OPERATIONS MANUAL

Stateful Traffic Generator®

STG-10G

11 January, 2014

FOR TECHNICAL SUPPORT CALL:

East Coast Datacom, Inc.
245 Gus Hipp Blvd., STE #3
Rockledge, FL 32955 USA
TEL: (800) 240-7948 or (321) 637-9922
FAX: (321) 637-9980
WEB: www.ecdata.com

Manufactured by:

East Coast Datacom, Inc.

Manual PT #
214001 Rev -

SAFETY WARNING

Always observe standard safety precautions during installation, operation and maintenance of this product. To avoid the possibility of electrical shock, be sure to disconnect the power cord from the power source before you remove the IEC power fuses or perform any repairs.

PROPRIETARY NOTICE

WARRANTY NOTICE

WARRANTIES: East Coast Datacom, Inc. (hereafter referred to as E.C.D.) warrants that its equipment is free from any defects in materials and workmanship. The warranty period shall be three (3) years from the date of shipment. E.C.D.'s sole obligation under its warranty is limited to the repair or replacement of defective equipment, provided it is returned to E.C.D., transportation prepaid, within a reasonable period. This warranty will not extend to equipment subjected to accident, misuse, alterations or repair not made by E.C.D. or authorized by E.C.D. in writing.

PUBLICATION NOTICE

This manual has been compiled and checked for accuracy. The information in this manual does not constitute a warranty of performance. E.C.D. reserves the right to revise this publication and make changes from time to time in the content thereof. E.C.D. assumes no liability for losses incurred as a result of out-of-date or incorrect information contained in this manual.

Contents

Stateful Traffic Generator®, model STG-10G.

Description

The Stateful Traffic Generator®, model STG-10G is an embedded COTS platform based on a well know traffic generation engine, D-ITG™[1]. STG-10G is composed of a Graphical User Interface (GUI) that wraps the D-ITG™ engine and other tools.

Using D-ITG™, STG-10G is capable of producing IPv4 and IPv6 traffic by accurately replicating the workload of current Internet or typical user applications. The platform supports 8-Ports 10/100/1000 and 4-Ports of 10GbE traffic generation managed via the easy to use GUI that.
The D-ITG™ generation engine provides many interesting and unique features. Thanks to it the STG-10G is also a network measurement tool able to measure the most common performance metrics such as throughput, delay, jitter and packet loss at the packet level. Also, using D-ITG™, the STG-10G can generate traffic following stochastic models for packet size (PS) and inter departure time (IDT) that mimic application-level protocol behavior. By specifying the distributions of IDT and PS random variables, it is possible to choose different renewal processes for packet generation: by using characterization and modeling results from literature, STG-10G is able to replicate statistical properties of traffic of different well-known applications such as Telnet, VoIP - G.711, G.723, G.729, Voice Activity Detection, Compressed RTP - DNS, network games.
At the transport layer, the STG-10G currently supports UDP, TCP, ICMP, DCCP, SCTP and soon to be released support for IGMP. Additionally an FTP-like passive mode is also supported to conduct experiments in the presence of NATs, and it is possible to set the TOS (DS) and TTL IP header fields. The STG-10G also supports Pcap files with an easy to use Pcap player.

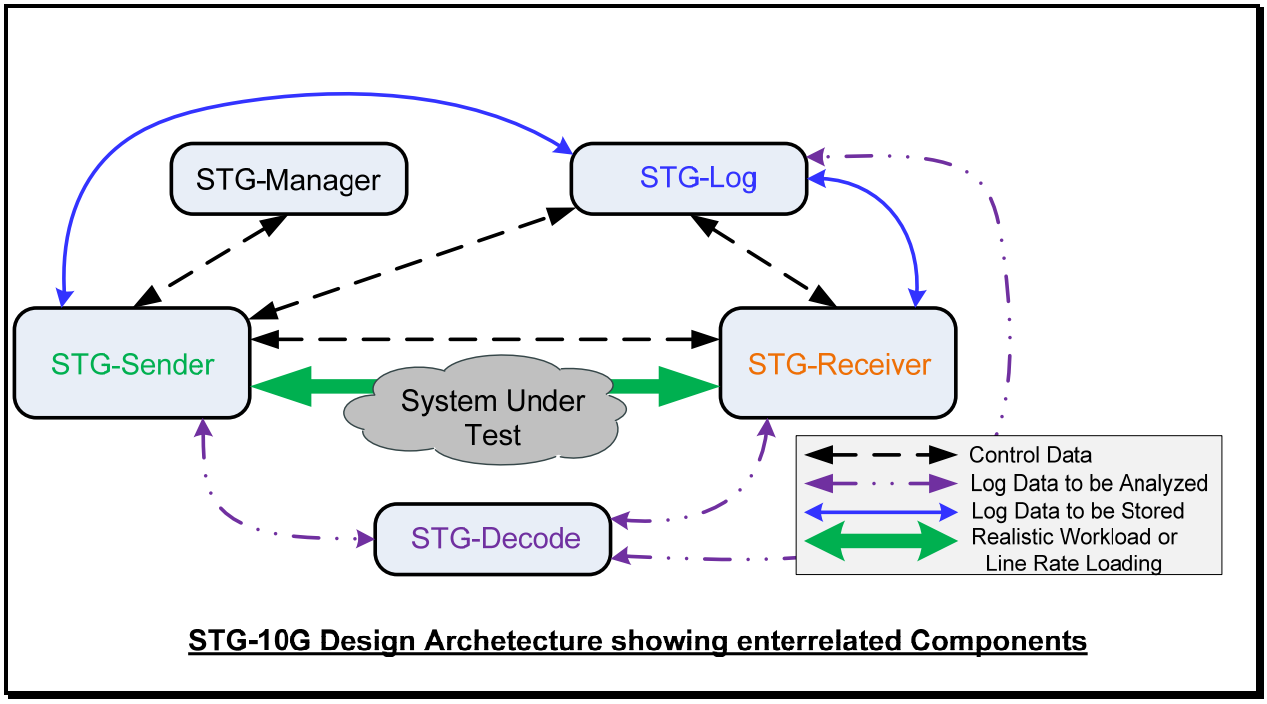
The STG-10G supports two modes of packet transmission. One being the Standard Mode for realistic traffic simulation allowing adjustable data rates. The Turbo Mode allows line rate transmission utilizing INTEL® DPDK drivers with Pcap files containing any type of traffic.

The core traffic generation features of STG-10G are provided by embedding the main components of the D-ITG™ engine (ITGSend™, ITGRecv™, ITGLog™, ITGDec™). ITGSend™ is the component responsible for generating time stamped traffic toward ITGRecv™. Exploiting a multithreaded design, ITGSend™ can send multiple parallel traffic flows toward multiple ITGRecv™ instances, and ITGRecv™ can receive multiple parallel traffic flows from multiple ITGSend™ instances. A signaling channel is created between each couple of ITGSend™ and ITGRecv™ components to control the generation of all the traffic

[1] http://traffic.comics.unina.it/software/ITG/

flows between them. This allows the STG10-G to generate a number of flows towards a single STG-10G, or towards different STG-10G at the same time.
ITGSend™ and ITGRecv™ can optionally produce log files containing detailed information about every sent and received packet. The logs can be saved locally or sent – through the network – to the Remote Box(s). The ITGDec™ component is in charge of analyzing the log files in order to extract performance metrics related to the traffic flows. STG-10G allows to easily create, store and analyze these logs so that the results are prominently displayed in real time as charts and data results, saved in a local log for viewing or exported in a text format for Matlab, Octave or Excel.

More information about D-ITG™ are provided in the following. All the following features are provided by STG-10G in a simple and easy-to-use fashion.



STG-10G Design Archetecture showing enterrelated Components

ITGSend™: Sender Component of the D-ITG™ Platform

The ITGSend™ component is responsible for generating traffic flows and can work in two different modes:
1) Single-flow - read the configuration of the single traffic flow to generate toward a single ITGRecv™ instance from the command line;
2) Multi-flow - read the configuration of multiple traffic flows to generate toward one or more ITGRecv™ instances from a script file. The script is made of a line for each traffic flow, which includes a set of command-line options as in the single-flow mode.

Every traffic flow generated is described by two stochastic processes relating to Packet Size (PS) and Internet Departure Time (IDT), through which well defined traffic profiles can be generated, emulating application protocols such as VoIP, DNS, etc.. PS and IDT series can also be loaded from a file for each flow. ITGSend™ can log information about every sent or received packet, when running in One Way or Round Trip mode respectively. In the first

case, timestamps (and other information) of sent packets are stored, while in the second case, timestamps (and other information) of sent and received packets are stored. For each flow the source IP address can be specified, which is useful for multi-homed hosts.

ITGRecv™: Receiver Component of the D-ITG™ Platform

The ITGRecv™ component is responsible for receiving multiple parallel traffic flows generated by one or more ITGSend™ instances. ITGRecv™ normally runs as a multi-threaded daemon listening on a TCP socket for incoming traffic reception requests. Each time a request is received from the network, a new thread is created, which performs all the operations related to the new request (e.g. receiving the packets of the flow). The port numbers on which STGRecv will receive each flow and any logging activity required on the receiver side can be remotely controlled by ITGSend™. A specific signaling protocol, called TSP™, allows ITGRecv™ and ITGSend™ to properly setup and manage the traffic generation process.

ITGLog™: Logger Component of the D-ITG™ Platform

The ITGLog™ component embeds the ITGLog™ and it is responsible for receiving and storing log information possibly sent by ITGSend™ and ITGRecv™. ITGLog™ runs as a multi-threaded daemon listening on a TCP socket for incoming log requests. Log information is received over TCP or UDP protocols on port numbers dynamically allocated in the range [9003–10003].

ITGDec™: Decoder Component of the D-ITG™ Platform

The ITGDec™ component embeds the ITGDec™ and it is responsible for decoding and analyzing the log files stored during the experiments. ITGDec™ parses the log files generated by ITGSend™ and ITGRecv™ and calculates the average values of bitrate, delay and jitter either on the whole duration of the experiment or on variable-sized time intervals. ITGDec™ analyzes the log files produced by ITGSend™, ITGRecv™, and ITGLog™ in order to produce the following results about each flow and about the whole set of flows:

- ***Synthetic reports Exported:***
  - Experiment duration
  - Packets transferred and Received
  - Payload bytes transferred
  - Round-trip delay (minimum, maximum, average, standard deviation)
  - Average bitrate
  - Average packet rate
  - Dropped packets
  - Duplicate packets
  - Loss events
  - Average loss-burst size
  - First/last sequence number
- ***Sampled QoS metrics time series:***
  - – Packet Sent / Packets Received
  - – Bitrate [Mbps]
  - – Round-trip Delay [ms]

- o – Jitter [ms] (i.e. delay variation)
- o – Packet loss [pps] (i.e. packets lost per second)

D-ITG™ Features

D-ITG™ is able to generate multiple unidirectional flows from many senders toward many receivers, each of them having the following features.

- ***Customizable flow-level properties***
  - o duration
  - o start delay
  - o total number of packets
  - o total number of KBytes

- ***Supported Layer-3 features***
  - o protocols: IPv4, IPv6
  - o customizable header fields:
    * source and destination IP addresses
    * source interface binding (for multi-homed devices)
    * initial TTL value
    * DS byte
  - o NAT traversal: FTP-like passive mode

- ***Supported Layer-4 features***
  - o protocols: TCP, UDP, ICMP, DCCP, SCTP
  - o customizable header fields:
    * source and destination port numbers

- ***Supported Layer-7 features***
  - o Predefined stochastic PS (Packet Size) and IDT (Inter Departure Time) profiles:
    * Telnet
    * DNS
    * Quake3
    * CounterStrike (active and inactive)
    * VoIP (G.711, G.729, G.723)
  - o Payload content: random or read from file
  - o Stochastic processes supported for both PS and IDT:
    * Supported distributions are Uniform, Constant, Exponential, Pareto, Cauchy, Normal, Poisson, Gamma, Weibull
    * Explicit random seed selection for replicating the same stochastic process
    * Loading of PS and IDT series from file

- ***Packet-level QoS metrics***
  - o Bitrate
  - o Packet rate
  - o One way delay (requires Future clocks synchronization)

- Round Trip Time
- Jitter
- Packet loss

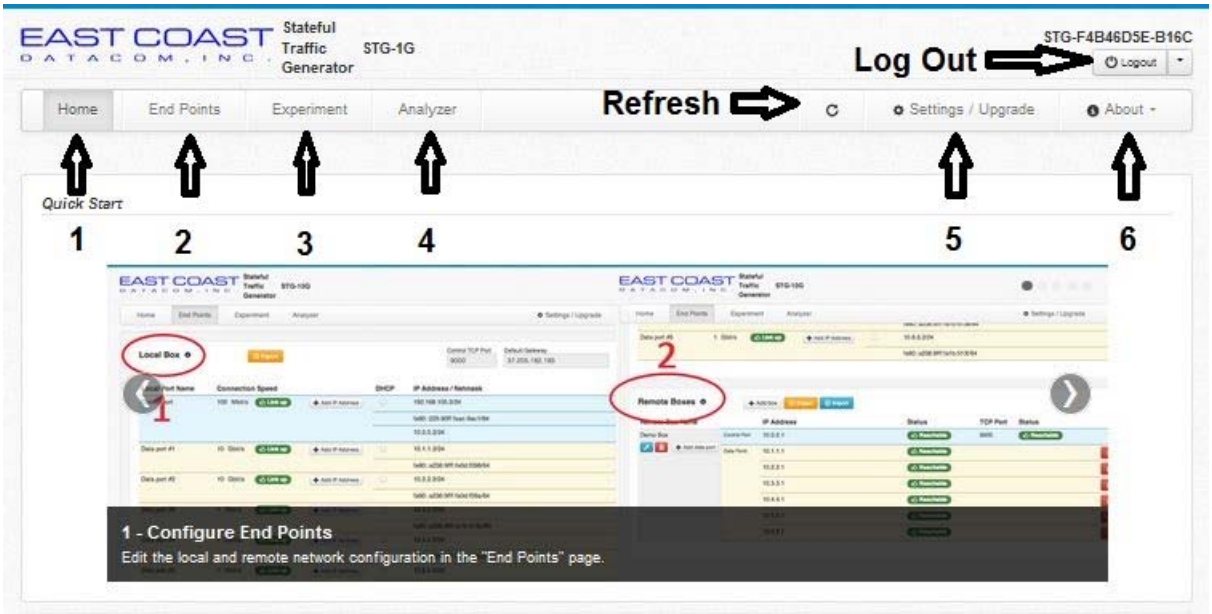
STG® Features

The STG Web User Interface component (referred in this guide also as "the Component" or as "WebUI") is designed to:

- manage the network configuration of the device;
- allow the traffic generation to local or remote devices;
- receive the traffic generation from local or remote devices;
- allow the usage of the product for a pre-defined trial period.

This guide is addressed to the generic user of the Component and provides instructions on how to use it once installed on a compatible hardware device (hereafter "Box").

The STG-10G Graphical User Interface (GUI) presents the user with Six main tabs. How the box works:



1) Home tab - this tab works as the browser *Home* buttons should. Back to the beginning!

2)End Points tab- for managing *Local* and *Remote box* LAN addressing. Managing the *Control Port* for Box to Box communications and Exporting Local configurations for remote box Import of LAN port settings. This allows the user to easily set-up multiple boxes and save the box *End Point* configurations.

3) Experiments tab - for creating or importing named experiments and selecting *Standard Mode* to replicate stochastic modeling or *Turbo Mode,* which supports replay of any Pcap file traffic type at Line Rates. The user then creates a single Flow or multiple flows within

an Experiment. The Flow screen allows the user to Name each Flow, define the Duration, End Points, Protocol, Payload Size, Bandwidth or Packets Per Second rate. The user also has the option of loading a Pcap file in the Flow and defining Cyclic Repetitions and Speed Scaling for playback. Many other options are also available such as Payload Size Distribution method, Inter Department Time Distribution, Packets to Generate, Kilobytes to Generate, a Meter for Round Trip or One way statistical collection, TTL and several other optional user defined settings. When the Flow settings are complete, the user clicks *Save* Flow.

NOTE: One Way Meter statistics are retrieved quickly to the user, while large experiments set to Round Trip Meter can result in large statistical files which can be time consuming to retrieve depending on the Log Options.

An overview screen now displays each the entire Experiment showing each Flow and the main characteristic of the Flow(s).

Now the users select one or both of the *Log Options* for statistical collection:

A) ***Local*** - Log Generation Sender Side

B) ***Remote*** - Log Generation Receiver Side

NOTE: local Log statistics are retrieved quickly to the user. Selecting Local and Remote with large Multi-Flow experiments can result in large statistical files which can be time consuming to retrieve.

After the user has defined all Flows and Log Options the user *Saves* the whole Experiment and begins the Experiment by clicking *Start*. As the Flow(s) are beginning, a status bar appears on the users monitor indicating the progress. Upon completion, the statistical results are displayed as well as graphs for each Flow. The results may be saved for viewing in the Analyzer tab or simply canceled.

4) Analyzer tab - for retrieving the final saved Experiment results. The results are saved with Experiment Name, Date the Log options as Local or Remote. The *Log File* results may be adjusted by Sampling Rate Time for further viewing or Exported. The export file is one packet per line and allows examination in Matlab, Octave, Excel ect...

5) Settings/Upgrade tab - This tab allows the user to set the box Name, Date and Time, Submit Trouble shooting Reports, Enable Remote Support (paid subscription), System Firmware Update that requires Key Codes and managing the all important Administration Port.

6) About tab - the about tab contains the two sections;

A) ***Information*** - selection which allows the user to view the current *Box Information*, *Installed Components* and *Licensing Information*. These include the software revision levels and open source codes contained in the STG-10G. This also includes an activation key shown as Full or 30 Days.

B) ***Help*** - selection that allows the user to contact *Technical Support* for the box and a holder for the soon to be released *User Manual*.

Also included are a **Log Out** button which has an additional function to Reset the STG-10G hardware box. As well the **Refresh** button that may be used within the STG-10G system to repaint a screen.

Conventions

In this guide the names of files, utilities and commands that are meant to be written as-is are rendered with fixed-size font, e.g. `filename.php`

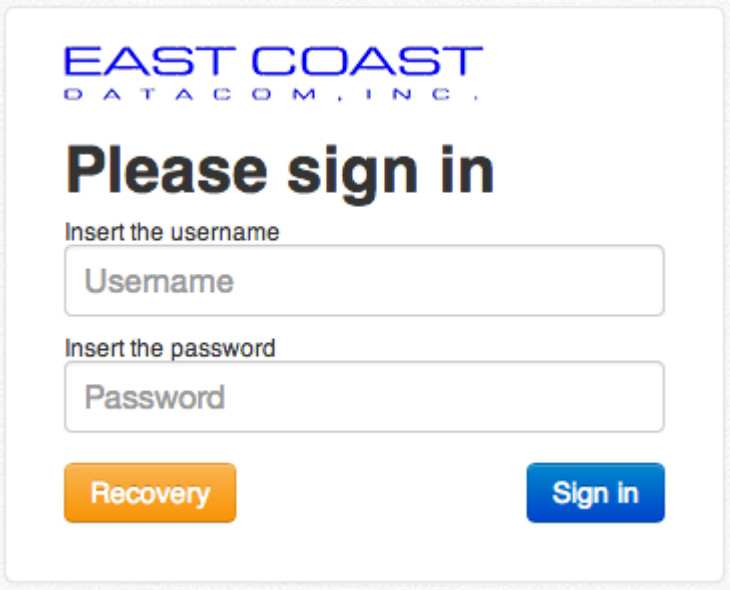
Usage Instructions

This section describes how the WebUI is made up, how you can use each components.

Login

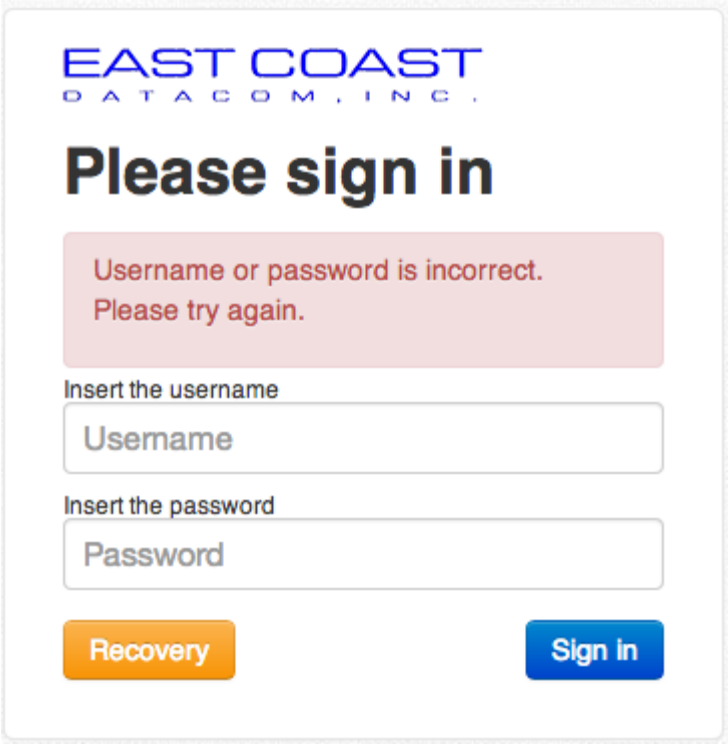
Once the Component is activated, you can launch WebUI in your browser connecting to http://192.168.50.1 where you will see the "Login Page" that shows:

- an input box to insert the username;
- an input box to insert the password;
- the button "Sign in" to send the credential to log in the box.
- the button "Recovery" to change the password of the box.



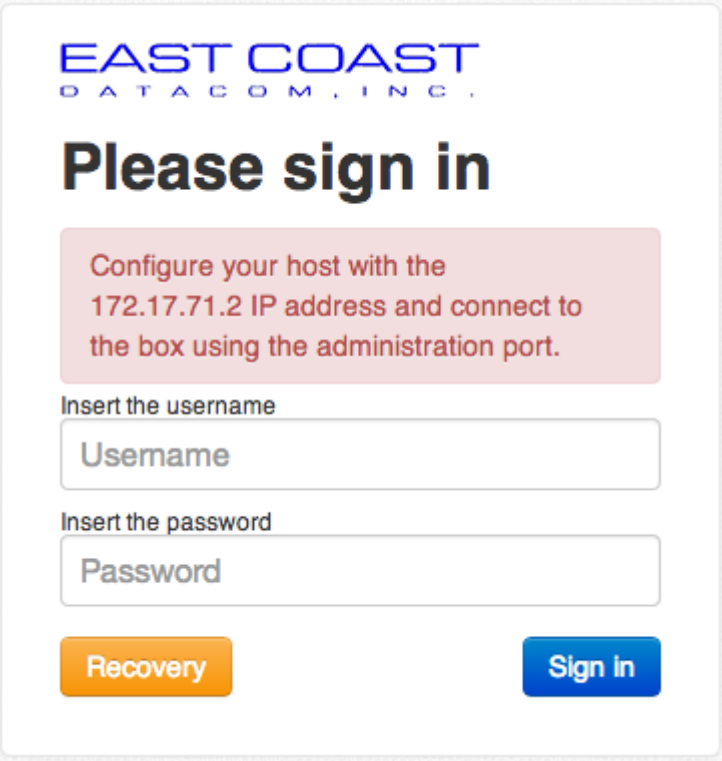
3.1 Login form.

If the username or the password is wrong, a message is displayed notifying the error, as shown in the following figure.



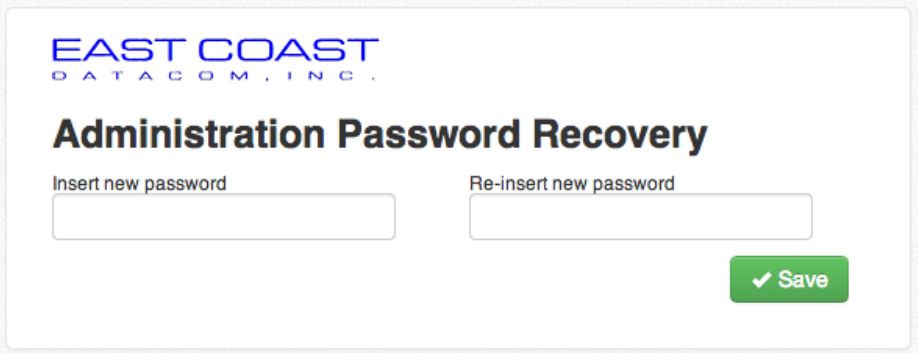
3.2 Error message of credential login.

In case you forget the password you can retrieve it using "Recovery" button. This operation can be done only connecting your host to the box using the administration port (on the IP address 172.17.71.2), configuring your network device with the 172.17.71.2 IP address. This preliminary step is essential to display the screen to change the credential otherwise the following error message will be shown:



3.3 Error message of password recovery.

The second step consists of inserting the new password twice to avoid typing errors as shown below:

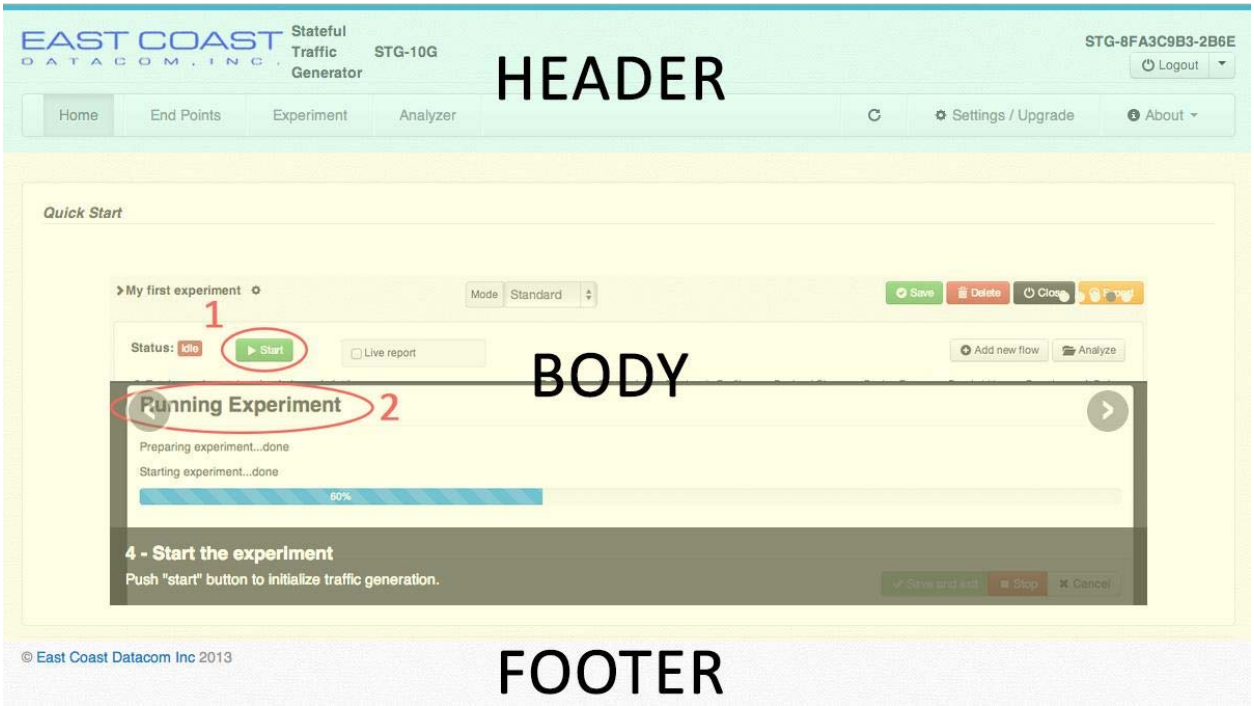


3.4 Password recovery form.

Common Section

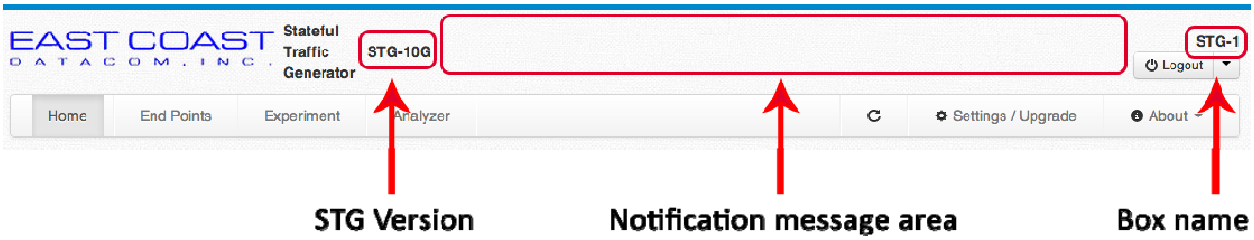
After login step, the page consists of three parts:

- header, which is described in this section;
- body, analyzed in details in the following sections;
- footer, that shows producer information.



3.5 WebUI Structure.

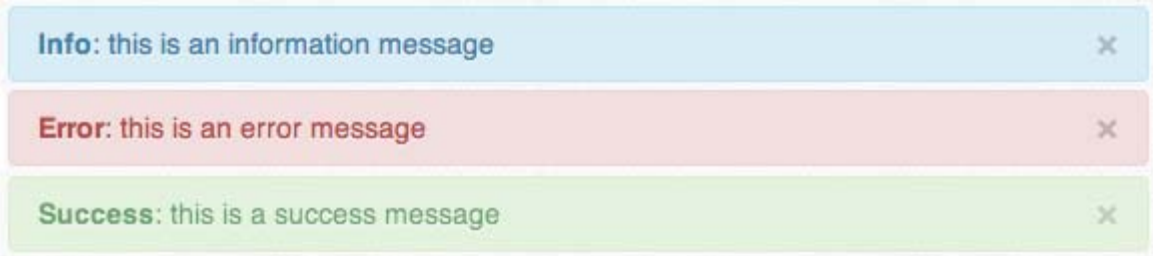
Header section is common for all WebUI pages.



3.5 WebUI Header.

It presents the East Coast Datacom logo, the name of the product (Stateful Traffic Generator) and the generator type, 1G or 10G, according to the hardware capability. The central area is used to show the notification messages which can be:

- information message: used to notify any information message (it automatically disappears);
- error message: used to notify error or alert (it has to be closed manually);
- success message: used to notify operation successfully finished (it automatically disappears).



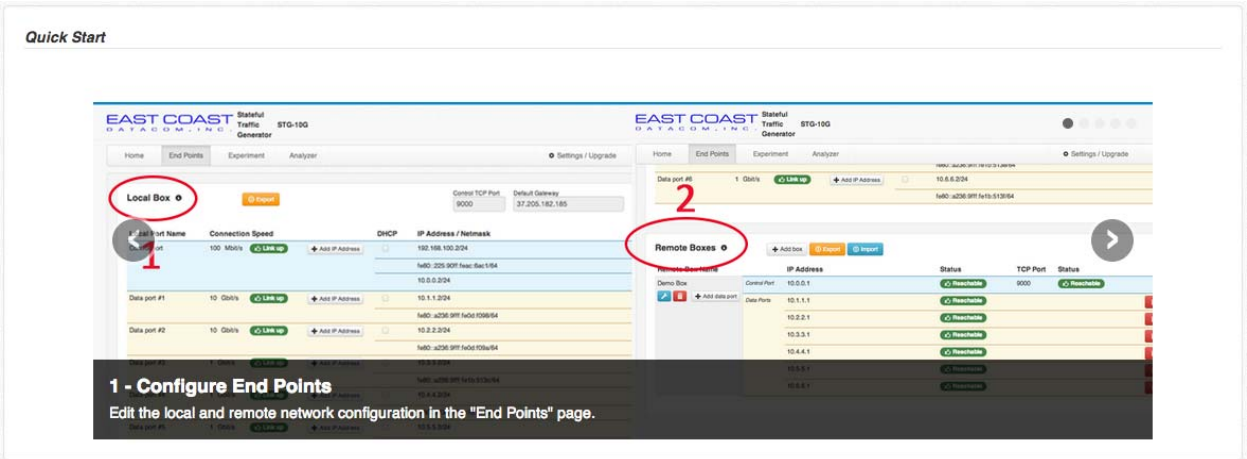
3.6 Notification messages.

On the right of header section there are the name of the local box and the "Logout" button to exit from the Component.
The last part of header is the menu which allows you to navigate in WebUI subsections, analyzed in the following sections:

- Home
- End Points
- Experiment
- Analyzer
- Settings / Upgrade
- About

Home

Home page gives a brief and quick tutorial on how to start an experiment. Following all the steps, in fact, you will be able to configure the network configuration of your box, create an experiment, execute it and analyze the results.



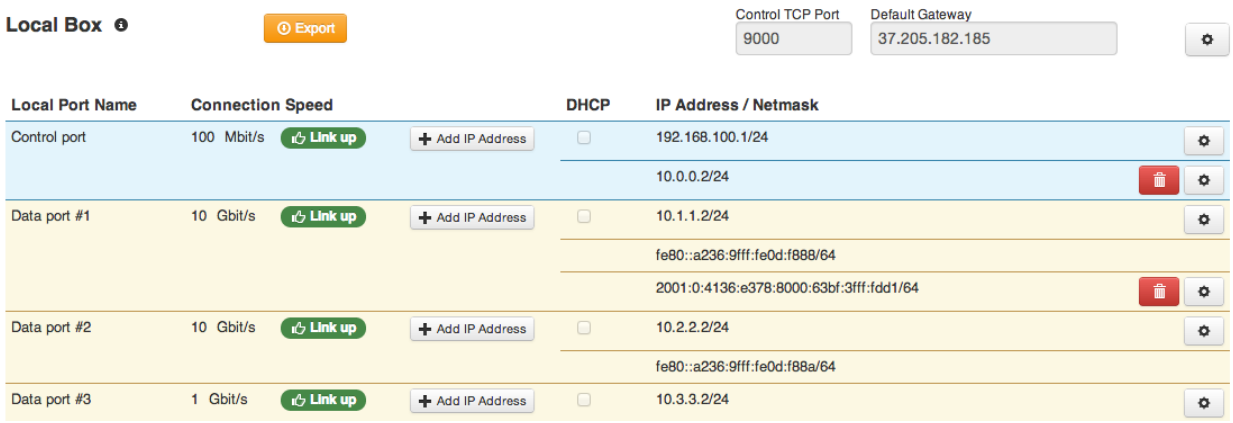
3.7 WebUI Home page.

End Points

"End Points" is made up of two mainly sections:

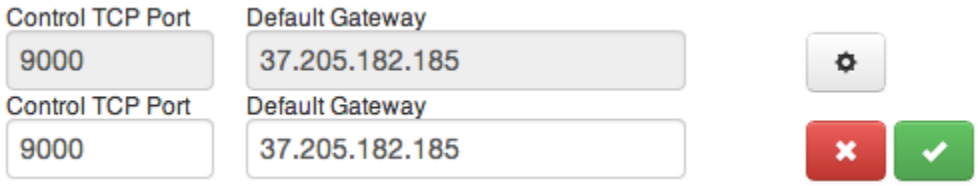
- Local box information, containing the network configurations of the local device.
- Remote boxes information, containing the network configurations of the boxes to which generate traffic.

The following figure gives an overview of local box section. In particular, in the head of this subsection you can configure information about "Control TCP Port", that is the signaling channel port number, and the "Default Gateway".



3.8 WebUI End Points: Local Box configuration.

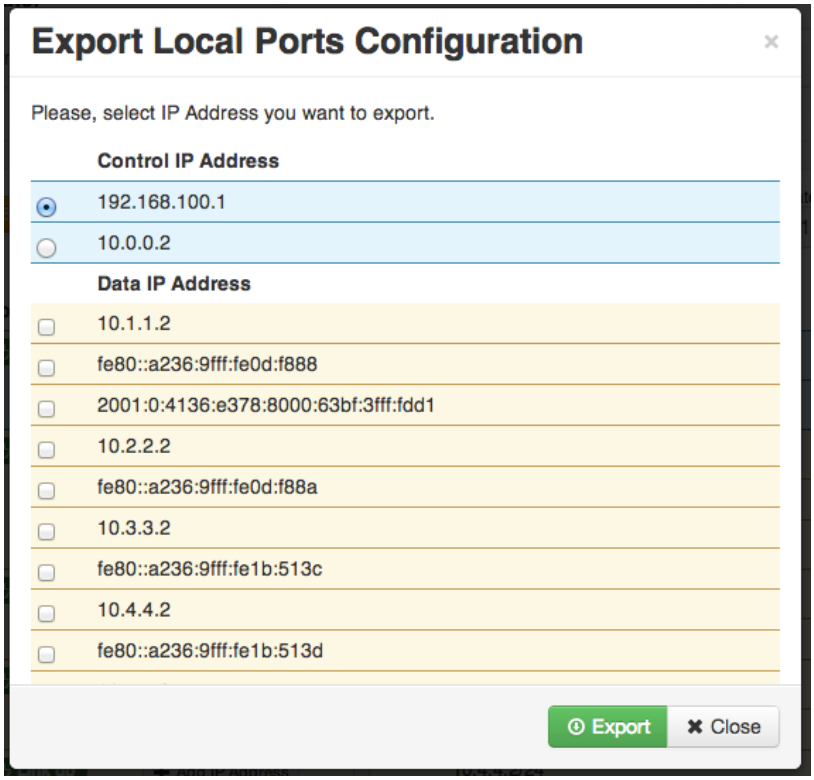
To modify them you should click on the wheel button that will enable the fields for editing. Two buttons will be shown, green and red ones, for saving or discarding the changes.



3.9 WebUI End Points: Control TCP Port and Default Gateway configuration.

The orange button "Export", on the top-left side in the figure 3.8, allows to export network configuration of the local box. Clicking on it, a dialog will be opened and you can select the IP addresses you want to export. The export configuration consists of:

- local box name, which is customizable in the "Settings/Upgrade" page;
- Control TCP Port;
- one Control IP address (a remote box can have only one Control IP address);
- zero or more Data IP address.

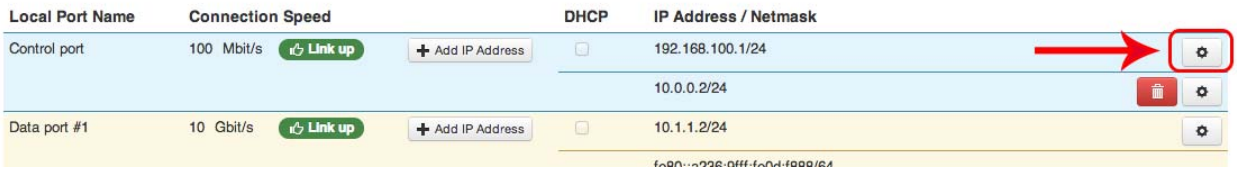


3.10 WebUI End Points: Export local box configuration.

The last section of local box area consists of a table for managing the entire network configuration of local host. There are two types of network interfaces: the control interface (in blue) is used as the sender or destination address for the signaling channel between the boxes, and data interfaces (in yellow) are used for the sender and destination addresses for the probing traffic.

Each interface has information about:

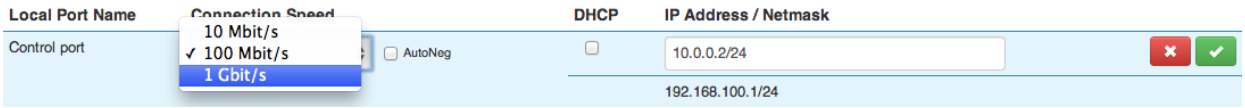
- connection speed;
- connection status: "link up" or "link down", which means if it is connected or not;
- dhcp, which allows to obtain, if checkbox is enabled, the IP address from a DHCP client;
- IP addresses and netmasks related to this interface.



3.11 WebUI End Points: Network configuration of local box.

The connection speed can be modified clicking on the wheel button of the first row of interface area. It is possible to specify "Autonegotiation", that enables device to automatically exchange information over a link about speed and duplex abilities, or you can

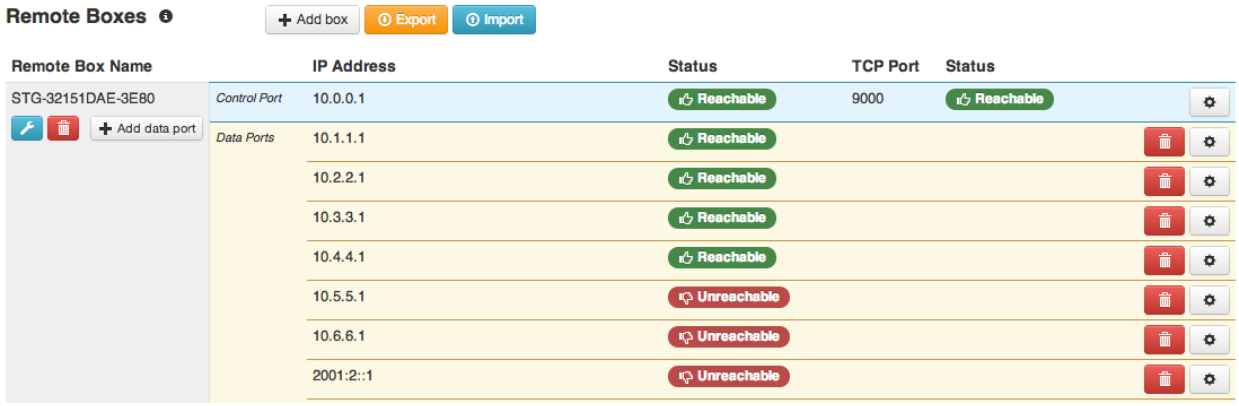
chose between the speeds supported by the interface (i.e. 10 Mbit/s, 100 Mbit/s or 1Gbit/s).



3.12 WebUI End Points: modify interface information.

The DHCP checkbox, if enabled, allows to the interface to contact the DHCP server to obtain, dynamically, an IP address (this step assumes there is a DHCP server in the network). If DHCP field is disabled you may specify statically IP Address version 4 and netmask (the IP Address version 6 is allowed only for data addresses).
The green and red buttons, that have replaced the wheel button, allow you to save or discard the configuration changes.
An interface may have related zero or multiple IP addresses. If it has no associated IP address, it is defined "not assigned". Besides if the IP address is defined by user it will be a static address and it has wheel button for editing and trash button for deleting. If the IP address is generated by device it has no button because it can neither be modified nor deleted.
It is important to note that in the experiment configuration step only the interfaces with at least one associated IP address are considered.

The second section of "End Points" page regards the network configuration of remote boxes, that are the devices toward which to generate traffic.



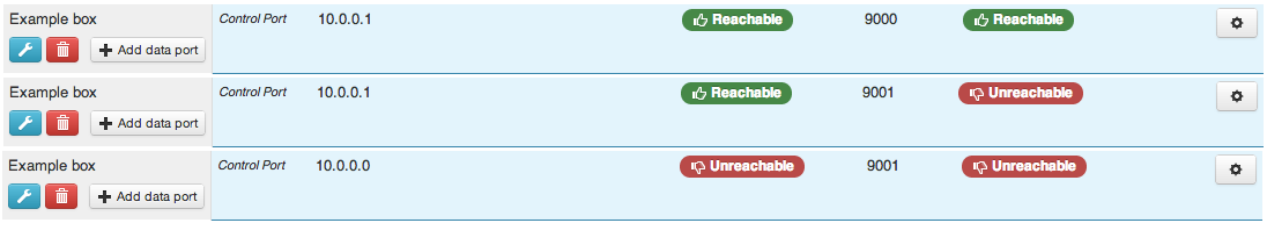
3.13 WebUI End Points: Remote boxes subsection.

The top area shows three buttons. "Add box" button allows to add a new remote host inserting a mnemonic name of box (which can differ from real box name), the Control IP address and the TCP Port, as shown in the figure 3.14.

3.14 WebUI End Points: add a new remote box

Clicking on the green button on the right side of the row, the inserted information are stored. To evaluate if the IP address and port are reachable is used the PING utility, so you have different cases:

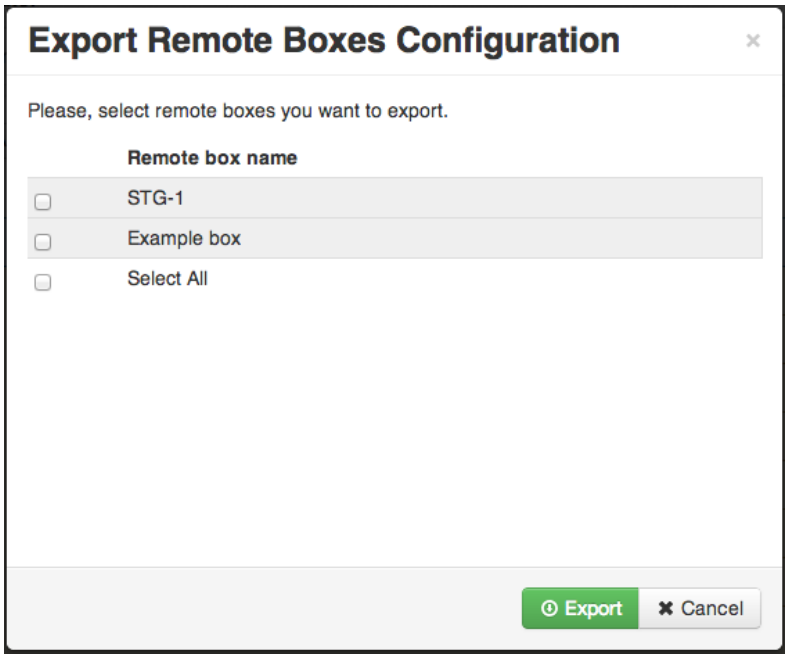
- IP address unreachable;
- IP address reachable:
  - TCP Port reachable;
  - TCP Port unreachable.



3.15 WebUI End Points: reachability of IP address and TCP port.

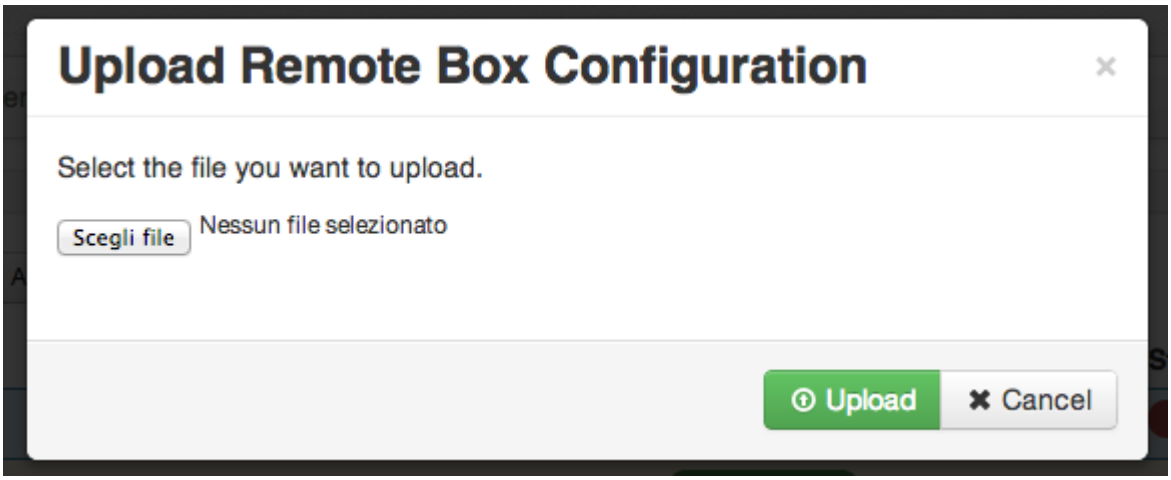
It is important to know that the remote box addresses are not synchronized automatically with the referred STG box.

"Export" button, similarly to "Local box" section, allows to export the section configuration. In fact, clicking on button, the following dialog appears which shows a list of all configured remote devices.



3.15 WebUI End Points: export remote boxes configuration

"Import" button allows to upload the configuration of a box or multiple boxes, choosing the exported file from local or remote sections.

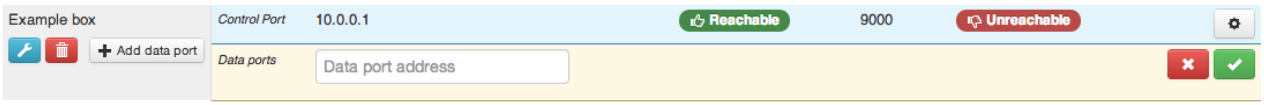


3.16 WebUI End Points: import remote box(es) configuration

The imported remote box (or boxes) will be append to the remote boxes table or merged to existing box where the box name are the same.
Remote boxes table shows a list of remote devices consisting of one control IP address and one or more data IP addresses, each of them can be modified or deleted using the buttons on the right side.

3.17 WebUI End Points: edit, delete and add a data IP address of a remote box

To modify the name of a remote box you can push the wrench button placed on the bottom of remote box name. After editing the name in the input field you must push on green button or red button to save or discard the change (as shown in the right image of the figure 3.17).
To delete a box you can use trash button, placed on the bottom of remote box name.
"Add data port" button allows you to add a new data IP address to the related remote device. As previously shown for local box, and pointed out in the following figure, a new row is appended to the box and an IP version 4 or 6 can be inserted. The green and red button on the right side allows you to save or discard the IP address.



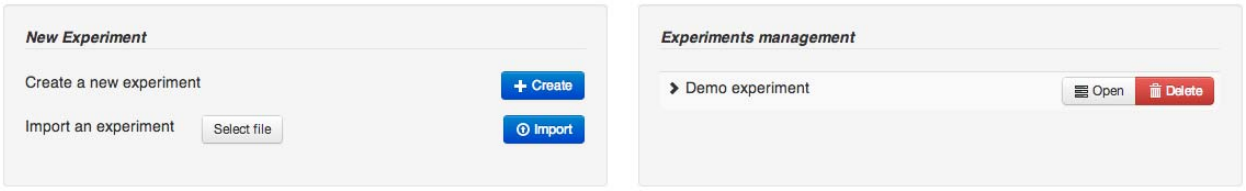
3.18 WebUI End Points: add data IP address to a remote box

If you want to modify an IP address you will push on wheel button placed on the right side of each IP address row, while the red trash button will allow you to delete the related address.

Experiment

"Experiment" page is divided in two subsection:

- left subsection allows you to:
  - create a new experiment clicking on "Create" button;
  - import an experiment clicking on "Import" button;
- right subsection lists all saved experiment, which can be reopened or deleted pushing on the related button on the right side.

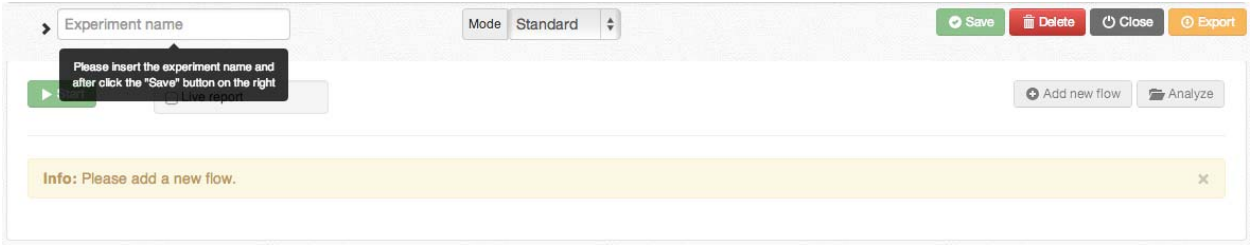


3.19 WebUI Experiment: management

3.5.1 Create a new experiment

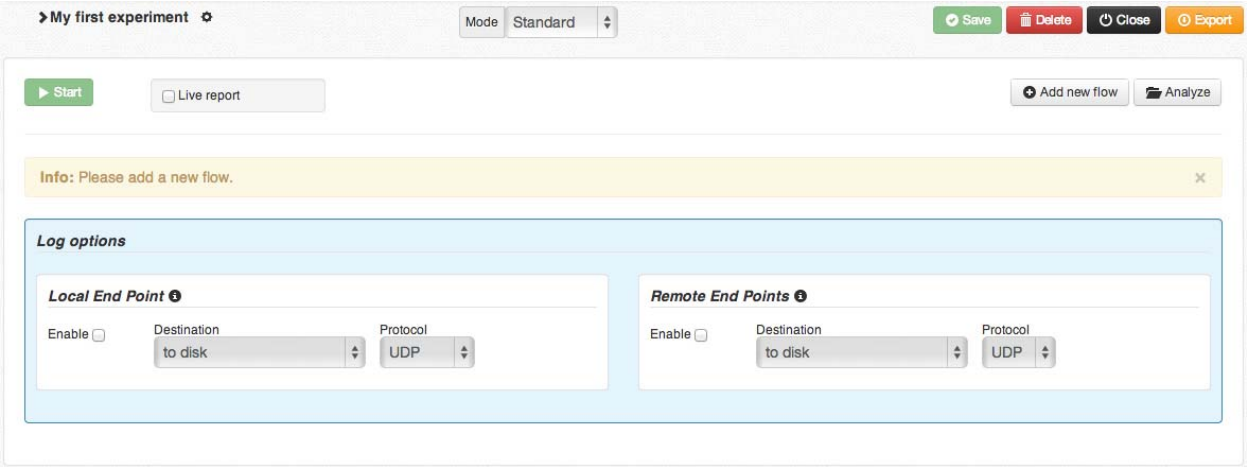
After clicking on "Create" button a new page is opened, shown in the following figure 3.20. This page considers:

- an input field for inserting experiment name;
- a select field for choosing the experiment operating mode, Standard or Turbo, which is better explained later;
- four buttons to:
  - save the experiment name and, in a second step, the experiment configuration;
  - delete the experiment and all its results;
  - close the current experiment, returning on the previous page;
  - export the experiment for using it on other STG box;
- a subsection containing the experiment details, analyzed in details later.



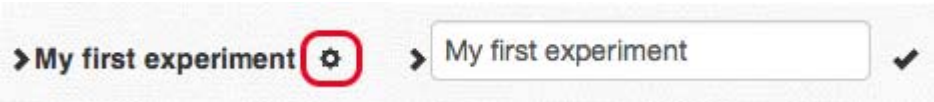
3.20 WebUI Experiment: create a new experiment

Once set the experiment name "Save" button becomes clickable to store it, enabling the subsection to add other experiment configurations. In fact, after this operation, the subsection appears as in the following figure.



3.21 WebUI Experiment: configure the experiment

If you want to modify the experiment name you must push on the wheel image highlighted in red in the following figure. This action will be appear an editable field from which you can modify the name. To save it, you have to push the checkmark button ✔.



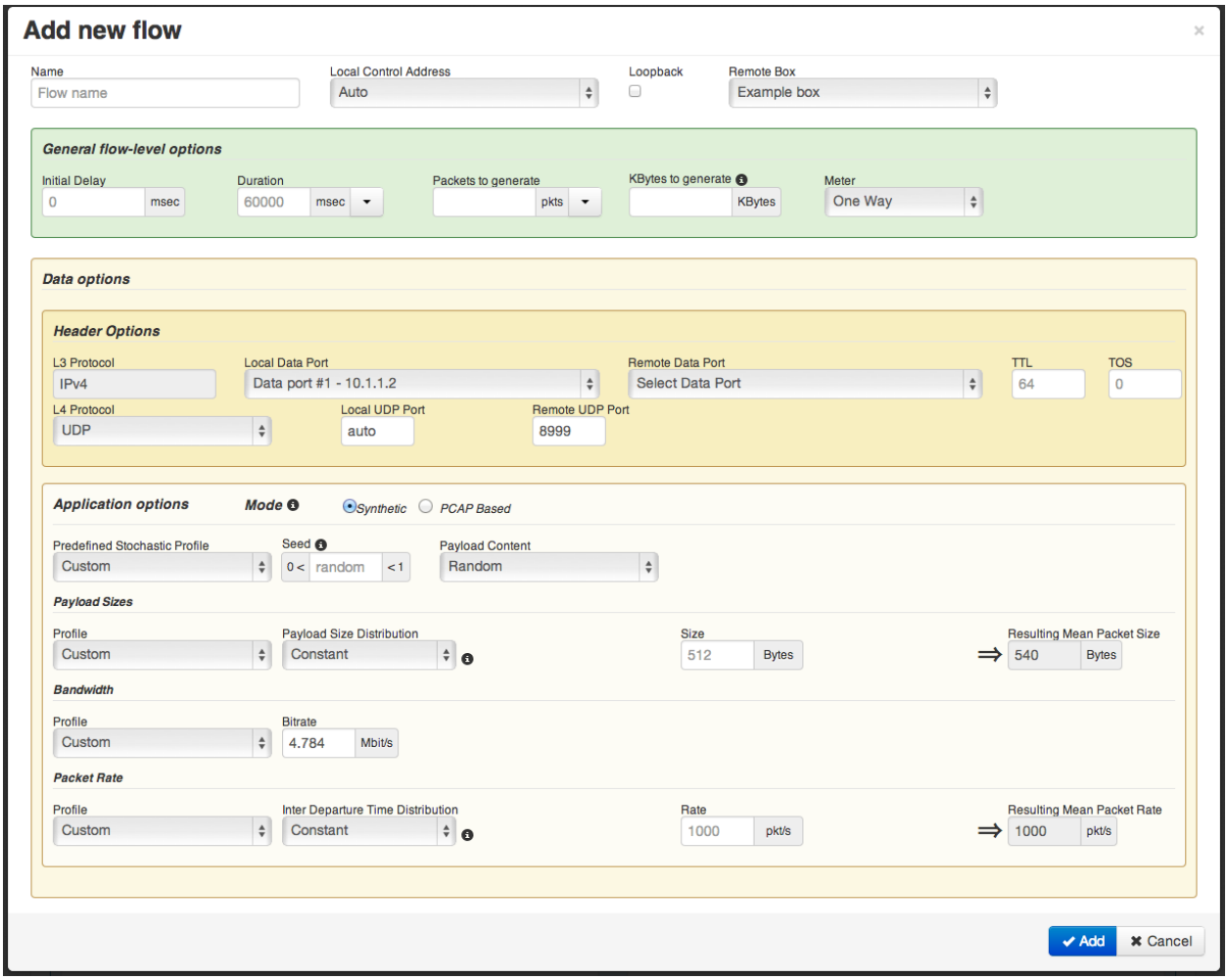
3.22 WebUI Experiment: change experiment name

The subsection consists of:

- "Start" button allows you to execute the experiment. It is disabled when the experiment configuration has no flow.
- "Live report" checkbox allows you to show real time analysis during experiment execution. Besides, enabling it, you can choose one or more parameter among delay, jitter, bitrate and packet loss you want to analyze and a graph checkbox if you want to see or not the graph during the experiment execution.
- "Add new flow" permits to open a dialog for creating a flow. This window is explained better in the following subsection.
- "Analyze" button cross-refer to analyze section of experiment results,
- The middle of this subsection is reserved for the configured flows. Initially there is no flow added to the experiment, so an info message is shown.
- The last area regards the "Log options" configuration, which is explained later.

Add a new flow

Pushing on the “Add new flow” button, the following dialog will be opened to configure a flow. In this section its functionalities will be explained in details.



3.22 WebUI Experiment: flow configuration window

The “Name” field is a mnemonic name that allows to give a custom name to the flow. It is not important for the experiment purposes but it may be helpful to recognize the flow when analyzing the experiment results.

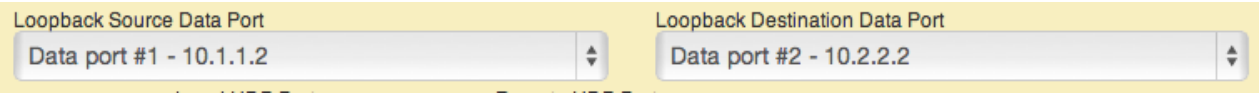
“Local Control Address” field allows to configure the source address for the signaling channel. You can select “Auto”, leaving the task of choosing the best address to use to the operating system, or any Control IP addresses of Local Box configured in the “End Points” section.

“Loopback” field allows to generate traffic toward the same local box. If enabled, in fact, the “Remote Box” field is disabled.

"Remote Box" field regards the hosts toward which you want to send the traffic. You can choose one of the remote boxes configured in the "End Points" section, defining in this way the IP address of the destination signaling.
The "Custom flow-level options" green section regards the configuration of initial and final delay, the generation duration, the number of packets and the number of KBytes to generate and the meter (see the D-ITG manual[2] for more explanations). It is important to note you can choose only one parameter between duration, packets and KByte number to generate, in fact setting one of the three values you can not specify the remaining others. Besides you can log information about every sent or received packet, when running in "One Way" or "Round Trip" mode respectively, by using "Meter" option. In the first case, the timestamps (and other information) of sent packet are stored, while in the second case, the timestamps (and other information) of sent and received packets are stored.
The "Data options" yellow section regards the configuration of packets and it consists of two subsection:

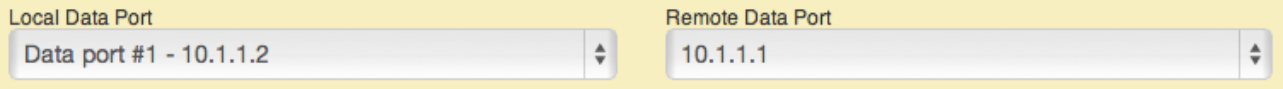
- "Header options", which gather information about level 3 and 4 of TCP/IP stack;
- "Application options" which includes application level information.

In the "Header options" the choices depend on what you have selected in the first configuration step, if loopback or which remote host. If you have selected loopback mode you will see the following fields:



3.23 WebUI Experiment: loopback source and destination data ports

The first of them, "Loopback Source Data Port", allows you to select the sender Data IP Address, while the latter, "Loopback Destination Data Port", represents the Data IP Address toward which the traffic is generated. The field shows the information about the interface (i.e. Data port #1 and Data port #2) and the IP Address that can be only an IP version 4, as shown in the "L3 Protocol" field. Another restriction is you cannot select the same interface for both data ports, in fact the interface that is selected in the source port does not appear in the destination field.
If in the first configuration step you chose a remote box instead of loopback you will see the following options:



3.24 WebUI Experiment: local and remote data ports

[2] http://traffic.comics.unina.it/software/ITG/documentation.php

“Local Data Port”, as said before, lists all data ports configured in “End Points” section, instead “Remote Data Port” lists all data ports related to the selected Remote host. In this case you can choose IP version 4 or 6. Also in this case there is the IP version restriction: the IP version selected by “Local Data Port” imposes the related version to “Remote Data Port”.
In the “TTL” field you may specify the IP Time To Live, which by default is 64, while in “TOS” field regards the Type of Service header value.
“L4 Protocol” lists the protocol type you can use for traffic generation:

- UDP, User Data Protocol;
- TCP, Transmission Control Protocol;
- ICMP, Internet Control Message Protocol;
- DCCP, Datagram Congestion Control Protocol;
- SCTP, Stream Control Transmission Protocol.

For UDP, TCP, DCCP and SCTP protocol you can choose the source and destination port. In addition, for the last protocol you may specify the association ID and SCTP session too. For ICMP protocol, instead, you can specify the Type number, which by default is 0 (Echo Reply). Note that if you generate ICMP echo request messages (type 8), you will solicit echo replies from the operating system of the remote box.

“Application Options” configuration has two operating mode:

- “synthetic” mode gives you the possibility to configure the stochastic models for packet size and inter departure time that mimics application-level protocol behavior.
- “pcap” mode allows you to use pcap trace containing real traffic to generate network workload with more semantic value.

In the first mode, “Synthetic Mode”, it is possible to choose different renewal processes for packet generation. Through “Predefined Stochastic Profile” and by using characterization and modeling results from literature, you can replicate the statistical properties of traffic of different well-known applications:

- “Telnet” option emulates Telnet characteristics. It works only with TCP transport layer protocol.
- “VoIP” option emulates Voice-over-IP traffic and you can select the audio codec type between G.711 and G.723 or G.729, the audio transfer protocol between RTP or CRTP and enabling or not the Voice Activity Detection. It only works with UDP transport layer protocol.
- “DNS” option emulates DNS traffic. It works with both UDP and TCP transport layer protocol.
- Network games option like “Quake3” or ”CounterStrike” (active or idle phase of the game). They only work with UDP transport layer protocol.

It is possible to generate traffic according to the different configurations of packet size, packet rate and bandwidth.
The bandwidth depends on bitrate value that can be a predefined or customized value at most equal to the selected interface connection speed.
The packet size depends on payload size and on header size (which changes according to the network layer protocol and transport layer protocol). It can be:

- a predefined value;
- calculated from an uploaded file;
- a variable value based on payload size distribution:
    - Constant;
    - Uniform;
    - Exponential;
    - Pareto;
    - Cauchy;
    - Normal;
    - Poisson;
    - Gamma;
    - Weibull.

The packet rate depends on the Inter Departure Time (IDT), that is the time between the transmission of two successive packets. It can be:

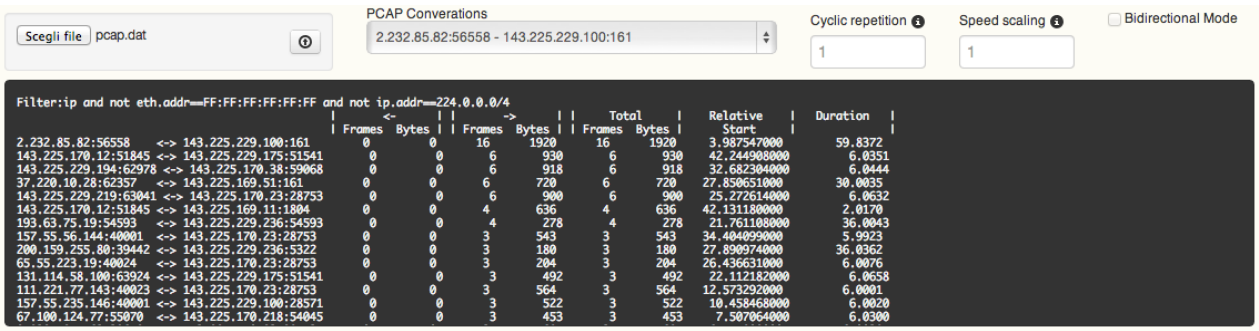
- a predefined value;
- calculated from an uploaded file;
- a variable value according to the IDT distribution:
    - Constant;
    - Uniform;
    - Exponential;
    - Pareto;
    - Cauchy;
    - Normal;
    - Poisson;
    - Gamma;
    - Weibull.
    -

For each distribution you must insert the characterizing parameters (one or two according to the distribution type) and the resulting packet rate and packet size values assume a statistical meaning in terms of mean or median, as shown in the related read-only field.
Besides, the packet rate and bandwidth values influence each other. Therefore, once you have set the packet size, setting also the packet rate, the bandwidth value will be automatically calculated while, on the other hand, if you set the bandwidth value the packet rate will be subsequently adapted.

In any case, if you choose a predefined stochastic profile or a custom profile, you can set the seed value for generating distribution and the payload content that can be generated in random mode or read from file.
The second way to configure the “Application options”, as said before, is the “PCAP” mode as shown in the following figure.

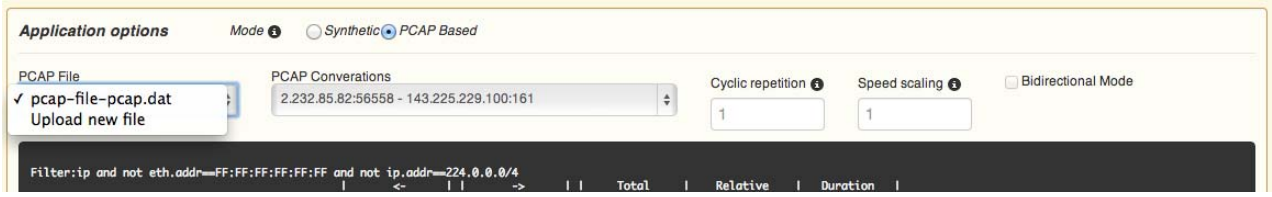
3.25 WebUI Experiment: PCAP mode

Initially, if you are configuring the first experiment flow, there are no uploaded PCAP trace you can choose so, after selecting the PCAP file on your system, you can upload it pushing on the button  . The uploaded file will be analyzed according to the selected network and transport layer protocols (in “Standard” Experiment you can choose UDP or TCP protocol, while in “Turbo” experiment there is no filter based on L4 protocol and the whole trace is selected) and in a black screen it will be shown the filtered PCAP traces.



3.26 WebUI Experiment: PCAP trace

In each row there is the source address and port, the destination address and port, the frame and byte numbers generated in the conversation from the destination to the source addresses, in the opposite side and in both direction, the relative start time and the duration of the conversation.
In “Standard” experiment you can choose the PCAP Conversation that you want to use from the related select field. This choice implies the modification of source and destination ports. Besides, specifying the “Cyclic Repetition” and the “Speed Scaling” you can replicate the selected PCAP conversation using a scale factor with which multiplies the IDT value. The resulting total duration is set in the “Duration” field in “Custom flow-level options”.
If you have already uploaded a PCAP trace file, the “Application options” section shows you a select field with each file. So you can choose one of them or upload a new file as said before.

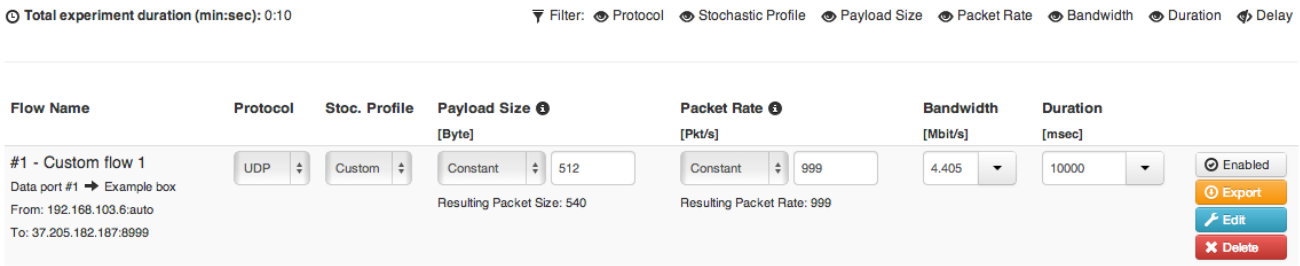


3.28 WebUI Experiment: PCAP trace selection

The flow configuration ends clicking on "Add" button in the footer of dialog window.
Please remember to save the experiment after adding a flow in order to save the flow information!!

Experiment flows

After adding your first configured flow, the "Experiment" page shows synthetic information about it as shown in the following figure:



3.29 WebUI Experiment: flows configurations overview

The row is divided in multiple column:

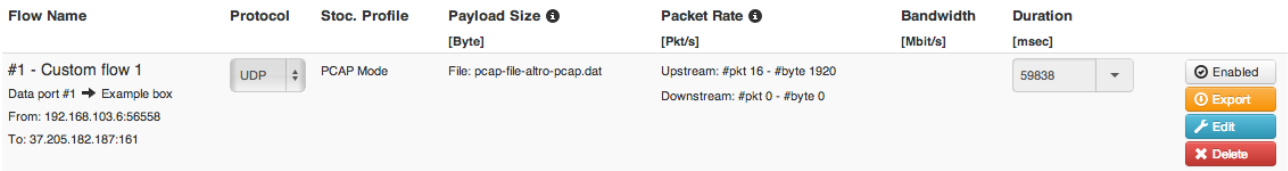
- the first column shows the flow name, the source port and the destination box (or the destination port if you chose "Loopback" option), the source address and port and, finally, the destination address and port;
- the second column shows the transport layer protocol;
- the third column is about the Stochastic Profile;
- the fourth column concerns the payload size (hence the related packet size);
- the fifth column, instead, shows the packet rate and IDT configuration;
- the sixth column is about the bandwidth value;
- the seventh column shows the duration time;
- the eighth column, which is hidden by default, contains the delay;
- the last column includes four button to:
  - enable or disable the flow that means to generate the traffic when experiment will be executed;
  - export the flow so it can be imported on another experiment box;
  - edit the flow configuration

- delete the flow configuration.

You can use the command from the second to the eight column to modify on the fly the single flow configuration.

If the flow has configured in PCAP mode the row contains different information, in fact, as shown in the figure 3.30, they assume the following meanings:

- the second column gives mode information;
- the third column the name of the PCAP file;
- the fourth column is about the number of packets and byte that are be generated from source to destination, i.e. upstream, and, if you chose bidirectional mode, the downstream traffic generation, from destination to source.



3.30 WebUI Experiment: PCAP flow configuration overview

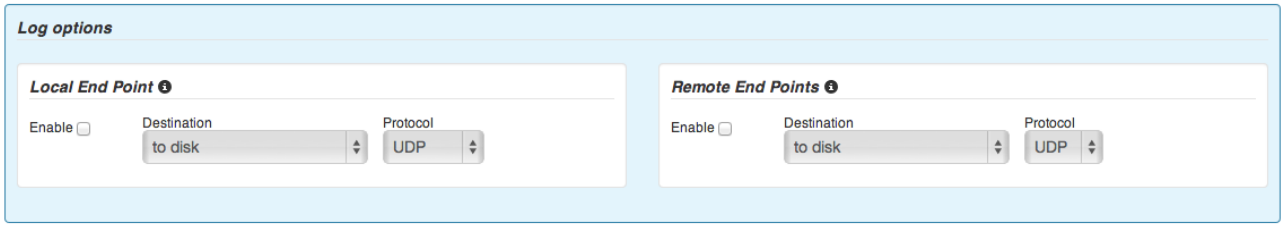
Experiment Log options

The "Log options" shown in the figure 3.31 allows you to enable the traffic logging options both sender and receiver side. This screen is divided into two boxes:

- Local End Point;
- Remote End Points.

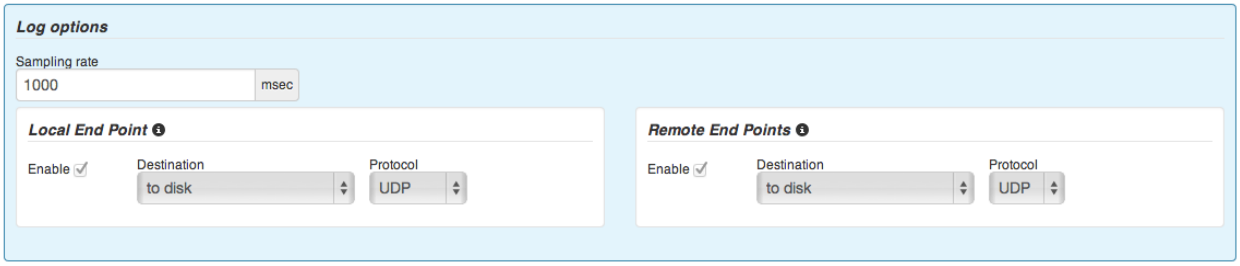
For each of them you can choose the destination box, which can be the local or a remote host, and the transport protocol type in the last case.

Please note that the log is necessary to obtain the performance measures (bitrate, jitter, etc.). The log can be disabled in case it is only necessary to generate the traffic without being interested in the performance measures.



3.31 WebUI Experiment: Logger configuration in "Standard" experiment

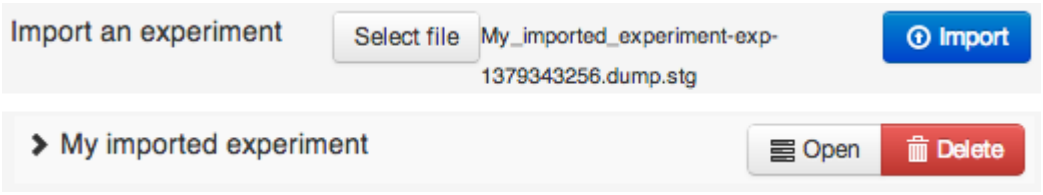
In the Turbo mode you can choose only the sampling rate.



3.32 WebUI Experiment: Logger configuration in "Turbo" experiment

Import an experiment configuration

As shown in the 3.19 figure, to import an experiment you must select a file and push on the "Import" button. After uploading you find it in the right experiment list. The following figure shows the two step.



3.33 WebUI Experiment: import experiment configuration

Open an existing experiment

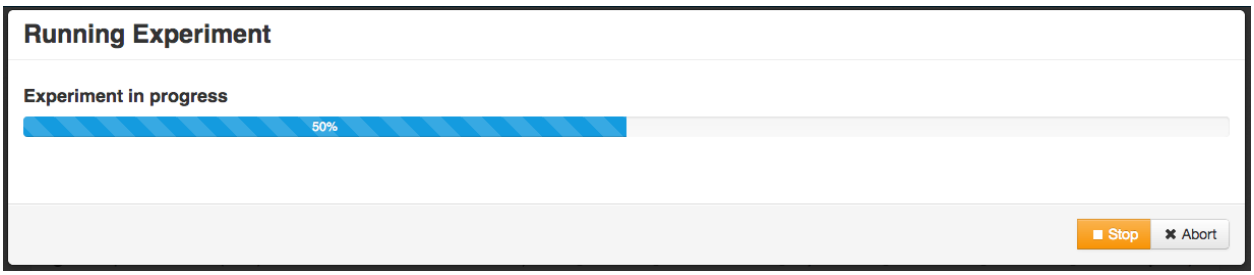
An experiment can be opened pushing on the related button of one of the items of the experiments list, showing the experiment details.
If one of the experiment flows has incoherent information compared to the box configuration (i.e. End Points configuration) the flow will be disabled and its name will be colored in red, as shown in the following figure.

3.34 WebUI Experiment: flow configuration disabled

In this case you must edit the flow configuration and solve the problem before enabling it.

Start an experiment

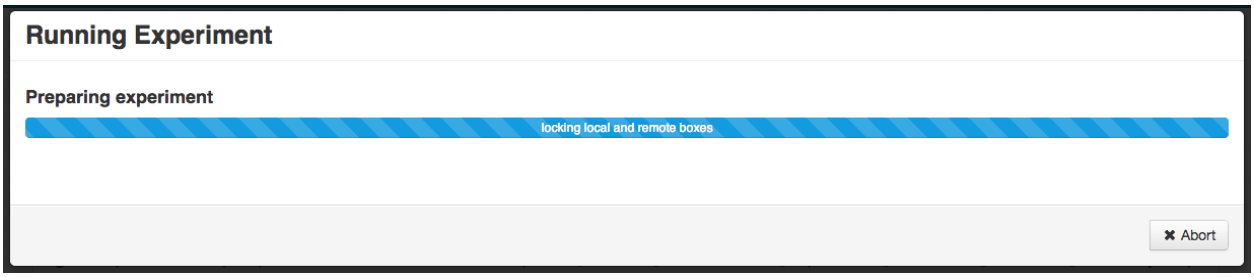
Once the experiment configuration is finished you can start the test pushing on the "Start" button. This action will open the following dialog box.



3.34 WebUI Experiment: experiment execution

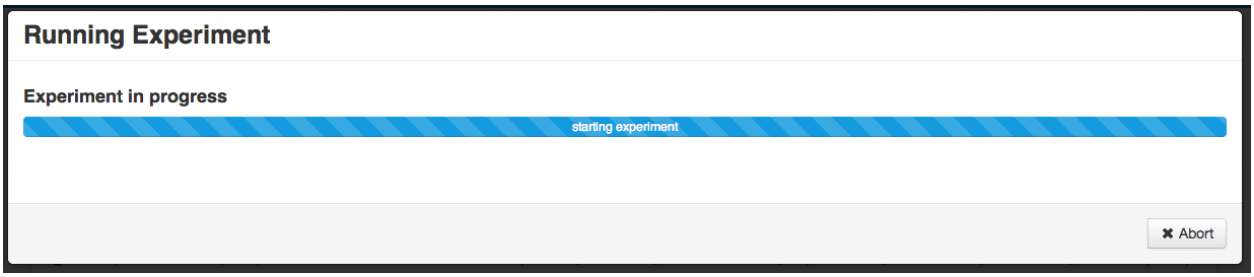
The experiment execution consist of four step:

1. "Preparing experiment": lock all selected boxes used as receiver or logger;



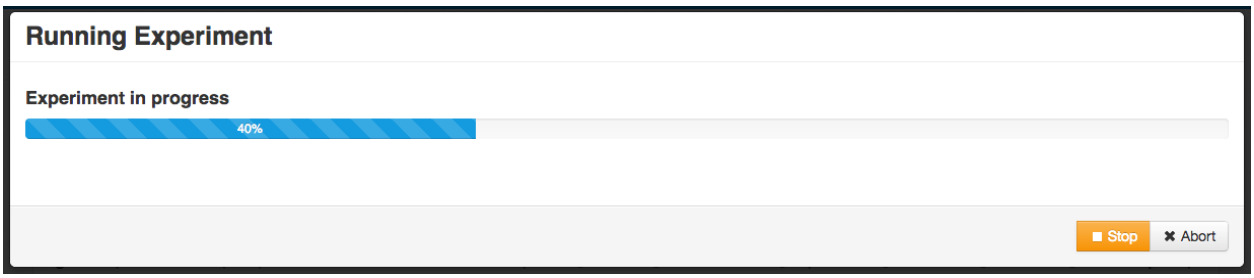
3.36 WebUI Experiment: experiment execution - "Preparing experiment" step

2. "Experiment in progress": prepare the execution of the test, copying if necessary PCAP traces on the remote boxes.



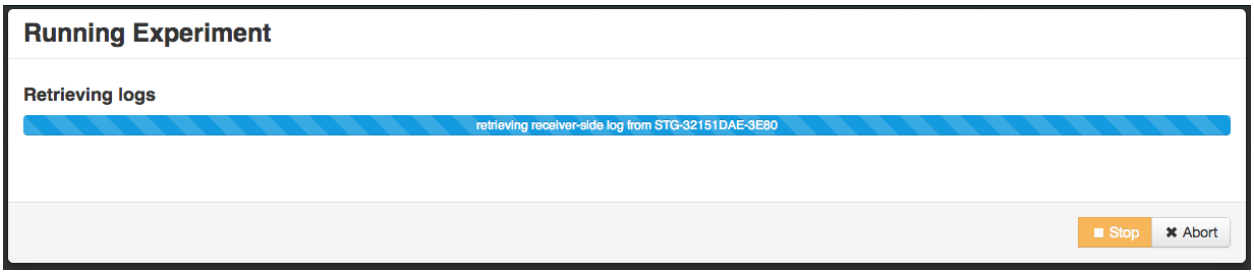
3.37 WebUI Experiment: experiment execution - "Experiment in progress" step

and run the experiment (a bar will show its progress);



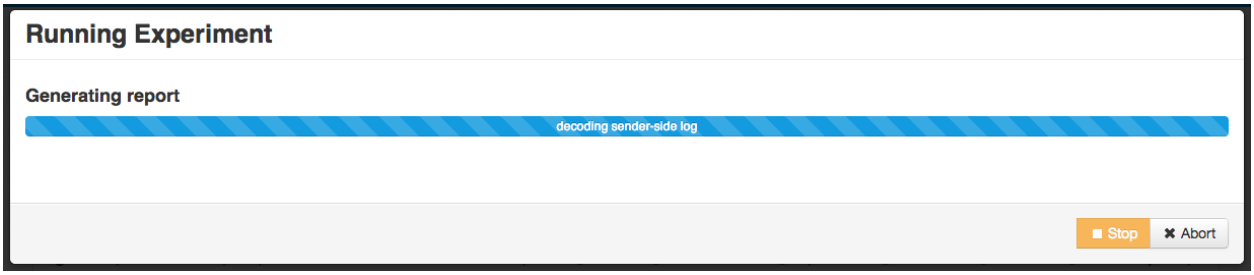
3.38 WebUI Experiment: experiment execution - "Experiment in progress" step

3. “Retrieving logs”: retrieve the sender and receiver logs from local or remote boxes in according to the logger configurations;



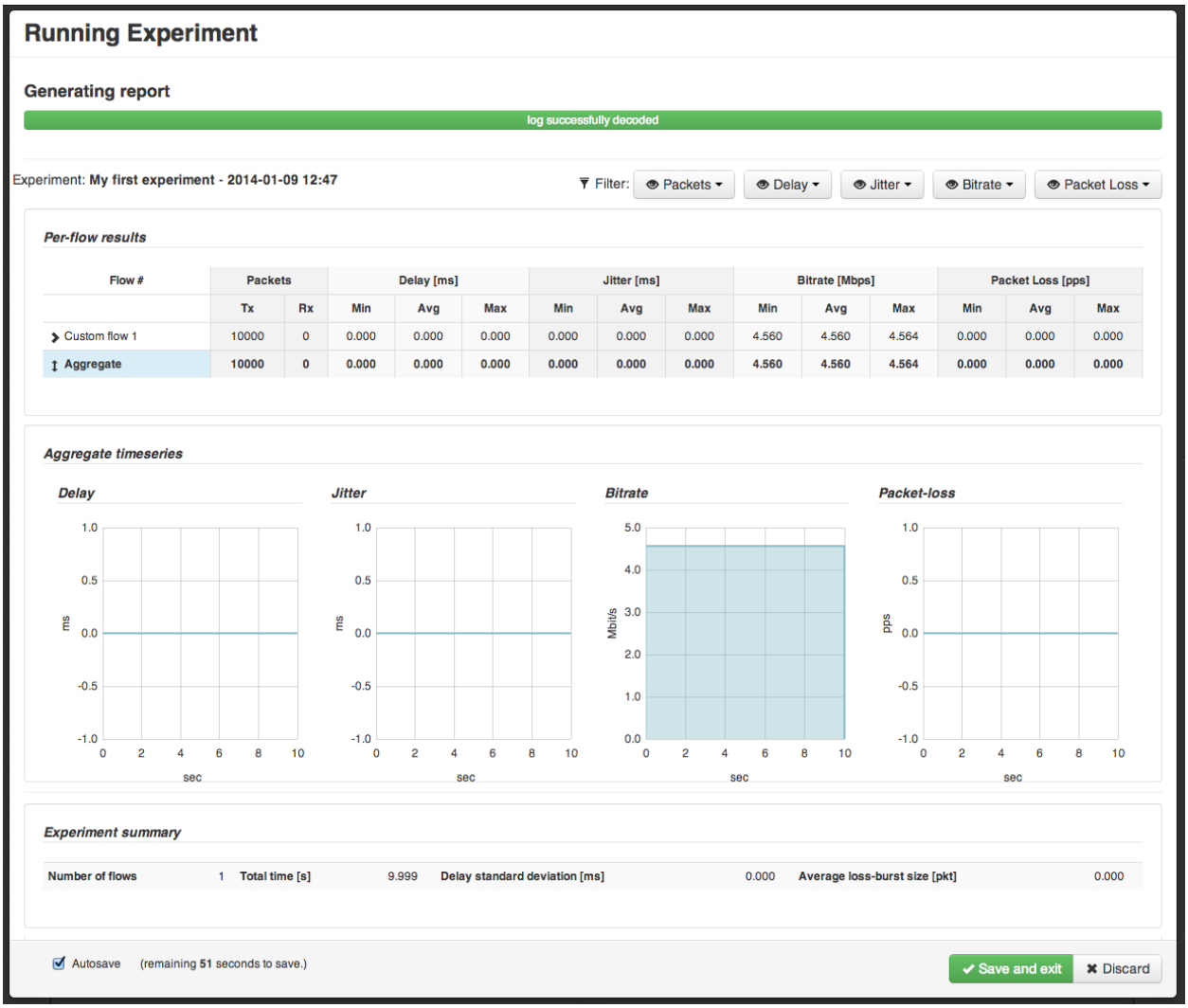
3.39 WebUI Experiment: experiment execution - “Retrieving logs” step

4. “Generating report”: if you have chosen to log at the sender side, on the local box you will see the report of the executed test.



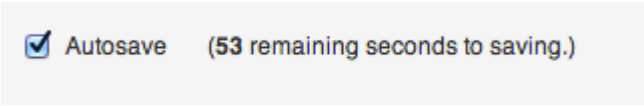
3.40 WebUI Experiment: experiment execution - “Generating report” step

Once the report is successfully decoded you will see the experiment results.



3.41 WebUI Experiment: experiment execution - "Generating report" step

At the end of fourth step an "autosave" timer will start. It can be disabled pushing on the related checkbox field.



3.42 WebUI Experiment: experiment result autosave

You can manage the experiment execution using the buttons placed to the bottom of dialog window, as shown in the 3.43 figure.

3.43 WebUI Experiment: experiment test buttons

The buttons have the following tasks:

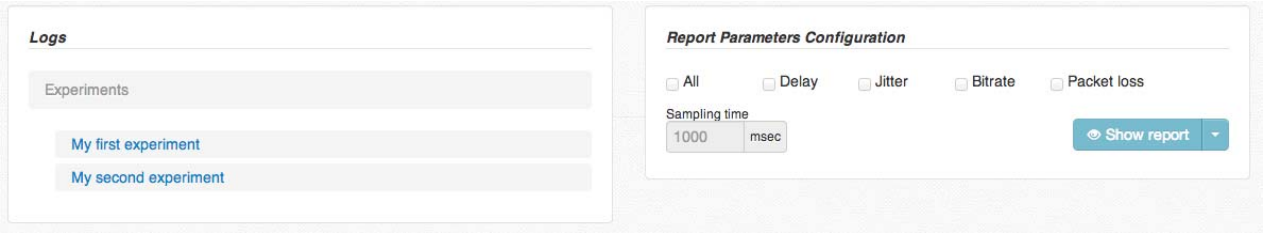
- "Stop": interrupts the test execution. Only partial data of the executed test will be analyzable.
- "Abort": if there is a pending test it will stop its execution and it discards the obtained data anyway.
- "Save and exit": allows to save the result of the executed test and return to flows configuration page. All the saved results are visible in "Analyzer" page.
- "Discard": discards the experiment results.

The first two buttons are visible during the experiment execution while the last ones at the end of the experiments.

Analyzer

"Analyzer" section allows you to evaluate the experiments report. It consists in two sections:

- "Logs" section is a navigable tree of all configured experiments. In the first step you can choose the experiment by its name, viewing all the experiment date in which they are executed. Selecting one of them you will choose the log report that you want to analyze, sender or remote one.
- "Report parameters configuration" allows you to set the "Sampling time" and which parameter you want to evaluate in the report. You can select all or a combination of the following parameters:
  - delay;
  - jitter;
  - bitrate;
  - packet loss.



3.44 WebUI Analyze: an overview

"Show report" button have two functionalities:

- pushing on the button (on the left side) it shows the report in the same page;
- pushing on the caret on the right side of button you can show only the report section in a blank page.

Analyze Experiment Report

The following figure shows the report of the selected log file of the experiment. In the header there are:

- the “Back” button to return the previous screen;
- the “Export Octave/Matlab Log” button to download the export results in the “MAT” format to load them in Octave or Matlab software;
- the experiment name and the execution date of the test.

The next section is about “Experiment summary” that resumes:

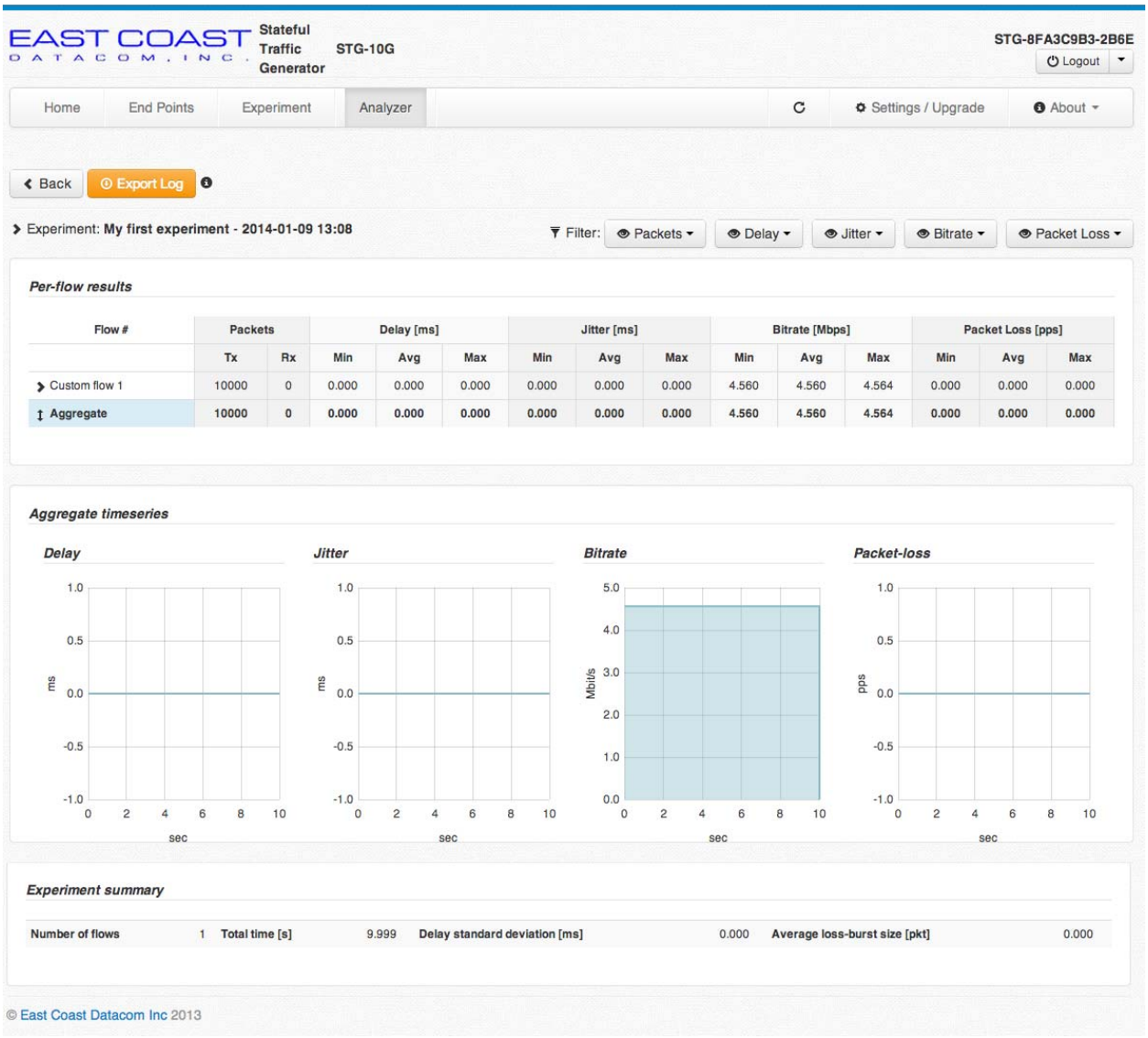
- the total number of flows involved in the experiment test;
- the total time, in second, used to execute the test;
- the delay standard deviation, in millisecond;
- the average loss-bust size, in packets number.

Other specific information about the experiment test are shown in the section “Per-flow results”, in which there is a table consisting a row for each experiment flow and, the last, an aggregate of flows values. The table columns are been categorized in four macro-information:

- packets: the number of packets will be involved in the test, that can be:
  - TX, sent packets from source to destination
  - RX, received packets from source that will be sent from the destination. In the case of “one way” test, they assumes as value 0.
- delay: in milliseconds
  - minumum
  - maximum
  - average
- jitter: in milliseconds
  - minimum
  - maximum
  - average
- bitrate: in Megabits per second
  - minimum
  - maximum
  - average
- packet loss: in packets per second
  - minimum
  - maximum
  - average.

Each column can be hidden using the filter menu that gives to you the possibility to select one or more information.

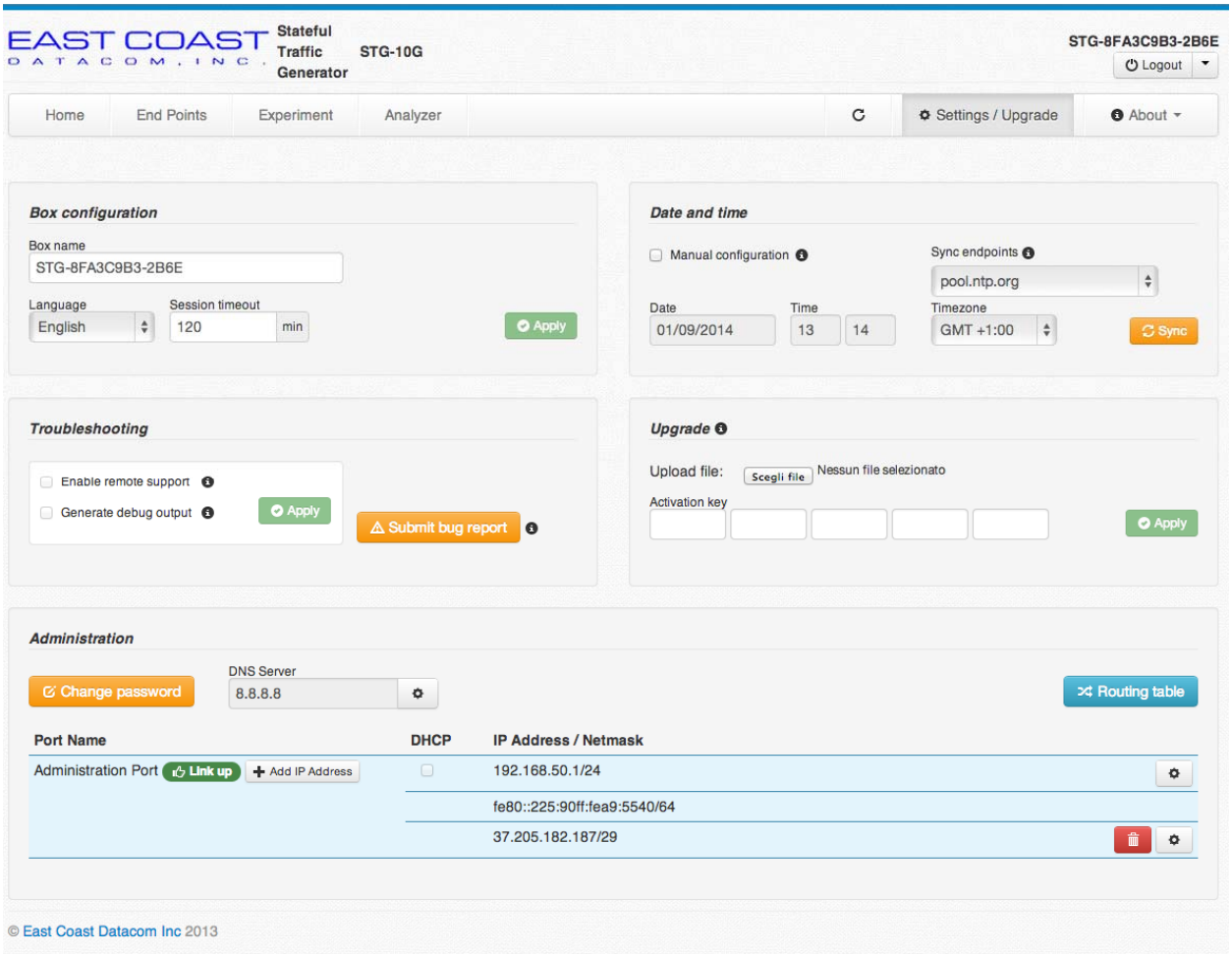
The last section shows a graphs for every selected parameter of the aggregate flow information.



3.45 WebUI Analyze: experiment report

Settings/Upgrade

The “Settings/Upgrade” page consists of several sections about general box configuration.



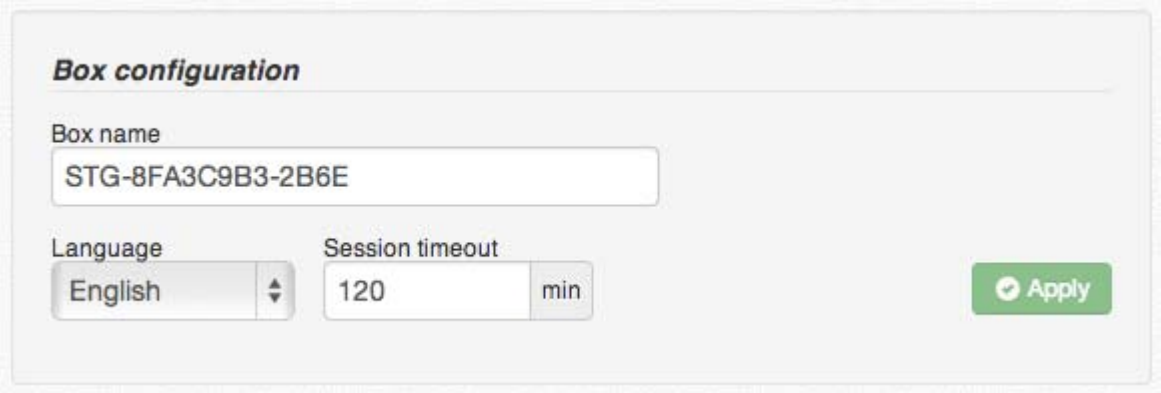
3.46 WebUI Settings/Upgrade: an overview

Box configuration

In “Box configuration” area you find:

- “Box name”: the name of the local box.
- “Language”: the language used in the WebUI. By default it is “English”.
- “Session timeout”: how long a session is valid after which, if you do not refresh, submit or request information, it will expire and you will be redirected to the login page. It is important to note that if you close the browser application session expires.

You can change one of these value and after save it pushing on “Apply” button.

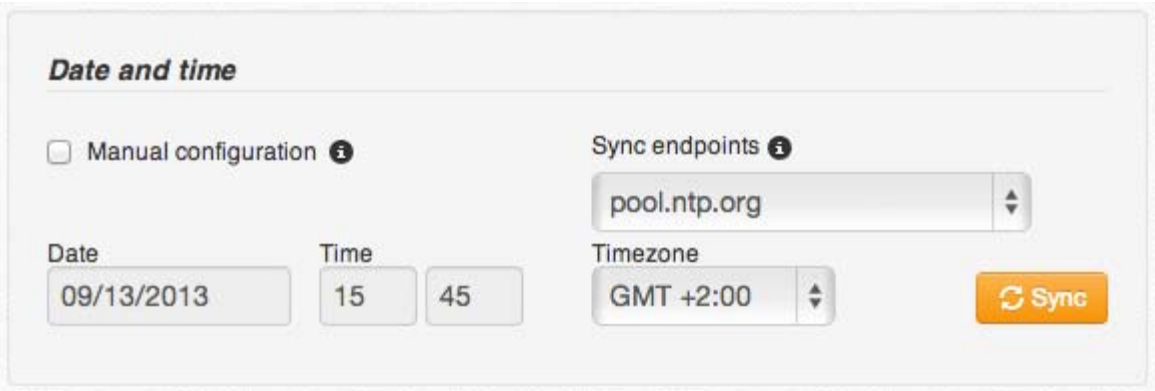


3.47 WebUI Settings/Upgrade: box configuration

Date and time

"Date and time" area allows you to configure the timing of the local STG box. You have two configuration type:

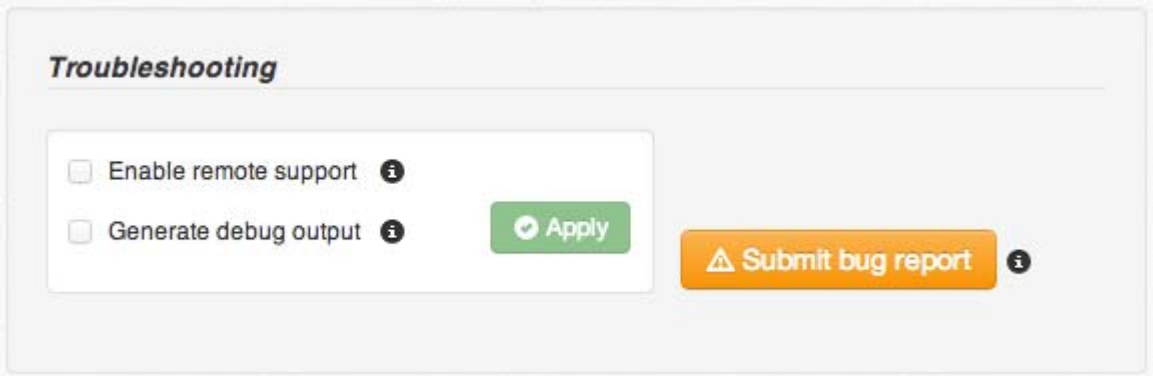
- manual configuration: you can specify the date, the time (hour and minute) and the timezone.
- automatic configuration: you can synchronize your box using the Network Time Protocol (NTP) or choosing a remote box, as pre-configured in "End Points" section. These options are listed in "Sync endpoints" select field.



3.48 WebUI Settings/Upgrade: date and time

It is important the synchronization among sender and receiver boxes in order to correctly measure packet one way delay. If you cannot assure this, we suggest to use the round-trip time meter when configuring the flow.

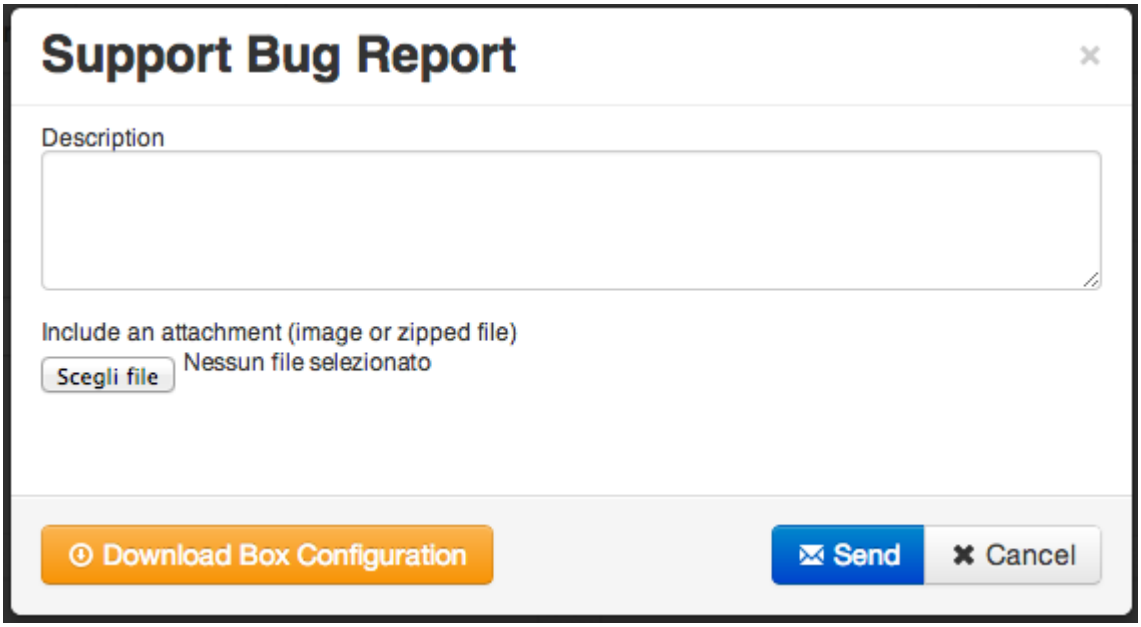
Troubleshooting



3.49 WebUI Settings/Upgrade: troubleshooting

"Troubleshooting" area allows you to:

- "Enable remote support" (CURRENTLY NOT IMPLEMENTED) for giving the possibility to the support team to connect to your box. This field must be enabled if you want to add a new network card to the box, so Ecdata Technical Support can configure it correctly;
- "Generate debug output" (CURRENTLY NOT IMPLEMENTED) enables a popup window for showing debug information.
  To save the changes you must push on "Apply" button.
- "Submit bug report" button allows you to send or to download all box configuration for bug reporting. Pushing on it the following popup will be opened.



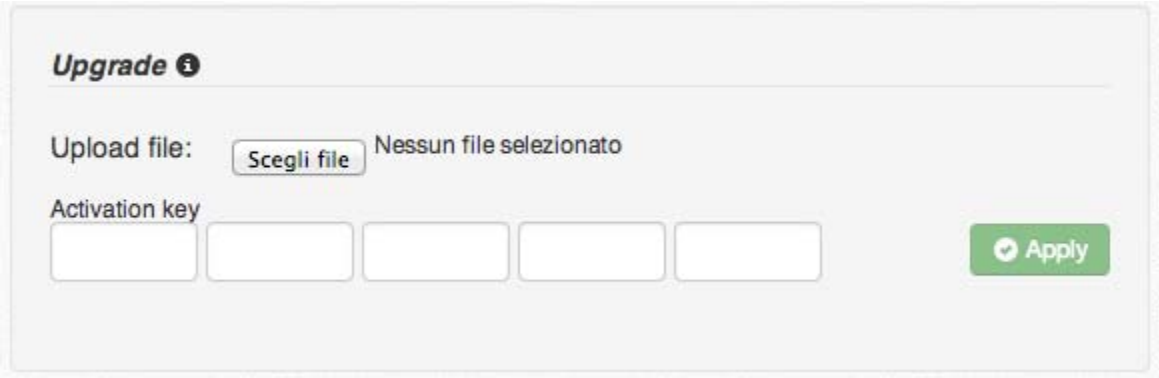
3.50 WebUI Settings/Upgrade: support bug report

In this window you can:

- describe the observed bug, attach, if you want, an image or a zipped file and sending them by email to ECData support (info@ecdata.com) using "Send" button;
- download to your system the box configuration pushing on the "Export Box Configuration" button.

Upgrade

"Upgrade" section allows to update each STG component. After choosing the file you must insert the "Activation key" that is composed of 5 string of 5 alphanumeric characters.



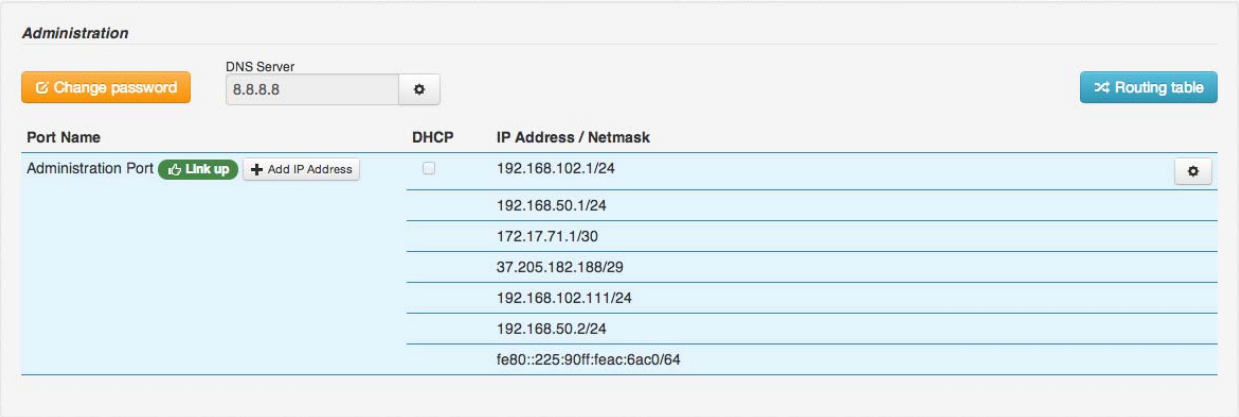
3.51 WebUI Settings/Upgrade: upgrade

Pushing on “Apply” button a dialog window will pop up with the changelog of the upgrade process. Now you can choose to install or abort the update process selecting the related buttons.

Administration

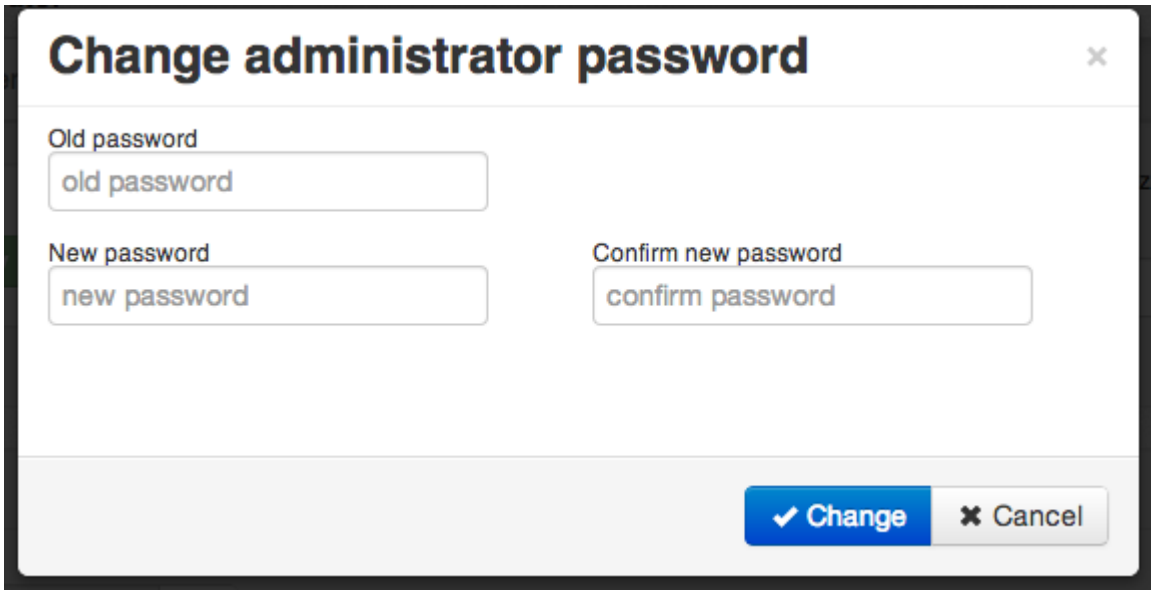
“Administration” section allows to manage:

- the change of password pushing on “Change password” button
- the DNS Server IP address using the wheel button
- the administration port configuration using the blue table as shown in “End Points” chapter.



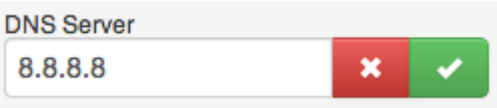
3.52 WebUI Settings/Upgrade: administration

So, pushing on “Change password” button a popup, as shown below, will be opened, in which you must insert the old and the new password.



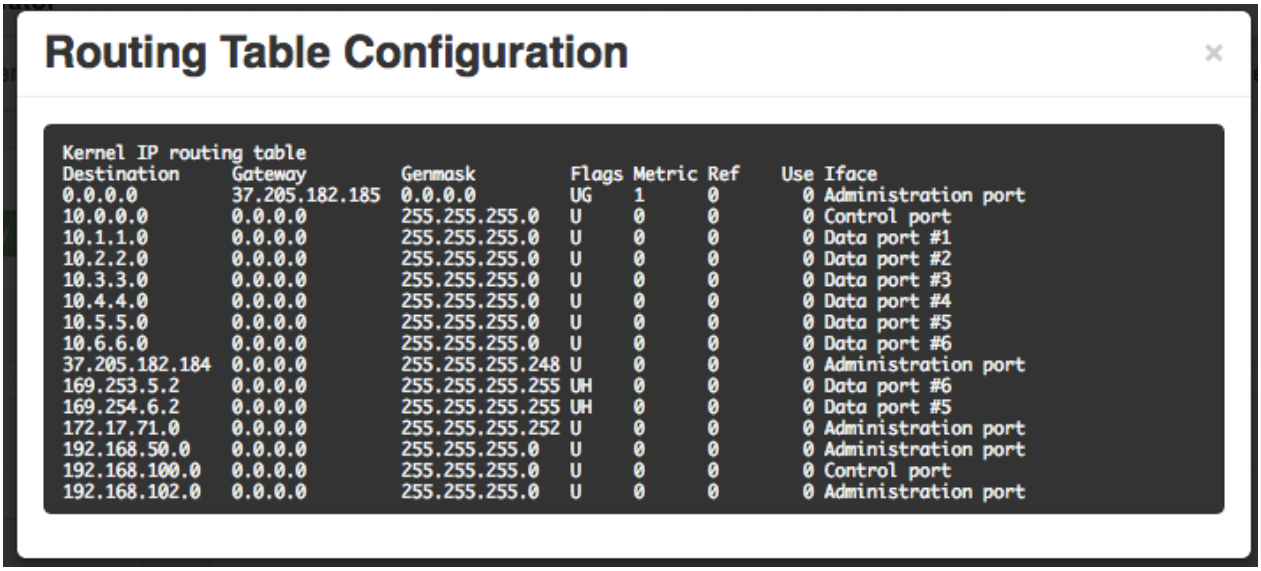
3.53 WebUI Settings/Upgrade: change administrator password

Pushing on wheel button, the “DNS Server” field will be enabled to modify the related IP address. As shown in the 3.39 figure, the green and red buttons allow you to save or discard the change respectively.



3.54 WebUI Settings/Upgrade: change DNS Server IP address

The “Routing table” button, located on the right side, will show a popup that resumes the information about routing configuration of the local box.



3.55 WebUI Settings/Upgrade: routing table configuration

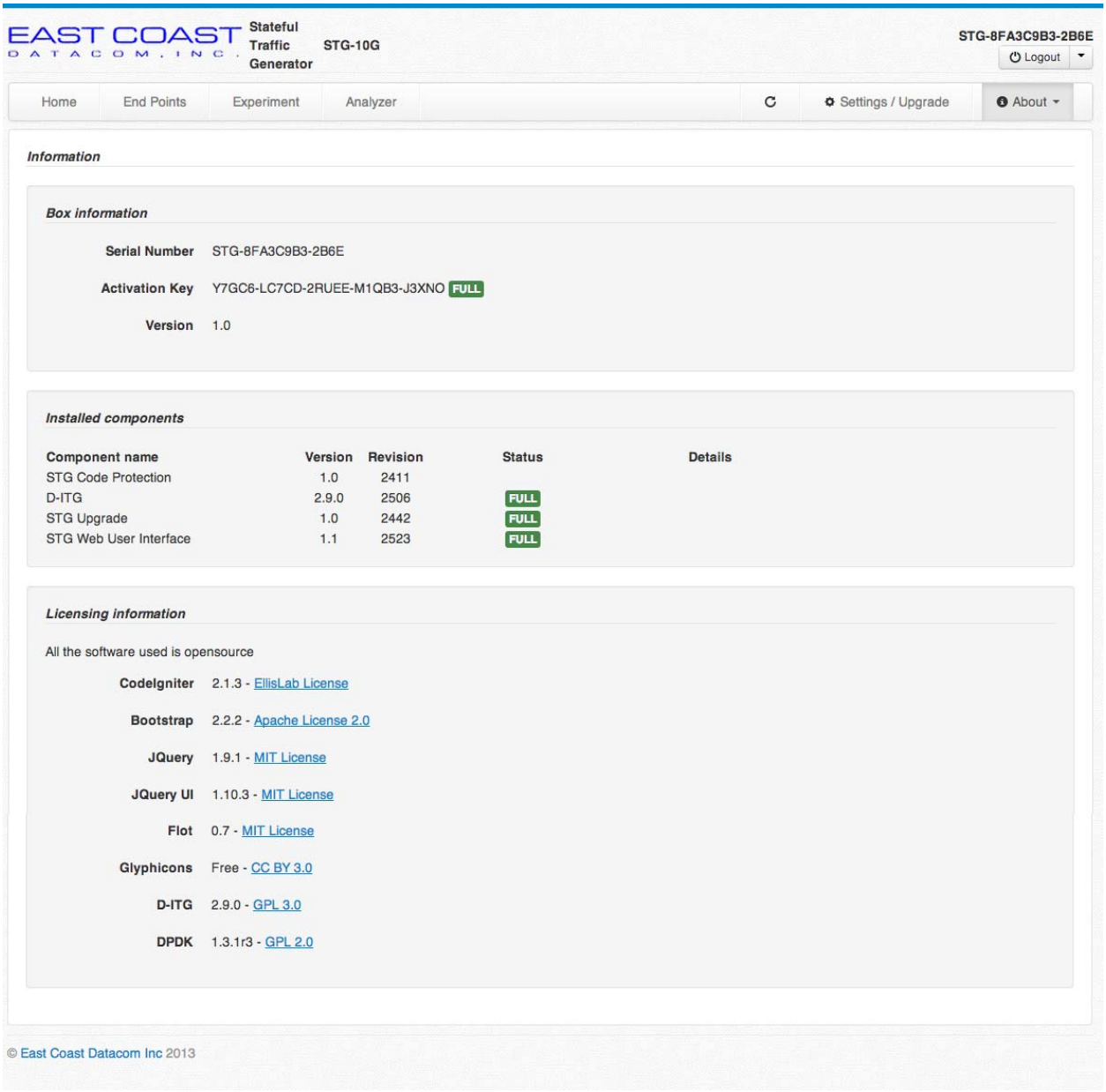
About

The “About” menu item consists of:

- Information
- Help

Information

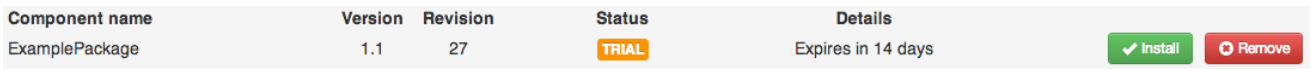
“Information” page is divided into three sub-section as shown in the following figure.



3.56 WebUI About: information overview

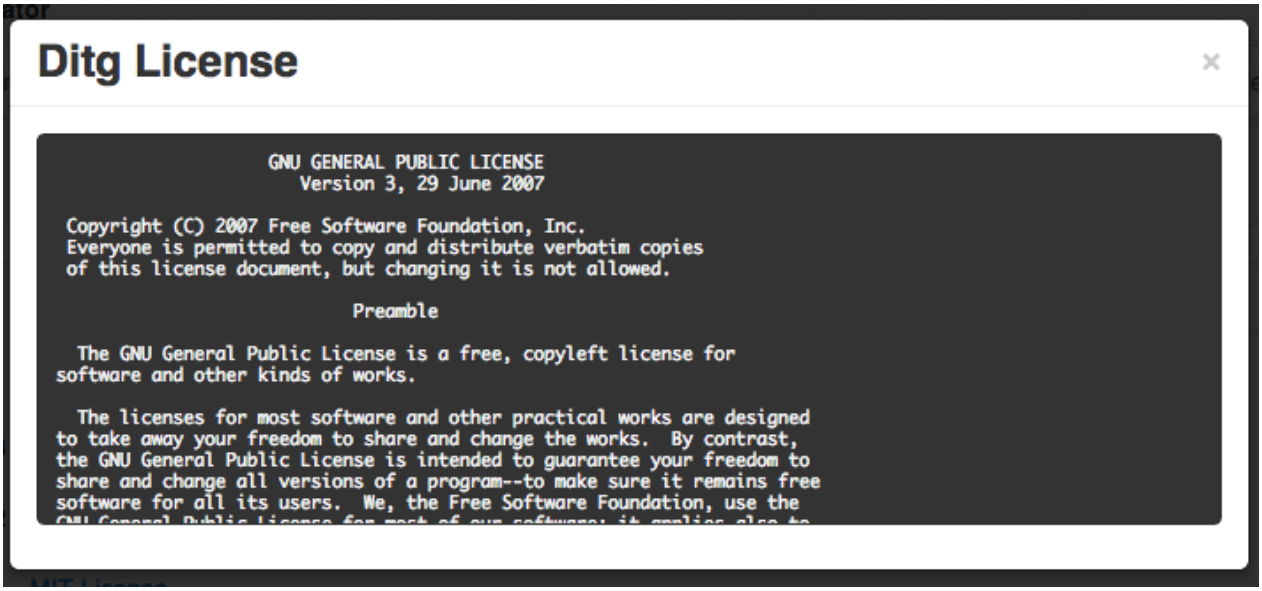
The subsections are:

- "Box information" containing:
  - the "Serial Number" of the box
  - the "Box Activation Key"
- "Installed components" lists every installed components, specifying the version, the revision, the status (full or trial) and the details about expiry date. The "Install" and "Remove" buttons allows you to make or not permanent the related package.



3.57 WebUI About: "Trial" installed component

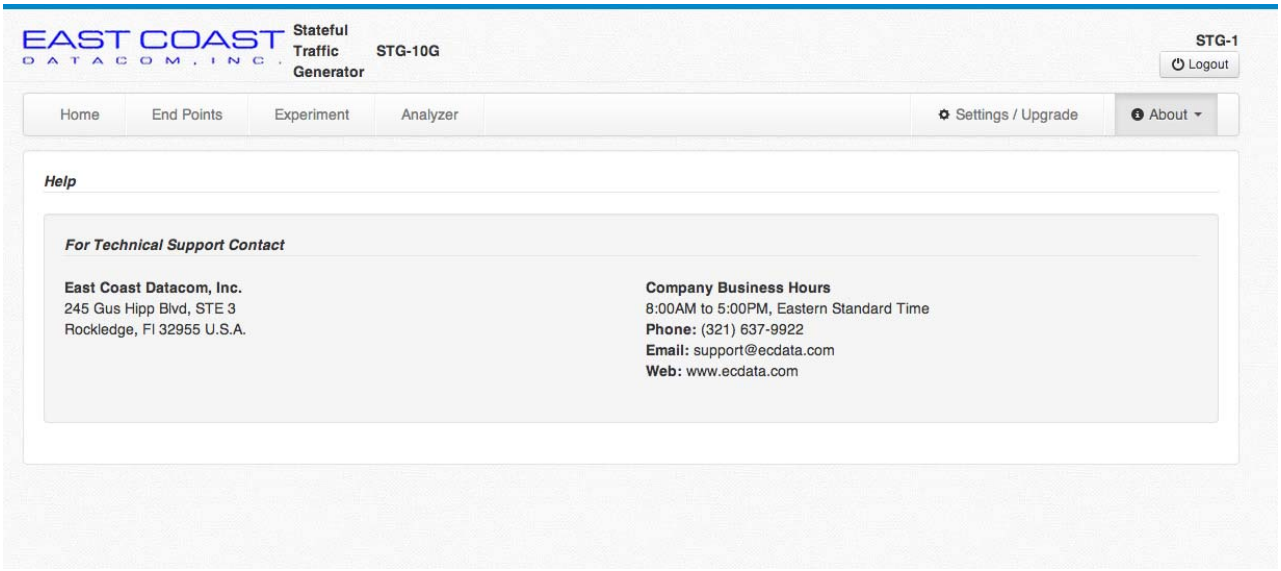
- "Licensing information" lists the open-source softwares used to realize the STG product. Pushing on each of them a popup window will show its license, as in the following 3.41 figure.



3.58 WebUI About: open-source software license

Help

"Help" page contains information about technical support contact.



3.59 WebUI About: technical support information