the date/time column, select the whole column and right click on the column. Choose "Format Cells ...", then, in the Category list, choose "Custom". In the "Type" area, enter the following string: mm/dd/yyyy hh:mm:ss.000. Using this string, the date/time format will be changed to: 04/20/2006 09:45:50.840.

Export an IP Answering file sample

In this example, 2 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
- Connection #02 is configured with the UDP protocol.

The "Refresh time" parameter is set to 2 seconds.

| IP Answering Date/Time | State Connection #01 | Tx Throughput Connection #01 (Kb/s) | Rx Throughput Connection #01 (Kb/s) | Rx Pkts Throughput Connection #01 (Pkts/s) | State Connection #02 | Tx Throughput Connection #02 (Kb/s) | Rx Throughput Connection #02 (Kb/s) | Rx Pkts Throughput Connection #02 (Pkts/s) |
|------------------------|----------------------------|--|--|---|----------------------------|--|--|---|
| 12/5/2005 15:12:15.850 | | | | | UDP START | 0 | 0 | 0 |
| 12/5/2005 15:12:15.850 | | | | | UDP | 0 | 0 | 0 |
| 12/5/2005 15:12:17.084 | TCP START | 0 | 0 | N/A | UDP | 0 | 0 | 0 |
| 12/5/2005 15:12:17.787 | TCP | 75.28 | 75.28 | N/A | UDP | 77.56 | 77.56 | 6 |
| 12/5/2005 15:12:19.787 | TCP | 303.41 | 303.41 | N/A | UDP | 305.69 | 305.69 | 26 |
| 12/5/2005 15:12:21.787 | TCP | 531.53 | 531.53 | N/A | UDP | 533.81 | 533.81 | 46 |
| 12/5/2005 15:12:23.787 | TCP | 568.03 | 568.03 | N/A | UDP | 568.03 | 568.03 | 49 |
| 12/5/2005 15:12:25.787 | TCP | 568.03 | 568.03 | N/A | UDP | 570.31 | 570.31 | 50 |
| 12/5/2005 15:12:27.787 | TCP | 570.31 | 570.31 | N/A | UDP | 570.31 | 570.31 | 50 |
| 12/5/2005 15:12:29.787 | TCP | 568.03 | 568.03 | N/A | UDP | 570.31 | 570.31 | 50 |
| 12/5/2005 15:12:31.787 | TCP | 570.31 | 570.31 | N/A | UDP | 568.03 | 568.03 | 49 |
| 12/5/2005 15:12:33.787 | TCP | 568.03 | 568.03 | N/A | UDP | 568.03 | 568.03 | 49 |
| 12/5/2005 15:12:35.787 | TCP | 570.31 | 570.31 | N/A | UDP | 568.03 | 568.03 | 49 |
| 12/5/2005 15:12:37.787 | TCP | 570.31 | 570.31 | N/A | UDP | 572.59 | 572.59 | 50 |
| 12/5/2005 15:12:39.787 | TCP | 572.59 | 572.59 | N/A | UDP | 572.59 | 572.59 | 50 |
| 12/5/2005 15:12:41.787 | TCP | 572.59 | 572.59 | N/A | UDP | 572.59 | 572.59 | 50 |
| 12/5/2005 15:12:43.787 | TCP | 572.59 | 572.59 | N/A | UDP | 570.31 | 570.31 | 50 |
| 12/5/2005 15:12:45.787 | TCP | 570.31 | 570.31 | N/A | UDP | 570.31 | 570.31 | 50 |
| 12/5/2005 15:12:47.787 | TCP | 568.03 | 568.03 | N/A | UDP | 568.03 | 568.03 | 49 |
| 12/5/2005 15:12:49.787 | TCP | 568.03 | 568.03 | N/A | UDP | 570.31 | 570.31 | 50 |
| 12/5/2005 15:12:51.787 | TCP | 572.59 | 572.59 | N/A | UDP | 572.59 | 572.59 | 50 |
| 12/5/2005 15:12:53.787 | TCP | 570.31 | 570.31 | N/A | UDP | 570.31 | 570.31 | 50 |
| 12/5/2005 15:12:55.787 | TCP | 570.31 | 570.31 | N/A | UDP | 570.31 | 570.31 | 50 |
| 12/5/2005 15:12:57.787 | TCP | 568.03 | 568.03 | N/A | UDP | 568.03 | 568.03 | 49 |
| 12/5/2005 15:12:59.787 | TCP | 572.59 | 572.59 | N/A | UDP | 570.31 | 570.31 | 50 |
| 12/5/2005 15:13:00.850 | TCP | 572.59 | 572.59 | N/A | UDP | 570.31 | 570.31 | 50 |
| 12/5/2005 15:13:00.850 | TCP END | 572.59 | 572.59 | N/A | UDP | 570.31 | 570.31 | 50 |
| 12/5/2005 15:13:00.912 | | | | | UDP END | 570.31 | 570.31 | 50 |

The delimiter mark used between each field is the comma character (respecting the CSV format).

11.10 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 displays the 'Traffic Sniffer' tab of the 'IP Traffic – Test & Measure' application. The interface is organized into three main numbered sections:

- Section 1: Capture Parameters**
 - Includes a 'Use filter(s)' section with buttons for 'New filter', 'Edit filter', and 'Delete filter'.
 - A table for defining filters with columns: Source IP addr., Destination IP addr., Source Port, Destination Port, and Protocol.
 - Current filter: Source IP 192.168.0.30, Destination IP 'To any destination', Source Port 'From any port', Destination Port 'To any port', Protocol 'TCP & UDP'.
 - Radio button: 'All TCP and UDP packets (unicast and/or multicast)'.
 - Buttons: 'Help' and 'Select adapters'.
- Section 2: Capture sniffed traffic in a file (used for statistics or traffic generator)**
 - File path: 'C:\LocalCapturedTraffic.trc' with a 'Browse' button.
 - Buttons: 'Start' and 'Stop'.
 - Checkboxes: 'Save only headers of the packets (Data are not registered)', 'Automatic refresh mode', and 'Enable automatic start and stop in 'Local operation''.
 - Area: 'Traffic overview during capture' (empty box).
- 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: 'C:\LocalCapturedTraffic.trc' with a 'Browse' button.
 - Output data traffic file 1 to replay after processing: 'C:\SplittedData1' with a 'Browse' button.
 - Output data traffic file 2 to replay after processing: 'C:\SplittedData2' with a 'Browse' button.
 - Area: 'Synthesis after processing' (empty box).
 - Buttons: 'Start' and 'Stop'.

Tab 4: "Traffic Sniffer"

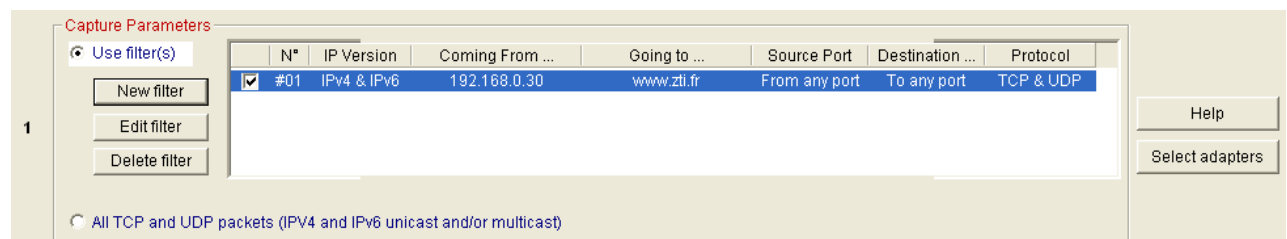
11.10.1 Capture Parameters (Step 1)

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. Up to 20 filters can be specified.

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.

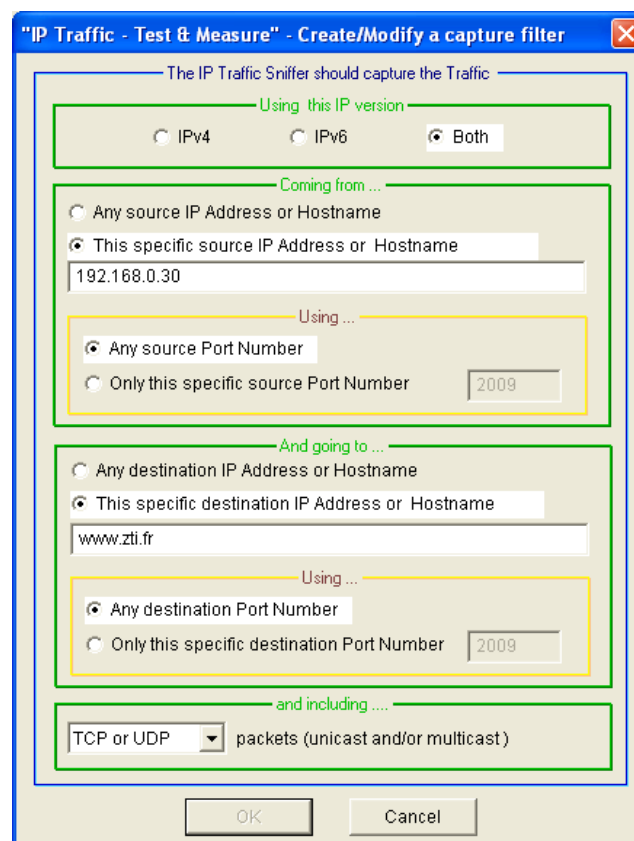


Step 1: Capture Parameters Specification

11.10.1.1 Create/Modify/Delete user defined filters

You can define up to 20 '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

Four main areas compose this window.

1. Specification of the IP version: Only IPv4, Only IPv6 or both IPv4 and IPv6
2. Specification of the "Coming ..." information
 - a. Specification of the source IP Address or Host Name of the traffic (IPv4 or IPv6)
 - b. Specification of a particular source port number
3. Specification of the "And going ..." information.
 - a. Specification of the destination IP Address or Host Name of the traffic (IPv4 or IPv6)
 - b. Specification of a particular destination port number
4. 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:

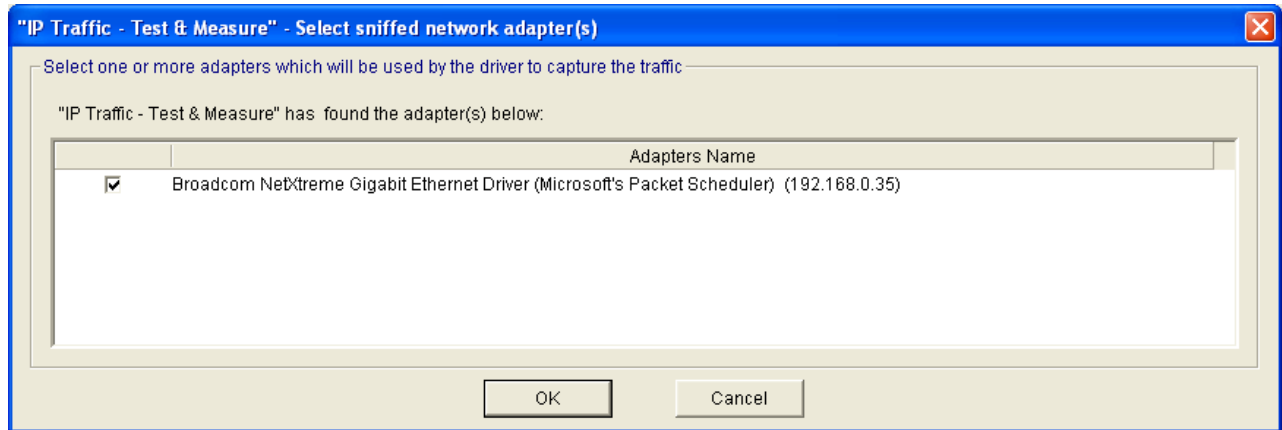
*You can input different filters, but **"IP Traffic – Test & Measure"** doesn't control the functional coherence between the filters.*

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.

11.10.1.2 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.



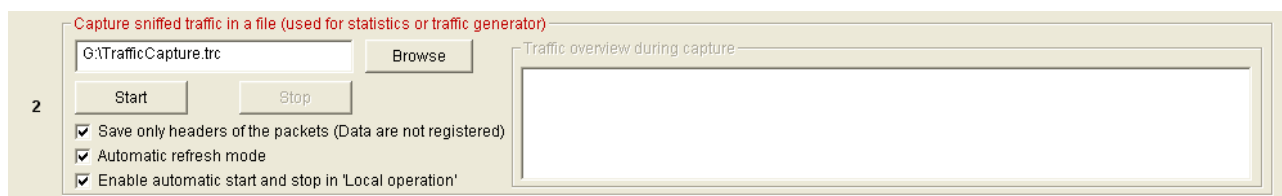
Adapters selection window

Note:

When loading a context, if the interface in this context saved can not be found, **"IP Traffic – Test & Measure"** selects the first interface available to replace the one saved.

11.10.2 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.

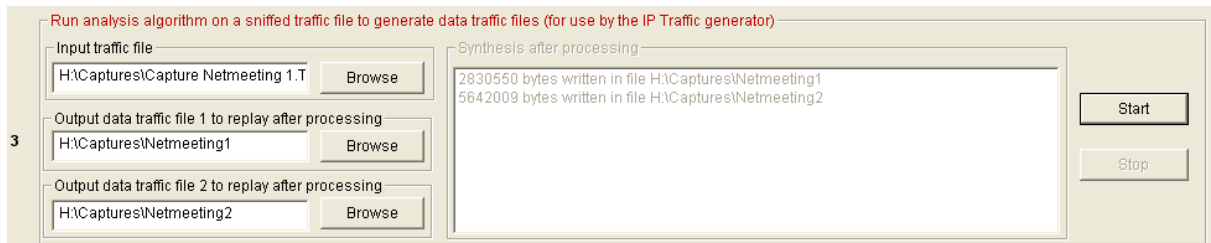
"Enable automatic start and stop in 'Local operation' check box: if checked, the "Start all processes" button of the "Local operation" will launch automatically the 'Traffic Sniffer'.

11.10.3 Run analysis algorithm (Step 3)

In step 2, the capture process has generated a capture traffic file.

Warning:

The aim of step 3 is to splits the captured data into two files. These two files are ONLY used by the IP Traffic Replay Mode available on the IP Generator and IP Answering parts. If you don't need to replay the traffic captured you keep time by avoiding reading this paragraph.



You specify a capture traffic file name in the “**Input traffic file**” object and two output files.

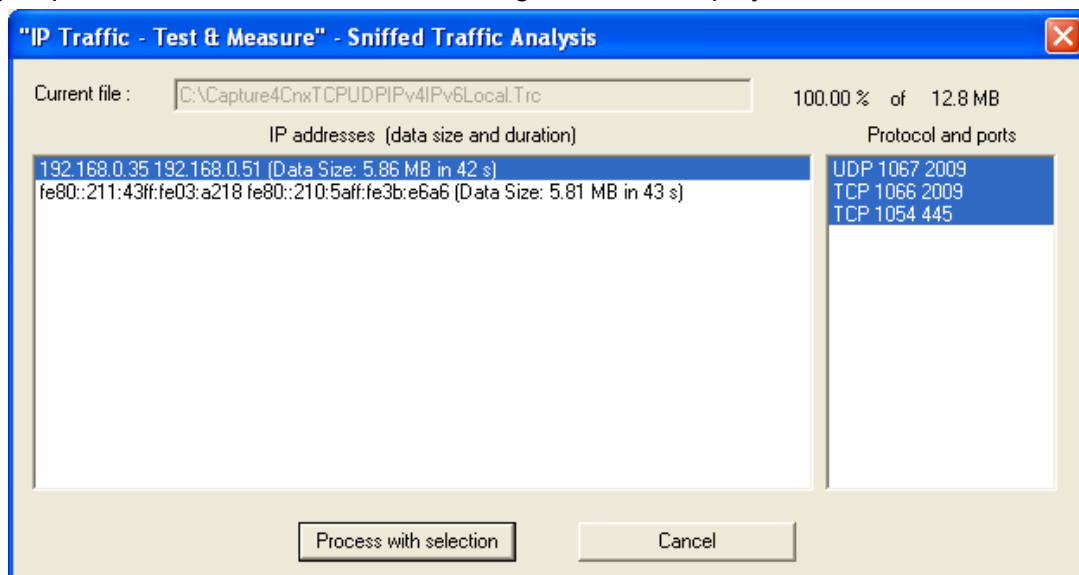
Note:

*The “**Input traffic file**” must contain data (see Step 2). The Step 3 can't use the files containing only headers.*

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**”. The extension of these files must be “.dtr” (data to replay). This is an owner format used only by the IP Generator and IP Answering parts. This algorithm reassembles the fragmented packets before dispatching them in the two files. It is able to handle up to 50 fragments to reassemble a packet.

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



You should select connections to consider (addresses + protocol and ports) and then press the “Process with selection” button.

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

11.11 The 'Traffic Observer' tab

This fifth tab allows:

- Visualizing statistics and graphs for different parameters: IP throughput, Inter packet delay, Packet Erasure Rate quality (PER quality) and Packet transit delay,
- Downloading remote statistics traffic files,
- Analyzing off-line traffic,
- Exporting the statistics into 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 CSV file and Start / Stop the export process.

IP Generator - Parameters

IP Generator - Traffic + Statistics

IP Answering - Parameters + Statistics

Traffic Sniffer

Traffic Observer

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 |

IP Generator

IP Answering

Statistics Display

Values

Graphics

IP Throughput

Inter Packet Delay

Packet Transit Delay

PER Quality

Packet Statistics

Reset Statistics

Help

Remote Traffic Files

Download...

Off-Line Traffic Analysis

Yes

No

Process Files...

Play >

Play >>

Pause

Stop

Index (On-Line or Off-Line)

Next >

Add

00 / 00

Remove

Remove all

Export Statistics

Parameters

Start

Stop

Tab 5: Traffic Observer (on-line mode)

Note:

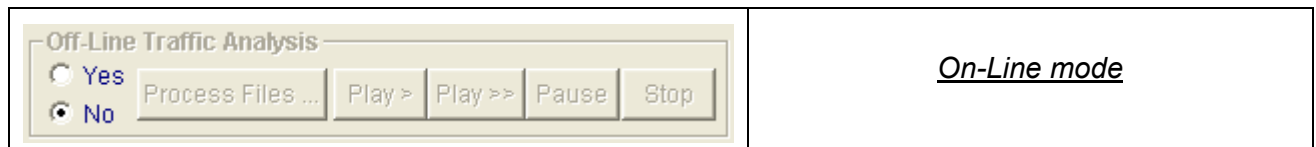
Values and statistics displayed in this tab are calculated at the 'time' point of reference (see "IP Traffic – Test & Measure" architecture in 1.2 Architecture) i.e. under the TCP/IP protocol stack.

11.11.1 "IP Traffic – Test & Measure": On-line and Off-line modes for statistics

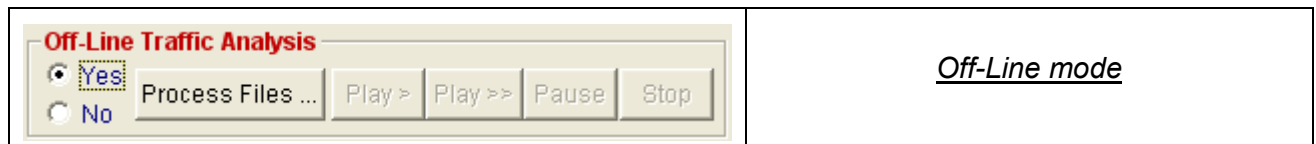
When **"IP Traffic – Test & Measure"** is operating ('IP Generator' is active and/or 'IP Answering' is active), this mode is named on-line. On-line statistics are displayed in the following tabs:

- '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.

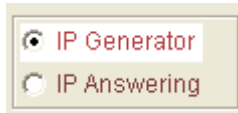
In order to analyze traffic files and obtain all statistics, the user must first download a traffic file from the remote. **"IP Traffic – Test & Measure"** uses two traffic files to do off-line statistics analysis: a 'local' traffic file (generated by the 'Traffic Sniffer') and a downloaded 'remote'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

11.11.2 Objects and command buttons

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

11.11.2.1 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.

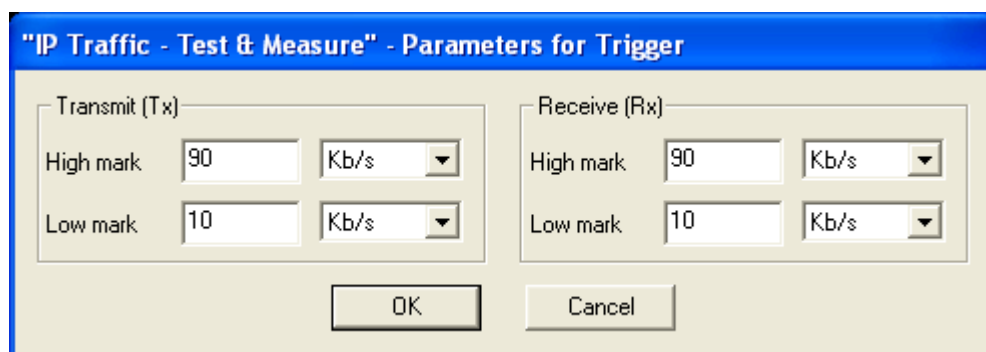
You can define different scale factors for the Transmit (Tx) and the Receive (Rx) graphs, and one value for the time scale.



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



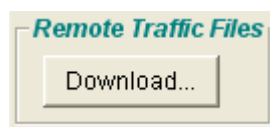
- **Values:** a values table (6 parameters for each connection with Tx and Rx values) is displayed (on-line and off-line),
- **Graphics:** select first 1 or all connections and then the parameter to display:
 - **IP Throughput** (on-line and off-line),
 - **Inter Packet Delay** (on-line and off-line),
 - **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).

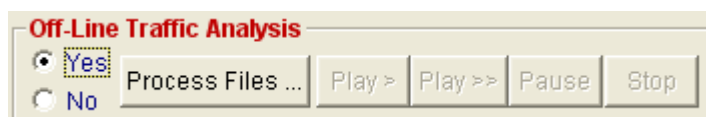
The command button **"Help"** displays a help window explaining all functionalities and commands for the 'Traffic Observer' tab.

11.11.2.2 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.

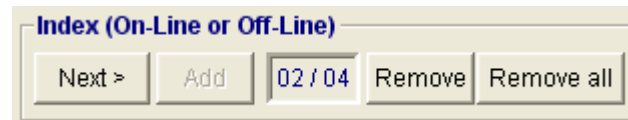
- **"Process files...":** to select two traffic files (a local traffic file and a remote traffic file downloaded via the previous **"Download..."** command button by example).
- **"Play >":** **"IP Traffic – Test & Measure"** replays the local traffic file at the beginning (selected via the previous "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.

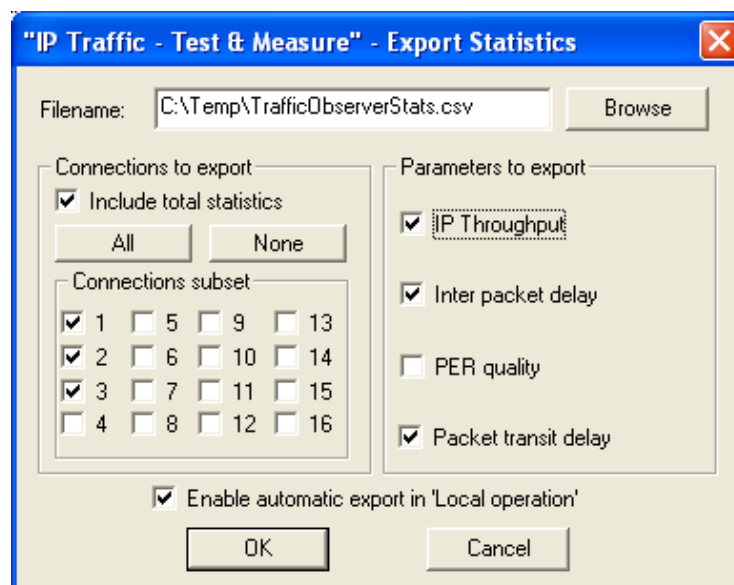
- **"Next >"**: the current position in the traffic file to analyze is set to the next display index set by the user.
- **"Add"**: adds a display index at the current position.
- **"XX/YY"**: displays the actual XX index number (YY is the total number of indexes set by the user).
- **"Remove"**: removes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

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



You define first the export filters and filename by using the command button **"Parameters"**. The export filters allow selecting: connection(s) and parameter(s). The statistics export file is a CSV file.

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



Parameters to export statistics

Filename

The statistics are saved in the specified CSV 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.

Note: Only up to 255 columns can be exported in the statistics file. It's impossible to select all statistics for all connections. A warning message is display if this limit is reached.

Format of the statistics file

The general format is defined for one line in the file (with the comma 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

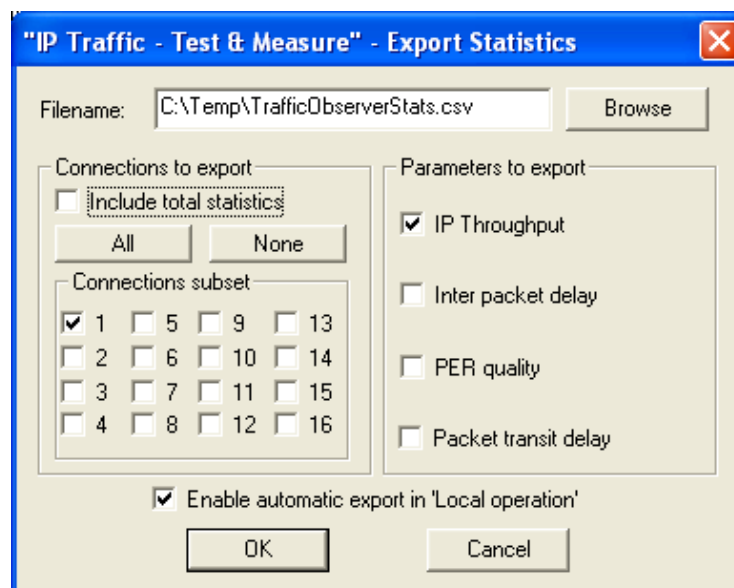
Note:

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:

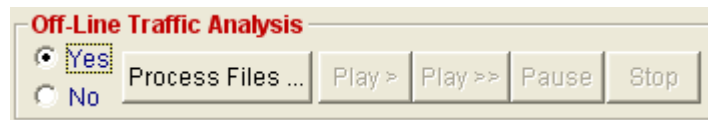


View of the generated file (by Excel):

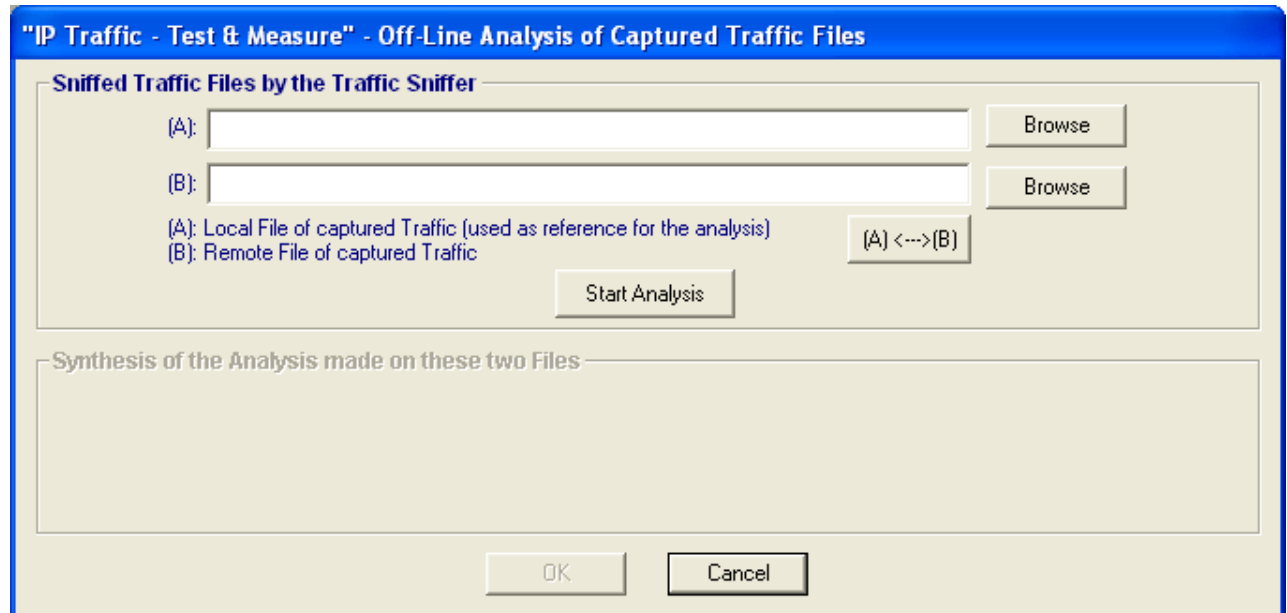
| Location | Date / Time | IP Generator - #01 Throughput Tx (Kb/s) | IP Generator - #01 Throughput Rx (Kb/s) | IP Answering - #01 Throughput Tx (Kb/s) | IP Answering - #01 Throughput Rx (Kb/s) |
|----------|---------------------|--|--|--|--|
| | 04/02/2005 10:05:32 | 585.37 | 7.80 | 7150.11 | 6724.68 |
| | 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 |
| | | | | | |
| | | Column 3 | Column 4 | Column 5 | Column 6 |

The columns 3 and 4 refer to the 'IP Generator' part and columns 5 and 6 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:

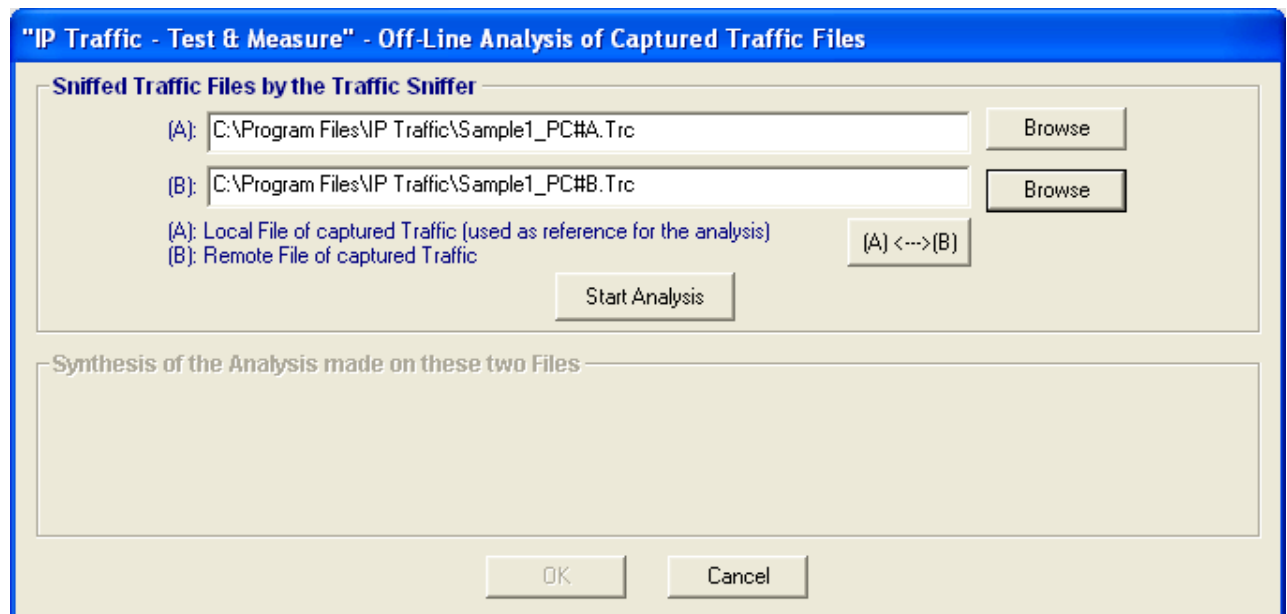


In order to proceed, you must input a local sniffed traffic file in (A) and a remote sniffed traffic file in (B).

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): C:\Program Files\IP Traffic\Sample1_PC#A.Trc (B): C:\Program Files\IP Traffic\Sample1_PC#B.Trc

(A) is used as reference for the analysis

Collapse Expand

Not Scanned Start Scan Stop Scan Not Scanned

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

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!"

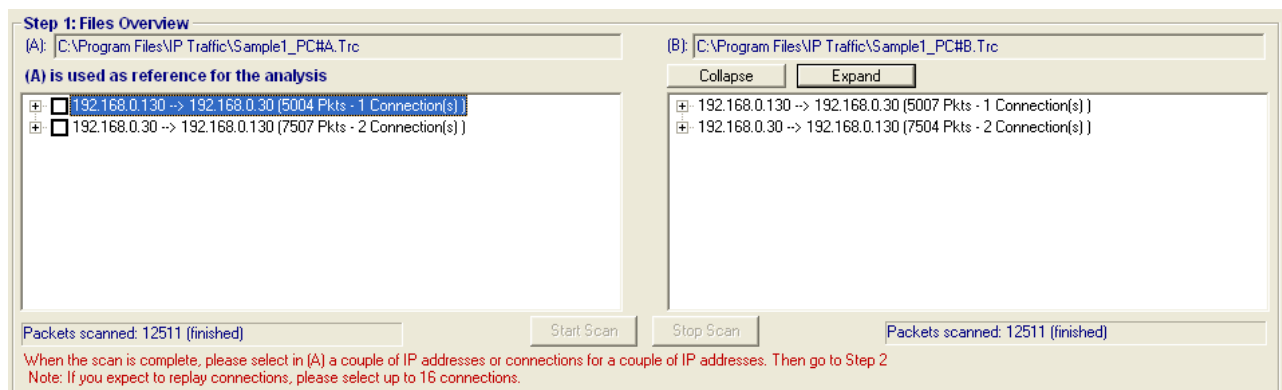
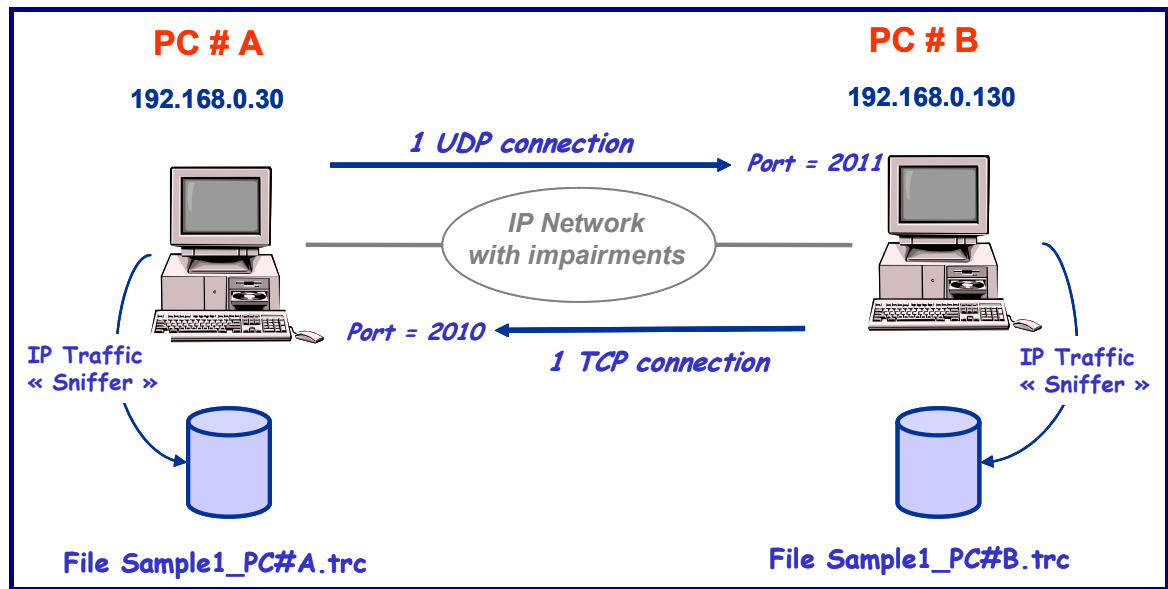
OK Cancel

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.

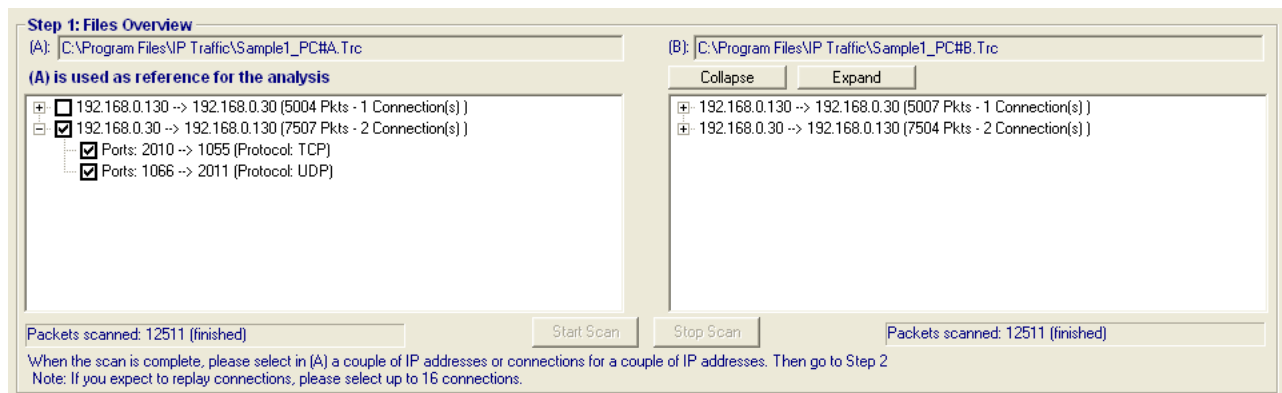
For (B), two additional buttons are available 'Collapse' and 'Expand'.

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.



The **Step 2** is aimed to find the synchronization between the two files by using up to 6 criteria:

- Source IP address
- Source Port Number
- Destination IP address
- Destination Port Number
- Identification number (corresponding to the Identification field of the IP header)
- Hash Code (MD5 Algorithm), available on the captured traffic files generated since the version 2.4.0 of "IP Traffic – Test & Measure". This Hash Code is based on the IP data payload.

The Hash Code is very useful to identify the packets captured for example on mobile or satellite networks. In this case, packets can go through a NAT. So the IP addresses and the IP Identifier may be replaced. If the port numbers are changed too, the Hash Code can't be used anymore to identify the packets.

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 synchronization found. Please check the criteria and check also if you have specified both good files. |

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:

The image shows two windows from a software application. The top window, titled 'Step 1: Files Overview', displays two file paths: (A) C:\Program Files\IP Traffic\Sample1_PC#A.Trc and (B) C:\Program Files\IP Traffic\Sample1_PC#B.Trc. Below each path is a list of connections. For file (A), the selected connection is 192.168.0.30 -> 192.168.0.130 (7507 Pkts - 2 Connection(s)), with sub-entries for Ports: 2010 -> 1055 (Protocol: TCP) and Ports: 1066 -> 2011 (Protocol: UDP). The bottom of this window shows 'Packets scanned: 12511 (finished)' and buttons for 'Start Scan' and 'Stop Scan'. The bottom window, titled 'Step 2: Criteria to search the Synchronization between these two files', shows search criteria for Source, Destination, and Others. Under Source and Destination, 'IP Address' and 'Port Number' are checked. Under Others, 'Identification (IP header field)' is checked, and 'Hash Code (MD5)' is unchecked. The status bar indicates 'Synchro Found (File A: Packet #1 <-> File B: Packet #1)'. Buttons for 'Start Scan' and 'Stop Scan' are present, along with the text '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).

The image shows a window titled 'Step 3: Analysis to compute Packets Statistics'. It features a text input field for 'Number of packets analysed:' with a 'Start Analysis' button next to it and a 'Stop Analysis' button to the right. Below this is a large empty rectangular box labeled 'Synthesis of the Analysis made on these two Files'. At the bottom of the window, a message states '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\ZTI\IPTraffic](#).

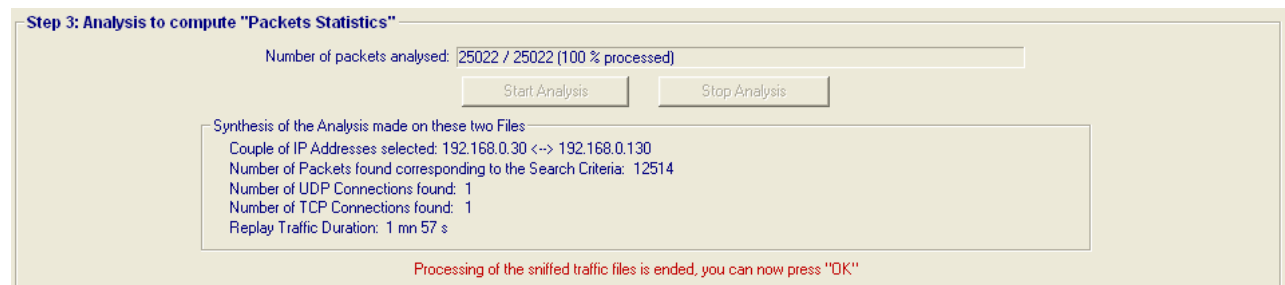
Moreover, this algorithm reassembles the fragmented packets before dispatching them in the two files. It is able to handle up to 50 fragments to reassemble a packet.

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:

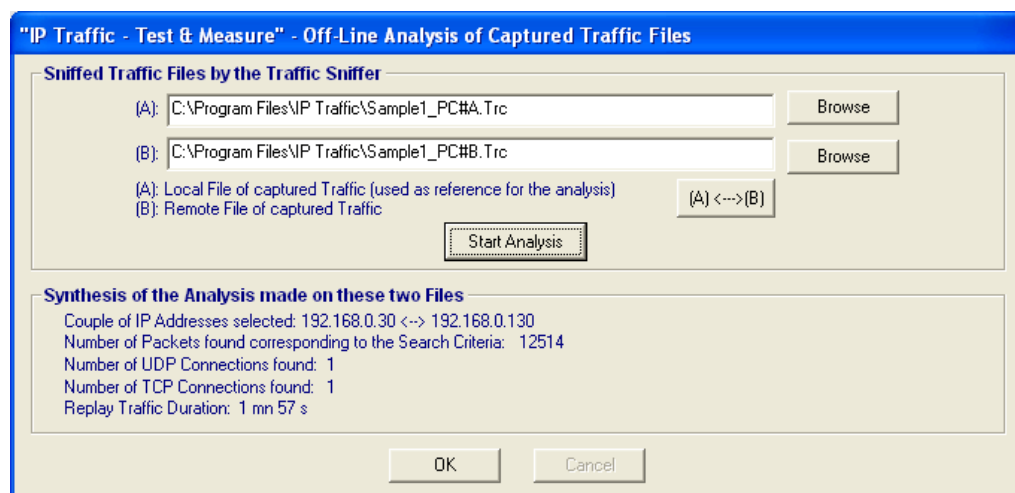
- Couple of IP addresses selected
- Number of packets found corresponding to the search criteria defined in the Step 2
- Number of UDP connections found
- Number of TDP connections found
- Replay traffic duration (useful if you want to play these sniffed traffic files via the Traffic Observer)



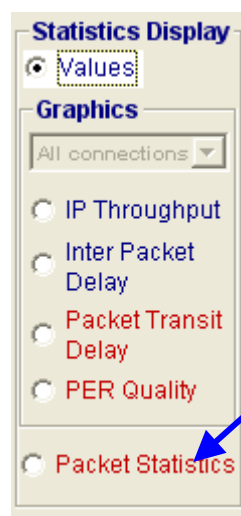
Note:

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

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... |
|-----------------|--------|--------|-------------|-----------------|-----------|
| 🕒 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(Pro... | Packets | Lost | % ... | Delay | Jitter | TCP... |
|---------------------|---------|------|-------|---------|--------|--------|
| Total Computer A | 7507 | 3 | 0% | 120 ... | 1 ms | 0 |
| 1066 -> 2011 (U... | 5000 | 3 | 0% | 178 ... | 1 ms | N/A |
| 2010 -> 1055 (T... | 2507 | 0 | 0% | 6 ms | 0 ms | 0 |

| 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 |

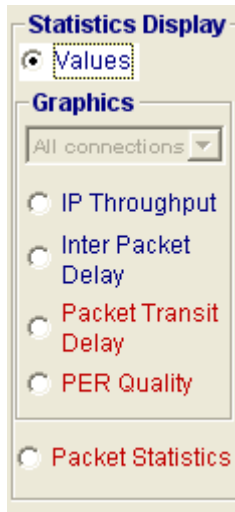
| Port -> Port(Pro... | Packets | Lost | % ... | Delay | Jitter | TCP... |
|---------------------|---------|------|-------|-------|--------|--------|
| Total Computer B | 5007 | 3 | 0% | 8 ms | 0 ms | 3 |
| 1055 -> 2010 (T... | 5007 | 3 | 0% | 8 ms | 0 ms | 3 |

More information on the 'Packet Statistics' object is explained further in this chapter.

Note:

If the captures have been realized without GPS and ZClock systems, the values show in the "delay" column are close to the definition of the jitter. Why ? The first packet found in the both files allows realizing the synchronization. "IP Traffic – Test & Measure" compares the two timestamps to calculate the delta time between the transmitting and the receiving of the packet. Then, this delta time is added or suppressed to each transit delay calculated for each packet. That is why the result is close to a variation of the transit delay and so close to the jitter notion.

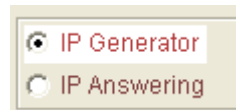
11.11.3 Values and statistics display



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.

11.11.3.1 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.

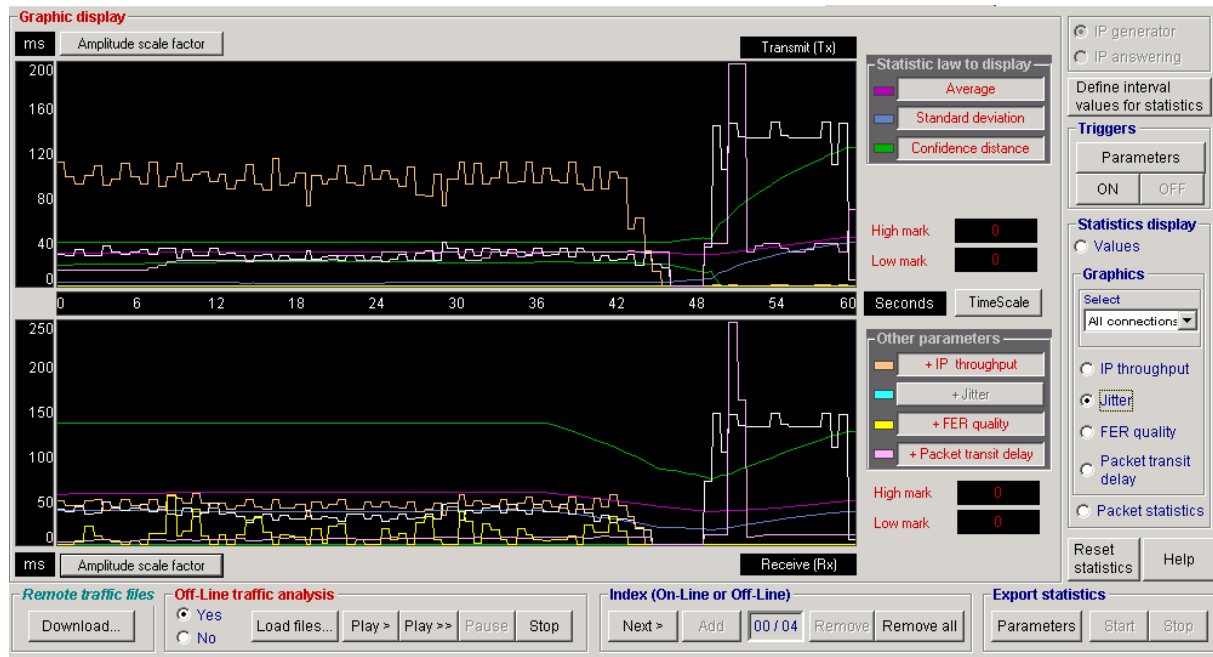
| Statistical Values (based on Driver Statistics) | | | | | | | | | | | | | | | |
|--|----------------------|------|-------|------------------------|----|-----------------------|----|-----------------------|----|--------------------|----|----------------------|----|---------------------------|----|
| | 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"/> | | | | | | | | | | | | | | | |

11.11.3.2 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:



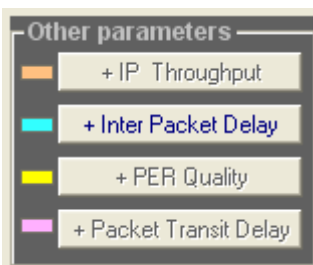
Example where all curves are displayed for all parameters

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.

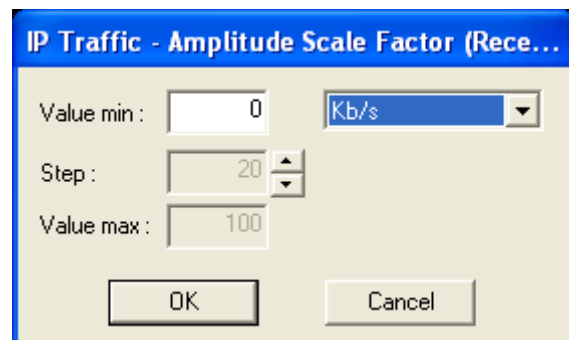
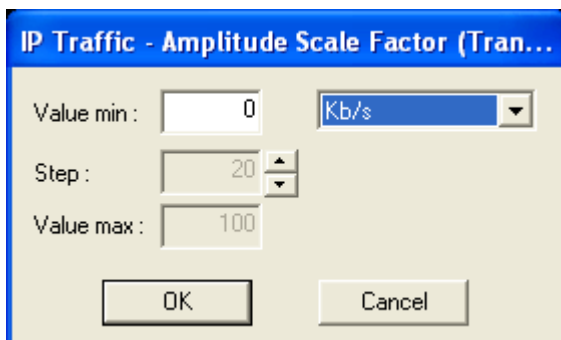
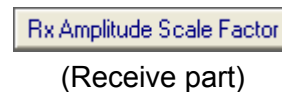
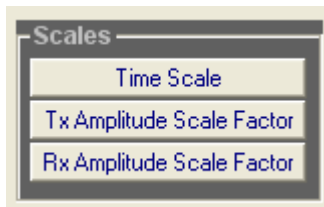
Time base scale for additional parameter to display is identical to the time base scale of the current parameter.

Formulas used for the statistical laws:

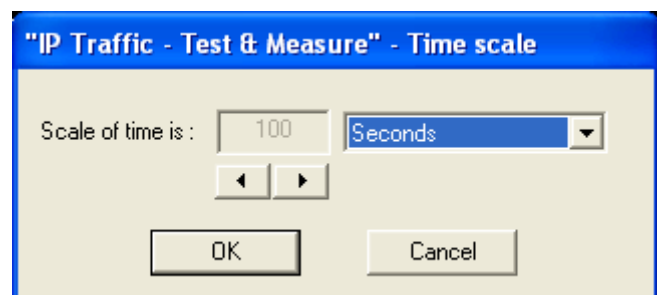
- Average m : $m = \frac{\sum_{i=1}^n x_i}{n}$
- Standard deviation σ : $\sigma = \sqrt{v}$ (with variance v defined as: $v = \frac{\sum_{i=1}^n x_i^2}{n} - m^2$)
- Confidence distance: 95.45 % of the values are between $(m - 2\sigma)$ and $(m + 2\sigma)$.

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.

11.11.3.3 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.

The screenshot shows the 'Offline Packet Statistics' window in the 'IP Traffic – Test & Measure' application. The window is titled 'Offline Packet Statistics' and has a tabbed interface with 'Traffic Observer' selected. It is divided into two main sections: 'Computer A ==> Computer B' and 'Computer B ==> Computer A'. Each section contains a table of packet statistics with columns for Time (UTC), Status, Direction, Port, IP size, and Identity. Below these tables are summary statistics for each computer, including Total Packets, Lost, % Lost, Delay, Jitter, and TCP... The interface also includes a 'Statistics Display' sidebar on the right with options for Values, Graphics, IP Throughput, Inter Packet Delay, Packet Transit Delay, and PER Quality. At the bottom, there are buttons for 'Remote Traffic Files', 'Off-Line Traffic Analysis', 'Index (On-Line or Off-Line)', and 'Export Statistics'.

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 of the jitter values calculated for all packets of the connection.

TCP Retransmission: number of TCP packets retransmitted

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. |

Note:

If the sniffed traffic files contain GPS location, the location is exported into the statistics file. Two columns are created. The first one is the GPS location of the computer when it sends the packet and the second one is the GPS location when the other computer receives the packet.

| 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 | TCP Retransmission | | | | |
| Total Computer A | 7508 | 5 | 0% | 122 ms | 1 ms | 0 | | | | |
| 2010 -> 1053 (TCP) | 2508 | 0 | 0% | 0 ms | 0 ms | 0 | | | | |
| 1064 -> 2011 (UDP) | 5000 | 5 | 0% | 184 ms | 1 ms | N/A | | | | |
| | | | | | | | | | | |
| Computer A ==> Computer B | | | | | | | | | | |
| Reference time | Location of Computer A | Location of Computer B | Time (UTC) | Status | Transit in ms (accuracy) | Source Port | Destination Port | IP size | (protocol) | Identifier |
| GPS | Lat +48° 44' 38.03" Lon - 3° 28' 21.11" Alt 121 Speed 0.000 m/s | Lat +48° 44' 37.94" Lon - 3° 28' 20.71" Alt 122 Speed 0.000 m/s | 21:55:03.559 | Sent | 180 (± 5) | 1064 | 2011 | 1488 | (UDP) | x9567 |
| GPS | Lat +48° 44' 38.03" Lon - 3° 28' 21.11" Alt 121 Speed 0.000 m/s | Lat +48° 44' 37.94" Lon - 3° 28' 20.71" Alt 122 Speed 0.000 m/s | 21:55:03.579 | Sent | 180 (± 5) | 1064 | 2011 | 1488 | (UDP) | x9568 |
| GPS | Lat +48° 44' 38.03" Lon - 3° 28' 21.11" Alt 121 Speed 0.000 m/s | Lat +48° 44' 37.94" Lon - 3° 28' 20.71" Alt 122 Speed 0.000 m/s | 21:55:03.598 | Sent | 171 (± 5) | 1064 | 2011 | 1488 | (UDP) | x9569 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| GPS | Lat +48° 44' 37.99" Lon - 3° 28' 20.99" Alt 122 Speed 0.000 m/s | Lat +48° 44' 37.96" Lon - 3° 28' 20.76" Alt 122 Speed 0.000 m/s | 21:56:36.804 | Sent | 185 (± 5) | 1064 | 2011 | 1488 | (UDP) | xAD1F |
| GPS | Lat +48° 44' 37.99" Lon - 3° 28' 20.99" Alt 122 Speed 0.000 m/s | Lat +48° 44' 37.96" Lon - 3° 28' 20.76" Alt 122 Speed 0.000 m/s | 21:56:36.826 | Sent | 183 (± 5) | 1064 | 2011 | 1488 | (UDP) | xAD20 |
| GPS | Lat +48° 44' 37.99" Lon - 3° 28' 20.99" Alt 122 Speed 0.000 m/s | Lat +48° 44' 37.96" Lon - 3° 28' 20.76" Alt 122 Speed 0.000 m/s | 21:56:36.837 | Sent | 1 (± 5) | 2010 | 1053 | 40 | (TCP) | xAD21 |
| PC | Lat +48° 44' 37.99" Lon - 3° 28' 20.99" Alt 122 Speed 0.000 m/s | | 21:56:36.845 | LOST | ... | 1064 | 2011 | 1488 | (UDP) | xAD22 |
| GPS | Lat +48° 44' 37.99" Lon - 3° 28' 20.99" Alt 122 Speed 0.000 m/s | Lat +48° 44' 37.96" Lon - 3° 28' 20.76" Alt 122 Speed 0.000 m/s | 21:56:36.867 | Sent | 182 (± 5) | 1064 | 2011 | 1488 | (UDP) | xAD23 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |

| Synthesis for Computer B | | | | | | | | | | |
|---------------------------|---|---|--------------|--------|--------------------------|--------------------|------------------|---------|------------|------------|
| Connection(Protocol) | Packets | Lost | % Lost | Delay | Jitter | TCP Retransmission | | | | |
| Total Computer B | 5007 | 4 | 0% | 1 ms | 0 ms | 4 | | | | |
| 1053 -> 2010 (TCP) | 5007 | 4 | 0% | 1 ms | 0 ms | 4 | | | | |
| 1053 -> 2010 (TCP) | 5007 | 4 | 0% | 1 ms | 0 ms | 4 | | | | |
| Computer B ==> Computer A | | | | | | | | | | |
| Reference time | Location of Computer B | Location of Computer A | Time (UTC) | Status | Transit in ms (accuracy) | Source Port | Destination Port | IP size | (protocol) | Identifier |
| GPS | Lat +48° 44' 37.94" Lon - 3° 28' 20.71" Alt 122 Speed 0.000 m/s | Lat +48° 44' 38.03" Lon - 3° 28' 21.11" Alt 121 Speed 0.000 m/s | 21:55:20.725 | Sent | 1 (± 5) | 1053 | 2010 | 48 | (TCP) | x3D21 |
| GPS | Lat +48° 44' 37.94" Lon - 3° 28' 20.71" Alt 122 Speed 0.000 m/s | Lat +48° 44' 38.03" Lon - 3° 28' 21.11" Alt 121 Speed 0.000 m/s | 21:55:20.726 | Sent | 1 (± 5) | 1053 | 2010 | 40 | (TCP) | x3D22 |
| GPS | Lat +48° 44' 37.94" Lon - 3° 28' 20.71" Alt 122 Speed 0.000 m/s | Lat +48° 44' 38.03" Lon - 3° 28' 21.11" Alt 121 Speed 0.000 m/s | 21:55:20.728 | Sent | 3 (± 5) | 1053 | 2010 | 1500 | (TCP) | x3D23 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| GPS | Lat +48° 44' 37.94" Lon - 3° 28' 20.72" Alt 121 Speed 0.000 m/s | Lat +48° 44' 38.01" Lon - 3° 28' 21.05" Alt 122 Speed 0.000 m/s | 21:55:56.395 | Sent | 2 (± 5) | 1053 | 2010 | 1500 | (TCP) | x43A7 |
| GPS | Lat +48° 44' 37.94" Lon - 3° 28' 20.72" Alt 121 Speed 0.000 m/s | Lat +48° 44' 38.01" Lon - 3° 28' 21.05" Alt 122 Speed 0.000 m/s | 21:55:56.415 | Sent | 1 (± 5) | 1053 | 2010 | 1500 | (TCP) | x43A8 |
| GPS | Lat +48° 44' 37.94" Lon - 3° 28' 20.72" Alt 121 Speed 0.000 m/s | Lat +48° 44' 38.01" Lon - 3° 28' 21.05" Alt 122 Speed 0.000 m/s | 21:55:56.435 | Sent | 2 (± 5) | 1053 | 2010 | 1500 | (TCP) | x43A9 |
| PC | Lat +48° 44' 37.94" Lon - 3° 28' 20.72" Alt 121 Speed 0.000 m/s | | 21:55:56.455 | LOST | ... | 1053 | 2010 | 1500 | (TCP) | x43AA |
| GPS | Lat +48° 44' 37.94" Lon - 3° 28' 20.72" Alt 121 Speed 0.000 m/s | Lat +48° 44' 38.01" Lon - 3° 28' 21.05" Alt 122 Speed 0.000 m/s | 21:55:56.475 | Sent | 2 (± 5) | 1053 | 2010 | 1500 | (TCP) | x43AB |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |

Four examples are shown more precisely in the Part 9 "Examples of sniffed traffic files" at the end of this user guide.

PART 12 Calculation Mode for the Statistics

12.1 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

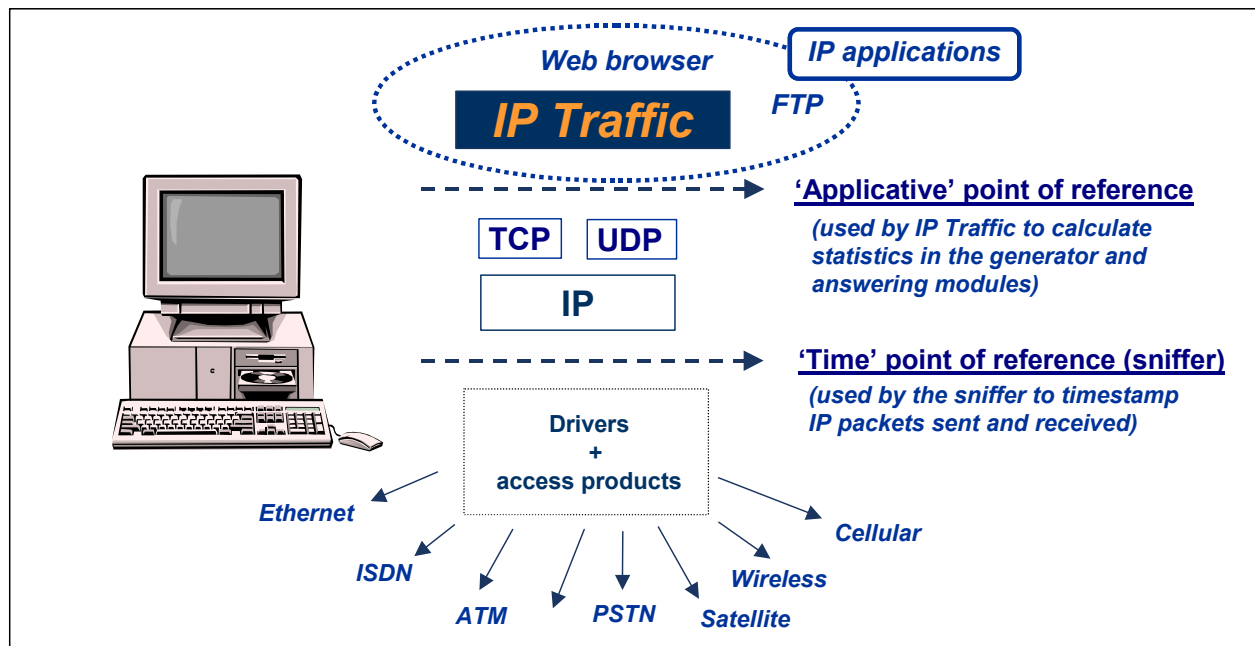
The statistics can be calculated on-line (real time mode) or off-line (differed time).

The off-line mode requires the analysis of two sniffed traffic files (the local traffic file and the remote traffic file sent back on the local machine) and allows calculating 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.

12.2 Statistics computed by "IP Traffic – Test & Measure"

12.2.1 Reference points to compute the statistics



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

- **'Applicative' point of reference**

In the 'IP Generator' and the 'IP Answering' modules, the 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 "IP Traffic – Test & Measure", and are independent of the protocol used (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. The 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).

12.2.2 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.

12.2.2.1 "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)
- Mean RTT (Round Trip Time)
- Min RTT
- Max RTT
- RTT summary (Minimum, Maximum and Mean RTT based on all RTT values calculated)

12.2.2.2 "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

12.2.2.3 The 'Traffic Observer' tab

With the **on-line** mode, the 'Statistics display' object displays the following parameters:

- ⇒ 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 'Statistics display' object displays the following parameters:

- ⇒ 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)

12.2.2.4 Main Window: IP Generator and IP Answering throughputs

This calculation is based using a sampling period (this parameter - Throughput sampling period, is defined by using the "Configuration / General Parameters" item menu. If the sampling period is for example 5 seconds, IP Traffic realizes the sum of received or sent data volume for the last 5 seconds and divides the result by 5 to obtain the throughput. Note that this throughput is an application level throughput (i.e this throughput corresponds to the TCP and/or UDP payload throughput). This calculation is realized for the both parts (IP Generator and IP Answering) and displayed at the bottom of the IP Traffic window.

12.3 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 - Test & Measure". This parameter also applies to statistics exportation. The throughput sampling period defines the number of seconds of traffic needed to calculate the throughput.

Refresh Time (1 to 60 seconds)

Throughput Sampling Period (1 to 60 seconds)

TCP and UDP received Data Timeout

These parameters are for the IP Generator Part only. When there is no more data to be sent, "IP Traffic - Test & Measure" continues to receive data until the timeout expires. Then the connection is released. When the timeout is 0, the connection is stopped as soon as there is no more data to be sent.

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

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

"IP Traffic - Test & Measure" Buffer Size (SO_RCVBUF and SO_SNDBUF)

The buffers used by "IP Traffic - Test & Measure" to dialog with the Winsock API influence the throughput performance for high speed network. The best performance can be reached with a high buffer size. Change in one of these sizes concerns the new connections only.

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

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

OK Cancel

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
- the Statistics Export Processes (on IP Generator and IP Answering Parts)

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.

12.4 The calculation method is used by "IP Traffic – Test & Measure" to compute statistics.

This document describes what calculation method is used by "IP Traffic – Test & Measure" to compute statistics.

12.4.1 The two calculation methods

12.4.1.1 Based on a sampling period

The statistics defined in this category are calculated by using a sampling period. The size of these sampling periods are defined either by the "Throughput Sampling Period" or by the "Acquisition period of statistics" specified in the "Configuration > General Parameters" window.

12.4.1.2 Cumulative

The statistics defined in this category are cumulative statistics. They are reset when a new connection or a new analysis is launched.

12.4.2 IP Traffic - IP Generator statistics

| Calculation method | Sampling | Cumulative |
|-------------------------------|----------|------------|
| Tx Throughput | X | |
| Rx Throughput | X | |
| Tx Packets Throughput | X | |
| Rx Packets Throughput | X | |
| Jitter | X | |
| Tx Packets | | X |
| Rx Packets | | X |
| Tx Volume | | X |
| Rx Volume | | X |
| Mean RTT (cumulative average) | X | |
| Min RTT | X | |
| Max RTT | X | |
| Sequence Error Number | X | |
| Mean RTT (summary) | X | |
| RTT Min (summary) | X | |
| RTT Max (summary) | X | |
| Tx+RxThroughput (Activity) | X | |

Table 1 - "IP Traffic - Test & Measure" - IP Generator calculation method

12.4.3 IP Traffic - IP Answering statistics

| Calculation method | Sampling | Cumulative |
|----------------------------|----------|------------|
| Tx Throughput | X | |
| Rx Throughput | X | |
| Tx Packets Throughput | X | |
| Rx Packets Throughput | X | |
| Jitter | X | |
| Tx Packets | | X |
| Rx Packets | | X |
| Tx Volume | | X |
| Rx Volume | | X |
| Date Not Echoed | | X |
| Sequence Error Number | X | |
| Tx+RxThroughput (Activity) | X | |

Table 2 - "IP Traffic - Test & Measure" - IP Answering calculation method

12.4.4 IP Traffic – Traffic Observer statistics

| Calculation method | Sampling | Cumulative |
|-------------------------|----------|------------|
| IP Throughput Snapshot* | X | |
| IP Throughput Average** | X | |
| UDP or TCP Throughput* | X | |
| Inter Packet Delay* | X | |
| Packet Transit Delay* | X | |
| Packet Erasure Rate* | X | |

*: These values are instantaneous values (the sampling is based on the "Acquisition period of statistics" specified in the "Configuration > General Parameters" window.

***: This value are an average based on the sampling period defined by the "Throughput Sampling Period" specified in the "Configuration > General Parameters" window.

Table 3 - "IP Traffic - Test & Measure" – Traffic Observer calculation method

12.4.5 IP Traffic –Packets Statistics Synthesis

| Calculation method | Sampling | Cumulative |
|--------------------|----------|------------|
| Packets | | X |
| Lost | | X |
| % Lost | | X |
| Delay | | X |
| Jitter | | X |
| TCP Retransmission | | X |

Table 4 - "IP Traffic - Test & Measure" – Packets Statistics calculation method

12.5 Detailed description for calculation of the statistics

12.5.1 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 = The jitter is the transit delay variation. This value is available only if the packets include the Timecode information (see "Parameters" in the IP Generator tab). For each received packet, the process to find the Timecode information is applied. If the RTT identifier is found, IP Traffic proceeds as follows: First, it compares the "time when sent" of the previously received packet with the "time when sent" of the last received packet. This information is added in the timecode structure just before sending the packet. Then, IP Traffic compares the arrival time of the previously received packet with the arrival time of the last received packet. After that, IP Traffic compares these two results. If the transit delay is a constant, the results should be the same. In the other case, it means that a jitter is found. IP Traffic adds the absolute value of this comparison and calculates the mean jitter (using a sampling period). Note that the jitter displayed on the IP Answering part is a one-way jitter and the jitter displayed on the IP Generator part is a two-ways jitter. Note also, that this jitter is an application level statistic. An IP level jitter is available with the offline mode analysis.

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 the sequence number is not correct. This value is available 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 tests if the sequence number of the received packet follows the sequence number of the previous received packet. If an error is detected, the 'Sequence numbering errors' parameter is incremented. Note that the sequence error number is incremented of one unit even if the sequence number gap is one unit, ten units or more. Moreover, no distinction is made about the origin of this error. IP Traffic doesn't know if the gap is due to a packet lost or a desequenced packet. To calculate this parameter on the IP Generator part, the remote 'IP Answering' module must be configured in 'echoer' mode (each packet received is transmitted to the originator).

Mean 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). This value is available 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 compares the "time when sent" of the last received packet with the arrival time of this packet. The difference gives a RTT value.

To calculate this parameter, the remote must be configured in echoer mode for the connection.

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
- 4 bytes time when sent
- 2 bytes length (without the RTT header)

Min RTT = minimum value 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) for one connection. This is the minimum RTT value since the connection beginning.

Max RTT = maximum value 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) for one connection. This is the maximum RTT value since the connection beginning.

RTT Summary = minimum, maximum and 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) but for all connections. The average is calculated on all RTT values of all connections that are using the Timecode option. In others words, the average is not an average of the Mean RTT of each 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.

12.5.2 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.

12.5.3 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.

12.5.3.1 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.

12.5.3.2 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.

12.5.3.3 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'.

12.5.3.4 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** σ : $\sigma = \sqrt{v}$ (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 13 Annexes

13.1 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.

13.1.1 Uniform Law

❖ Presentation:

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

With 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:

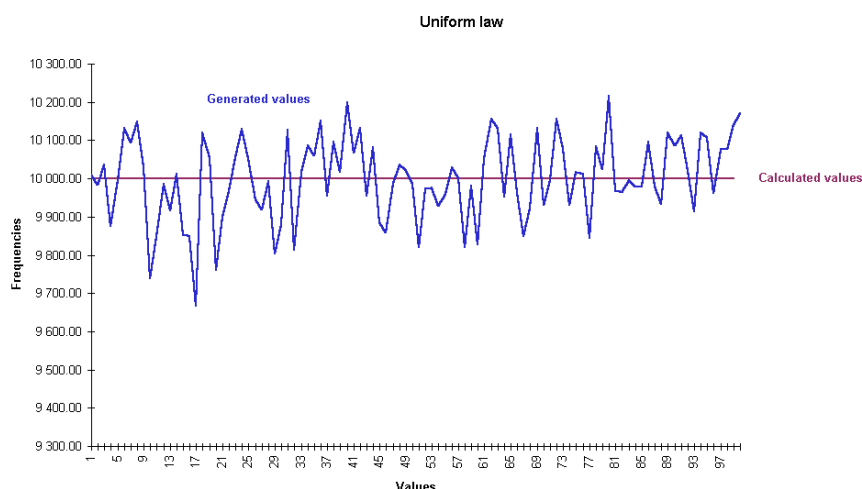
Uniform law on (α, β) range

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

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

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

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



13.1.2 Exponential Law

❖ Presentation

The Exponential law has only one parameter: λ . The more λ 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:

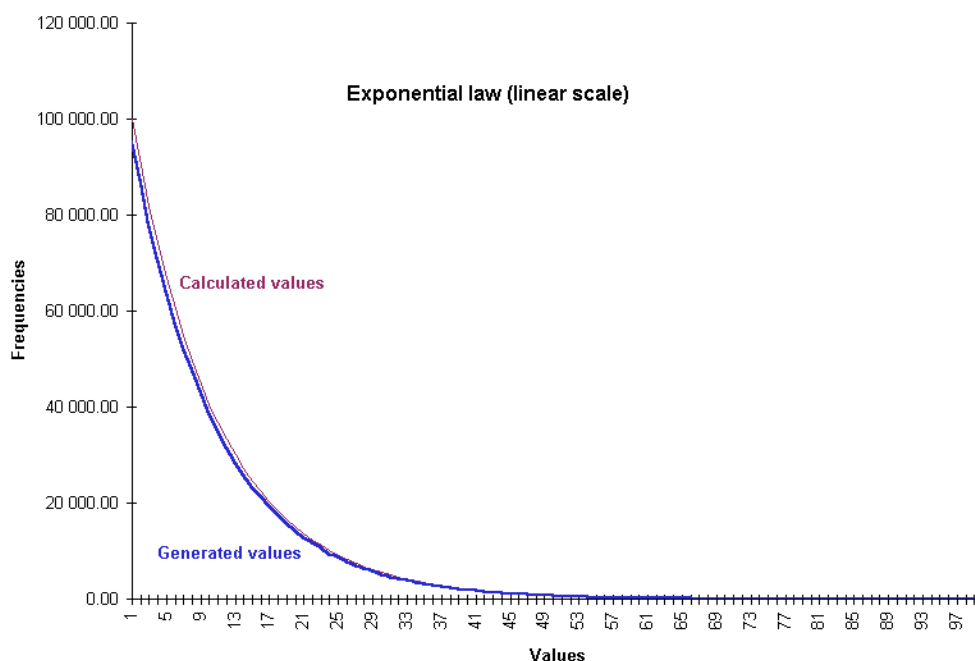
Exponential law ($\lambda > 0$)

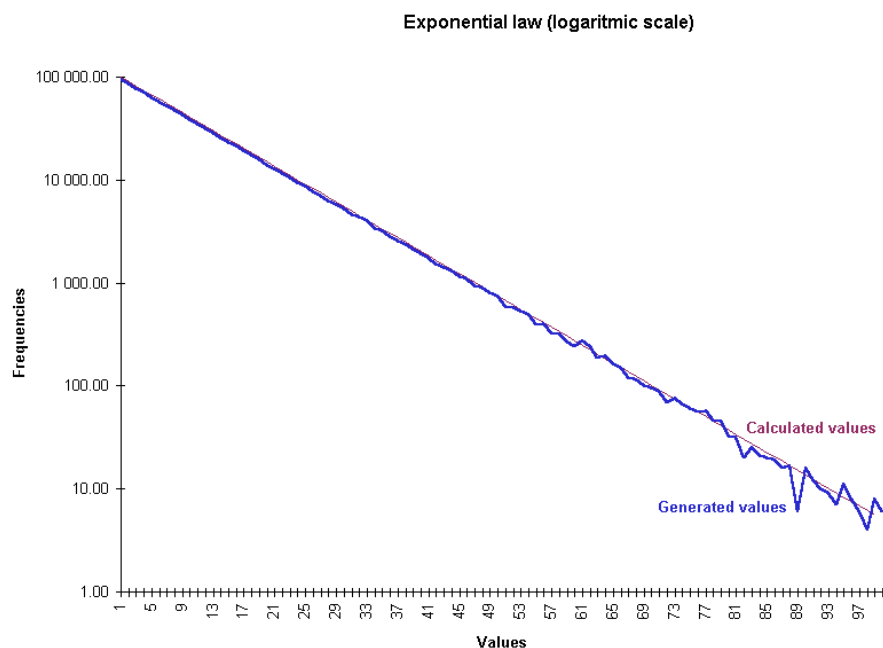
$$f(x) = \lambda e^{-\lambda x} \quad \text{if } x \geq 0$$

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

❖ 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 λ | | |

13.1.3 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 β . a unit is the final unit of the volume. β does not have unit because it represents a coefficient of variation of result around a value.

The following values have been noticed:

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

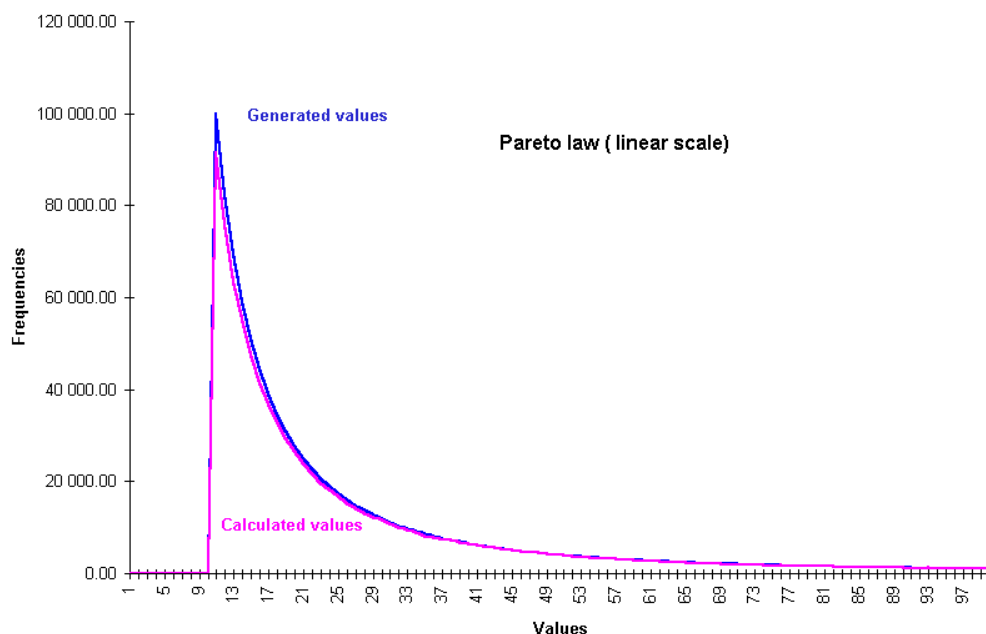
❖ Mathematical function:

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 $\beta = 1$.



13.1.4 Gauss law

❖ *Presentation:*

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

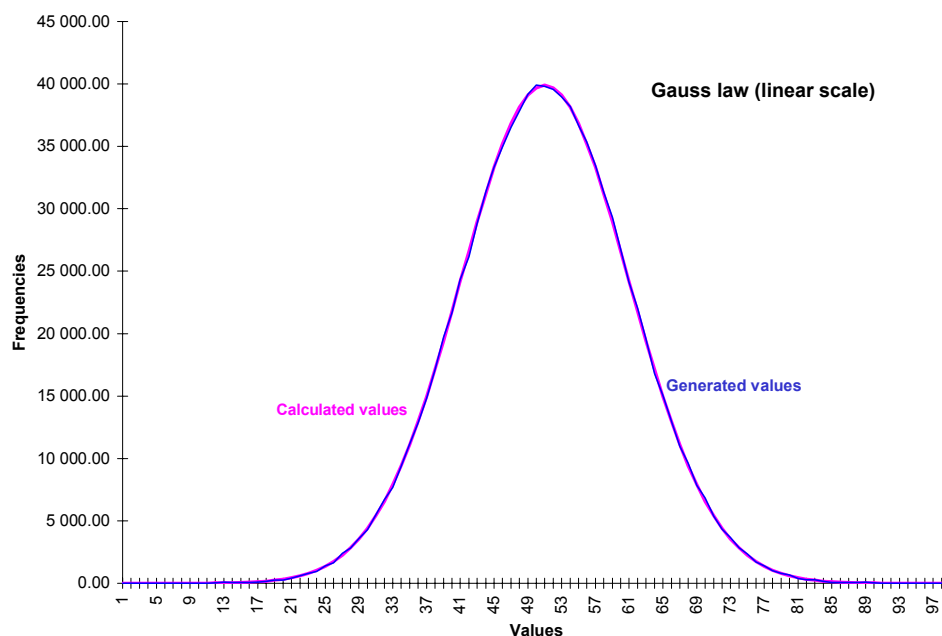
With this law, the unit used is the millisecond for the starting time connection generation laws and byte for the data volume to send laws.

❖ *Mathematical function:*

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

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

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



13.2 "IP Traffic – Test & Measure" Traces

In case of problem when using "IP Traffic – Test & Measure", the trace functionality allows retrieving 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.**

13.3 Configuration parameters saved in the Registry database

The based key to access these parameters is [\\HKEY_LOCAL_MACHINE\Software\ZTI\IPTraffic](#).

| Key name | Type | Default value (dec) | Description |
|-------------------------------|-----------|---------------------|--|
| DEBUGLEVEL | 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 0x00004000 Provide information via the GPS. 0x00010000 Detail operations of the Replay mode 0x00020000 Detail operations for the Off-line mode. 0x00080000 Specific flag for statistics generated at the 'IP Generator' and 'IP Answering' levels. |
| DEBUGFILENAME | REG_SZ | DEBUG.LOG | Filename to save the traces. |
| DEPTHFORPACKETANALYSIS | REG_DWORD | 500 | Parameter used in the search algorithm of the 'Traffic Observer' to calculate the packets statistics. |
| UDPINACTIVITY | 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). |
| TCPINACTIVITY | REG_DWORD | 10 | For TCP connections, timer (expressed in seconds) to detect the 'IP Generator' has stopped the connection (10 seconds by default). "IP Traffic" closes the TCP connection. |
| SENDTIMEOUT | REG_DWORD | 500 | Maximal period (expressed in milliseconds) allocated to send/receive data (default is 500 milliseconds). |
| TCPCONNECTRETRYCOUNTER | REG_DWORD | 0x1 | Number of retry to establish a TCP connection |
| TCPNODELAY | REG_DWORD | 0x0 | 0x0: Nagle algorithm enabled Other value: Nagle algorithm disabled |
| TCPRECEIVERPACKETSIZE | 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 |
| FILETRANSFERINACTIVITY | 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). "IP Traffic" closes the file transfer connection when the timer is reached. |
| FILETRANSFERPACKETSIZE | REG_DWORD | 1460 | Maximum size of a packet used during a file transfer. (Expressed in bytes. Default value = 1460. Max value = 65,535). |
| RPCPORT | REG_DWORD | 1001 | This is the port number used by the RPC server to dialog with the Automation Tool. |

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 |
|---------------------------|-----------|---------------------|---|
| ACROREADINFO | REG_SZ | x | Reserved |
| ACROREADTIMER | REG_DWORD | x | Reserved |
| HELP-GENERAL | REG_DWORD | x | Reserved |
| HELP-OBSERVER | REG_DWORD | x | Reserved |
| HELP-AUTOMATICMODE | REG_DWORD | x | Reserved |
| HELP-UNITARYMODE | REG_DWORD | x | Reserved |
| HELP-SNIFFER | REG_DWORD | x | Reserved |
| HELP-GPS | REG_DWORD | x | Reserved |
| HELP-REPLAYMODE | REG_DWORD | x | Reserved |
| HELP-REPLAYMODE-RCV | REG_DWORD | x | Reserved |
| HELP-FILEMANAGER | REG_DWORD | x | Reserved |
| HELP-EXPORTSTATS-SENDER | REG_DWORD | x | Reserved |
| HELP-EXPORTSTATS-RECEIVER | REG_DWORD | x | Reserved |
| HELP-PARAMCNX-SENDER | REG_DWORD | x | Reserved |
| HELP-FILEDOWNLOADING | REG_DWORD | x | Reserved |
| HELP-PARAMCNX-RECEIVER | REG_DWORD | x | Reserved |
| AUTOMATION PATH | REG_SZ | | Full path name to Aut_IPTraff .exe ("Automation Tool for IP Traffic" binary file. |
| IPTRAFFICPATH | REG_SZ | | Full path name to the "IP Traffic – Test & Measure" binary file. |
| CURRENTVERSION | REG_SZ | V 2.4.0 | Current version installed. |
| INSTALLATIONPATH | REG_SZ | | Selected installation path ('[Your Windows Drive]\Program Files\IP Traffic' by default. |
| USELOCALTIME | REG_DWORD | x | Save in the registry the time reference used by the Automation Tool |

13.4 Default Values of a Context

The default values when opening a new context are:

♦ IP Generator parameters

| | | | |
|---------------------|--------------|---------------------------|---|
| IP address | NO_ADDRESS | | |
| Port Number | 2009 | | |
| Protocol | TCP | | |
| Testing mode | Unitary mode | Data source | Packet generator (number of packets: infinite, packet contents: fix = 5A) |
| | | Packets size | Fix = 1460 bytes |
| | | Inter Packet Delay | Fix = 20 ms |
| | | RTT option | No |

♦ IP Answering parameters

| | |
|-------------------------------|-------------|
| IP address | ANY_ADDRESS |
| Port number | 2009 |
| Protocol | TCP |
| Receiving working mode | Absorber |

♦ Configuration

TCP stack parameters

| | | |
|-------------------------|----------------------|---------------------------------|
| TCP Buffer size | | |
| | S0_RCVBUF | 8192 |
| | S0_SNDBUF | 8192 |
| TCP Windows size | | |
| | TCPWindowSize | Windows configuration dependant |
| | SACKS Options | Windows configuration dependant |

Display parameters

| | |
|-----------------------------------|-----|
| Refresh time | 2 s |
| Throughput sampling period | 5 s |

Connection parameters

| | |
|--|---------|
| Timeout for TCP packets echoed | 500 ms |
| Timeout for UDP packets echoed | 700 ms |
| Acquisition period for statistics | 1000 ms |

File Operating Modes parameter

| | |
|----------------------------|-----------|
| File Operating Mode | Overwrite |
|----------------------------|-----------|

♦ File transfer

| | |
|--------------------|------|
| Port number | 2500 |
|--------------------|------|

◆ Remote port

| | |
|-------------|-------------|
| Port number | 2600 |
| IP address | ANY_ADDRESS |

◆ GPS parameter

| | |
|-------------|---------|
| Port number | COM1 |
| Speed | 9600 |
| Data | 8 bytes |
| Stop | 1 bit |
| Parity | Odd |

◆ Traffic Observer

| | |
|--------------------|-----------|
| Mode | Generator |
| Statistics display | Values |

◆ Graphical units

| UNIT | Value | Trigger |
|----------------------|------------|------------|
| IP throughput | 0-100 Kb/s | 10-90 Kb/s |
| Inter packet delay | 0-50 ms | 10-90 ms |
| PER quality | 0-100 | 10-90 |
| Packet transit delay | 0-1000 ms | 100-900 ms |

◆ Driver polling interval

| | |
|--------|---------|
| Period | 1000 ms |
|--------|---------|

◆ Sniffer

| | |
|---------------------|-----|
| Auto refresh period | 5 s |
|---------------------|-----|

13.5 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

13.6 External DLL for the 'IP Generator' module

The 'IP Generator' module loads this external DLL. 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).

13.6.1 TrafficInit

BOOL CALLBACK TrafficInit(int CnxID, unsigned long IPAddr, unsigned char protocol, unsigned port)

To init a new connection identified by par CnxID.

Parameters:

| | |
|-----------------|------------------------------|
| CnxID | Connection identifier |
| IPAddr | Remote IP address |
| Protocol | Protocol to use (UDP or TCP) |
| Port | Port number |

Return codes:

| | |
|--------------|---|
| True | The DLL is ready to provide data to the IP Generator. |
| False | 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.

13.6.2 PacketDelay

BOOL CALLBACK PacketDelay(int CnxID, unsigned long *pulDelay)

Parameters:

| | |
|-----------------|---|
| CnxID | Connection identifier |
| pulDelay | Address for delay expressed in milliseconds |

Return codes:

| | |
|--------------|--|
| True | The DLL has provided the delay for the next packet. If this delay equals 0, the IP Generator calls immediately PacketData() . |
| False | 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.

13.6.3 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:

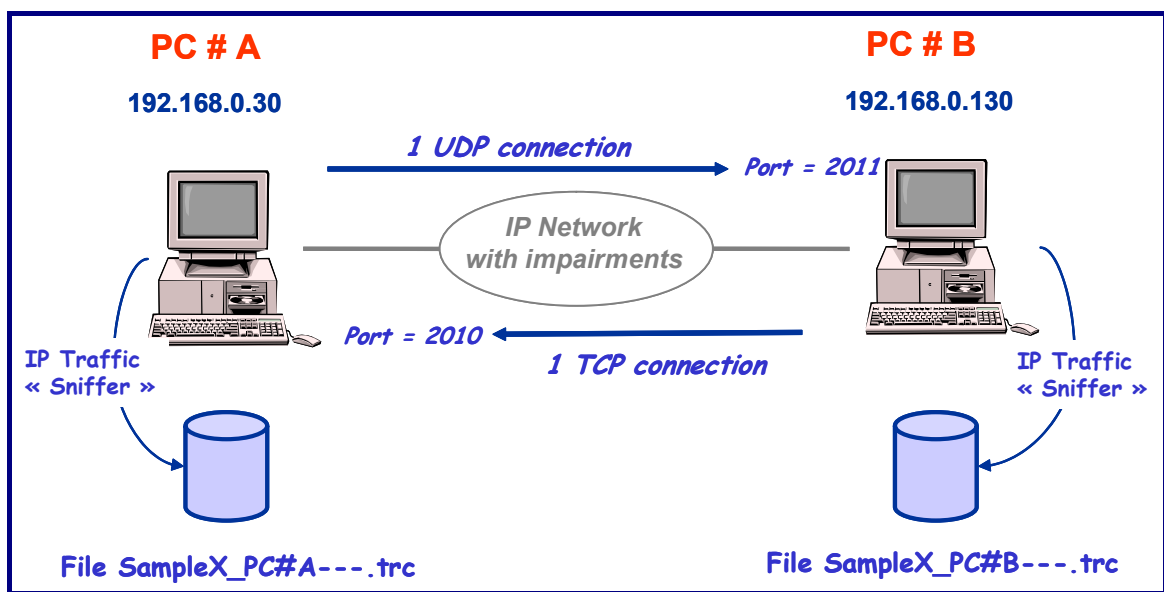
Before calling the [PacketData\(\)](#) function, the buffer pointed by pBuffer is initialized with zeros. The used length is initialized with zeros. The maximum size is 1460 in the sample.

PART 14 Examples of sniffed traffic files

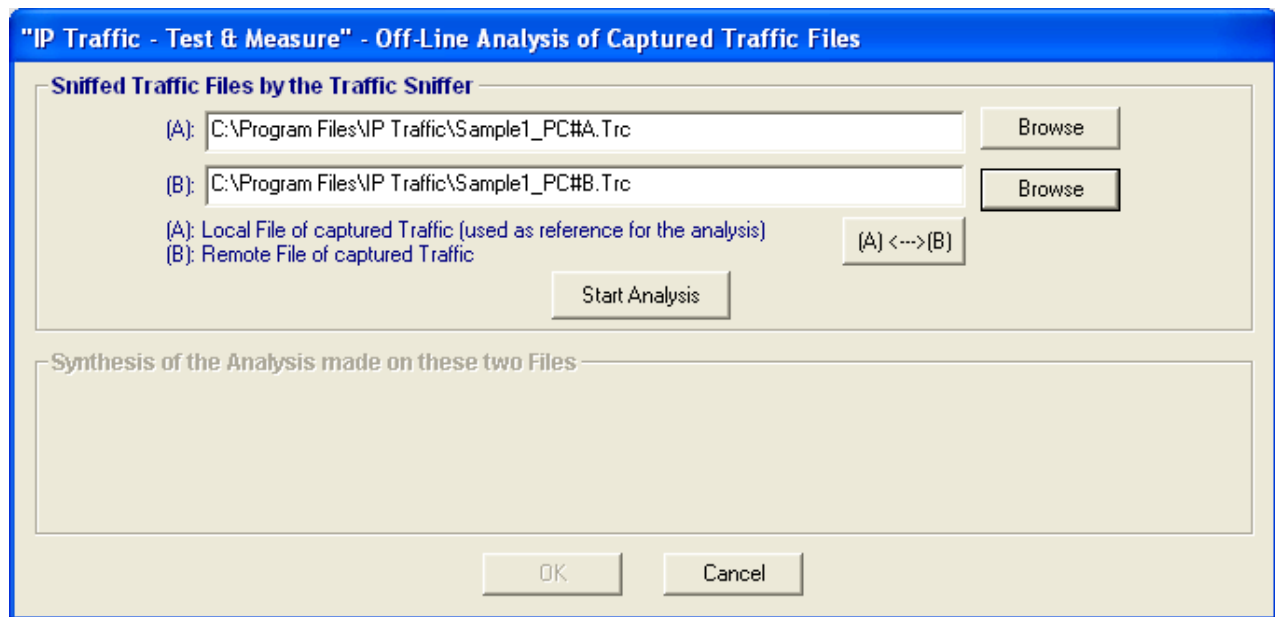
Six traffic captured files are provided to illustrate the off-line analysis:

- 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](#))
- Example 4: two files with IPv6 packets
([Sample4_PC#A_with_IPv6.Trc](#) and [Sample4_PC#B_with_IPv6.Trc](#))

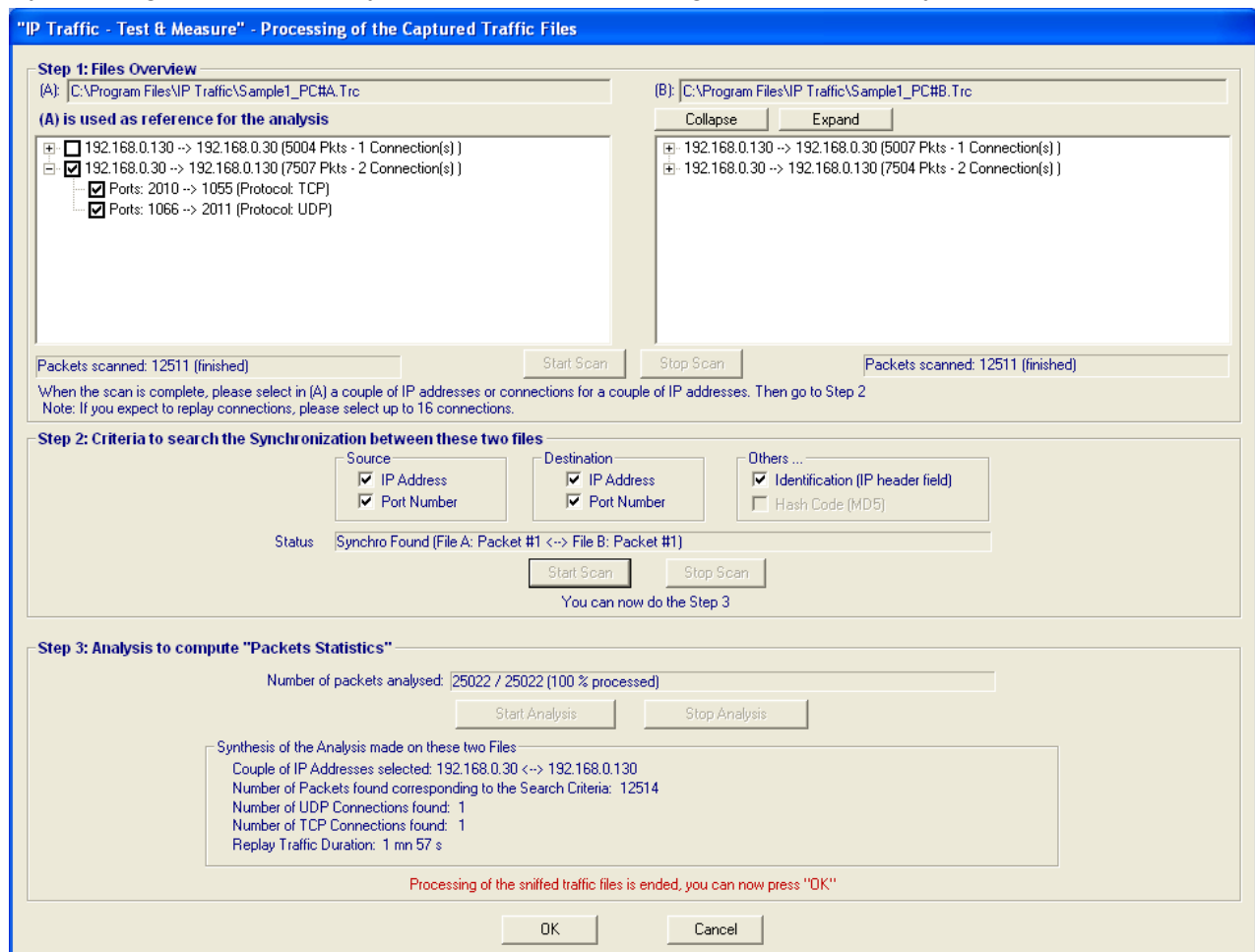
The test configuration used to generate three first traffic files is defined as below:



Example 1: no GPS kit and no ZClock module



By pressing the « Start Analysis » button, the following window is displayed.



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

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... |
|-----------------|--------|--------|-------------|-----------------|-----------|
| 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(Pro... | Packets | Lost | % ... | Delay | Jitter | TCP... |
|---------------------|---------|------|-------|--------|--------|--------|
| Total Computer A | 7507 | 3 | 0% | 120 ms | 1 ms | 0 |
| 1066 -> 2011 (U... | 5000 | 3 | 0% | 178 ms | 1 ms | N/A |
| 2010 -> 1055 (T... | 2507 | 0 | 0% | 6 ms | 0 ms | 0 |

| 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 |

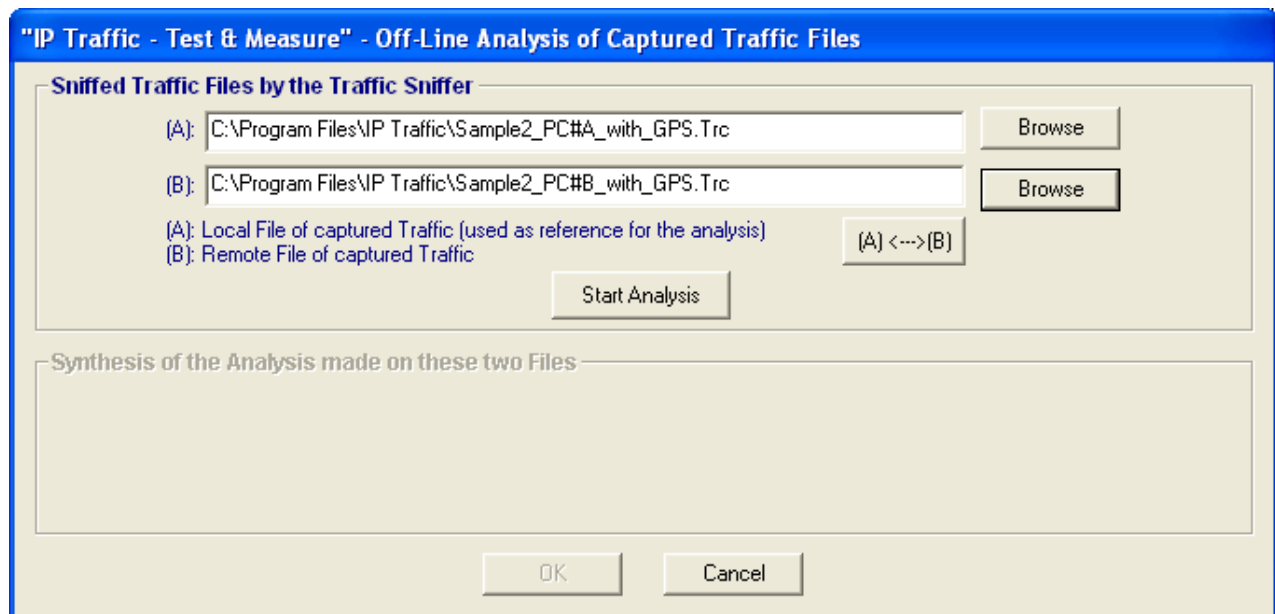
| Port -> Port(Pro... | Packets | Lost | % ... | Delay | Jitter | TCP... |
|---------------------|---------|------|-------|-------|--------|--------|
| Total Computer B | 5007 | 3 | 0% | 8 ms | 0 ms | 3 |
| 1055 -> 2010 (T... | 5007 | 3 | 0% | 8 ms | 0 ms | 3 |

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 8 ms. Note also that 3 TCP packets sent by the PC #B have been retransmitted.

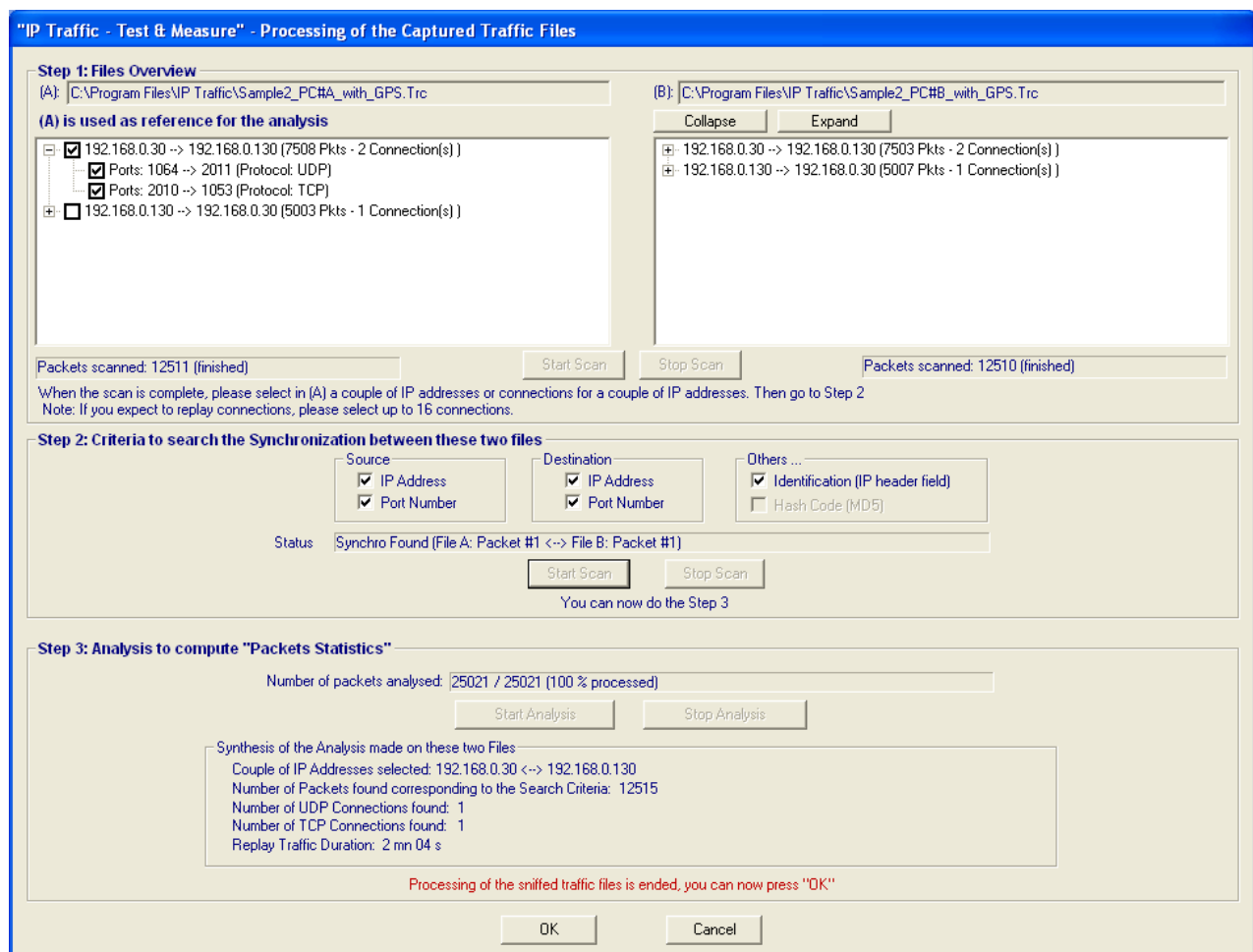
Note:

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



By pressing the « Start Analysis » button, the following window is displayed.



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 (on Driver 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) | St... | Transit ... | Port -> ... | IP size (p... | Identi... |
|--------------|-------|-------------|-------------|---------------|-----------|
| 21:55:03.559 | Sent | 180 (± 5) | 1064->2... | 1488 (UDP) | x9567 |
| 21:55:03.579 | Sent | 180 (± 5) | 1064->2... | 1488 (UDP) | x9568 |
| 21:55:03.598 | Sent | 171 (± 5) | 1064->2... | 1488 (UDP) | x9569 |
| 21:55:03.620 | Sent | 179 (± 5) | 1064->2... | 1488 (UDP) | x956A |
| 21:55:03.639 | Sent | 179 (± 5) | 1064->2... | 1488 (UDP) | x956B |
| 21:55:03.661 | Sent | 178 (± 5) | 1064->2... | 1488 (UDP) | x956C |
| 21:55:03.685 | Sent | 173 (± 5) | 1064->2... | 1488 (UDP) | x956D |
| 21:55:03.717 | Sent | 171 (± 5) | 1064->2... | 1488 (UDP) | x956E |
| 21:55:03.739 | Sent | 180 (± 5) | 1064->2... | 1488 (UDP) | x956F |
| 21:55:03.758 | Sent | 170 (± 5) | 1064->2... | 1488 (UDP) | x9570 |
| 21:55:03.780 | Sent | 179 (± 5) | 1064->2... | 1488 (UDP) | x9571 |
| 21:55:03.799 | Sent | 179 (± 5) | 1064->2... | 1488 (UDP) | x9572 |
| 21:55:03.821 | Sent | 178 (± 5) | 1064->2... | 1488 (UDP) | x9573 |

| Port -> Port(Pro... | Packets | Lost | % ... | Delay | Jitter | TCP... |
|---------------------|---------|------|-------|---------|--------|--------|
| Total Computer A | 7508 | 5 | 0% | 122 ... | 1 ms | 0 |
| 2010 -> 1053 (T... | 2508 | 0 | 0% | 0 ms | 0 ms | 0 |
| 1064 -> 2011 (U... | 5000 | 5 | 0% | 184 ... | 1 ms | N/A |

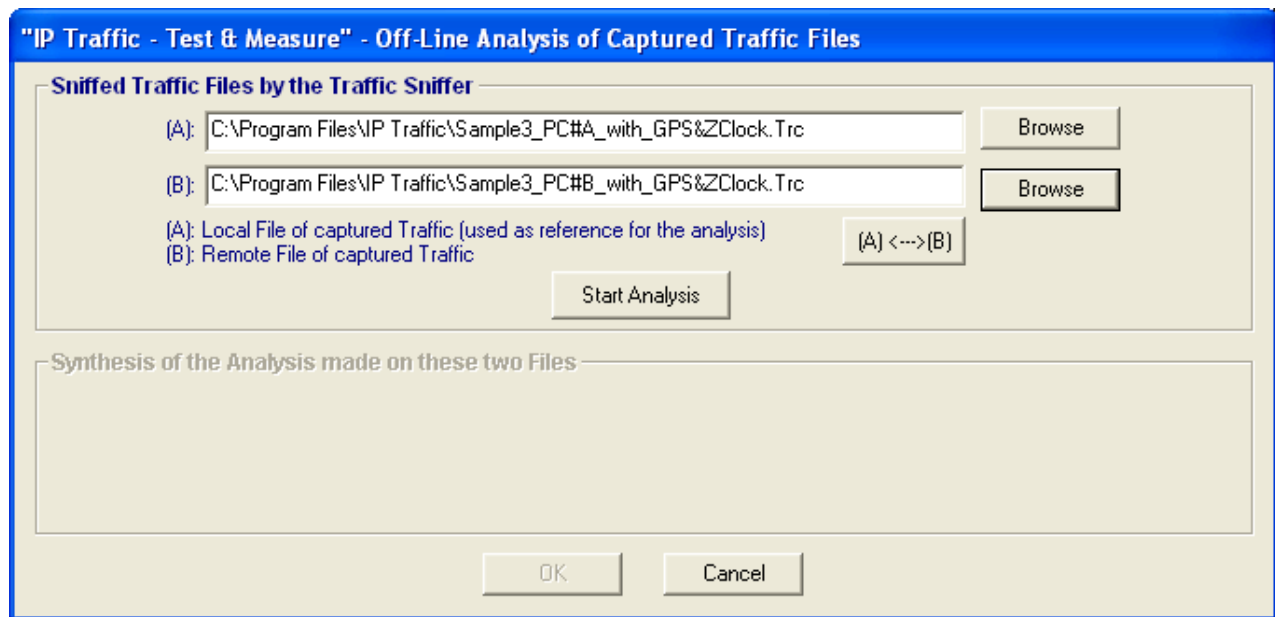
| Time (UTC) | St... | Tran... | Port -> ... | IP size (pro... | Identi... |
|--------------|-------|---------|-------------|-----------------|-----------|
| 21:55:20.725 | Sent | 1 (± 5) | 1053->2... | 48 (TCP) | x3D21 |
| 21:55:20.726 | Sent | 1 (± 5) | 1053->2... | 40 (TCP) | x3D22 |
| 21:55:20.728 | Sent | 3 (± 5) | 1053->2... | 1500 (TCP) | x3D23 |
| 21:55:20.747 | Sent | 1 (± 5) | 1053->2... | 1500 (TCP) | x3D24 |
| 21:55:20.767 | Sent | 2 (± 5) | 1053->2... | 1500 (TCP) | x3D25 |
| 21:55:20.787 | Sent | 1 (± 5) | 1053->2... | 1500 (TCP) | x3D26 |
| 21:55:20.807 | Sent | 1 (± 5) | 1053->2... | 1500 (TCP) | x3D27 |
| 21:55:20.827 | Sent | 1 (± 5) | 1053->2... | 1500 (TCP) | x3D28 |
| 21:55:20.847 | Sent | 1 (± 5) | 1053->2... | 1500 (TCP) | x3D29 |
| 21:55:20.866 | Sent | 2 (± 5) | 1053->2... | 1500 (TCP) | x3D2A |
| 21:55:20.886 | Sent | 1 (± 5) | 1053->2... | 1500 (TCP) | x3D2B |
| 21:55:20.906 | Sent | 2 (± 5) | 1053->2... | 1500 (TCP) | x3D2C |
| 21:55:20.926 | Sent | 1 (± 5) | 1053->2... | 1500 (TCP) | x3D2D |
| 21:55:20.947 | Sent | 2 (± 5) | 1053->2... | 1500 (TCP) | x3D2E |

| Port -> Port(Pro... | Packets | Lost | % ... | Delay | Jitter | TCP... |
|---------------------|---------|------|-------|-------|--------|--------|
| Total Computer B | 5007 | 4 | 0% | 1 ms | 0 ms | 4 |
| 1053 -> 2010 (T... | 5007 | 4 | 0% | 1 ms | 0 ms | 4 |

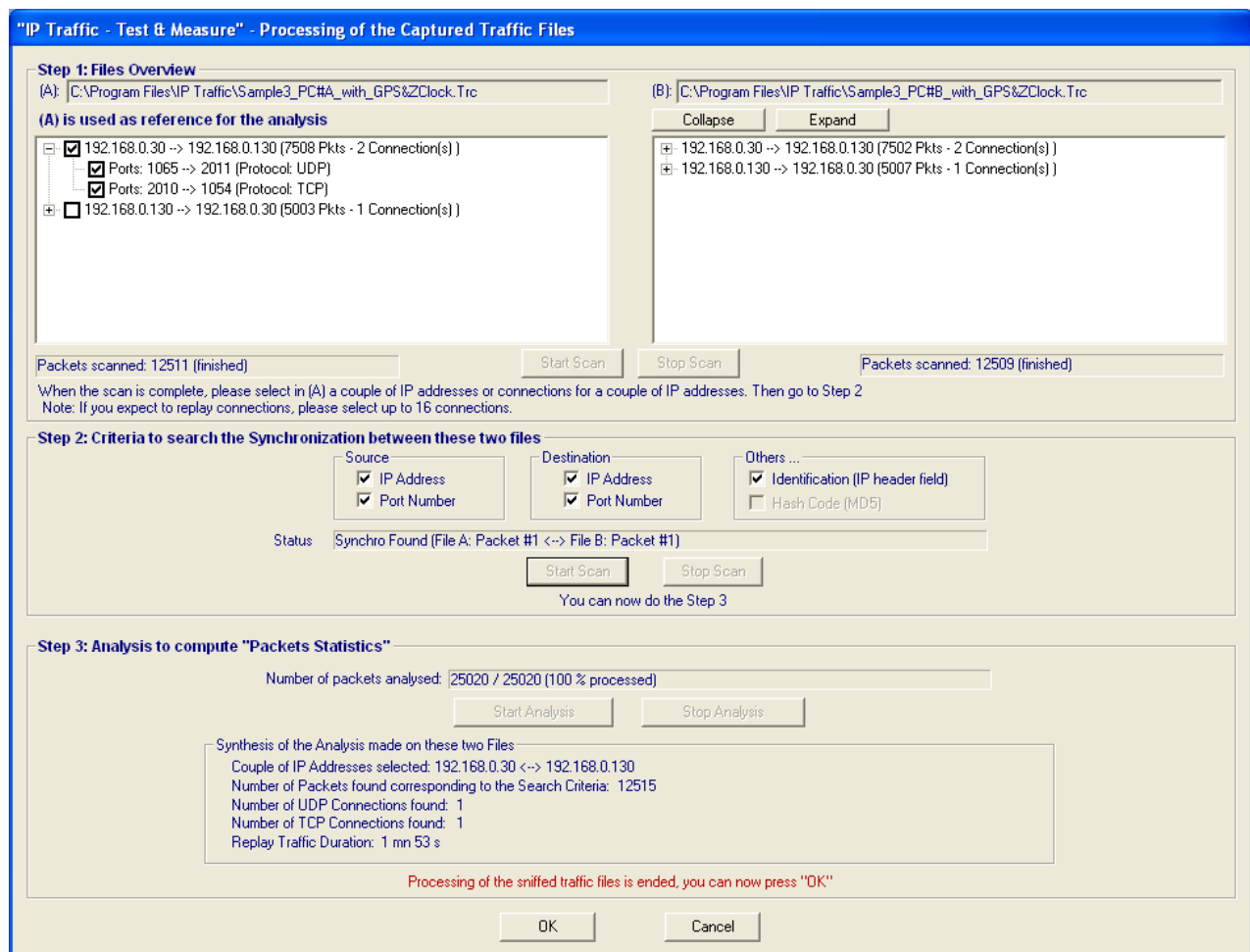
In this example, 5 UDP packets have been lost and the transit delay has an average of 184 ms for the UDP connection. 4 TCP packets sent by the PC #B have been lost and the average for the transit delay is 1 ms. Note also that 4 TCP packets sent by the PC #B have been retransmitted.

Note: the 'Transit ...' column indicates the symbols (± 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



By pressing the « Start Analysis » button, the following window is displayed.



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) | St... | Transit ... | Port -> ... | IP size (p... | Identi... |
|--------------|-------|-------------|-------------|---------------|-----------|
| 21:57:54.267 | Sent | 182 (± 1) | 1065->2... | 1488 (UDP) | xB2BC |
| 21:57:54.285 | Sent | 184 (± 1) | 1065->2... | 1488 (UDP) | xB2BD |
| 21:57:54.306 | Sent | 183 (± 1) | 1065->2... | 1488 (UDP) | xB2BE |
| 21:57:54.326 | Sent | 183 (± 1) | 1065->2... | 1488 (UDP) | xB2BF |
| 21:57:54.347 | Sent | 182 (± 1) | 1065->2... | 1488 (UDP) | xB2C0 |
| 21:57:54.367 | Sent | 182 (± 1) | 1065->2... | 1488 (UDP) | xB2C1 |
| 21:57:54.388 | Sent | 191 (± 1) | 1065->2... | 1488 (UDP) | xB2C2 |
| 21:57:54.408 | Sent | 181 (± 1) | 1065->2... | 1488 (UDP) | xB2C3 |
| 21:57:54.427 | Sent | 182 (± 1) | 1065->2... | 1488 (UDP) | xB2C4 |
| 21:57:54.449 | Sent | 191 (± 1) | 1065->2... | 1488 (UDP) | xB2C5 |
| 21:57:54.468 | Sent | 191 (± 1) | 1065->2... | 1488 (UDP) | xB2C6 |
| 21:57:54.490 | Sent | 190 (± 1) | 1065->2... | 1488 (UDP) | xB2C7 |
| 21:57:54.509 | Sent | 190 (± 1) | 1065->2... | 1488 (UDP) | xB2C8 |

| Port -> Port(Pro... | Packets | Lost | % ... | Delay | Jitter | TCP... |
|---------------------|---------|------|-------|---------|--------|--------|
| Total Computer A | 7508 | 6 | 0% | 123 ... | 1 ms | 0 |
| 2010 -> 1054 (T... | 2508 | 0 | 0% | 0 ms | 0 ms | 0 |
| 1065 -> 2011 (U... | 5000 | 6 | 0% | 186 ... | 1 ms | N/A |

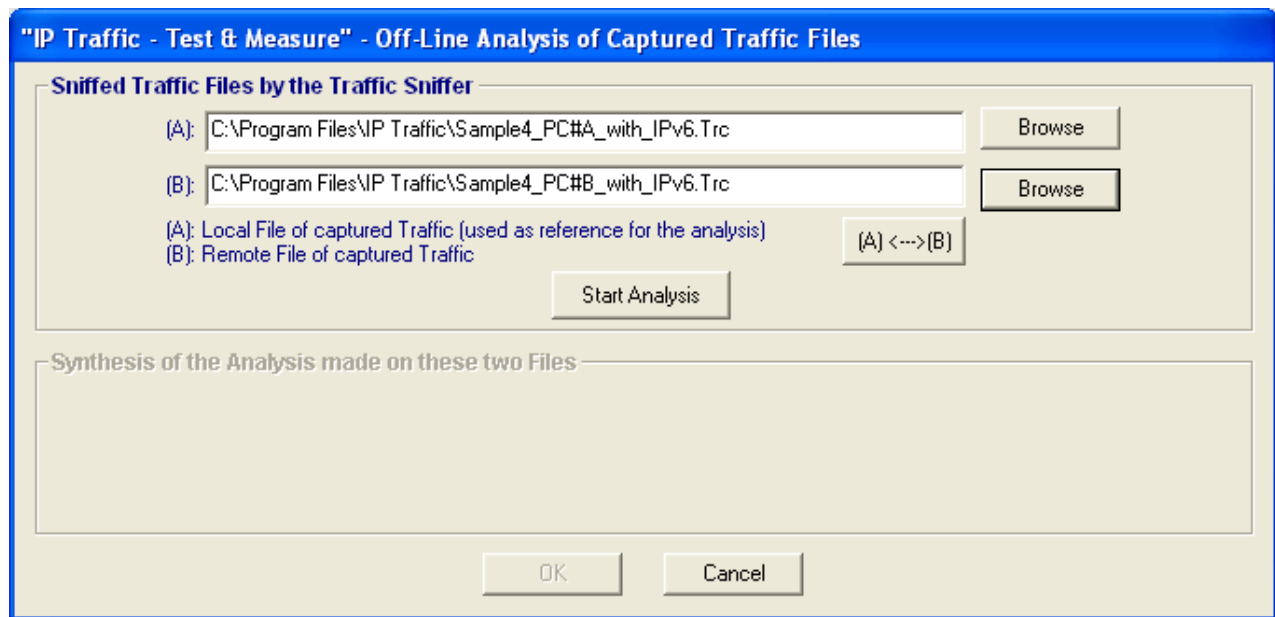
| Time (UTC) | St... | Tran... | Port -> ... | IP size (pro... | Identi... |
|--------------|-------|---------|-------------|-----------------|-----------|
| 21:58:00.793 | Sent | 0 (± 1) | 1054->2... | 48 (TCP) | x50B1 |
| 21:58:00.794 | Sent | 0 (± 1) | 1054->2... | 40 (TCP) | x50B2 |
| 21:58:00.796 | Sent | 1 (± 1) | 1054->2... | 1500 (TCP) | x50B3 |
| 21:58:00.815 | Sent | 1 (± 1) | 1054->2... | 1500 (TCP) | x50B4 |
| 21:58:00.835 | Sent | 1 (± 1) | 1054->2... | 1500 (TCP) | x50B5 |
| 21:58:00.855 | Sent | 1 (± 1) | 1054->2... | 1500 (TCP) | x50B6 |
| 21:58:00.875 | Sent | 1 (± 1) | 1054->2... | 1500 (TCP) | x50B7 |
| 21:58:00.895 | Sent | 1 (± 1) | 1054->2... | 1500 (TCP) | x50B8 |
| 21:58:00.915 | Sent | 1 (± 1) | 1054->2... | 1500 (TCP) | x50B9 |
| 21:58:00.935 | Sent | 1 (± 1) | 1054->2... | 1500 (TCP) | x50BA |
| 21:58:00.955 | Sent | 1 (± 1) | 1054->2... | 1500 (TCP) | x50BB |
| 21:58:00.975 | Sent | 1 (± 1) | 1054->2... | 1500 (TCP) | x50BC |
| 21:58:01.046 | Sent | 1 (± 1) | 1054->2... | 1500 (TCP) | x50BD |
| 21:58:01.066 | Sent | 1 (± 1) | 1054->2... | 1500 (TCP) | x50BE |

| Port -> Port(Pro... | Packets | Lost | % ... | Delay | Jitter | TCP... |
|---------------------|---------|------|-------|-------|--------|--------|
| Total Computer B | 5007 | 4 | 0% | 1 ms | 0 ms | 4 |
| 1054 -> 2010 (T... | 5007 | 4 | 0% | 1 ms | 0 ms | 4 |

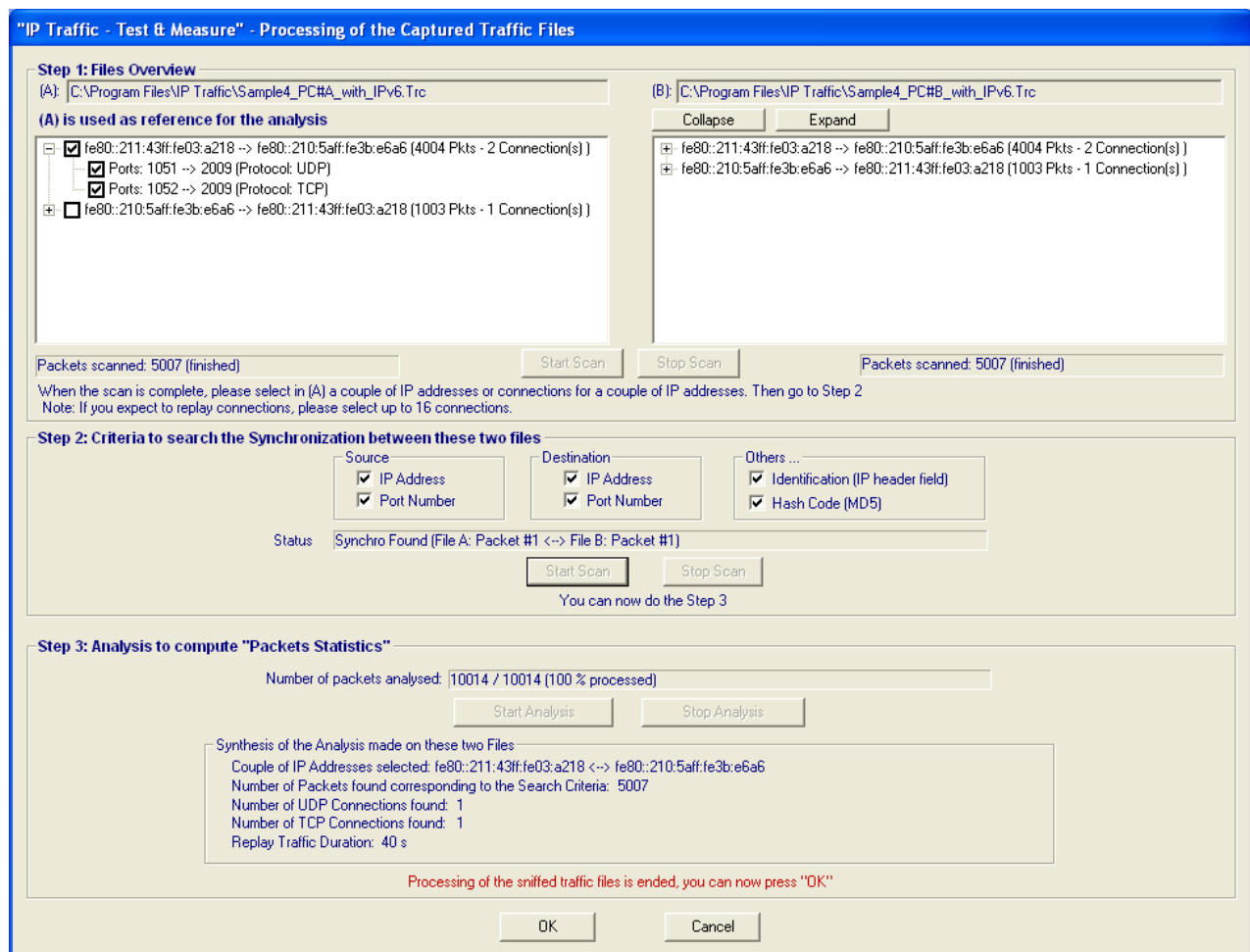
In this example, 6 UDP packets have been lost and the transit delay has an average of 186 ms for the UDP connection. 4 TCP packets sent by the PC #B have been lost and the average for the transit delay is 1 ms. Note also that 4 TCP packets sent by the PC #B have been retransmitted.

Note: the 'Transit ...' column indicates the symbols (± 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).

Example 4: capture containing IPv6 packets



By pressing the « Start Analysis » button, the following window is displayed.



In Step 1, the couple of IP addresses fe80::211:43ff:fe03:a218 → fe80::210:5aff:fe3b:e6a6 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: fe80::211:43ff:fe03:a218

IP address of B : fe80::210:5aff:fe3b:e6a6

| Time (UTC) | Sta... | Tra... | Port -> ... | IP size (pro... | Identi... |
|-----------------|--------|--------|-------------|-----------------|-----------|
| 16:27:49.350 | Sent | ... | 1051->2... | 1488 (UDP) | N/A |
| PC 16:27:49.351 | Sent | 0 (?) | 1052->2... | 64 (TCP) | N/A |
| PC 16:27:49.351 | Sent | 0 (?) | 1052->2... | 60 (TCP) | N/A |
| PC 16:27:49.354 | Sent | 0 (?) | 1052->2... | 1500 (TCP) | N/A |
| PC 16:27:49.370 | Sent | 0 (?) | 1051->2... | 1488 (UDP) | N/A |
| PC 16:27:49.375 | Sent | 0 (?) | 1052->2... | 1500 (TCP) | N/A |
| PC 16:27:49.389 | Sent | 0 (?) | 1051->2... | 1488 (UDP) | N/A |
| PC 16:27:49.394 | Sent | 0 (?) | 1052->2... | 1500 (TCP) | N/A |
| PC 16:27:49.410 | Sent | 0 (?) | 1051->2... | 1488 (UDP) | N/A |
| PC 16:27:49.415 | Sent | 0 (?) | 1052->2... | 1500 (TCP) | N/A |
| PC 16:27:49.429 | Sent | 0 (?) | 1051->2... | 1488 (UDP) | N/A |
| PC 16:27:49.434 | Sent | 0 (?) | 1052->2... | 1500 (TCP) | N/A |
| PC 16:27:49.450 | Sent | 0 (?) | 1051->2... | 1488 (UDP) | N/A |

Port -> Port(Pro...

Packets

Lost

% ...

Delay

Jitter

TCP...

Total Computer A

4004

0

0%

0 ms

0 ms

0

1052 -> 2009 (T...

2004

0

0%

0 ms

0 ms

0

1051 -> 2009 (U...

2000

0

0%

0 ms

0 ms

N/A

| Time (UTC) | Sta... | Tra... | Port -> ... | IP size (pro... | Identi... |
|-----------------|--------|--------|-------------|-----------------|-----------|
| 16:27:57.618 | Sent | ... | 2009->1... | 64 (TCP) | N/A |
| PC 16:27:57.642 | Sent | 0 (?) | 2009->1... | 60 (TCP) | N/A |
| PC 16:27:57.682 | Sent | 0 (?) | 2009->1... | 60 (TCP) | N/A |
| PC 16:27:57.722 | Sent | 0 (?) | 2009->1... | 60 (TCP) | N/A |
| PC 16:27:57.762 | Sent | 0 (?) | 2009->1... | 60 (TCP) | N/A |
| PC 16:27:57.802 | Sent | 0 (?) | 2009->1... | 60 (TCP) | N/A |
| PC 16:27:57.842 | Sent | 0 (?) | 2009->1... | 60 (TCP) | N/A |
| PC 16:27:57.882 | Sent | 0 (?) | 2009->1... | 60 (TCP) | N/A |
| PC 16:27:57.921 | Sent | 0 (?) | 2009->1... | 60 (TCP) | N/A |
| PC 16:27:57.962 | Sent | 0 (?) | 2009->1... | 60 (TCP) | N/A |
| PC 16:27:58.002 | Sent | 0 (?) | 2009->1... | 60 (TCP) | N/A |
| PC 16:27:58.042 | Sent | 0 (?) | 2009->1... | 60 (TCP) | N/A |
| PC 16:27:58.082 | Sent | 0 (?) | 2009->1... | 60 (TCP) | N/A |

Port -> Port(Pro...

Packets

Lost

% ...

Delay

Jitter

TCP...

Total Computer B

1003

0

0%

0 ms

0 ms

0

2009 -> 1052 (T...

1003

0

0%

0 ms

0 ms

0

In this example, no lost packets, no delay. In fact, in this example, GPS and Zclock systems were not used. That is why, "IP Traffic – Test & Measure" can't give a transit delay. In that case, the values show in the "delay" column are closed to the jitter.

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).