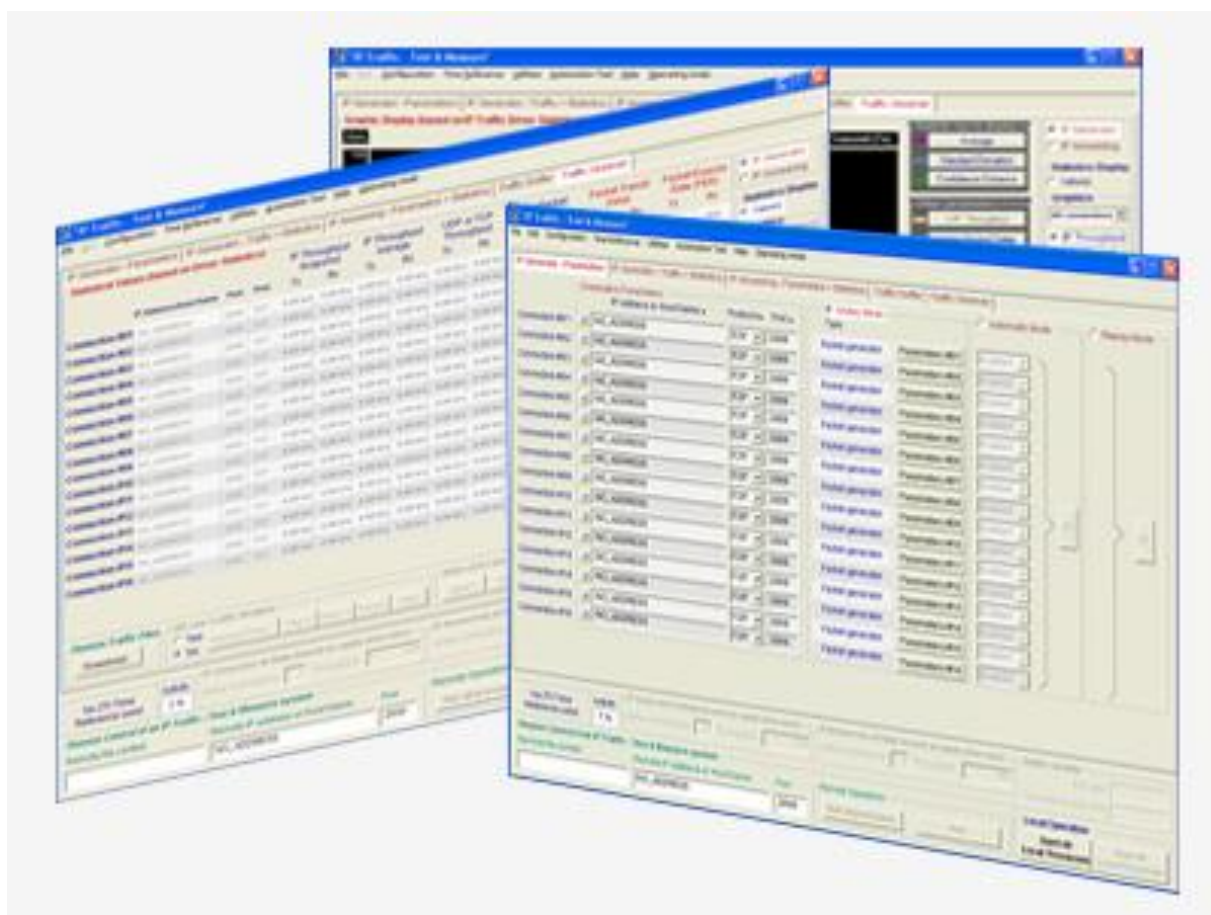


Version 2.7

IP Traffic Generator & QoS Measurement Tool for IP Networks (IPv4 & IPv6)

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



Read Me First

Table of contents

| | | |
|---------------|--|-----------|
| PART 0 | PREFACE | 4 |
| 0.1 | ORGANIZATION OF THIS MANUAL | 4 |
| 0.2 | MINIMUM SYSTEM REQUIREMENTS | 5 |
| 0.3 | REFERENCES | 5 |
| 0.4 | TERMS USED IN THIS DOCUMENT | 5 |
| 0.5 | TECHNICAL SUPPORT | 5 |
| PART 1 | OVERVIEW | 7 |
| 1.1 | GENERAL DESCRIPTION | 7 |
| 1.2 | ARCHITECTURE | 10 |
| 1.3 | USE A HARDWARE TIME DEVICE TO GET HIGH PRECISION MEASUREMENTS | 11 |
| 1.4 | IP TRAFFIC - TEST & MEASURE KEY FEATURES | 13 |
| 1.5 | THE AUTOMATION TOOL FOR IP TRAFFIC - TEST & MEASURE | 19 |
| PART 2 | WHAT'S NEW IN VERSION 2.7 | 20 |
| PART 3 | INSTALL IP TRAFFIC - TEST & MEASURE | 21 |
| 3.1 | FOREWORDS BEFORE UPGRADING FROM VERSION 2.0 AND HIGHER | 21 |
| 3.2 | FOREWORDS BEFORE UPGRADING FROM VERSIONS 1 (INCLUDING VERSION 1.3) | 21 |
| 3.3 | RUN THE SOFTWARE INSTALLATION FROM THE DOWNLOADED FILE | 22 |
| 3.4 | RUN THE SOFTWARE INSTALLATION FROM THE CD-ROM | 22 |
| 3.5 | DURING THE INSTALLATION | 23 |
| 3.5.1 | <i>IP Traffic - Test & Measure Packages in a few words</i> | 23 |
| 3.5.2 | <i>Which package should I install?</i> | 24 |
| 3.5.2.1 | <i>I want to evaluate IP Traffic - Test & Measure V2.7</i> | 24 |
| 3.5.2.2 | <i>I already use IP Traffic - Test & Measure</i> | 24 |
| | ... and I want to upgrade and keep my permanent license | 24 |
| | ... and I want to upgrade and use the USB Software Protection Key I bought | 24 |
| 3.5.2.3 | <i>I just bought IP Traffic - Test & Measure</i> | 24 |
| | ... and I chose the Electronic Software Delivery (ESD) | 24 |
| | ... and I received the CD-ROM & USB Software Protection Key | 24 |
| | ... and I will receive the CD-ROM & USB Software Protection Key in a few days | 24 |
| 3.6 | WHAT HAS BEEN INSTALLED ON MY COMPUTER? | 25 |
| 3.7 | HOW TO REINSTALL ANOTHER PACKAGE? | 26 |
| 3.8 | HOW TO TRANSFER THE SOFTWARE TO ANOTHER COMPUTER? | 26 |
| PART 4 | HOW TO HANDLE YOUR LICENSE? | 27 |
| 4.1 | IP TRAFFIC - TEST & MEASURE TRIAL VERSION | 27 |
| 4.1.1 | <i>IP Traffic - Test & Measure License Information window</i> | 27 |
| 4.1.2 | <i>End of the 15-day trial period</i> | 27 |
| 4.2 | IP TRAFFIC - TEST & MEASURE & SOFTWARE PROTECTION KEY | 28 |
| 4.2.1 | <i>Installation of the Software Protection Key</i> | 28 |
| 4.2.2 | <i>Software Protection Key Transfers</i> | 31 |
| 4.2.2.1 | <i>Direct Transfer: move the Software Protection Key from one local directory to another</i> | 31 |
| 4.2.2.2 | <i>Transfer by Media (USB key) from a source PC to a target PC</i> | 32 |
| 4.3 | IP TRAFFIC - TEST & MEASURE & USB SOFTWARE PROTECTION KEY | 37 |
| PART 5 | UNINSTALL IP TRAFFIC - TEST & MEASURE | 37 |
| PART 6 | GETTING STARTED | 38 |
| PART 7 | RUN IP TRAFFIC - TEST & MEASURE | 43 |

| | | |
|---------------|--|-----------|
| PART 8 | IP TRAFFIC - TEST & MEASURE AND WINDOWS FIREWALL | 44 |
| 8.1 | HOW TO AUTHORIZE TCP AND UDP CONNECTIONS BLOCKED BY THE WINDOWS FIREWALL UNDER WINDOWS XP AND SERVER 2003 | 44 |
| 8.2 | HOW TO AUTHORIZE UDP AND TCP CONNECTIONS UNDER WINDOWS VISTA AND AFTER | 45 |
| 8.3 | HOW TO AUTHORIZE ICMPv4 AND ICMPv6 TRAFFIC UNDER WINDOWS VISTA AND AFTER | 46 |

PART 0 Preface

0.1 Organization of this manual

This manual is aimed at helping you to discover and use **IP Traffic - Test & Measure**. It is organized as follows:

- **Part 1: Product Overview**

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 2.7**

Is a general overview of new features, main improvements provided with **IP Traffic - Test & Measure** version 2.7.

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

Presents the product requirements, how to install the software downloaded from the Internet or from the CD-ROM, provides important information to upgrade from previous versions and explains how to choose the most suitable **IP Traffic - Test & Measure** package.

- **Part 4: How to handle your license?**

Describes how to proceed for the license transfer

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

Explains how to uninstall the software

- **Part 6: 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**

Details how to run the software.

- **Part 8: IP Traffic - Test & Measure and Windows Firewall**

Gives details about the way to configure the Windows firewall to authorize the use of **IP Traffic - Test & Measure**.

0.2 Minimum System Requirements

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

- All modern versions of Microsoft Windows are supported - from XP to Windows 8 with 32-bit or 64-bit environment, including Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows Seven and Windows 8.
- Pentium processor with 512 MB memory
- 1024 x 768 display
- 25 MB free hard disk space

0.3 References

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

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

[RFC2544] “Benchmarking Methodology for Network Interconnect Devices”

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

[RFC2373] “IP Version 6 Addressing Architecture”

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

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

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

- Product name and version.
- Demo version or licensed product.
- System configuration.

- Problem details: settings, error messages...
- If the problem is persistent, give the details of how to create the problem.

You can contact Technical Support by:

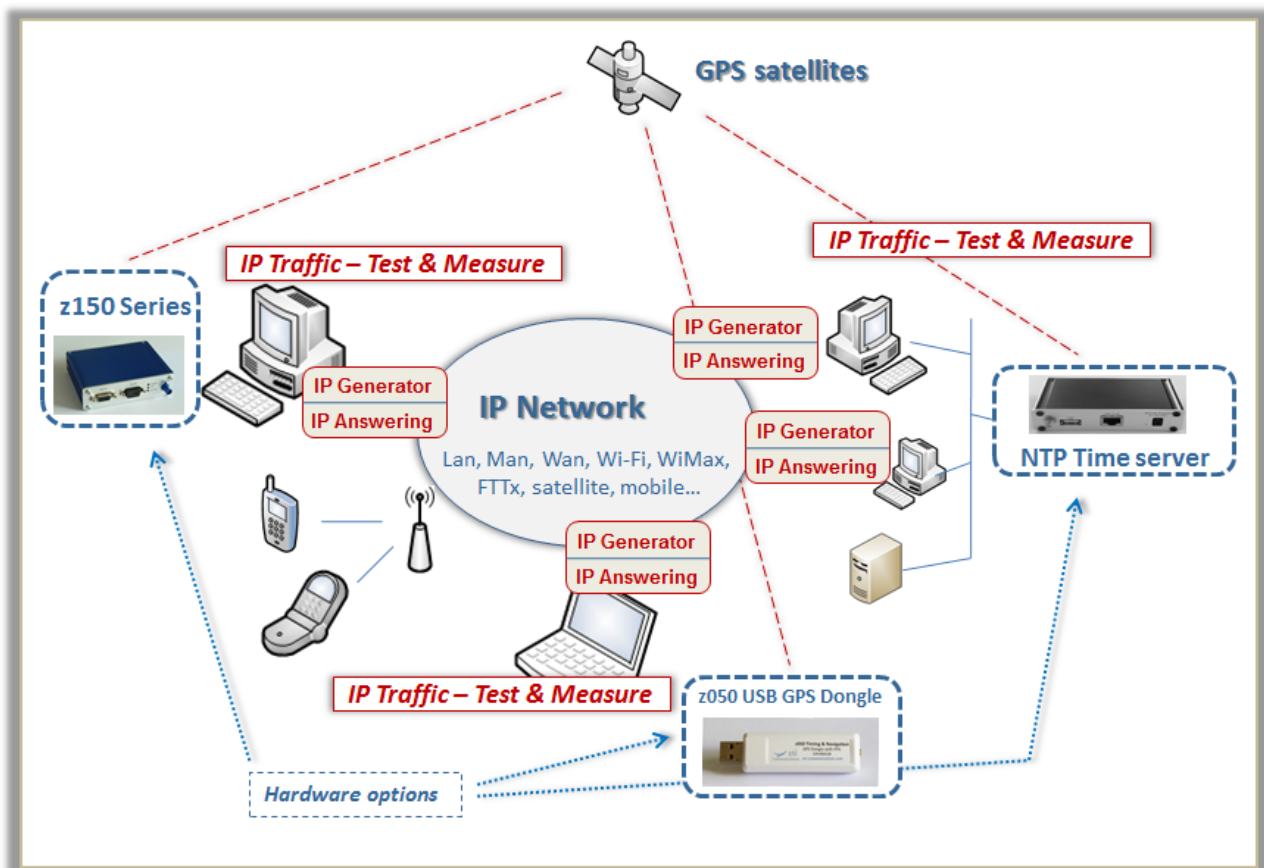
| | |
|-----------|---|
| Email | Send as many details as possible to support@zti-communications.com |
| Telephone | Telephone support is available from 09:00 am to 06:00 pm (GMT Time +01:00 or +02:00), Monday to Friday. Call on +33 2 9613 4003 |

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.

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

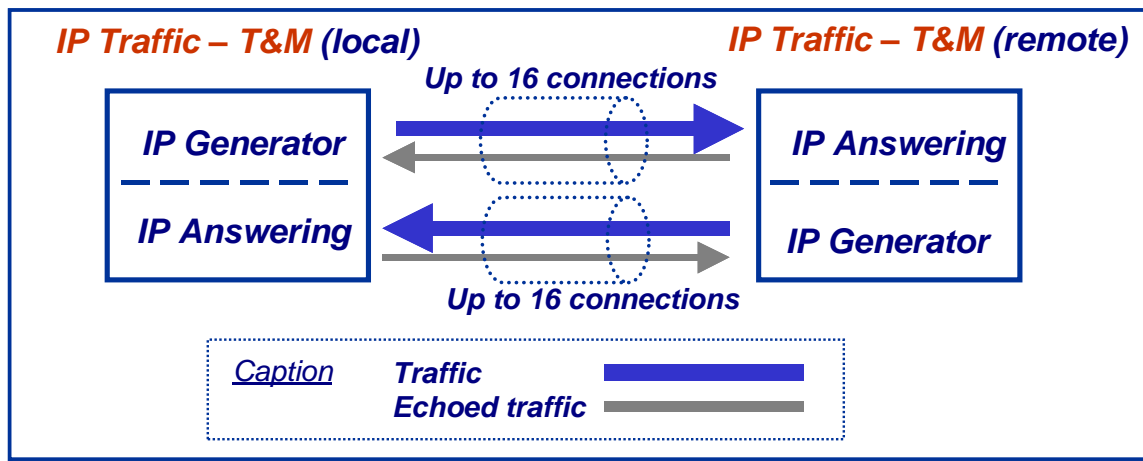


IP Traffic - Test & Measure is an IP software testing tool using the Microsoft Windows TCP/IP stack (Winsock2 interface). So, **IP Traffic - Test & Measure** is independent of any transmission or telecom link and can use any transmission link managed by the Windows operating system: LAN (Ethernet, Token-ring,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

IP IP Traffic - Test & Measure can be used to get high accuracy measurements by using optional hardware providing a very precise time reference thanks to both the Time Devices synchronized by GNSS receivers GPS devices or Network Time Servers).

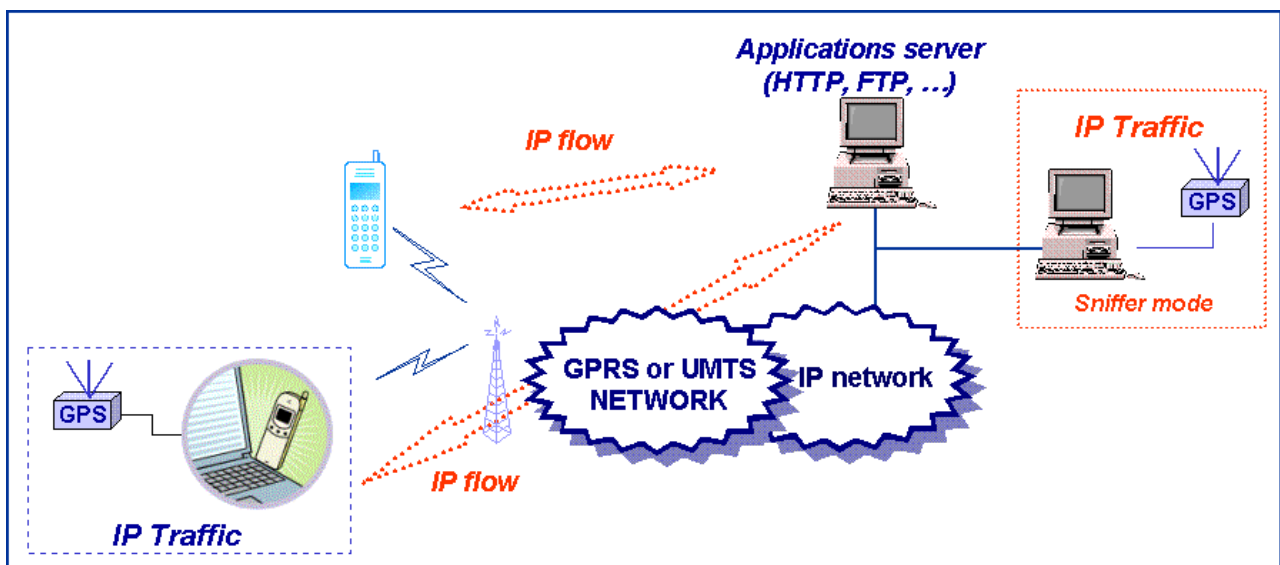
IP Traffic - Test & Measure is composed of four modules: 'IP Generator', 'IP Answering', 'Traffic Sniffer' and 'Traffic Observer'.

- 'IP Generator' is able to generate IP traffic on 16 simultaneous connections.
- 'IP Answering' is able to receive IP traffic on 16 simultaneous connections with different working modes (Absorber, Absorber file, Echoer, Echoer file and Generator).



The 'IP Generator' and 'IP Answering' modules

- **'Traffic Sniffer'** is able to capture traffic files at the driver level (under the TCP/IP stack) in order to calculate traffic statistics and to add a timestamp to the IP packets and to put them into a file. The **'IP Generator'** module can replay these traffic files.



IP Traffic - Test & Measure: Sniffer mode

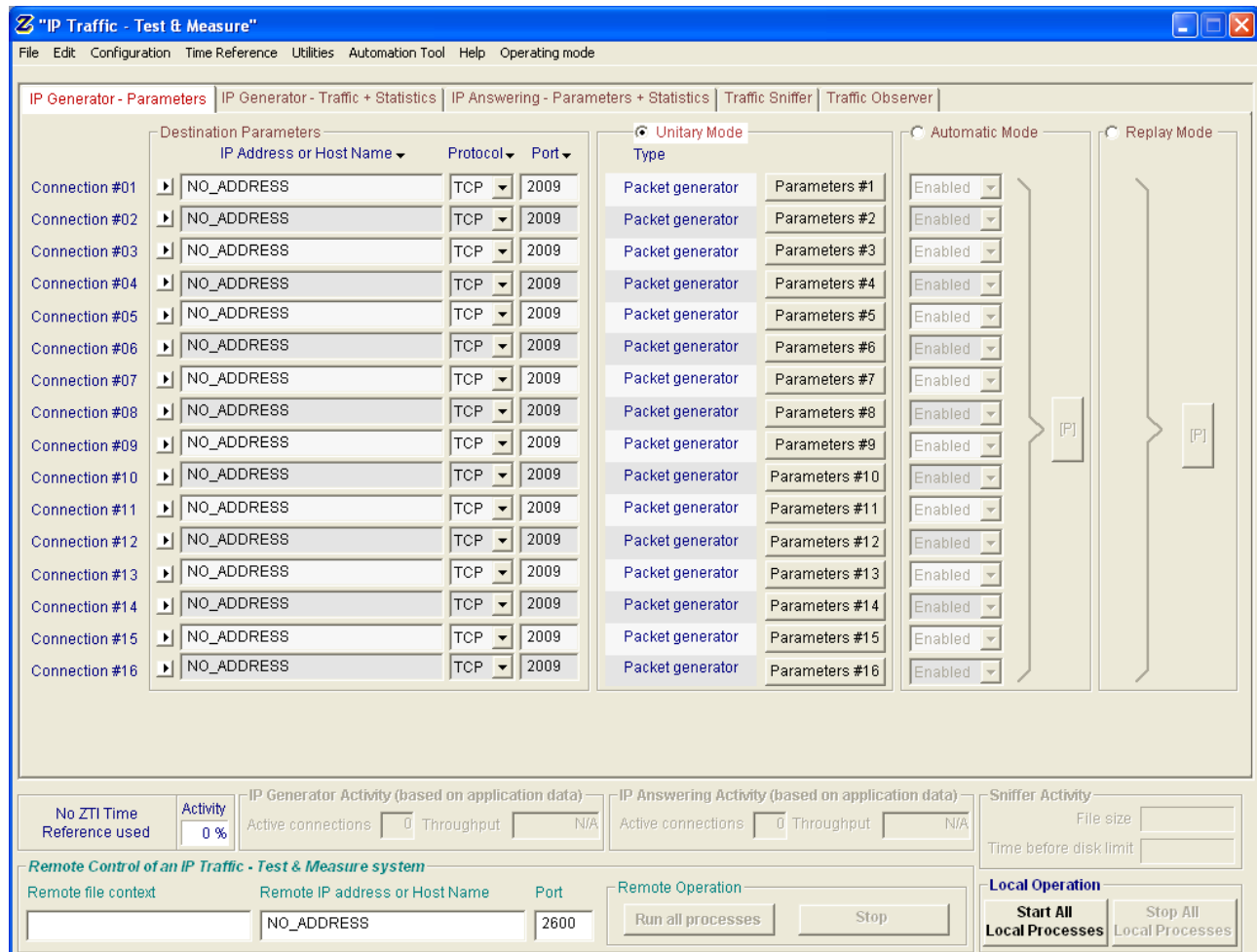
IP Traffic - Test & Measure can be used to capture IP traffic with the 'Traffic Sniffer': for example, the IP flows between a mobile and an application server (web, video telephony...) can be captured and saved in a file. IP packets are time-stamped, to replay IP traffic with the same timing as for the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

- **'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].
'Traffic Observer' online mode displays real time statistics for the **'IP Generator'** or the **'IP Answering'** modules.
'Traffic Observer' offline mode provides QoS statistics as 'Packet Erasure Rate' and 'Packet Transit Delay'.

IP Traffic - Test & Measure can be operated with two main modes:

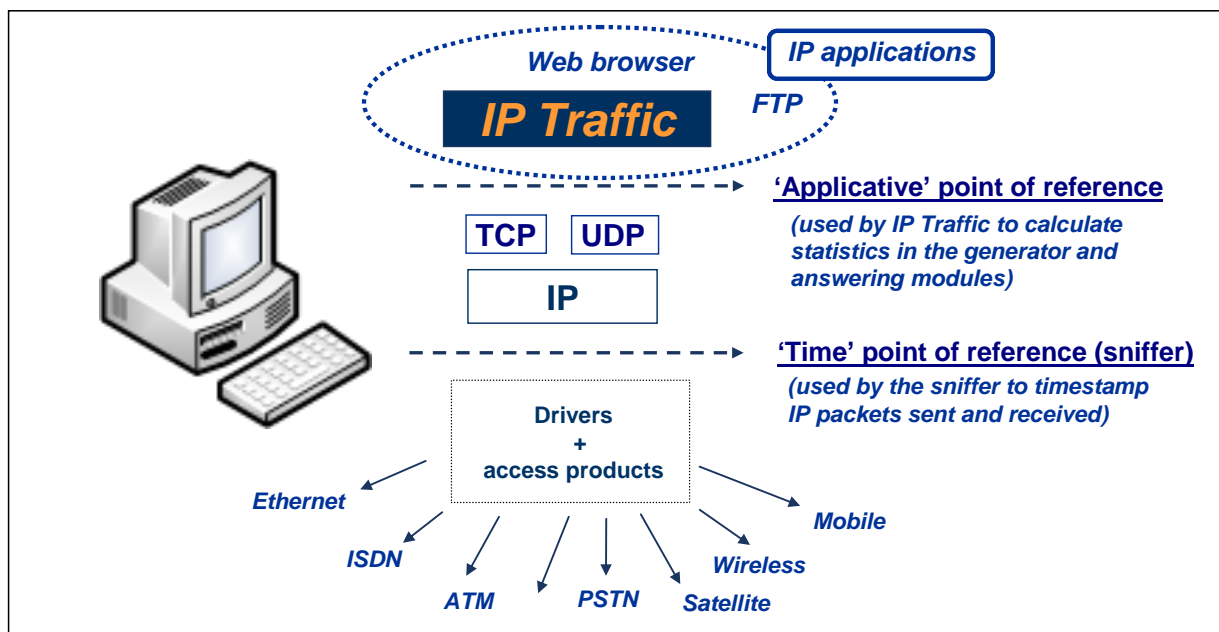
- The **normal** mode: the user can access all commands and functionalities
- The **remote control** mode: the user can't access locally commands of **IP Traffic - Test & Measure**. It's mainly used for control by a remote **IP Traffic - Test & Measure** system. It's very useful for example to use an **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 sent and received IP packets. 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 get a good accuracy to timestamp IP packets, additional time devices are available as described in the following paragraph.

When no additional hardware is used the '**Traffic Sniffer**' uses the PC internal clock to timestamp sent and received IP packets. 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 Communications recommends an additional time device to allow a precise calculation of the propagation delays through IP networks.

1.3 Use a hardware time device to get high precision measurements

Thanks to our hardware add-ons, you are able to get a precise time reference which can be used to get precise measurements of QoS metrics provided by **IP Traffic - Test & Measure**. With such add-ons, you can measure for example the transit delay of IP packets sniffed on the network with an uncertainty of 1 millisecond maximum depending on the configuration you chose.

GNSS Device (*Timing & Navigation or High Precision Timing*)



z050 Timing & Navigation Module: GPS USB Dongle with PPS (Pulse Per Second usable for timing applications via serial port emulation). Based on the Trimble technology (Trimble OEM), this sensitive GPS receiver acquires autonomously GPS satellite signals and quickly generates reliable position in extremely challenging environments and even under poor signal conditions. It is recommended to use an outdoor antenna for best results.

z150 Series: GNSS Multi Receivers Platform for Timing & Navigation (Static or mobile application) in robust aluminum enclosure.

3 models available:

- * Model P200 (GPS): 1 port RS232 + 1PPS-out

- * Model P300 (GPS): 1 port RS232 + 1 port USB + 1PPS-out

- * Model P400 (GPS, GLONASS, GALILEO, COMPASS): 1 port RS232 + 1 port USB + 1PPS-out

Operating temperature range: -30°C (-22°F) to +85°C (185°F).



Designed to provide an accurate pps (pulse per second) signal to use in measurement and industrial applications, this GPS/Glonass/Galileo timing module is designed to be used in indoor or outdoor static applications, requiring accurate time stamp reference information. It delivers accurate pps signal, even in very poor signal level environments (indoor, urban canyons and obscured environments) or when only 1 satellite is visible and being tracked..

NTP Time Server



As an example, z250 NTP Time Server has been designed around the Trimble® BD910 GNSS receiver module, originally for applications requiring high accuracy from multiple GNSS constellations in a very small enclosure. Mobile platforms can now embed proven Trimble RTK technology using a very compact enclosure 108.5 x 84 x 30mm form factor. z250 supports the L1 frequency from the GPS, GLONASS, Galileo, and Compass constellations. Customers benefit from the Ethernet connectivity available from RJ45 connection, allowing high speed data transfer and configuration via standard web browsers. USB and RS-232 are directly available from the enclosure..

Time Reference Accuracy vs configuration chosen

| Configuration | Absolute Time reference | Accuracy for Measurement |
|--|--|-------------------------------------|
| IP Traffic – Test & Measure | None or user defined. | Undefined (PC clock used) |
| IP Traffic – Test & Measure + z150 Series unit (Serial or USB port) | YES , provided by the time device synchronized by the GNSS chipset (GPS, GLONASS, etc.). Absolute reference. | 5 milliseconds |
| IP Traffic – Test & Measure + z050 (USB GPS dongle) | YES , provided by the time device synchronized by GPS. Absolute reference. | 1 millisecond |
| IP Traffic – Test & Measure + NTP Time Server (e.g. z250) (one unit for multiple PCs running IP Traffic – T&M) | YES , provided by the NTP Time Server synchronized by GNSS chipset (GPS, GLONASS, etc.). Absolute reference. | 1 millisecond |

1.4 IP Traffic - Test & Measure Key Features

Module 1: 'IP Generator' Overview

- The **'IP Generator'** module generates up to 16 simultaneous UDP (Unicast, Multicast or Broadcast) and/or TCP connections and/or ICMP connections. The connections can be established following three different testing modes:
 - ⇒ **Unitary Mode:** you can choose among two type of data generator
 - Internal data generator:** you can select the traffic generator data source and configure packets size and inter packet delay for each connection. With the ICMP protocol you can set:
 - Request packet number and content: packet generator (fixed, randomized, alternated and increasing / decreasing).
 - Request data size: fixed, randomized, alternated and increasing / decreasing.
 - Reply receiving timeout: fixed, randomized, alternated, increasing / decreasing or use of a mathematical law.
 - IP Traffic - Test & Measure** offers three different data sources:
 - Automatic data generator by using mathematical laws⁽²⁾,
 - Packets generator: many parameters can be defined (number of packets to send, inter packet delay, packet contents, ...)
 - File: selection of a file to send⁽²⁾.
 - External data source generator**⁽²⁾: 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**⁽²⁾: 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. This mode can not be used with ICMP connections.
 - ⇒ **Replay sniffed traffic**⁽²⁾: 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⁽¹⁾
 - Received throughput⁽¹⁾
 - Sent packet throughput⁽¹⁾
 - Received packet throughput⁽¹⁾
 - Sent data volume⁽¹⁾
 - Received data volume (volume of data sent by the remote)⁽¹⁾
 - Sent packets
 - Received packets (packets sent by the remote)
 - Data volume to send⁽¹⁾
 - Remaining volume (of data to send)⁽¹⁾
 - Seq. numb errors (sequence numbering errors)
 - Mean RTT (Round Trip Time)
 - Min RTT
 - Max RTT
 - Jitter⁽¹⁾

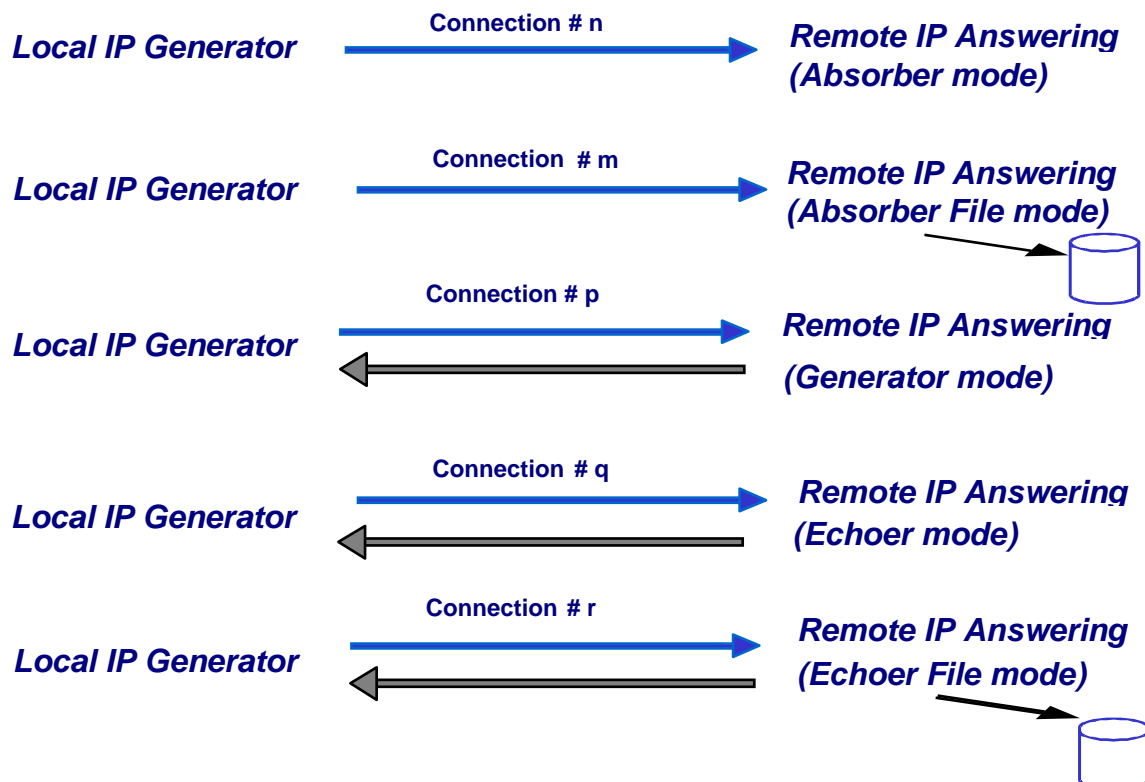
⁽¹⁾ These statistics are not available with ICMP protocol.

⁽²⁾ Not available with ICMP.

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**', '**Generator**' or '**Disable**'. We will consider hereafter 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

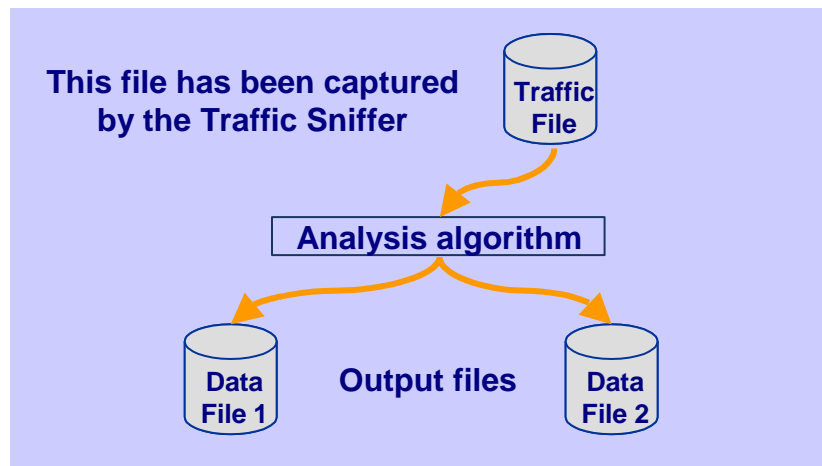
These statistics can be saved in a CSV file defined by the user.

Module 3: 'Traffic Sniffer' Overview

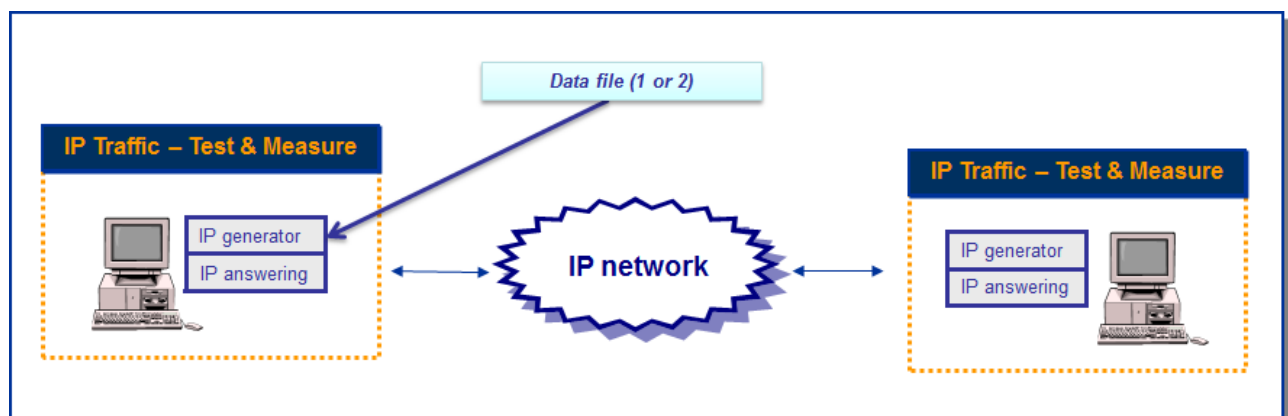
Sent and received IP packets are time-stamped by the '**Traffic Sniffer**' and then saved in a file to generate capture traffic files.

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:

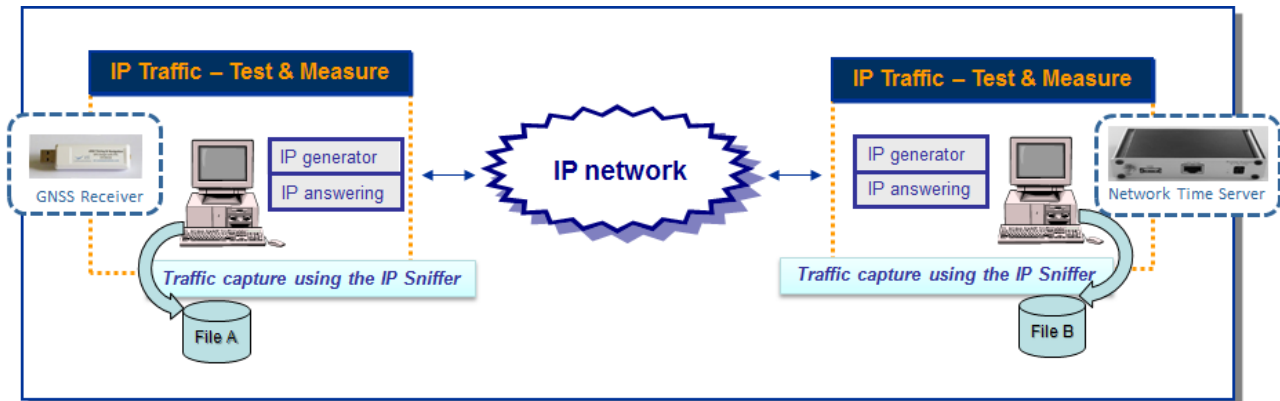


Module 4: 'Traffic Observer' Overview

The '**Traffic Observer**' **online mode** displays real time statistics for the '**IP Generator**' or the '**IP Answering**' modules.

The '**Traffic Observer**' **offline mode** provides QoS statistics as 'Packet Erasure Rate' and 'Packet Transit Delay'. But some QoS statistics as the packet Transit Delay need to have time-stamped packets from the local and the remote systems.

The off-line (batch mode) statistics are obtained using the two traffic files, File A and File B, produced by the local and remote '**Traffic Sniffer**' containing the sniffed traffic. Then, the '**Traffic Observer**' uses these files in order to calculate off-line statistics.



Below is the list of the statistics provided by the '**Traffic Observer**':

- In **red**, the statistics only available with the **offline mode**
- In **green**, the statistics available with **both 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

- ⇒ Loading of the sniffed traffic files to analyze them and to check their coherency
- ⇒ 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

IP Traffic - Test & Measure performs the RFC 2544 with 2 differences:

- 1) It doesn't support the automatic recognition of the throughput.
- 2) Consequently, it doesn't generate the resulting graph for the automatic recognition of the throughput.

IP Traffic - Test & Measure performs latency calculation for each packet, and then calculates the average value, where RFC2544 expects the latency calculation for ONE packet in the flow of 120 seconds long (then calculate the average for 20 tests).

The RFC 2544 latency can be calculated using a script that gets 1 value returned from IP Traffic - Test & Measure for each test of 120 seconds long.

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 UDP protocol only.

- **Multicast & IPV4:** IPv4 addresses from 224.0.0.0 to 239.255.255.255 are MULTICAST IP addresses. These addresses can be used to generate multicast IP traffic (define the multicast IP address in the Sender part) or to receive multicast IP traffic (define the multicast IP address in the Receiver part).



- **Multicast & IPv6:** IPv6 multicast addresses are defined in "IP Version 6 Addressing Architecture" [RFC2373].

This defines fixed and variable scope multicast addresses.

IPv6 multicast addresses are distinguished from unicast addresses by the value of the high-order octet of the addresses: a value of 0xFF (binary 11111111) identifies an address as a multicast address; any other value identifies an address as a unicast address (FE80::/10 are Link local addresses, FEC0::/10 are Site Local addresses where FF00::/8 are Multicast addresses).

Multicast addresses from FF01:: through FF0F:: are reserved.

The complete list of Reserved IPv6 multicast addresses can be found in "IPv6 Multicast Address Assignments" [RFC 2375].

The ICMPv6 messages are used to convey IPv6 Multicast addresses resolution.

Broadcast feature (with IPv4 only)

IP Traffic - Test & Measure is able to generate and receive Broadcast IP traffic (IPv4 only). The broadcast feature is used for UDP protocol only.



- **Broadcast & IPV4:** IPv4 addresses as 255.255.255.255 or 192.168.0.255 are BROADCAST IP addresses. These addresses can be used to generate broadcast IP traffic (define the broadcast IP address in the IP Generator part). To receive broadcast IP traffic, specify the unicast IP address of the IP Generator in the IP Answering part.

- **Broadcast & IPv6:** broadcast does not apply to IPv6.

IP version selection (Windows XP and later)

Please note that **IP Traffic - Test & Measure** supports IPv6 for Windows XP and later versions. IPv6 is not installed by default under Windows XP and Server 2003: 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.

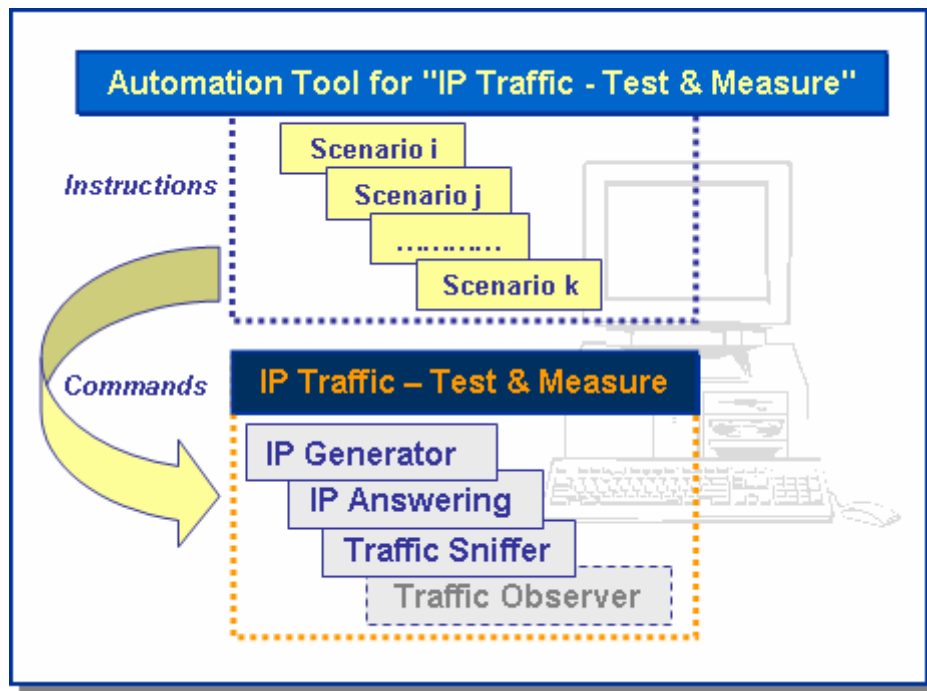
IP Traffic - Test & Measure is able to generate and receive Unicast, Multicast or Broadcast IP traffic on a selected interface, giving the user a deeper control where data are exchanged and makes multiple routes definition easily.



We have noticed that some operating systems may choose automatically the best network interface to use when several NICs are plugged on the same network when it comes to network interface selection. In that case, data can be sent on one interface and received on another one.

1.5 The Automation Tool for IP Traffic - Test & Measure

The add-on software **Automation Tool for IP Traffic - Test & Measure** allows 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 Version 2.7

This part is a general overview of new features and main improvements of **IP Traffic - Test & Measure** version 2.7. 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 the software from the versions 1.3, 2.0 up 2.6 to the version 2.7, please refer to paragraphs below.

⇒ IP Traffic - Test & Measure (Version 2.7)

- Remove zClock support
- Add generic GNSS receiver
- Review the statistics calculation
- Add number of packets & bytes transferred
- Add handler for z050 device

The contexts created with versions 2.0 and higher are reused automatically. When saved, they become the new 2.7 context file format.

⇒ Automation Tool for IP Traffic - Test & Measure (Version 1.7.1)

- Remove zClock support
- Add Generic GNSS receiver

The scenarios created with older versions are reused automatically. When saved, they become the new 1.7 scenario file format.

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 XP, Server 2003 or 2008, Vista, Seven or 8, you must log on with the administrator 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 installation procedure is a standard installation program for Windows that needs Administrator rights.

3.1 Forewords before upgrading from version 2.0 and higher

There is no need to uninstall earlier version of **IP Traffic - Test & Measure** before upgrading to version 2.7. **IP Traffic - Test & Measure** version 2.5 has introduced a new protection using the USB Software Protection Key. But previous users of **IP Traffic - Test & Measure** can continue using their Site Key license.

When upgrading from a previous version of IP Traffic - Test & Measure, do not uninstall the previous version to keep your existing license: please refer to the following paragraph: "3.5.2

Which package should I install?" here after to get more details.

3.2 Forewords before 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 2.7. Due to changes in the license scheme introduced with version 2.0, the reinstallation will not keep the unlimited license information. You should contact ZTI Communications (contact@zti-communications.com) to get back a new unlimited license number when upgrading to version 2.7 with the new site code. Context files from version 1.3 and earlier are not compatible with the version 2.7. There is no converter tool to translate versions 1's context files into version 2.7.

3.3 Run the software installation from the downloaded file

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.

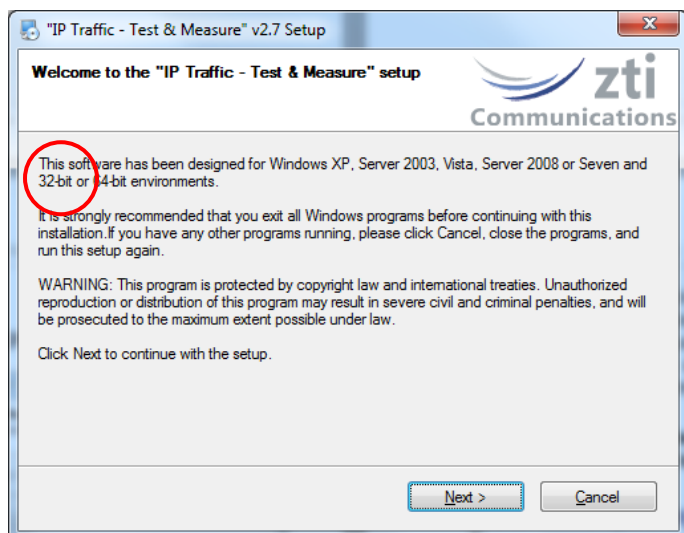
3.4 Run the software installation from the CD-ROM

The installation procedure is a standard installation program.

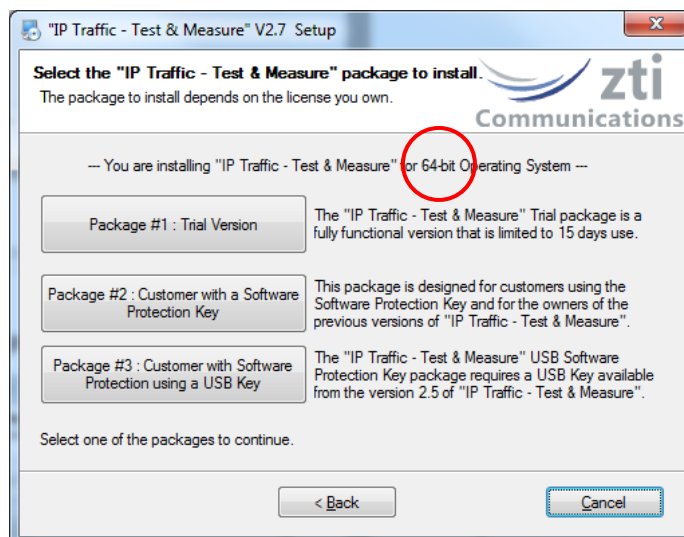
- First, insert the **IP Traffic - Test & Measure** CD-ROM in your CD-ROM drive.
- Click on “Start”, “Execute” or “Run...” and type
[CD unit> \ Setup_IPTrafficBundle.exe](#)

3.5 During the installation

Follow the instructions until reaching the IP Traffic – T&M package selection window.



Install on a **32-bit** platform



Install on a **64-bit** platform



The setup procedure detects and installs automatically the 32-bit or 64-bit version depending of your target operating system.

3.5.1 IP Traffic - Test & Measure Packages in a few words

To use the **IP Traffic - Test & Measure** software, there are 3 license schemes:

- **Package #1:** the **IP Traffic - Test & Measure Trial package** allows you to use **IP Traffic - Test & Measure** during 15 days after the first run. When the trial period has expired, the license should be purchased.
- **Package #2:** the **IP Traffic - Test & Measure Software Protection Key package** has been designed for users owning a Software License key and for the users of the previous versions of **IP Traffic - Test & Measure**. It keeps your current installation and files, without additional requirement.
- **Package #3:** the **IP Traffic - Test & Measure USB Software Protection Key package** requires a USB key with the **IP Traffic - Test & Measure** license. The **USB key** is provided with **IP Traffic - Test & Measure** from version 2.5. This package allows the installation of **IP Traffic - Test & Measure** on several PCs but the only PC able to run **IP Traffic - Test & Measure** is the one having the USB key plugged in.



As previous users, you may be interested to move to a USB Software Protection Key: please contact your distributor or ZTI Communications to get more details about the license migration program (see 4.3 IP Traffic - Test & Measure & USB Software Protection Key for more details).



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



**The USB Software Protection Key contains only the license information.
The software is available on a separate CD-ROM.**

3.5.2 Which package should I install?

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

3.5.2.1 I want to evaluate IP Traffic - Test & Measure V2.7

In that case, choose the Package #1 *“IP Traffic - Test & Measure Trial Version”*.
You will be able to use **IP Traffic - Test & Measure** during 15 days only.

3.5.2.2 I already use IP Traffic - Test & Measure ...



*This paragraph is dedicated to the users owning a previous version of **IP Traffic - Test & Measure**.*

... and I want to upgrade and keep my permanent license

In that case, choose the Package #2 *“Customers with a Software Protection Key”*.
Your installation will be upgraded and your existing permanent license will be kept.

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

In that case, choose the Package #3 *“Customers with Software Protection using a USB Key”*. Plug the USB Software Protection Key before launching **IP Traffic - Test & Measure**.

3.5.2.3 I just bought IP Traffic - Test & Measure ...



*This paragraph is related to the users purchasing **IP Traffic - Test & Measure V2.7** for running.*

... and I chose the Electronic Software Delivery (ESD)

In that case, choose the Package #2 *“Customers with a Software Protection Key”*.
When you launch the software for the first time, press the “Enter” key when the ZTI Communications logo appears. Then, get the Site Code and email it to us with your details and your purchase order reference at contact@zti-communications.com.

We will email you back the Site Key enabling your permanent license.

More details about the way to proceed are available in paragraph *“4.2.1 Installation of the Software Protection Key”*.

... and I received the CD-ROM & USB Software Protection Key

In that case, choose the Package #3 *“Customers with Software Protection using a USB Key”*.

Plug the USB Software Protection Key before running **IP Traffic - Test & Measure**.

... and I will receive the CD-ROM & USB Software Protection Key in a few days

In that case, choose the Package #2 *“Customers with a Software Protection Key”*.
You will get a fully functional but time-limited Software Protection Key.

3.6 What has been installed on my computer?

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

- IPTraff.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 (with the Software Protection Key package only)
- Automation scenario samples and other files required by the software
- Samples of sniffed traffic files
- Viewer.exe: program file installed with the USB Software Protection package only
- ElevateIPTraff.exe : allows running IP Traffic as administrator (for Windows Vista only)
- Version.txt: a 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 installation procedure automatically installs the packet capture driver named 'znpf.sys' on your system in the 'IP Traffic' installation directory.

Start Menu shortcuts created:

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

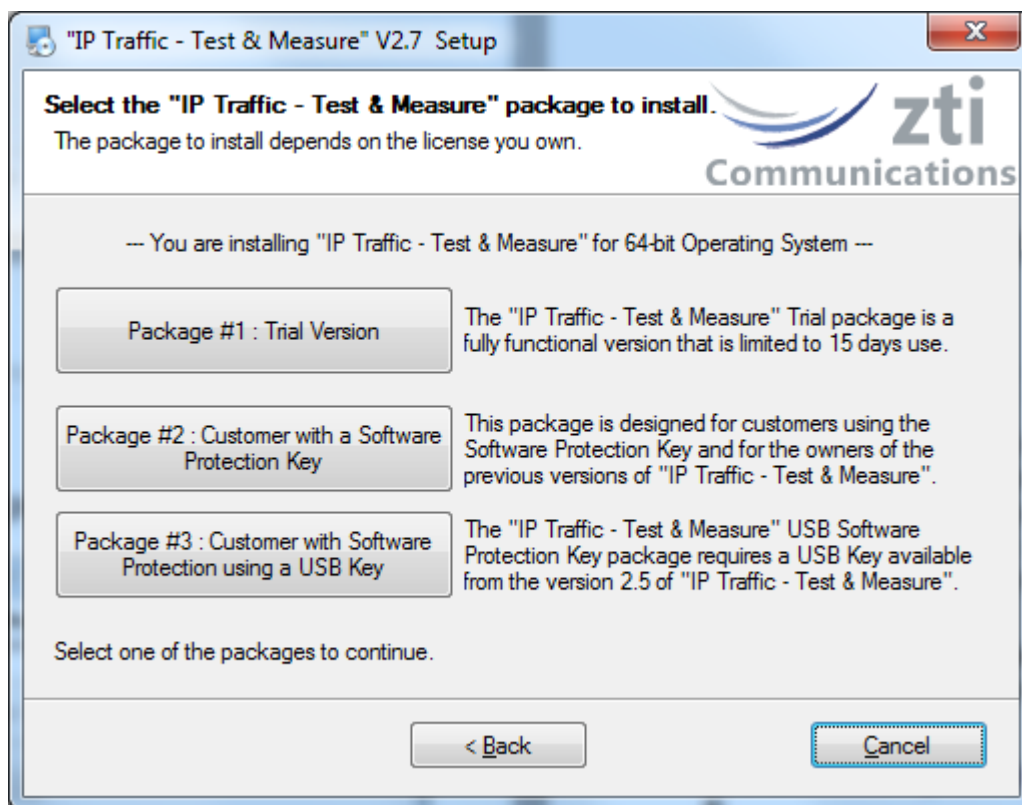
- ⇒ **IP Traffic - Test & Measure** (click to launch)
- ⇒ **Automation Tool for IP Traffic - Test & Measure** (click to launch)
- ⇒ **Uninstall IP Traffic - Test & Measure** (click to launch)
- ⇒ **IP Traffic - Test & Measure User Guide** (PDF file)
- ⇒ **Automation Tool for IP Traffic - Test & Measure User Guide** (PDF file)
- ⇒ **Read Me First** (PDF file)
- ⇒ **License help** (Software Protection Key only / Package #2)
- ⇒ **USB Software Protection Key Viewer** (Software Protection using a USB key only / Package #3)



*If the RPC mechanism is disabled, a message will ask automatically for the system reboot at the end of the installation. This is mandatory to allow the dialog between the Automation Tool and **IP Traffic - Test & Measure**.*

3.7 How to reinstall another package?

If you already have installed one of the **IP Traffic - Test & Measure** V2.7 packages, click [Setup_IPTrafficBundle.exe](#) and select, in the window below, the new package you want to install.



3.8 How to transfer the software to another computer?

Install the software on the target computer. You don't need to do any particular operation with the *"Customers with Software Protection using a USB Key"* and *"IP Traffic - Test & Measure Trial"* packages.

With **IP Traffic - Test & Measure** & USB Software Protection Key, you do need to plug the USB key before running the software on the target computer.

With the Package #2 *"Customers with a Software Protection Key"*, install the software on the target computer and refer to the paragraph *"4.2.2 Software Protection Key Transfers"* to know how to transfer the software license.

PART 4 How to handle your license?

4.1 IP Traffic - Test & Measure Trial Version

You don't require any license to use the trial version of **IP Traffic - Test & Measure**. After the first run of **IP Traffic - Test & Measure**, the **IP Traffic - Test & Measure** trial version can be used during 15 days.

4.1.1 IP Traffic - Test & Measure License Information window

When you run **IP Traffic - Test & Measure**, the information about your trial license is displayed, as shown below.



You are now able to use **IP Traffic - Test & Measure** during the next 15 days.

4.1.2 End of the 15-day trial period

Once the trial period is finished, you are not allowed to use **IP Traffic - Test & Measure** anymore, as shown below:



When you press the **OK** button, **IP Traffic - Test & Measure** will stop running. To continue to use the software please contact your local distributor or **ZTI Communications** to get a permanent license.

4.2 IP Traffic - Test & Measure & Software Protection Key

Licensed users of **IP Traffic - Test & Measure** that are already using the Software Protection Key should not need to refer to the section 4.2.1. To transfer the owned license to another PC or to another directory, please go directly to section 4.2.2.

4.2.1 Installation of the Software Protection Key

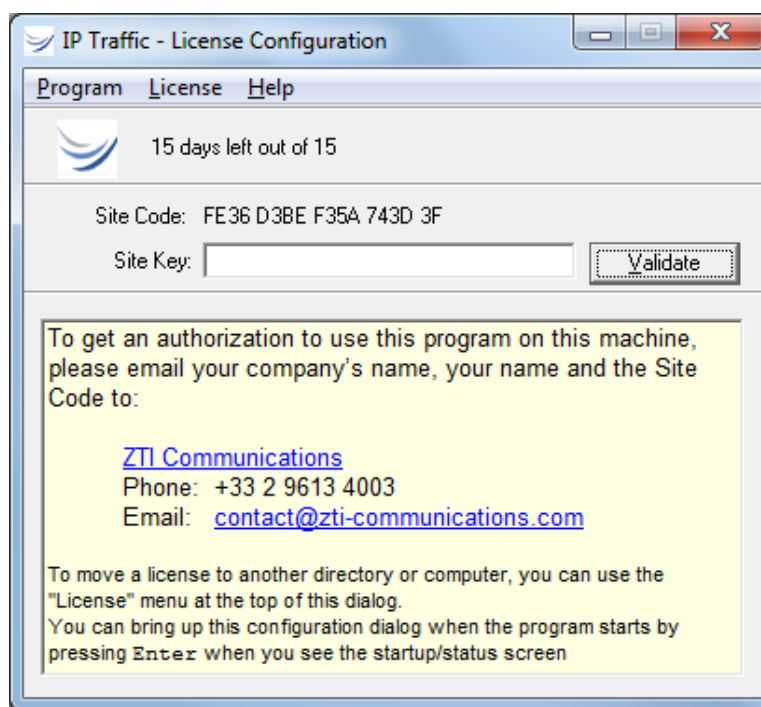


*This software is licensed on a per workstation basis. This means that you will need to get a separate license for each machine you will install it on. Each licensed copy of the software installed on a system has a unique **Site Code** that requires a corresponding unique **Site Key** to work. A period of 15-day is automatically enabled at the first installation of the software. If you try to install the software again, the Software Protection Key will disable the trial period.*

If you want to configure your Software Protection Key before the time-limited period end, press **Enter** just after launching the **IP Traffic - Test & Measure** when the following message is displayed:

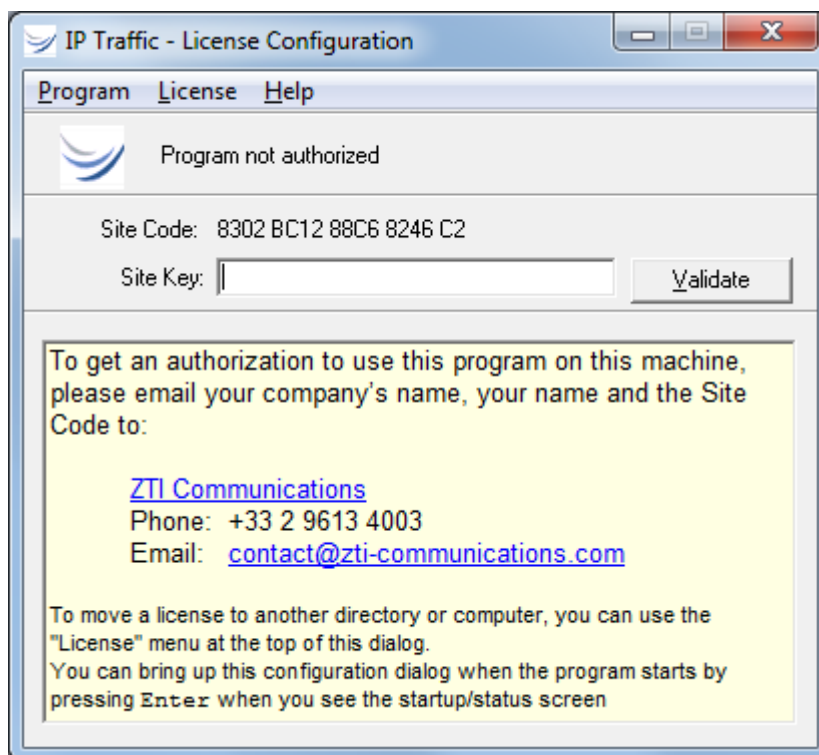


Then, you will see the following license configuration window:





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

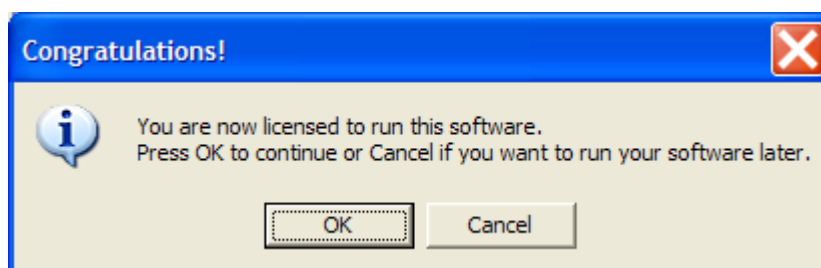


To get the **Site Key** and obtain a permanent license, please send an email to contact@zti-communications.com with the following information:

- The **Site Code** (you can copy and paste the Site Code displayed in the license window)
- The name of the software: **IP Traffic - Test & Measure**
- The OS used
- Your details
- The purchase order's number and date of purchase

We will then email you the **Site Key**. You can now close the license's 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 Software License program generates a new **Site Code** automatically.

⇒ For any question or further information, please contact our technical support:

Email: support@zti-communications.com

Phone: +33 2 9613 4003

*When you launch **IP Traffic - Test & Measure** with a Software Protection Key related to a permanent license, you will see the following window:*



4.2.2 Software Protection Key Transfers



A Software Protection Key transfer is not a duplication of any type. Please contact ZTI Communications or your authorized distributor for site Software Protection Key information and for several Software Protection Keys purchase.

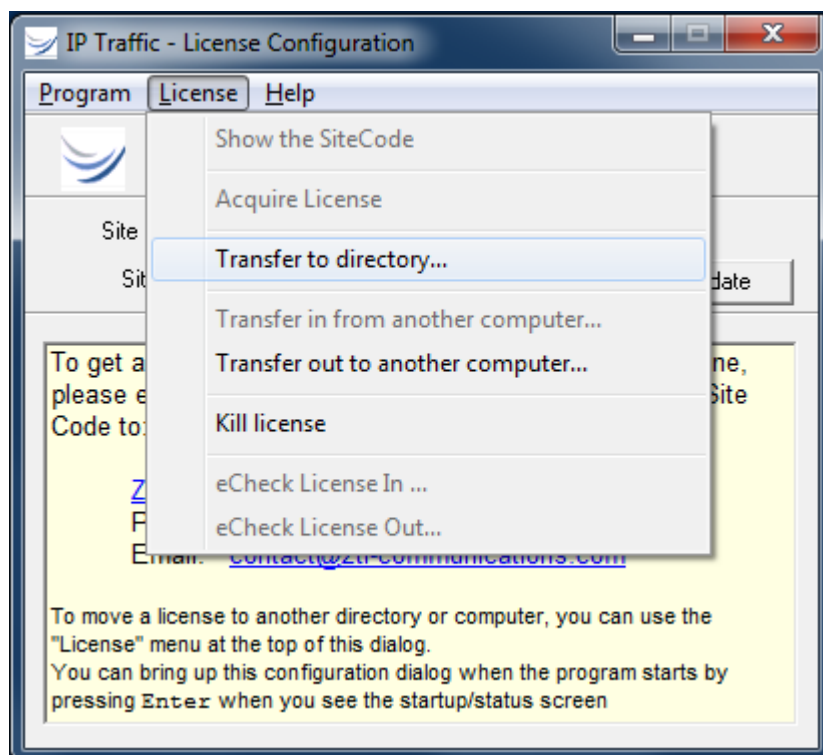
Software Protection Keys can be transferred using one of the following methods:

- ⇒ **Direct transfer:** move the Software Protection Key to another directory of the same PC or between two PCs linked to the same network.
- ⇒ **Transfer by media:** move the Software Protection Key from a source PC to a target PC by using a USB key or an external hard disk.

4.2.2.1 Direct Transfer: move the Software Protection Key from one local directory to another

This transfer mechanism must be used to move a Software Protection Key in two cases:

- From a source to a target directory of the same PC
 - From a source to a target directory of networked PCs
- First, copy the program (copy the **IP Traffic - Test & Measure** folder) to the target directory.
For example from "C:\Program Files\IP Traffic" to "C:\Temp\IP Traffic"
 - Then run the program from its original directory (from "C:\Program Files\IP Traffic"). When the Software Protection Key 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:\Temp\IP Traffic \IPTraff.exe)
- The Software Protection Key is now transferred to the new directory.

4.2.2.2 Transfer by Media (USB key) from a source PC to a target PC



A USB key or an external hard disk is needed for this kind of transfer.

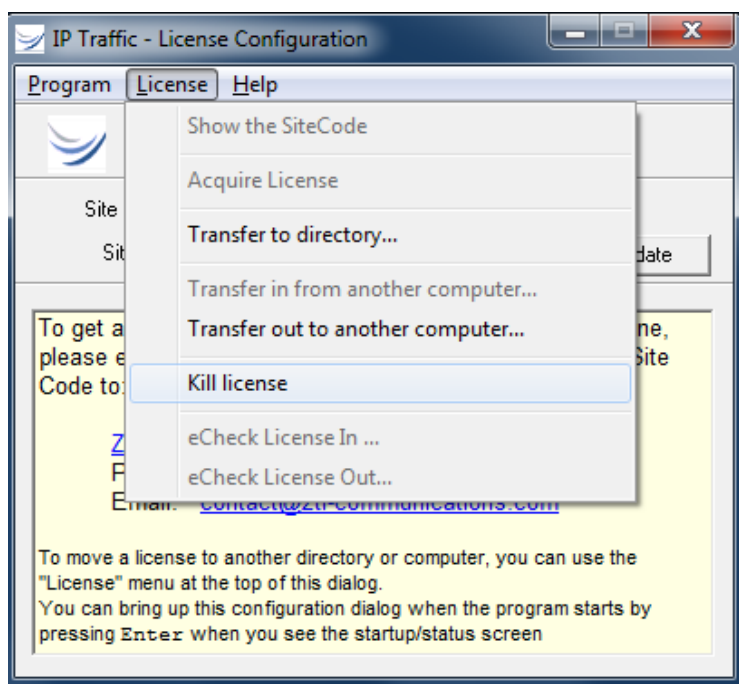
To transfer the Software Protection Key from the source PC (PC #1) to the target PC (PC #2), proceed as described in the following order:

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

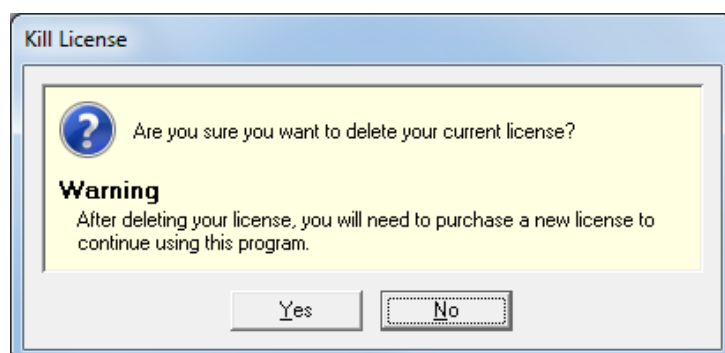
If the "Transfer in from another computer ..." item of the license menu is disabled, you must kill the time-limited license.

How to kill the Software Protection Key?

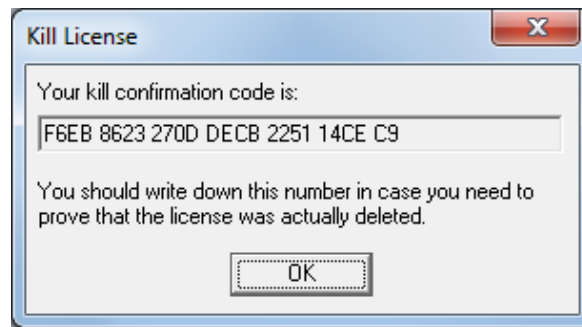
When the license configuration window appears, press **Enter** and select "License > Kill license" in the license menu.



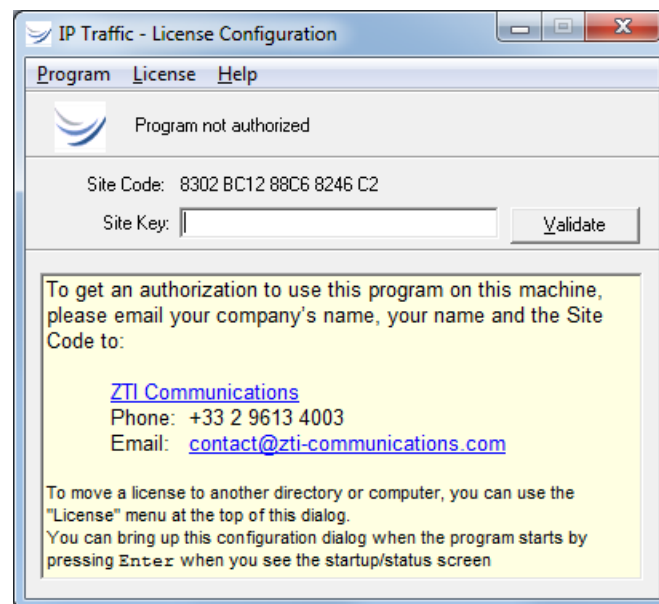
A message box will appear:



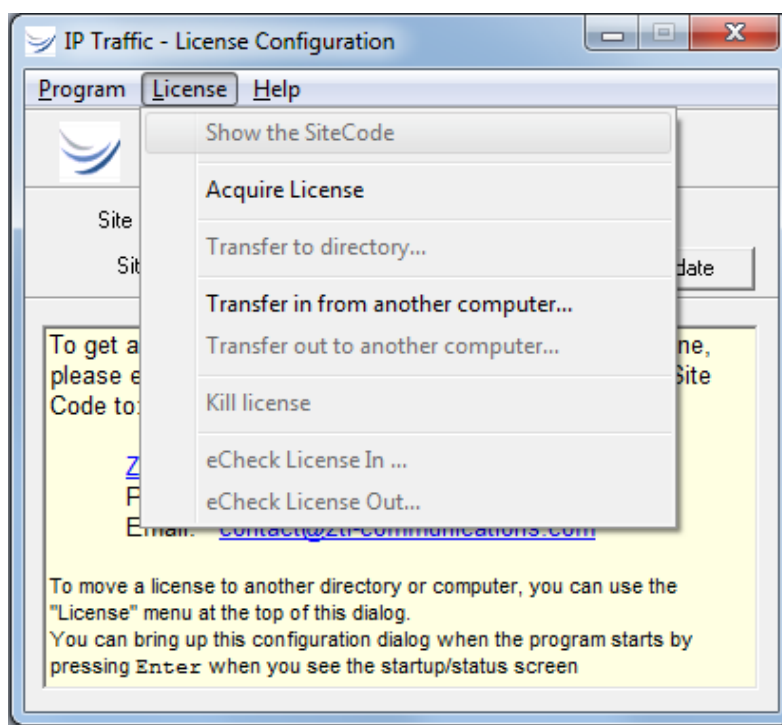
Press 'Yes' to kill the license and a confirmation code is displayed:



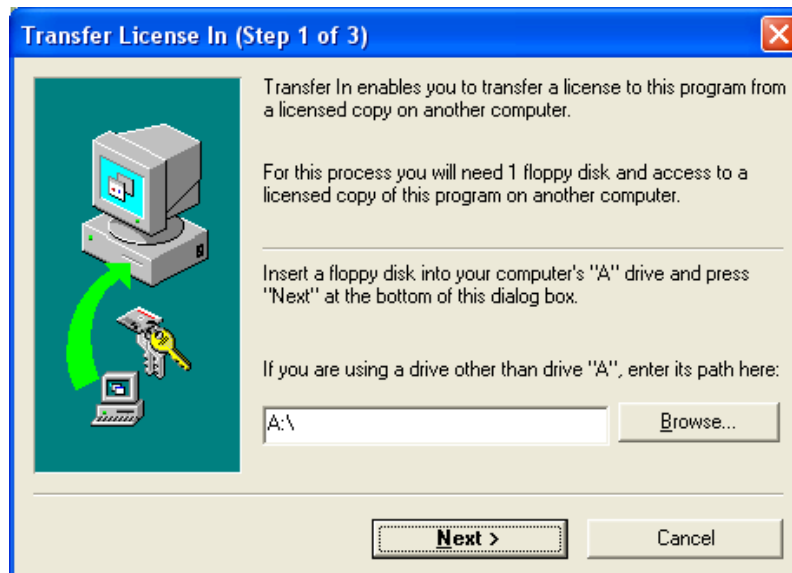
Click 'OK' and the license configuration window displays now "Program not authorized":



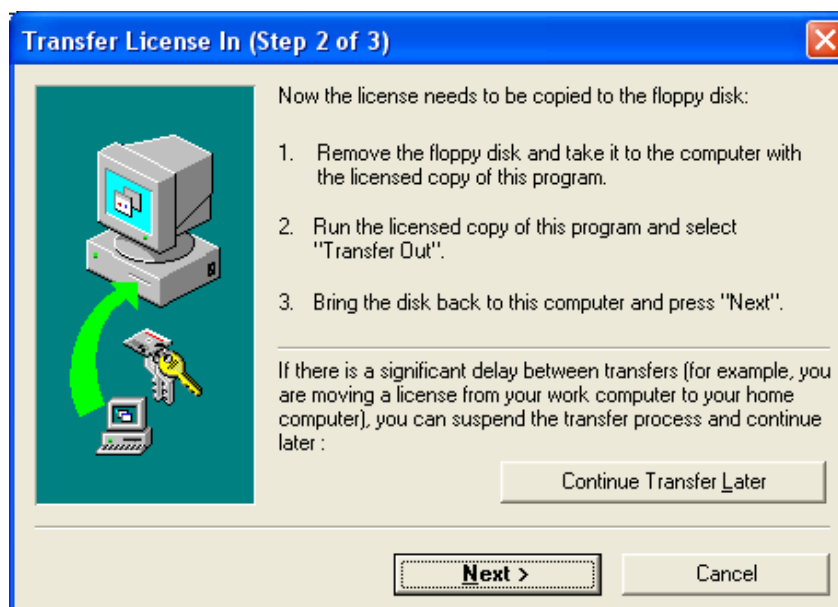
3) Select "License > Transfer in from another computer ..." in the License menu:



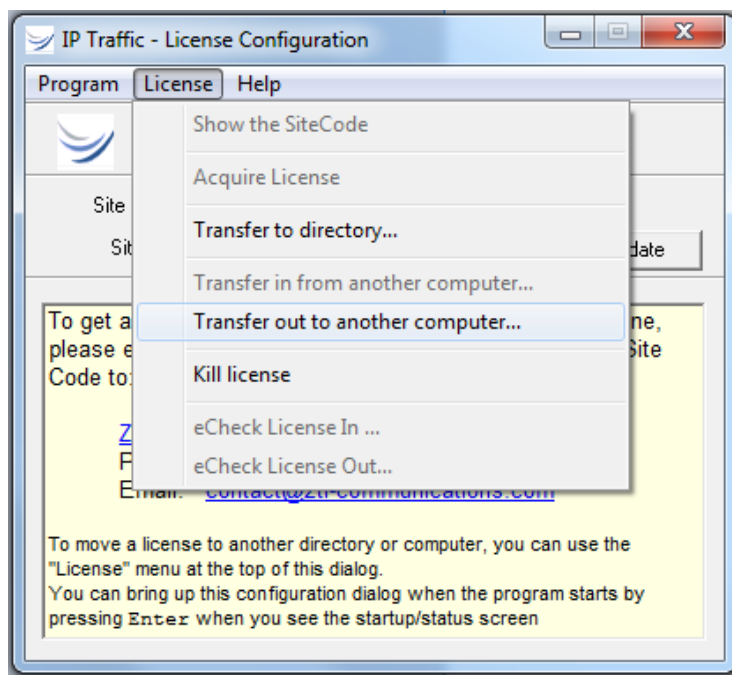
The "Transfer License In (Step 1 of 3)" window is displayed:



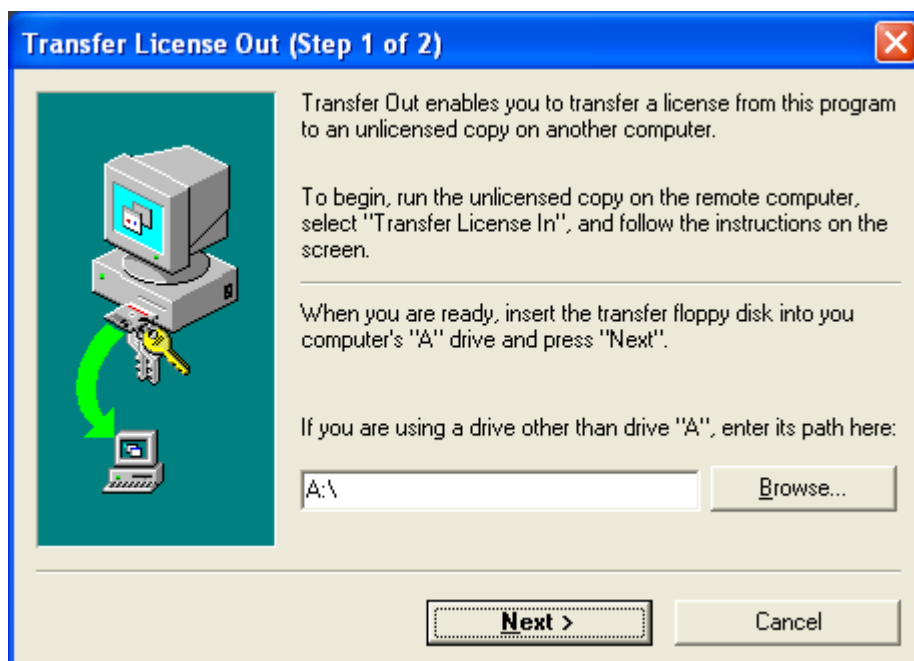
4) Insert a USB key as requested in step 1 of 3 and specify the path. Then press "Next >": the "Transfer License In (Step 2 of 3)" window is displayed:



5) Go to the source PC (PC #1) and insert the media (USB key or external hard disk). 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:

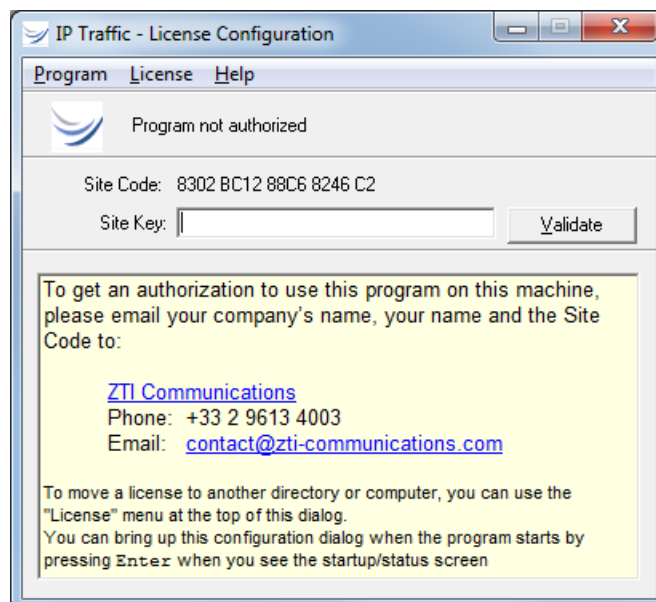


The following window is displayed:



Input the media path (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 a Site Software Protection Key (contact@zti-communications.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 license is now transferred from the source PC to the target PC, and you get the following message:



Click Finish to continue.

4.3 IP Traffic - Test & Measure & USB Software Protection Key

The USB Software Protection Key is the most flexible way to transfer your license to any other PC. Plug it in the computer you want to use **IP Traffic - Test & Measure** on.

If you are a user of a previous version of **IP Traffic - Test & Measure** (version 2.4 and under) change for more flexibility to a **USB Software Protection Key** by contacting ZTI Communications Sales Offices (sales@zti-communications.com) and get some information about how to exchange your software key to a **USB Software Protection key**.

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.

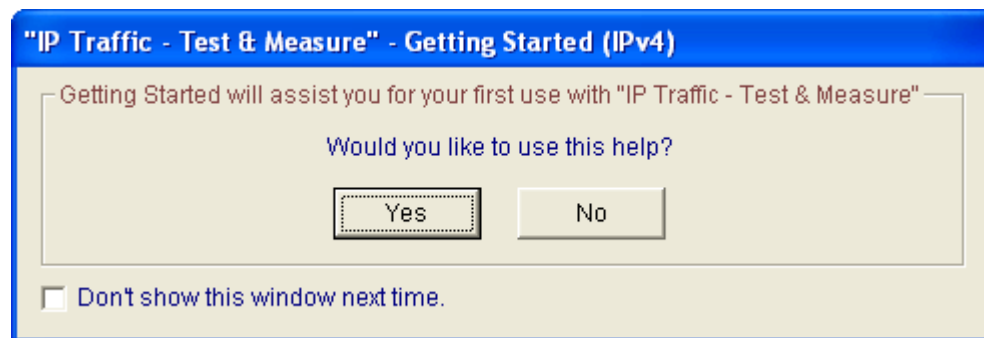
PART 6 Getting Started



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).

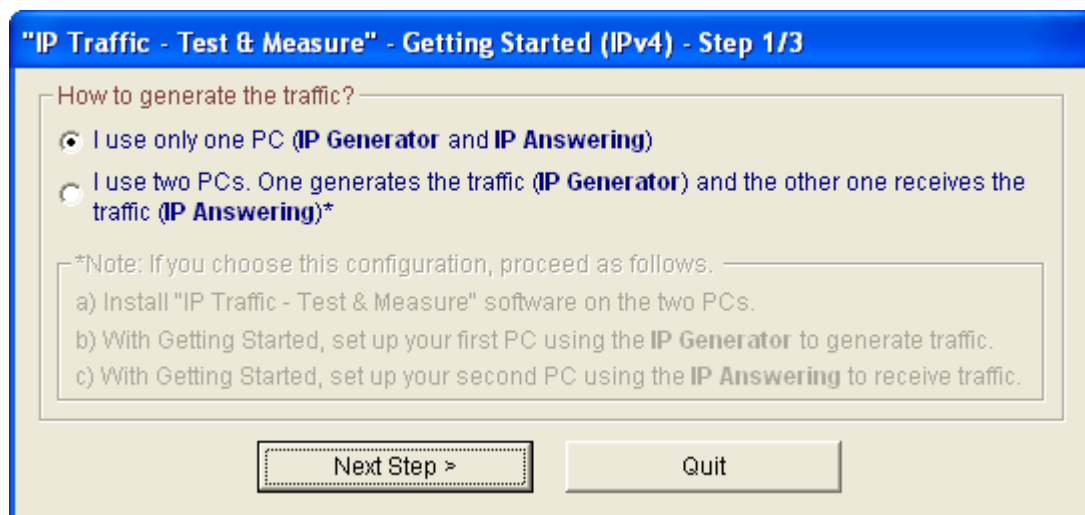
New users can use this help as an introduction to **IP Traffic - Test & Measure** and generate or receive traffic with the IPv4 protocol in a few clicks.

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

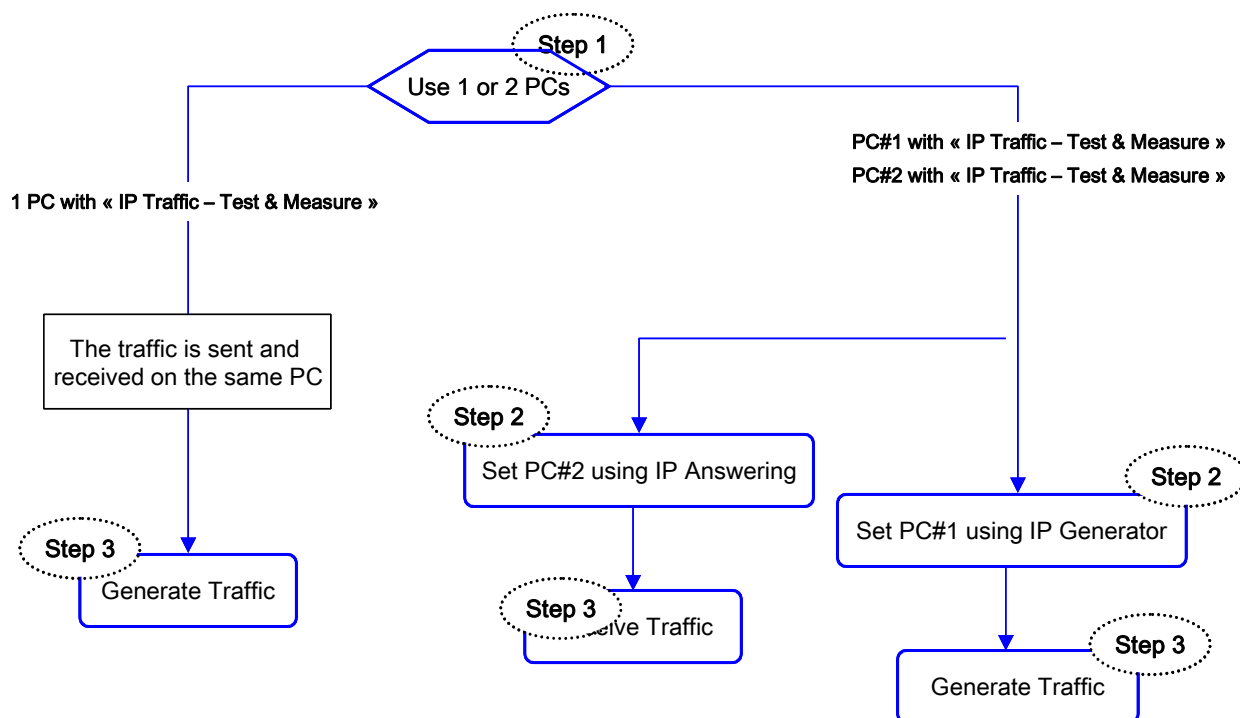


Press **No** if you don't want to use this help.

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

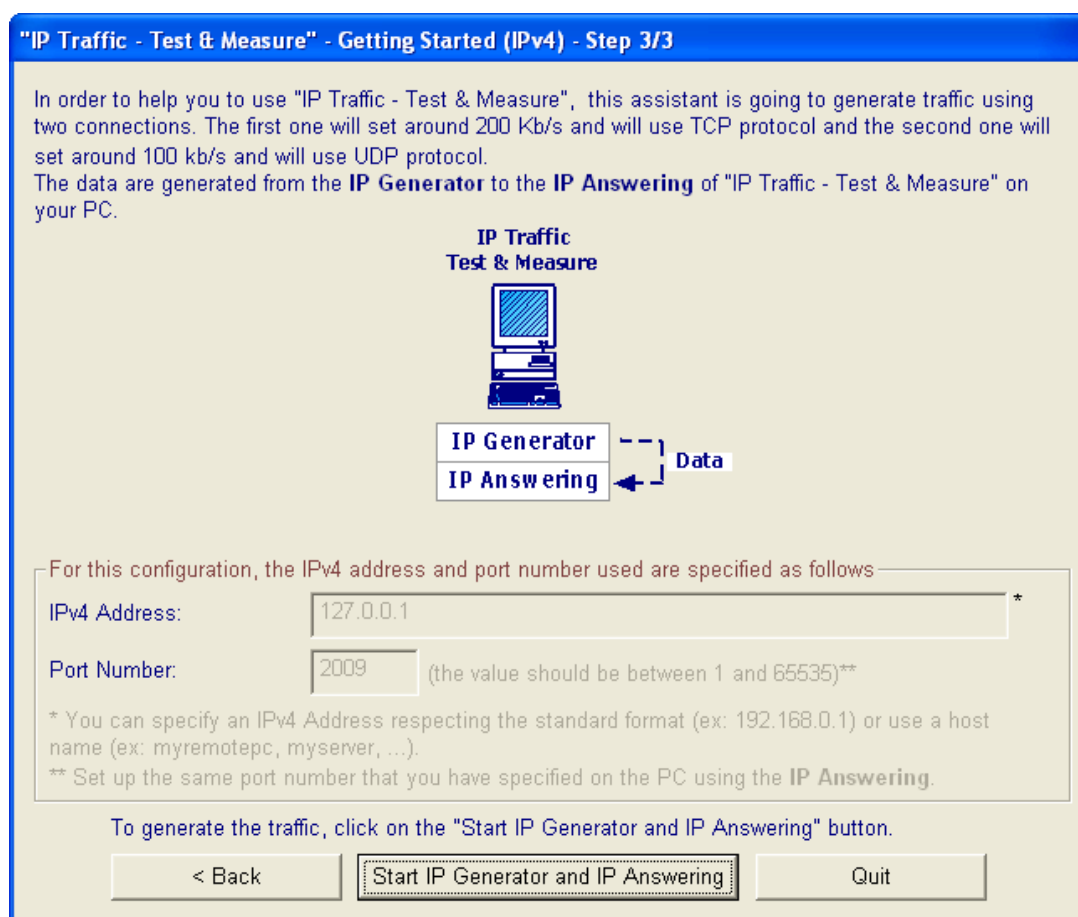


Depending on your choice to use 1 or 2 PCs, the plan below shows the steps:

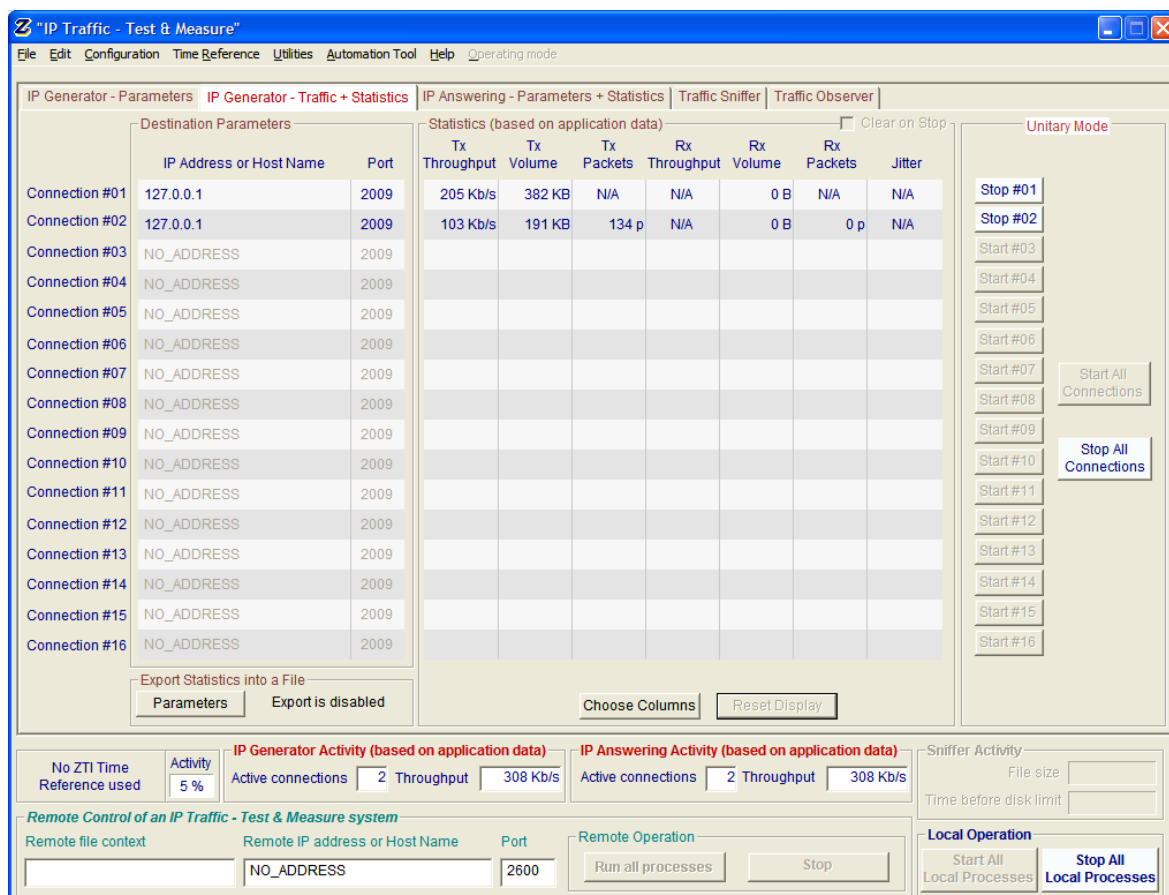


For the use of 1 PC

The following windows are displayed.

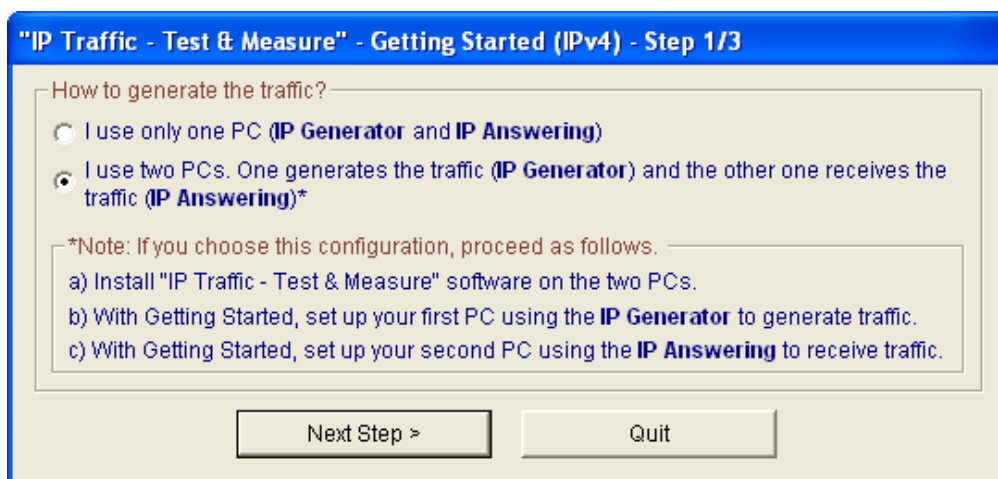


Then press the "Start IP Generator and IP Answering" button to continue. The "IP Generator – Traffic + Statistics" tab of **IP Traffic - Test & Measure** will display the two first active connections as shown on the following window:

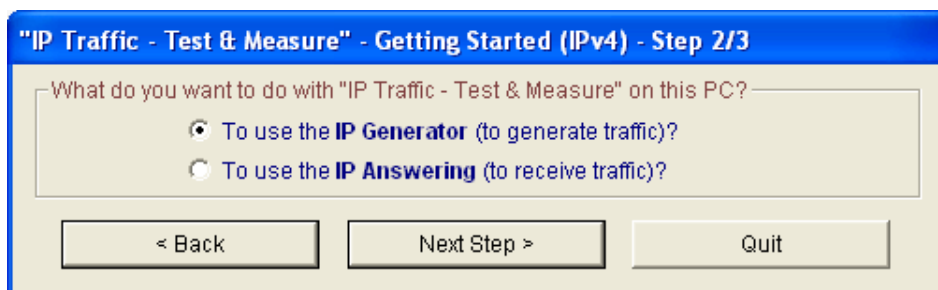


For the use of 2 PCs

If you select the option: **I use two PCs**, read the following instructions. **IP Traffic - Test & Measure** must be installed on the two PCs.

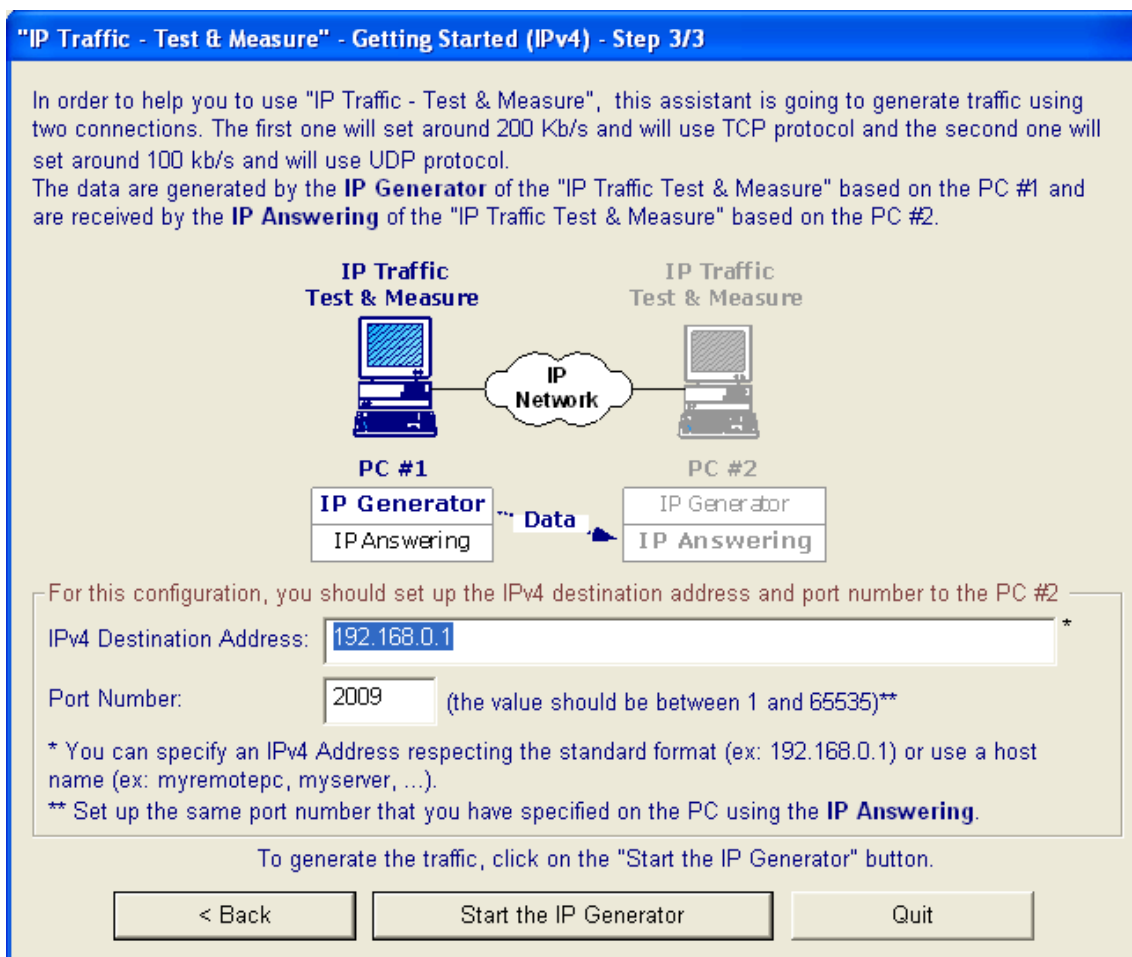


Press "Next Step >" to continue.



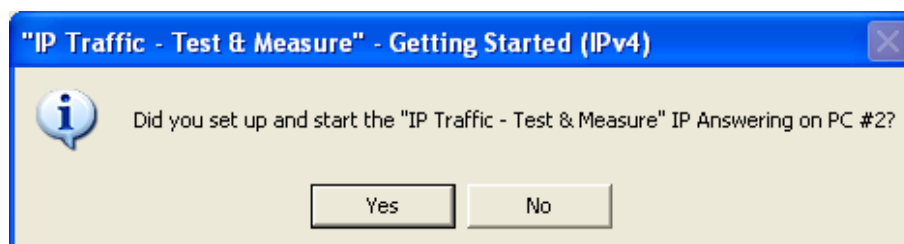
Then choose if you want to generate or receive the traffic on this PC.

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

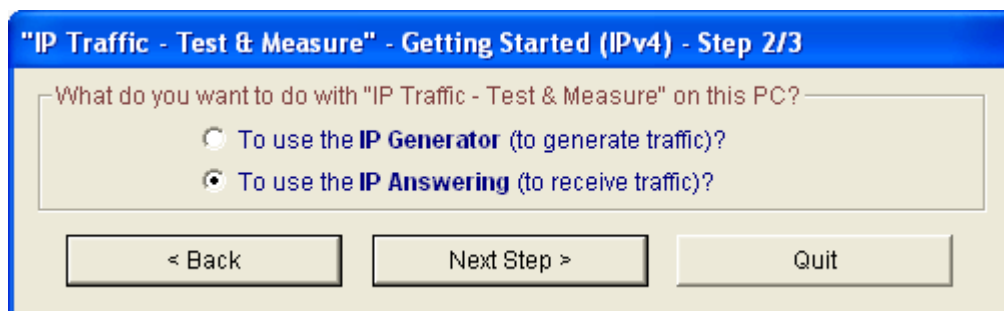


Define the IPv4 address and port number to use.

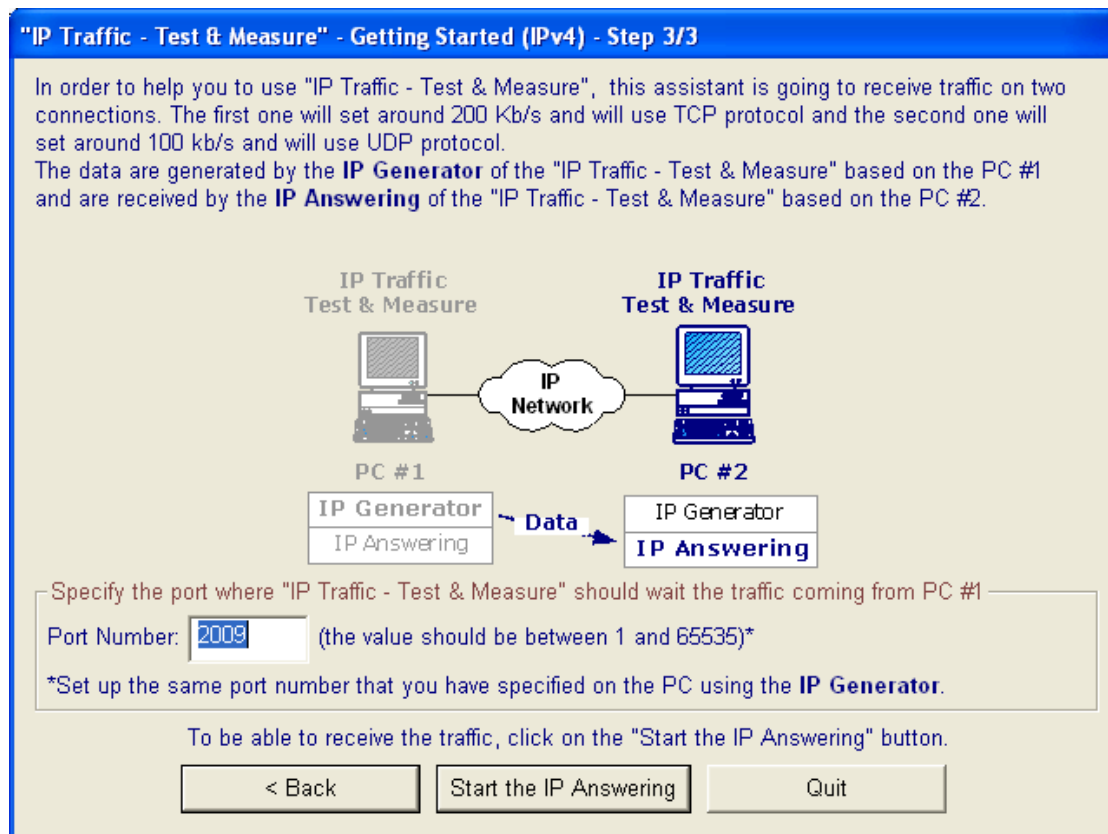
Then press the "Start the IP Generator" button and a warning dialog is displayed:



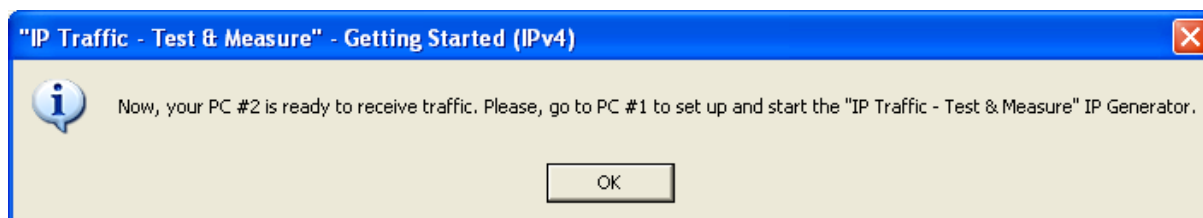
Before generating traffic towards PC #2, the PC #2 must be configured as IP Answering.



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.



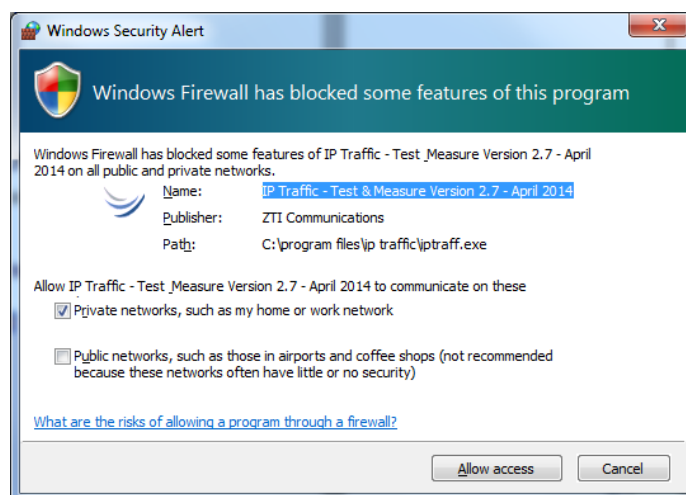
For Vista and after, you must have the administrator rights to be able to use the DSCP field. To launch IP Traffic with the administrator rights, right-click on the IP Traffic - Test & Measure shortcut as shown above and choose "Run as administrator".

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

| 15-day Trial Version | Software Protection Key Version |
|--|---|
|  |  |
| USB Software Protection Key Version | |
| If you use a USB Software Protection Key, there is no window! | |

With some Windows O.S., 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 and 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**.



Windows Firewall may also disrupt the **IP Traffic - Test & Measure** performances. To get best performances, you should disable Windows Firewall.



To use the NTP Server under Window Vista, the ICMP exchange must be allowed. Please refer to the paragraph 8.3 "How to authorize ICMPv4 and ICMPv6 traffic under Windows Vista."

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** to work.

8.1 How to authorize TCP and UDP connections blocked by the Windows Firewall under Windows XP and Server 2003

Windows Firewall blocks incoming network connections except for the authorized programs. To allow **IP Traffic - Test & Measure** receiving incoming TCP or UDP connections, you must add it in the exceptions list of Windows Firewall by proceeding as follows:

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

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

```
%> netsh firewall add allowedprogram program="C:\Program Files\IP Traffic\IPTraff.exe" name=IP Traffic - Test & Measure mode=ENABLE scope=ALL profile=ALL
```

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



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

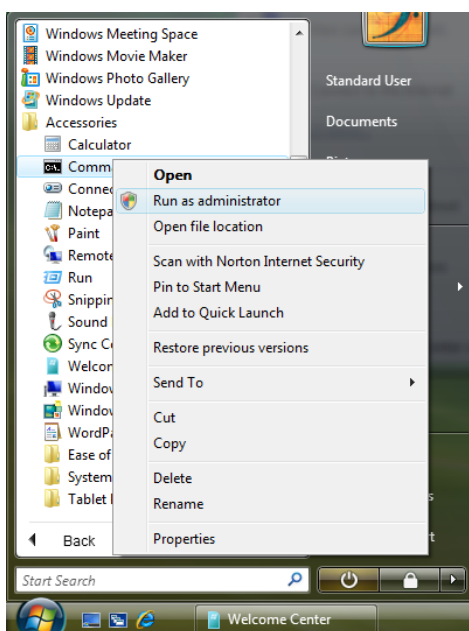


This command line allows IGMP protocol used by the IPv4 multicast connections.

8.2 How to authorize UDP and TCP connections under Windows Vista and after

Windows Firewall on Windows Vista and after blocks incoming and outgoing network connections except for the authorized programs. By default, all outgoing connections are allowed. But to authorize **IP Traffic - Test & Measure** receiving incoming connections, you must add it in the exceptions list of Windows Firewall by proceeding as follows:

Step 1: Open a command prompt window with the administrator rights. The administrator rights are mandatory to set up the firewall configuration. Open the "All Programs / Accessories" folder and right-click on the "Command Prompt" icon as shown on the figure below and choose "Run as administrator". A command prompt window is opened.



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

```
%> netsh firewall add allowedprogram program="C:\Program Files\IP Traffic\IPTraff.exe" name="IP Traffic - Test & Measure" mode=ENABLE scope=ALL profile=ALL
```

Make sure that "C:\Program Files\IP Traffic\" is the installation directory of **IP Traffic - Test & Measure**. A message of confirmation is returned by *netsh* if the command is succeeded. If the path you have specified is invalid, *netsh* returns an error message close to the following message: *The system cannot find the file specified.*

In that case, please renew Step 2 with the correct path.



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



This command line allows IGMP protocol used by the IPv4 multicast connections.

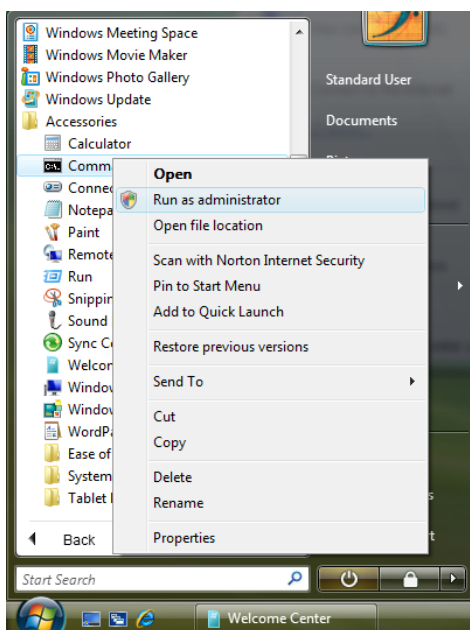


To use a NTP Server under Window Vista and after, the ICMP exchange must be allowed. Please refer to the paragraph 8.3 "How to authorize ICMPv4 and ICMPv6 traffic under Windows Vista."

8.3 How to authorize ICMPv4 and ICMPv6 traffic under Windows Vista and after

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

Step 1: Open a command prompt window with the administrator rights. The administrator rights are mandatory to do the firewall configuration. Open the "All Programs / Accessories" folder and right-click on the "Command Prompt" icon as shown on the figure below and choose "Run as administrator". A command prompt window is opened.



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

```
%> netsh advfirewall firewall add rule name="Echo Reply ICMPv4 (used by IP Traffic - Test & Measure)"  
dir=in action=allow profile=any localip=any remoteip=any protocol=icmpv4:0,0 interfacetype=any
```

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

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

```
%> netsh advfirewall firewall add rule name="Echo Reply ICMPv6 (used by IP Traffic - Test & Measure)"  
dir=in action=allow profile=any localip=any remoteip=any protocol=icmpv6:129,0 interfacetype=any
```

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



ICMP exchanges must be allowed to enable the use of the NTP Server.