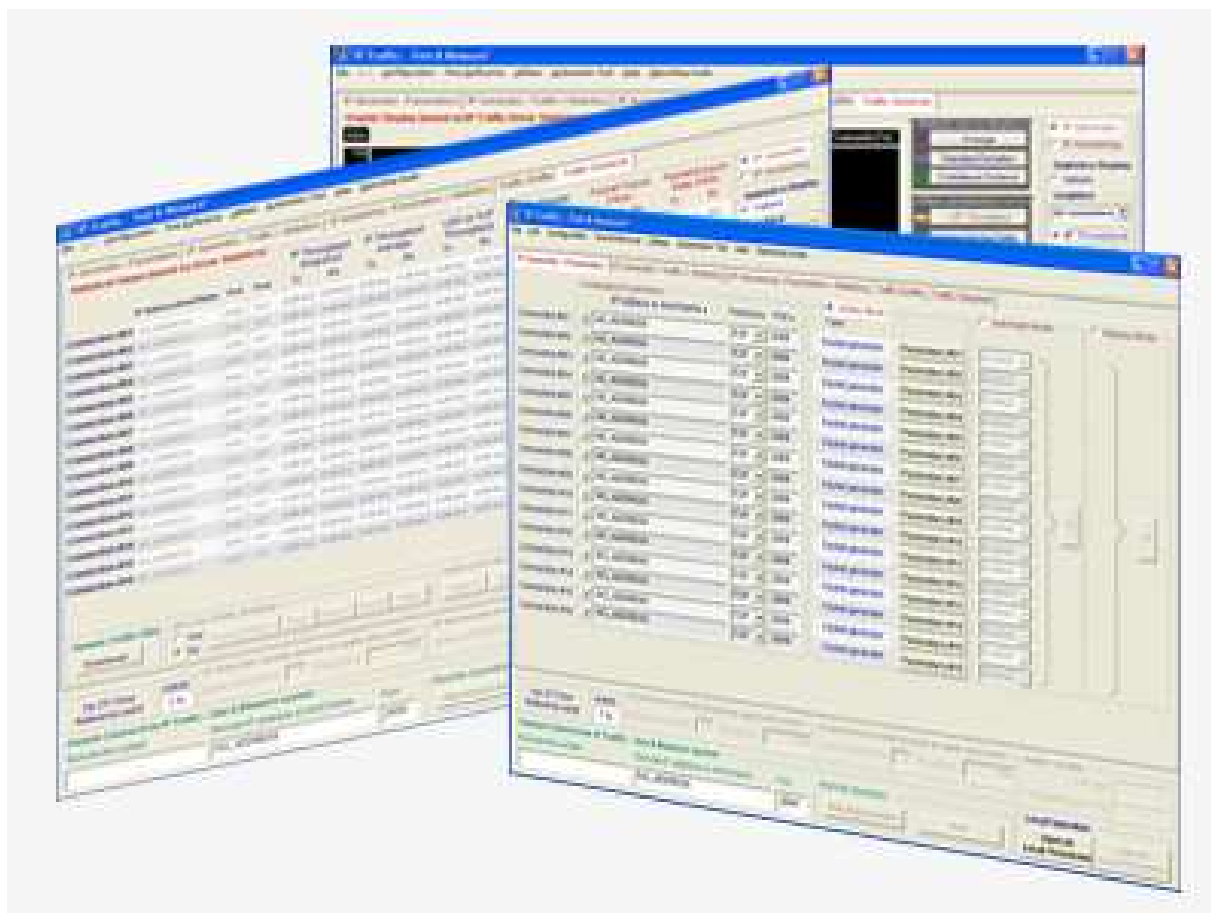




Version 2.6

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

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



Product Overview

Minimum System Requirements

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

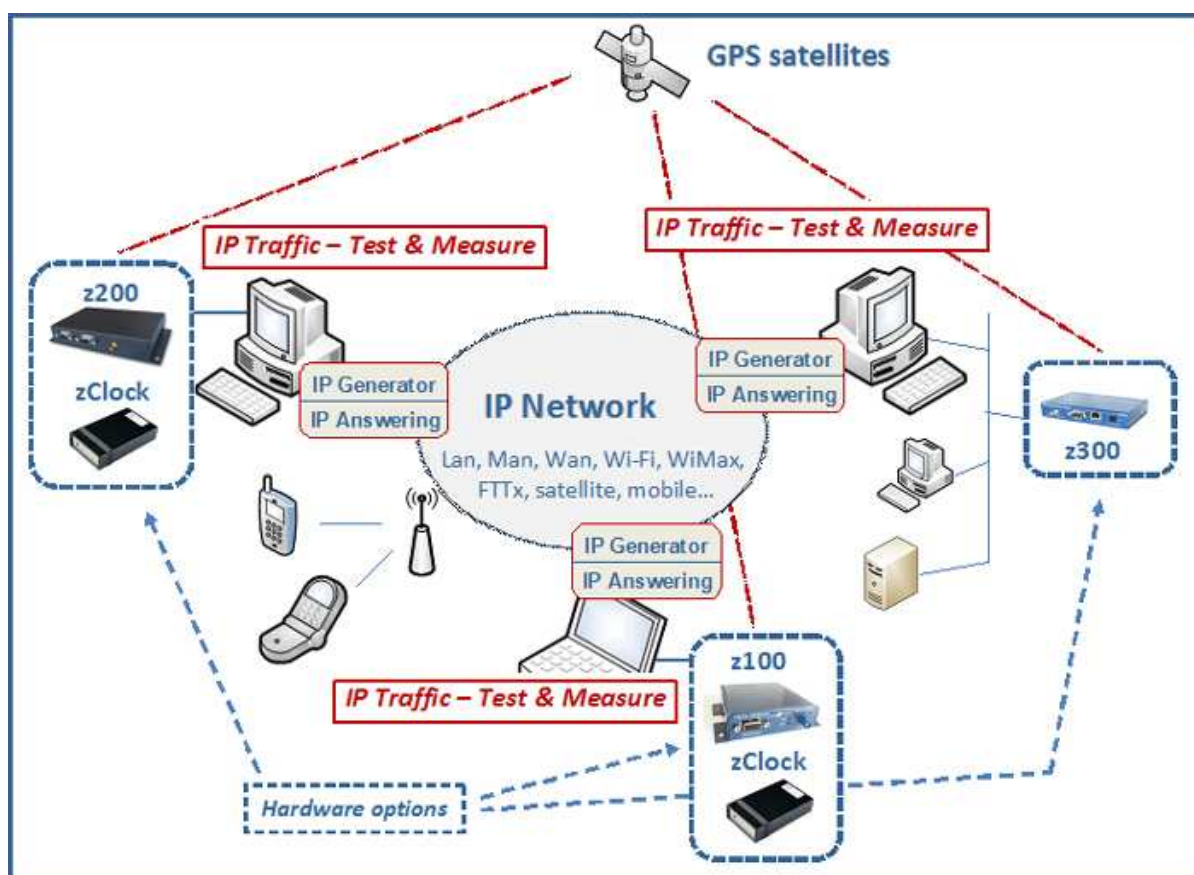
- All modern versions of Microsoft Windows are supported - from 2000 to Windows 7 with 32-bit or 64-bit environment, including Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 and Windows Seven.
- Pentium processor with 512 MB memory
- 1024 x 768 display
- 25 MB free hard disk space

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.

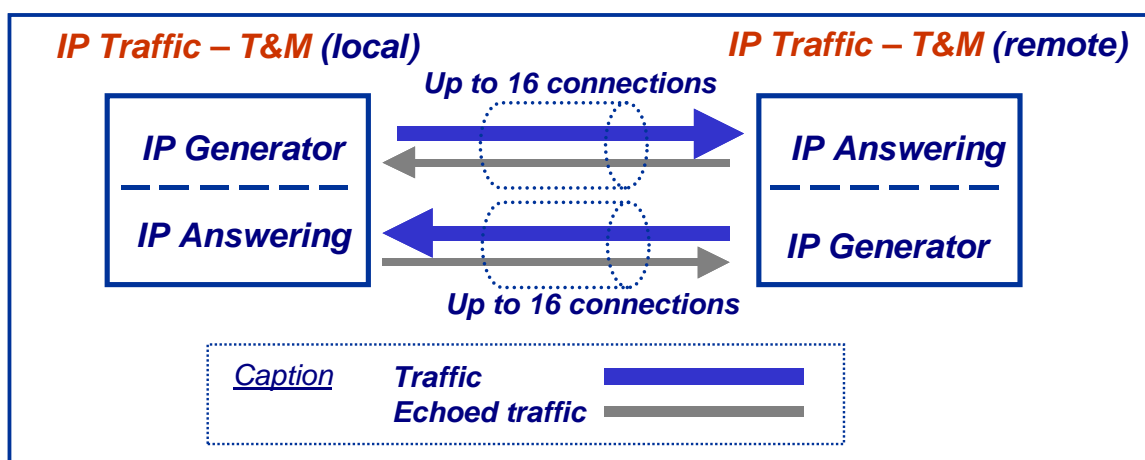


IP Traffic – Test & Measure is an IP software testing tool using the Microsoft Windows TCP/IP stack (Winsock2 interface). So, **IP Traffic – Test & Measure** is independent of any transmission or telecom link and can use any transmission link managed by the Windows operating system: LAN (Ethernet, Token-ring,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

IP 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 GPS (z100, z200 or z300 device) and a very precise clock (zClock).

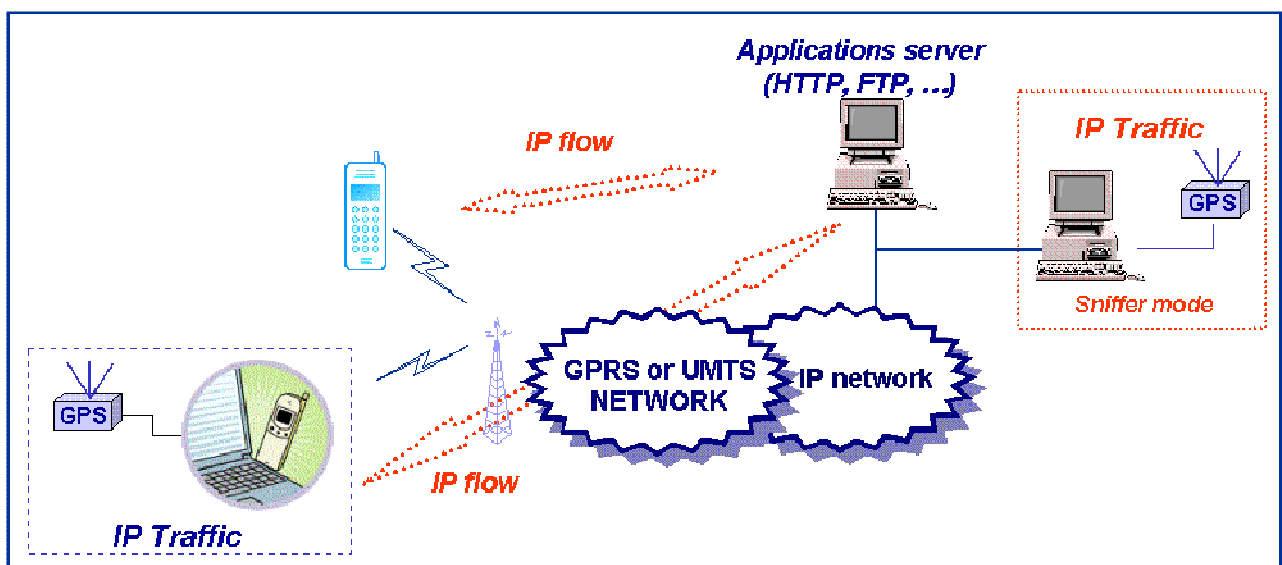
IP Traffic – Test & Measure is composed of four modules: 'IP Generator', 'IP Answering', 'Traffic Sniffer' and 'Traffic Observer'.

- '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

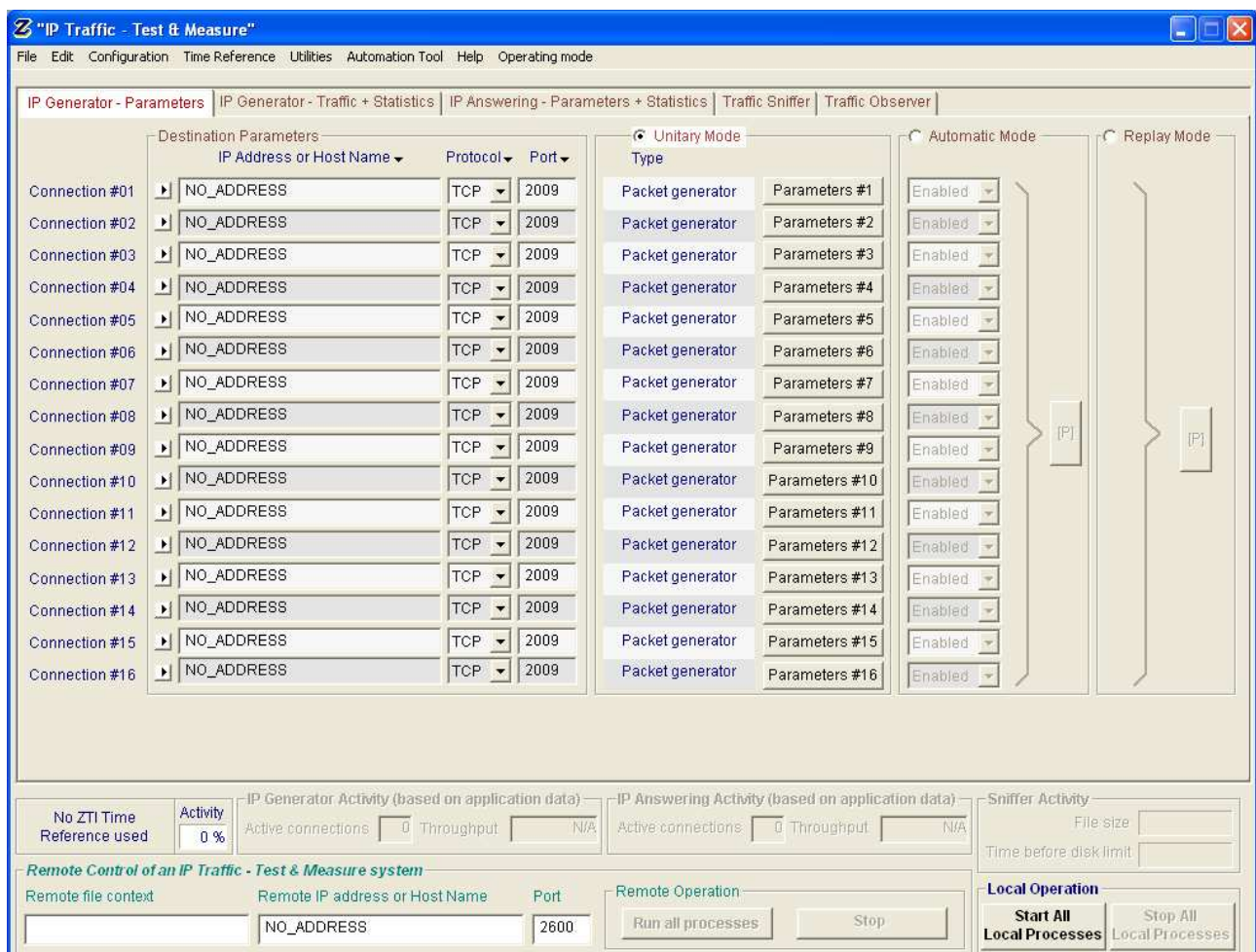
telephony...) can be captured and saved in a file. IP packets are time-stamped, to replay IP traffic with the same timing as for the capture. The user can then use an internal **IP Traffic – Test & Measure** algorithm in order to obtain two traffic files (traffic client file and traffic server file). 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:

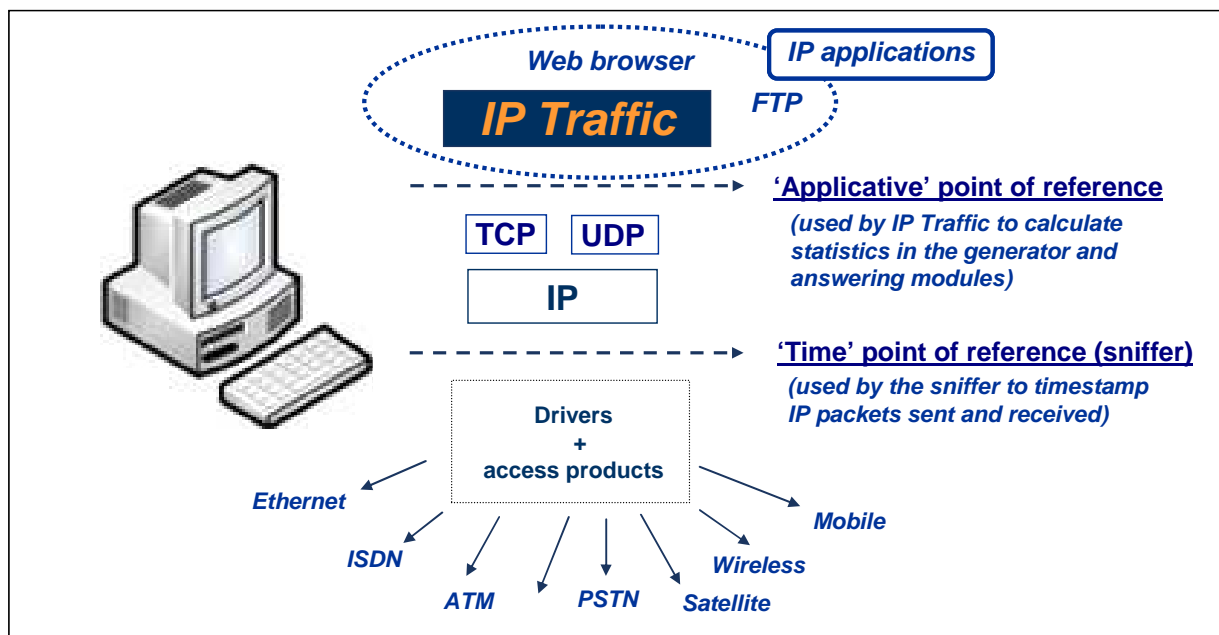
- The **normal** mode: the user can access all commands and functionalities
- The **remote control** mode: the user can't access locally commands of **IP Traffic – Test & Measure**. It's mainly used for control by a remote **IP Traffic – Test & Measure** system. It's very useful for example to use an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

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 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 recommends an additional time device to allow a precise calculation of the propagation delays through IP networks.

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.

z100 - Time Device synchronized by GPS (*Timing & Navigation*)



Based on the Trimble Copernicus 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.

z200 - Time Device synchronized by GPS (*High Precision Timing*)



Designed to provide an accurate pps (pulse per second) signal to use in measurement and industrial applications, this GPS 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. If the satellites signals are completely lost, the hold-over mode enables the module to keep sending the pps signal, with low drift over time.

z300 – High Precision Time Server synchronized by GPS



This high precision NTP time server with PoE (Power over Ethernet) is designed for indoor or outdoor use and synchronized by GPS, in order to provide accurate timing information for network synchronization and measurement applications. It delivers accurate timing information, even in poor signal level conditions as z200. Thanks to its self-survey mode, the accuracy of the timestamp (compliant with SNTP protocol) is less than 10 μ s, and is achievable even with only 1 satellite being tracked. z300 is available in different metal housings, either compact (z300-C) or 19" rack mounted form factor (z300-R).

zClock – High Precision Clock



The Real Time Clock (RTC) built into most common machines is far from being reliable and most RTCs drift considerably over time. Based on a high stability OCXO (Oven-Controlled Crystal Oscillator) with a fast warm up, the zClock product offers a very precise clock (0,27 ppm) to any PC applications all that in a small and compact device. By using zClock, the application can rely on a precise clock with a drift lower than 1 millisecond for 1 hour on 1 year.

Time Reference Accuracy vs configuration chosen

| Configuration | Absolute Time reference | Accuracy for Measurement |
|---|---|---------------------------------------|
| IP Traffic – Test & Measure | None or user defined. | Not defined (PC clock used) |
| IP Traffic – Test & Measure + z100 or z200 | YES , provided by the time device synchronized by GPS. Absolute reference. | 5 milliseconds |
| IP Traffic – Test & Measure + zClock | NO or user defined (zClock is initialized with the PC clock). Relative reference. | 1 millisecond |
| IP Traffic – Test & Measure + z100 or z200 + zClock | YES , provided by the time device synchronized by GPS (zClock is initialized with the GPS time). Absolute reference. | 1 millisecond |
| IP Traffic – Test & Measure + z300 (one z300 unit for multiple machines running IP Traffic – T&M) | YES , provided by the NTP Time Server synchronized by GPS. Absolute reference. | 1 millisecond |

4. IP Traffic – Test & Measure Key Features

Module 1: 'IP Generator' Overview

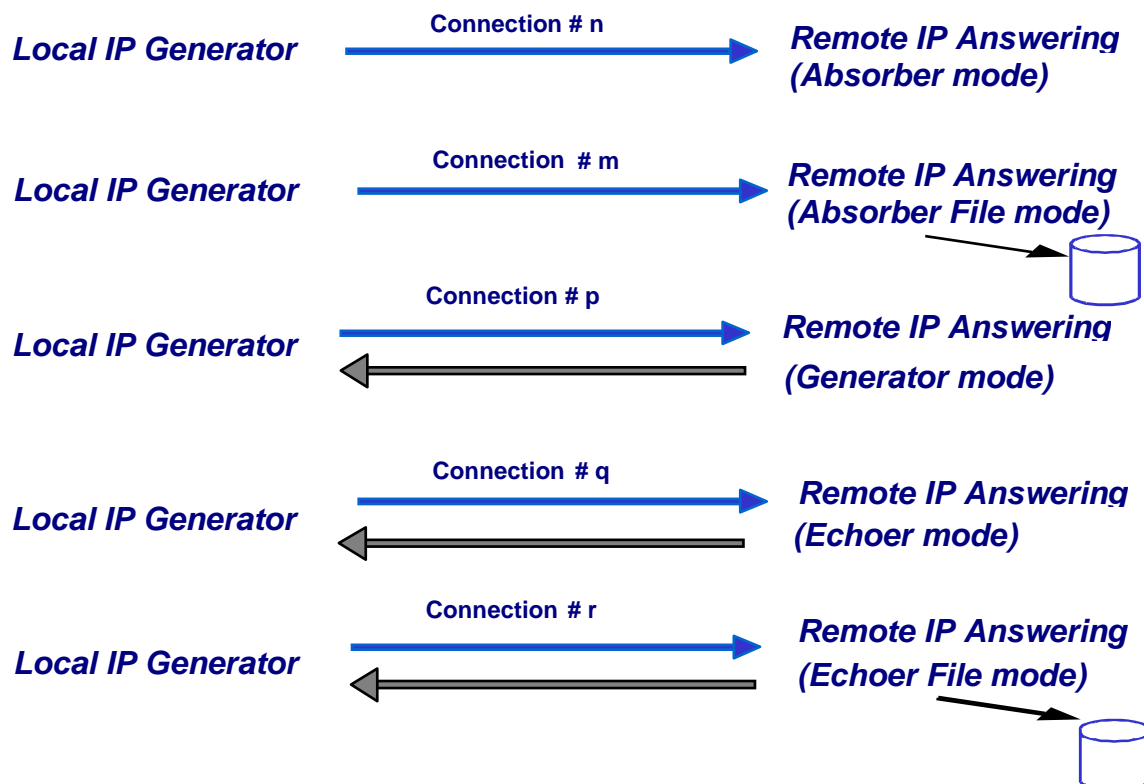
- The '**IP Generator**' module generates up to 16 simultaneous UDP (Unicast, Multicast or Broadcast) and/or TCP connections and/or ICMP connections. The connections can be established following three different testing modes:
 - ⇒ **Unitary Mode:** you can choose among two type of data generator
 - Internal 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

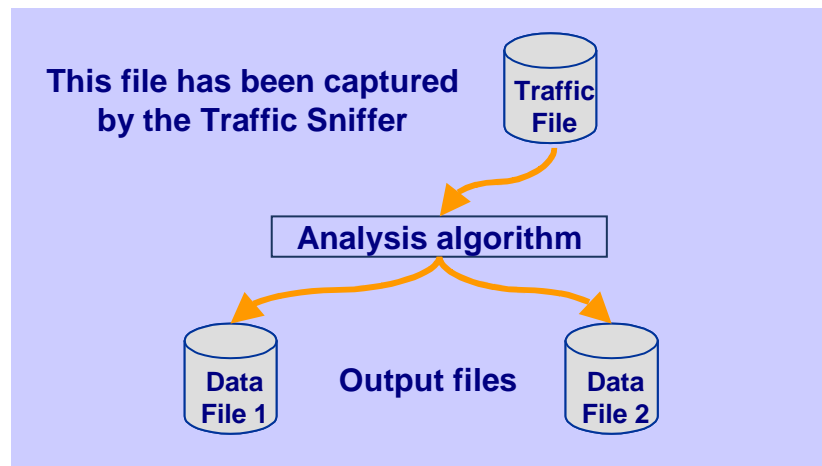
These statistics can be saved in a CSV file defined by the user.

Module 3: 'Traffic Sniffer' Overview

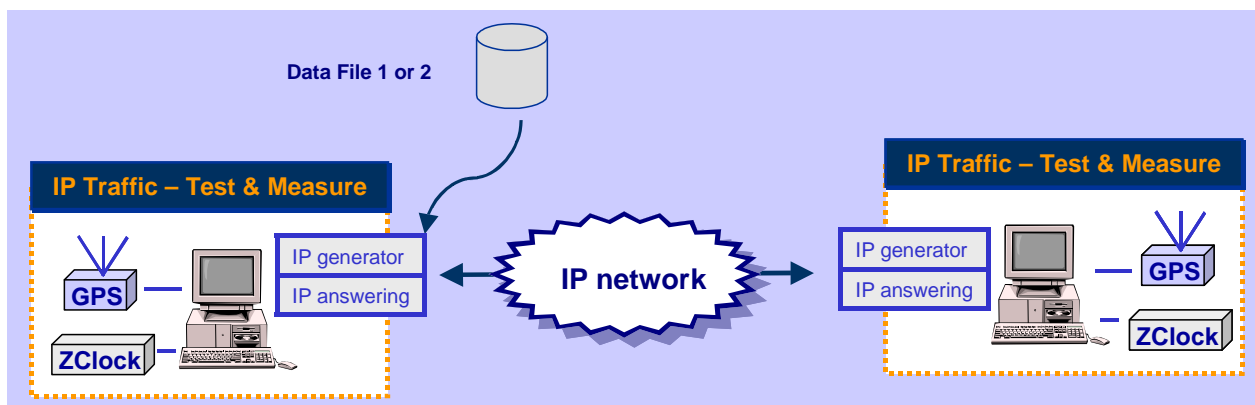
Sent and received IP packets are time-stamped by the '**Traffic Sniffer**' and then saved in a file to generate capture traffic files.

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:

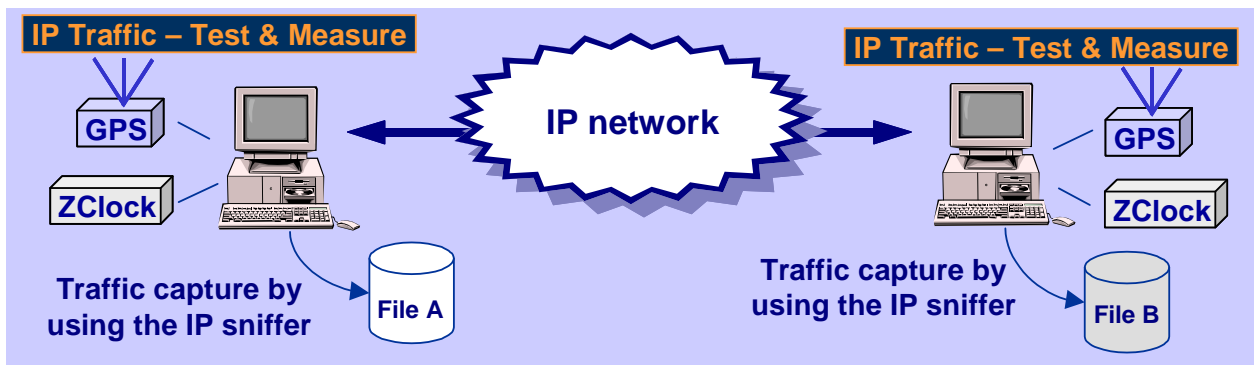


Module 4: 'Traffic Observer' Overview

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 but doesn't support IPv6 for Windows 2000. 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.

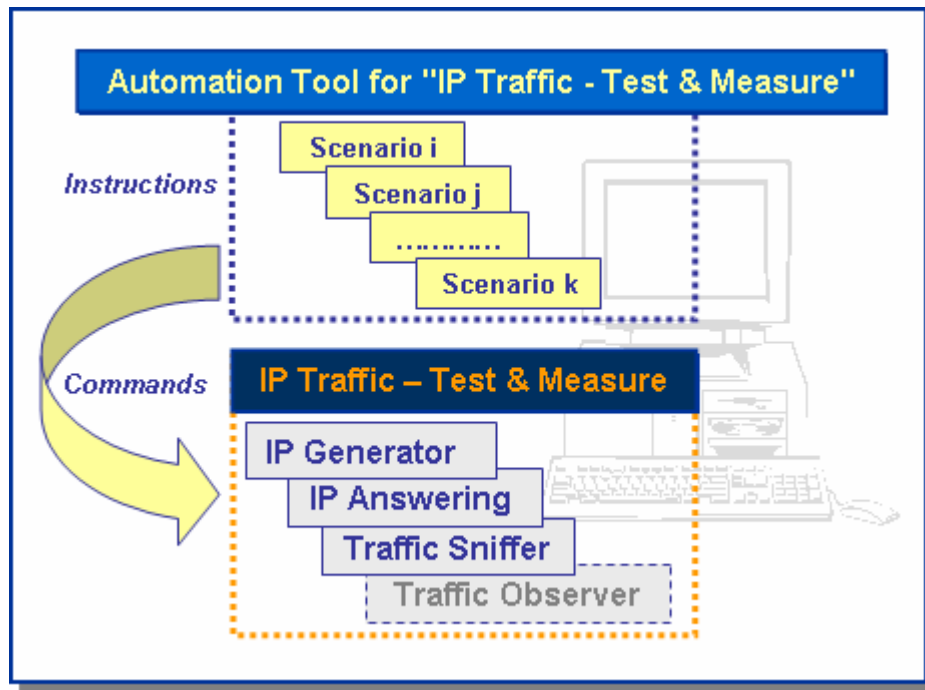
IP Traffic – Test & Measure is able to generate and receive Unicast, Multicast or Broadcast IP traffic on a selected interface, giving the user a deeper control where data are exchanged and makes multiple routes definition easily.



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.

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...