User's Manual

Net.Storm

Network Impairment Generator

ALBEDO Telecom

Copyright

The information contained in this document is the property of ALBEDO Telecom S.L. and is supplied without liability for errors and omissions.

No part of this document may be reproduced or used except as authorised by contract or other written permission from ALBEDO Telecom S.L. The copyright and all restrictions on reproduction and use apply to all media in which this information may be placed.

ALBEDO Telecom S.L. pursues a policy of continual product improvement and reserves the right to alter without notice the specification, design, price or conditions of supply of any product or service.

© ALBEDO Telecom S.L. 2012
All rights reserved

Issue 3, 06/12

For any query or requirement regarding the *Net.Storm Network Impairment Generator*, contact with ALBEDO Telecom using the following contact details:

ALBEDO Telecom S.L.
C/ Joan d'Àustria 112

08018 Barcelona - Spain

E-mail: *support.telecom@albedo.biz*
Telephone: *+34 93 221 28 73*

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - **www.telecom.albedo.biz**

Table Of Contents

Chapter 1: Introduction 1
- Important Notice 2
  - Warranty 2
  - Battery Safety 2
  - WEEE Notice 3
- The Tester 3
  - Test Connectors 4
  - Platform Connectors 5
- The Graphical User Interface 6
- Running Tests 9
- Upgrading the Unit 9

Chapter 2: Connection to the Network 11
- Connecting the Tester to the Network 11
  - Checking Port A and Port B Auto-negotiation 12
  - Using the SFP Ports 14

Chapter 3: Frame and Event Counts 17
- Global Frame Analysis 17
- Frame Size Histogram 20
- The LEDs Panel 20

Chapter 4: Multi-stream Analysis 25
- Enabling and Disabling Filters 25
- Configuring Filters 26
  - MAC Selection 27
  - VLAN Selection 29
  - IPv4 Selection 31
  - TCP Selection 34
  - UDP Selection 36
  - Generic Selection 36
- Getting Statistics about Filters 37

Chapter 5: Inserting Events 39
- Introduction to Performance Metrics for Ethernet 39
  - One-way Delay 39
  - One-way Delay Variation 40
  - Frame Loss 41
  - Frame Corruption and Duplication 41
- Adding Impairments to Ethernet Traffic 42
  - Frame Loss 42
  - Delay & Jitter 45
  - Bandwidth 46

Frame Duplication 47
Frame Errors 48
Adding Impairments to Selected Traffic Flows 49
Chapter 6: Test Management 51
Generating Reports 51
File Management 53
Saving Configurations 54
Renaming Files 54
Deleting Files 54
Exporting Files to External Devices 55
Importing Configurations 55
Using the Embedded Web Server 56
Programming Tests 57
Using the System Menu 59
Using the Network 60
Installing Software Options 63
Using the Remote Control 64
Appendix A: Technical Specification 67
Ports and Interfaces 67
Formats and Protocols 67
Configuration 67
Results 67
Filters 68
Ethernet filters 68
IP filters 68
Statistics 68
Event Insertion 68
Frame Delay and Jitter 69
Packet Loss 69
Frame Duplication 70
Errored Frames 70
User Interface 70
General 71

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Chapter 1
Introduction

The ALBEDO Telecom Net.Storm is a handheld tester which is capable to emulate different degradations or impairments that are often found in Ethernet / IP networks. Thanks to this capability, Net.Storm is useful in determining whether a network application or device is appropriate for operation in such networks.

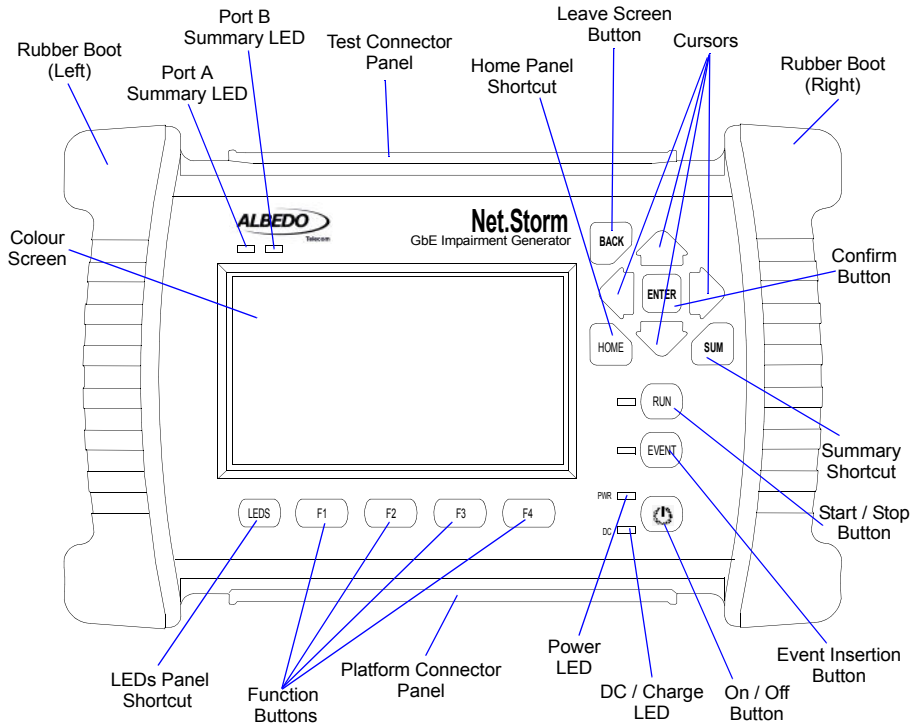

Figure 1.1: Net.Storm Front view. The tester presents results by means of a colour screen and the LEDs. The configuration is performed through the keyboard.

The Net.Storm has an external DC input but it also has internal batteries. This makes this tester suitable both for laboratory applications and field applications which require versatile and reliable operation.

Within your Net.Storm test kit you will find the following items:

- One Net.Storm test unit.
- One AC/DC adapter with a power cord specific for your country.
- One Carrying bag.
- Two Cat. 5e cables with RJ-45 connectors certified for operation at 1 Gb/s rates.
- Two SFPs for connection to optical interfaces (if ordered).
- Two MMF or SMF cables to be used with the SFPs (if ordered).
- One CD-ROM with user documentation.
- One printed copy of this user manual (if ordered).

Check with your distributor the availability of other optional items for your Net.Storm unit.

1.1. Important Notice

Operation, manipulation and disposal warnings for your Net.Storm unit are listed below.

1.1.1. Warranty

The ALBEDO Telecom Net.Storm is supplied with a warranty that includes replacement of damaged or faulty components in the terms and period described in the ordering information. This Warranty does not apply to:

1. Product subjected to abnormal use or conditions, accident, mishandling, neglect, unauthorized alteration, misuse, improper installation or repair or improper storage.
2. Product whose mechanical serial number or electronic serial number has been removed, altered or defaced.
3. Damage from exposure to moisture, humidity, excessive temperatures or extreme environmental conditions.
4. Damage resulting from connection to, or use of any accessory or other product not approved or authorized by the Company;
5. Product damaged from external causes such as fire, flooding, dirt, sand, weather conditions, battery leakage, blown fuse, theft or improper usage of any electrical source.

1.1.2. Battery Safety

The ALBEDO Telecom Net.Storm tester contains a built-in battery, improper use of which may result in explosion. Do not heat, open, puncture, mutilate, or dispose of the

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

product in fire. Do not leave the device in direct sunlight for an extended period of time, which could cause melting or battery damage.

1.1.3. WEEE Notice

This product must not be disposed of or dumped with other waste. You are liable to dispose of all your electronic or electrical waste equipment by relocating over to the specified collection point for recycling of such hazardous waste. For more information about electronic and electrical waste equipment disposal, recovery, and collection points, please contact your local city centre, waste disposal service, or manufacturer of the equipment.

1.2. The Tester

Interaction with Net.Storm is based on a high resolution colour screen, different kinds of status LEDs, and a keyboard. These are the keyboard elements:

- *Cursors*: Enable navigation through the graphical user interface. Including menus, keyboards and configuration lists. To leave a menu or configuration list, the left arrow can be used. In menus, the right arrow enters in the lower level menu or list.
- *ESC*: Leaves the current panel (menus, lists, and special panels).
- *ENTER*: In menus, enters in the lower level menu or list. In a configuration list, it selects the current item and leaves. In keyboards and some special panels, it selects the current item without leaving.
- *HOME*: Shortcut to the *Home* panel. From any menu, list, or special panel, it returns directly to *Home*.
- *SUMMARY*: Displays the *Summary* panel. If the Summary panel is already shown, it returns to the previous panel.
- *LEDS*: Displays the *LEDs* panel. If the LEDs panel is already shown, it returns to the previous panel.
- *EVENT:* Starts (and sometimes stops) the event insertion. The exact way this button works depends on the actual event insertion mode. For example, if single event inversion is configured, each time you press *EVENT* a new event will be inserted but if continuous insertion is the current configured value, you will need to press *EVENT* during event insertion to stop the action.
- *RUN:* This button starts / stops a new test. Some results (LEDs, some analogue values) are available without an ongoing test. Most of the configuration is blocked during a test execution.
- *Function keys (F1, F2, F3, F4)*: These keys do not have a fixed purpose. Their associated action depends on the panel being displayed.
- *On/Off key*: If the tester is in off status, push to switch it on. If the tester is on, use this key to switch it off (long push).

There are four LEDs (PWR, DC, Port A summary, Port B summary). Their description is given below:

- *PWR*: Displays the current tester on / off status. The green colour is displayed under normal operation conditions. Orange and red are shown to indicate a low battery load.
- *DC*: This led is lit when the DC input is connected. Orange indicates a charging batteries status and green means that the internal batteries are ready.
- *Port A / Port B Summary*: These LEDs provide a permanent indication of the current input signal (or signals) status. The LEDs summarize the Port A and Port B information given by the event LEDs. If any event LEDs for a test port is in 'red' status, the port summary led will be set to 'red'. If any event LED is 'orange' but there is no 'red' event, the summary led will be set to 'orange. The 'green' colour is used when no events are found in the input signal. Finally, the LED is switched of when the port is disabled.

1.2.1. Test Connectors

The Net.Storm is connected to the DUT / SUT through the test connector panel. Ports and elements included in this panel are described in the following list:

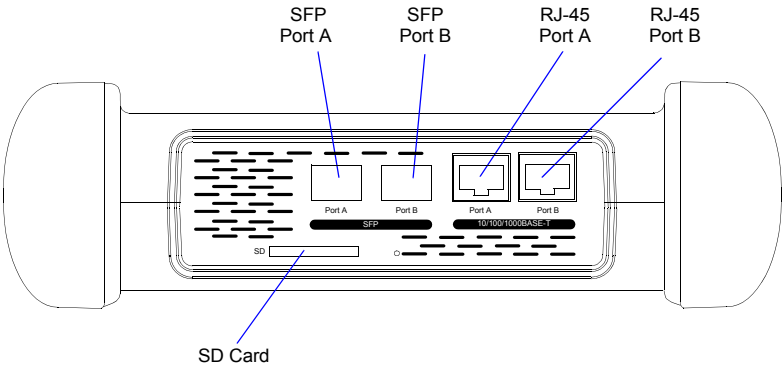

Figure 1.2: Net.Storm test connector panel. Connection to the DUT / SUT is done in this panel

- *RJ-45 Port A*. This is the first full featured 10/100/1000BASE-T port for Ethernet transmit and receive.
- *RJ-45 Port B*. This is the second full featured 10/100/1000BASE-T port for Ethernet transmit and receive. This port is identical to the RJ-45 Port A.
- *SFP Port A*. This port is used to connect the tester to the network through an optical interface with the help of an SFP module.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

- *SFP Port B*. This port is used to connect the tester to the network through an optical interface with the help of an SFP module. This port is identical to the SFP Port A.
- *SD Card*: Slot for SD Cards. These cards can be used as external storage devices.

1.2.2. Platform Connectors

There is a connector panel specifically devoted to the platform ports. This panel includes capabilities like remote control and external device connection. A more detailed description is given below:

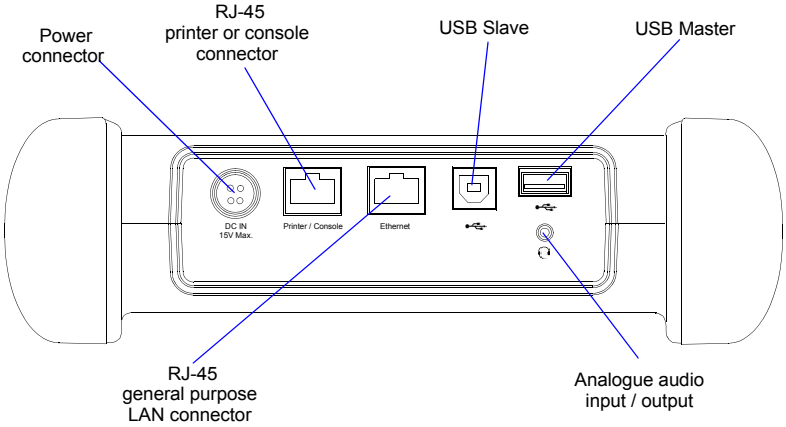

Figure 1.3: Net.Storm platform connector panel. This panel includes connectivity to USB devices,

- *Power connector*: The input must be 12 V DC, 4 A. A suitable external AC/DC adapter for your country is provided with the tester.
- *RJ-45 printer or console*. Console connector. This interface is prepared for connecting a serial printer.
- *USB Slave*. Use a USB cable with Slave type connector (Type B, *Device*) for this port. Currently this port enables connection of a PC to the tester and access to the internal tester file system.
- *USB Master*: Use a USB cable with a Master type connector (Type A, *Host*) for this port. Currently this port is used for software upgrades and connection of external storage devices.
- *RJ-45 general purpose LAN connector*: This is the platform Fast Ethernet connector (10/100BASE-T). It is used for remote management of the test unit.
- *Analogue audio input / output*: It is a 2.5 mm audio jack for connecting external speakers and microphone.

1.3. The Graphical User Interface

The Net.Storm graphical user interface is based in a 480 x 272 colour screen and a set of keys attached to the front panel. Some of these keys have a permanent purpose but the specific function for some other keys depend on the context.

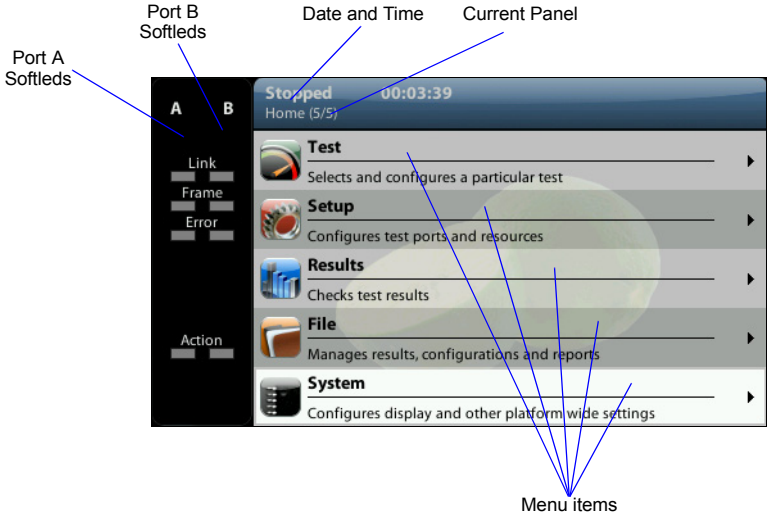

Figure 1.4: Net.Storm, the Home panel.

The keyboard and the screen allow the user setting configuration values, starting tests and displaying results. The user is always aware of the current status of the received signal through the Softleds shown on the left. The Softleds are always displayed and they work even when there is no test running. On the top side of the screen there is a header zone which contains information about the current tester status (date, time, tests running, event insertion active) and an identifier for the currently displayed panel.

Most of the graphical user interface panels are menus containing a variable number of items. All the menus are available from the *Home* panel. Users can press the HOME button at any time to go to the *Home* panel. The *Home* panel contains the following menu items:

- *Test*: Contains configuration items related with general test configuration like delayed test settings, performance objectives, event insertion, and report configuration.
- *Setup*: Provides access to test resource configuration. For the impairment generation application, the setup submenus contain configuration of Port A and Port B.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

- *Results*: This item enables the user to browse test results. Most of them are not available if a measurement has not been previously started but there are some exceptions to this rule like the LEDs.
- *File*: File management menus. Includes configuration, result and report file management. Files can be deleted, copied, exported or imported.
- *System*: Provides platform management tools. For example language selection, screensaver configuration and others.

There are two special panels as well. These are the *Summary* panel and the *LEDs* panel. The *Summary* provides some details about the current configuration and results. The *LEDs* panel gives extended the information about the received signal status already given by the Softleds. Both the *Summary* panel and the *LEDs* panel can be displayed at any moment by pressing the *SUM* and *LEDS* buttons.

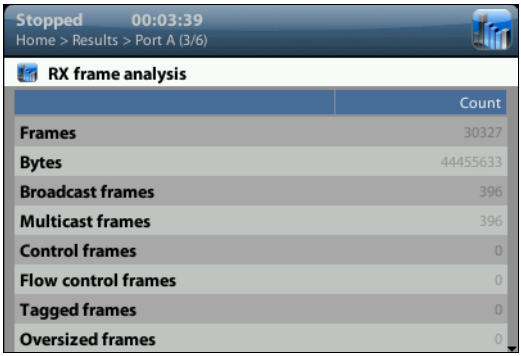

Figure 1.5: Net.Storm test results represented as a counter list

Menus and submenus are organized in a tree. The root of the tree is the *Home* panel and the leaves are configuration or result panels. Results are usually presented in a list or a table. If all results cannot be simultaneously displayed, then the user is allowed to use the cursors up and down to browse the list.

Configuration panels are usually selection lists. Sometimes you can select only one simultaneous item in the list and sometimes selection of several items at the same time

is possible. Keyboards are available if selection through lists is not possible. There is one keyboard for numeric settings and one for alphanumeric settings.

Figure 1.6: Different kinds of configuration panels: (a) Selection list, (b) Alphanumeric keyboard, (c) Numeric keyboard.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

1.4. Running Tests

Most of the results provided by Net.Storm are not available until you start a test. This section provides a high level description of the procedure to follow to configure your unit, start a test and review the results.

1. Configure the tester to send / receive signals in the right operation mode and through the right ports. Connect it to the network.
2. Program the test start time and duration with the help of the *Program* menu (within *Test*) or start the test immediately by pressing RUN.
   Note: Most of the configuration is blocked when there is an ongoing test.
3. Wait for the test to finish or press RUN to finish immediately.
4. Check the test results in the *Results* menu.
   Note: All test results are upgraded in real time as the test progresses. That means that is not really necessary to wait for the test to finish to check current results.

1.5. Upgrading the Unit

The test unit software can be upgraded with the help of a USB memory stick. Before proceeding with the upgrade copy the ALBEDO software to the root directory in the memory stick. The file name of the upgrade package must not be modified. The USB must have a FAT32 file system.

Once the USB memory stick is ready. Follow this procedure to install the new software:

1. Switch the unit off
2. Press HOME and ENTER simultaneously and, without releasing the keys, press the On / Off button.
3. Now, keeping all three the keys pressed, wait until you hear a beep. Then release the keys.
   The ALBEDO Software Installer is loaded and executed. An informative panel displays the Net.Storm software version number found in the storage device.
4. Press ENTER to continue with the installation process.
5. Select *Install* or *Upgrade. Install* regenerates all the software in the unit even if it is up to date. Upgrade regenerates only the software that has changed since the last upgrade. Use *Install* (F2 key) if you need to recover the unit after operation failure due to corrupted software. Use *Upgrade* (F1 key) otherwise.
6. Confirm your previous selection by pressing ENTER or cancel with ESC.
7. Wait for the installation process to finish.
   Note: The full process may take a few minutes.
   Note: Do no disconnect the unit or remove the USB memory stick during installation.
8. Press ENTER to close the Software Installer and finish the installation process. The unit will be automatically restarted. The new software will be loaded.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Chapter 2
Connection to the Network

The Net.Storm is equipped with two identical 1 Gb/s RJ-45 ports and two 1 Gb/s SFP ports. The RJ-45 ports are used for connection to Ethernet electrical interfaces. The SFP ports are normally used for optical connections. Each RJ-45 / SFP interface constitutes a single logical port. These ports are labelled as Port A and Port B.

This chapter describes how to connect the tester to the network and how to configure it to receive and send signals. The general procedure to do that is:

1. Connect the test cables to the network. Use the electrical or optical ports depending on the particular network properties.
2. Configure the Port A / Port B. You will not be able to see any information before you set the right line parameters within the test ports.

2.1. Connecting the Tester to the Network

The right way to connect the tester for Ethernet impairment generation is in pass through mode, allowing the traffic to go through the tester. If the equipment is to be connected to the network through optical interfaces, the right SFPs have to be connected first.

Net.Storm operation is bi-directional. That means that both transmission directions are simultaneously processed by the equipment. If impairment generation is disabled, traffic is not altered by Net.Storm.

The procedure for configuring the connector (RJ-45 or SFP) is the following

1. From the *Home* panel, go to *Setup*,
   The test port settings panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific configuration.
3. Select *Connector* to display the available options for the port connector.
4. Choose the right connector and confirm by pressing ENTER.
   Note that Port A and Port B do not need to be both optical or electrical at the same

time. Net.Storm is compatible with operation requiring conversion between optical and electrical transmission if all other operation conditions are met.

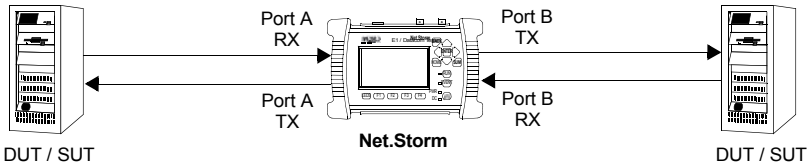

Figure 2.1: Bidirectional impairment generation with ALBEDO Net.Storm connected in pass through mode

2.1.1. Checking Port A and Port B Auto-negotiation

Interfaces connected to Port A and Port B are required to have at least one common operation bit rate. Also, interfaces to be connected to Port A and Port B must support full duplex operation. Half duplex operation involves collisions and frame retransmission and this is not compatible with predictable delay insertion as it is carried out by Net.Storm.

If these two conditions are met, Net.Storm will be able to forward traffic between ports A and B. Bit rate configuration can be automatic using Ethernet auto-negotiation but users are allowed to force a fixed bit rate as well. If auto-negotiation is enabled in Net.Storm, the equipment will configure its ports to the common maximum rate for port A and port B. If auto-negotiation is not enabled, The user will configure the desired bit rate, but Port A and Port B configuration are always coupled so that the bit rate in both ports always remains the same.

To configure the auto-negotiation settings in your Net.Storm unit follow these steps:

1. From the *Home* panel, go to *Setup*,
   The port setup panel is displayed.
2. Go to *Auto-negotiation*.
3. Set *Enable auto-negotiation* to *Yes* to configure the link speed using auto-negotiation or to *No* to disable auto-negotiation and force the link speed to a fixed value
4. If you have enabled auto-negotiation in the previous step configure the allowed bit rates through the *1000*, *100* and *10* menus. If auto-negotiation is disabled, set the *Forced bit-rate* to *10* or *100*.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Note: The 1000 Mb/s rate cannot be forced and it is only available through auto-negotiation due to IEEE 802.3 restrictions.

Figure 2.2: Albedo Net.Storm auto-negotiation results panel.

Once the tester has been connected to the network and the right connector type as been configured, follow these steps to check auto-negotiation:

1. From the *Home* panel, go to *Results*,
   The test port results panel is displayed.
2. Press Auto-negotiation
   The auto-negotiation status table for Port A is displayed.
3. Check that the *Local*, *Remote* and *Current* table rows display *A/B* (supported in port A and port B), *A* (supported in port A only), *B* (supported in port B only) or an empty space (not supported) in the right places.

Table 2.1: Auto-negotiation results

Result	Description
Local	Displays the bit rate and duplex mode supported by the Net.Storm Port A or Port B. If the current connector is the RJ-45, the supported bit rates are 10 Mb/s, 100 Mb/s and 1000 Mb/s (1000FD, 100FD and 10FD). If the connector is set to SFP the supported bit rate is 1000 Mb/s (1000FD). Impairment generation in through mode requires full-duplex operation. For this reason, Net.Storm always forces full-duplex mode. An alarm is displayed if this cannot be achieved.

Table 2.1: Auto-negotiation results

Result	Description
Remote	Displays the bit rate and duplex mode supported by the remote device connected to Port A or Port B. It is one or several of the 1000FD, 1000HD, 100FD, 100HD, 10FD, 10HD set. If the remote device does not support auto-negotiation or auto-negotiation is disabled in this device, it will behave as if no interfaces were supported and the impairment emulator will be unable to work.
Current	Bit rate and duplex operation agreed during the auto-negotiation process. It is one (and only one) of the 1000FD, 100FD and 10FD set. If there is more than one compatible interfaces, the one with higher bit rate is preferred.

2.1.2. Using the SFP Ports

The SFP ports are the only choice available for optical tests. They can also be used for electrical tests if compatible SFPs are connected but this is usually not necessary due to the attached RJ-45 ports which require no adapters.

To display the SFP interface information follow these step sequence:

1. From the *Home* panel, go to *Results*,
   The test port results panel is displayed.
2. Enter in *SFP*.

Check the *Interface*, *SFP present*, *SFP vendor* and *SFP part number*.

Table 2.2: Ethernet SFP Results

Result	Description
SFP present	Shows information about presence of an SFP in the current port. The information is displayed even if the port is configured to operate over the attached RJ-45 interface

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Table 2.2: Ethernet SFP Results

Result	Description
Interface	Displays the current Ethernet interface. Supported interfaces are listed below: • 10BASE-T: Used for transmission at 10 Mb/s over two pairs of Cat. 3 UTP cable with range of 100 m. • 100BASE-TX: Used for transmission at 100 Mb/s over two pairs of Cat. 5 UTP cable with range of 100 m. • 1000BASE-T: Used for transmission at 1000 Mb/s over four pairs of Cat. 5e UTP cable with range of 100 m. • 100BASE-FX: Optical interface for transmission of 100 Mb/s over MMF operating in the 1310 nm optical window. This interface is available by an external compatible SFP supplied by ALBEDO Telecom. • 1000BASE-SX: Used for transmission at 1000 Mb/s over two MMF operating in the 850 nm optical window. Ranges are usually a few hundred metres. This interface is supported by means an external SFP only. • 1000BASE-LX: Used for transmission at 1000 Mb/s over two MMF or SMF in the 1310 nm optical window. Ranges use to be a few kilometres. This interface is supported by means an external SFP only.
SFP vendor	If there is an SFP connected to the port, this field shows information about the vendor. This information is recorded within a memory in the SFP when it is manufactured.
SFP part number	If there is an SFP connected to the port, this field shows information about the vendor. This information is recorded within a memory in the SFP when it is manufactured.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - **www.telecom.albedo.biz**

Chapter 3
Frame and Event Counts

The ALBEDO Telecom Net.Storm can be used to get basic traffic statistics about Ethernet networks operating at rates up to 1 Gb/s. These statistics include frame and error counts. The next sections provide details about how to use the equipment to get network statistics.

3.1. Global Frame Analysis

Statistics for Port A and Port B are identical. Most of the results are given for each interface transmitter and receiver. Global frame statistics are controlled by the RUN button. That means that results are not collected if a test is not started before. Once the test is running results are upgraded in real time.

To display the transmitter statistics follow these step sequence:

1. From the *Home* panel, go to *Results*,
   The test port results panel is displayed.
2. Enter in *TX frame analysis*.
3. Check the *Frames*, *Bytes*, *Broadcast frames*, *Multicast frames*, *Control frames, Tagged frames* and *FCS errored frames* counters.

Table 3.1: TX Frame Analysis

Metric	Description
Frames	Total number of frames transmitted by one tester port since the test started.
Bytes	Total byte count transmitted by the test port from the beginning of the test. One byte is defined as an 8-bit word.
Broadcast frames	Total number of Ethernet broadcast frames transmitted from the beginning of the test. Broadcast frames carry the broadcast Ethernet address (*FF:FF:FF:FF:FF:FF*) in the destination field.

Table 3.1: TX Frame Analysis

Metric	Description
Multicast frames	Transmitted Ethernet multicast frames from the beginning of the test. Ethernet multicast frames have their multicast bit in their destination MAC address set to '1'. The multicast bit of a MAC address is the least significant bit of the more significant address byte.
Control frames	Total number of Ethernet MAC control and supervision frames transmitted from the beginning of the test. Ethernet control frames are recognised due to an special Ethertype (Type / Length field) value (*0x8808*).
Tagged frames	Total number of Ethernet VLAN frames transmitted from the beginning of the test. IEEE 802.1Q VLAN frames contain an special Ethertype (Type / Length field) value (*0x8100*).
FCS errored frames	Frames with FCS errors transmitted from the beginning of the test. An FCS errored frame may be the result of bit error insertion or a forwarded frame with a previous FCS error.

The procedure to get the statistics corresponding to the receiver is similar to the mechanism already described. These are the steps to follow:

1. From the *Home* panel, go to *Results*,
   The test port results panel is displayed.
2. Enter in *RX frame analysis*.
3. Check the *Frames*, *Bytes*, *Broadcast frames*, *Multicast frames*, *Control frames*, *Flow control frames*, *Tagged frames*, *Oversized frames*, *Undersized frames*, *Jabbers* and *FCS errors* counters.

Net.Storm does not automatically drop frames with errors. If configured in pass-through mode, errored frames are forwarded if possible. However, Net.storm is unable to add impairments to frames with errors. They are, therefore, resent without any alteration.

Table 3.2: RX Frame Analysis

Metric	Description
Frames	Total number of frames received by one tester port since the test started.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Table 3.2: RX Frame Analysis

Metric	Description
Bytes	Total byte count received by the test port from the beginning of the test. One byte is defined as an 8-bit word.
Broadcast frames	Total number of Ethernet broadcast frames received from the beginning of the test. Broadcast frames carry the broadcast Ethernet address (*FF:FF:FF:FF:FF:FF*) in the destination field.
Multicast frames	Received Ethernet multicast frames from the beginning of the test. Ethernet multicast frames have their multicast bit in their destination MAC address set to '1'. The multicast bit of a MAC address is the least significant bit of the more significant address byte.
Control frames	Total number of Ethernet MAC control and supervision frames received from the beginning of the test. Ethernet control frames are recognised due to an special Ethertype (Type / Length field) value (*0x8808*).
Flow control frames	Total number of Ethernet *Pause* frames received from the beginning of the test. Pause frames are an special type of control frames and therefore their Ethertype is 0x8808. The specific features of *Pause* frames is that their *Opcode* field is 0x0001 and their destination MAC address is *01:80:C2:00:00:01* (a multicast MAC address).
Tagged frames	Total number of Ethernet VLAN frames received from the beginning of the test. IEEE 802.1Q VLAN frames contain an special Ethertype (Type / Length field) value (*0x8100*).
FCS errored frames	Count of all the FCS errors detected from the beginning of the test. A frame with a FCS error is a frame with a legal size which contains an invalid FCS field. FCS errors are caused by transmission errors. An optical Ethernet link with a poor power budget may experience FCS errors
Oversized frames	Total number of received frames which are larger than the configured MTU.
Undersized frames	Total number of received frames which are smaller than 64 bytes.

Table 3.2: RX Frame Analysis

Metric	Description
Jabbers	Jabber count from the beginning of the test. A Jabber is defined as a frame greater than 1518 bytes with a bad CRC.

3.2. Frame Size Histogram

Frame size is important because it tell how a network is used. Some applications, like VoIP use short frames while most data applications based on a client / server use short frames length for the client requests and long frames for the server replies. The ALBEDO Telecom Net.Storm provides frame size results as described in standard RFC 2819. The procedure for displaying the received frame size histogram is as follows:

1. From the *Home* panel, go to *Results*,
   The test port results panel is displayed.
2. Enter in *Frame size histogram*.
3. Check the frame size intervals: *size 64 or less*, 65 - 127, *128-255*, *256 - 511*, *512-1023*, *1024 - 1518*.

3.3. The LEDs Panel

The LEDs panel offers a quick view of the current Net.Storm connection and operation status. They are permanent indicators. That means that no test has to be started to get the information from the LEDs.

There are two hardware global summary LEDs in the equipment (one for Port A and one for Port B), four summary LEDs for each test port (*Link*, *Frame*, *Error* and *Action*). These summary LEDs summarize the information of the events shown in the LEDs

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

panel. To display the LEDs panel use the LEDS key. If the LEDs panel is already visible press LEDS again to return to the previous screen.

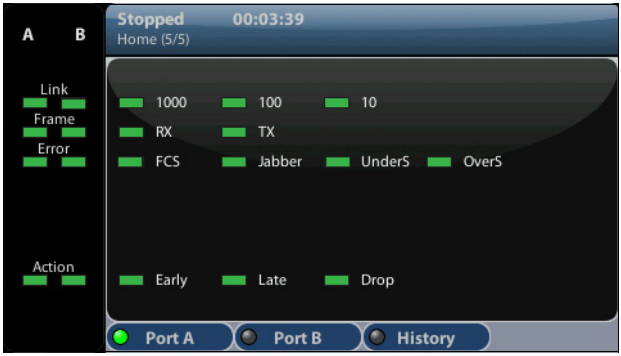

Figure 3.1: Albedo Net.Storm LEDs panel.

The LEDs have two operation modes:

- *Live*: Events are shown in real time. If something happens the corresponding LEDs change their colour to signal the event. LEDs return to their original status once the event disappears.
- *History*: The LEDs keep their original Anomaly / Defect status when the event disappears. This is useful when the tester is left a long time under operation and the user wants to receive quick feedback of past events.

The live or history modes can be configured from the LEDs panel by means the contextual keyboard. The *History* (F3) contextual button sets or unsets the history mode. If the history mode is enabled, then the Reset (F4) button resets the LEDs history.

Orange is used to signal anomalies and red indicates defects but there are more possible LED status:

- : OK, the event or events that correspond with the LED are not found in the incoming signal.
- and : This is the colour displayed if faulty conditions are found in the signal. Conditions marked with tend to be more important than the ones marked with .
- : Shows that no operation condition can be established due to the lack of matching traffic for the corresponding event. For example, the FCS led is if no traffic is received because there are no frames where to check the FCS. It can

also indicate that the LED has been disabled due to the presence of a more important event.

Table 3.3: LED Indications

Metric	Description
1000	The port is operating at 1000 Mb/s either from the optical or the electrical port. Port speed is decided immediately after connecting the port to the test interface using Ethernet auto-negotiation. Bit rate negotiated for one specific port depends on the auto-negotiation results for the second port.
100	The port is operating at 100 Mb/s from the electrical port. Port speed is decided immediately after connecting the port to the test interface using Ethernet auto-negotiation. Bit rate negotiated for one specific port depends on the auto-negotiation results for the second port.
10	The port is operating at 10 Mb/s from the electrical port. Port speed is decided immediately after connecting the port to the test interface using Ethernet auto-negotiation. Bit rate negotiated for one specific port depends on the auto-negotiation results for the second port.
RX	At least one frame was received during the current second in the current interface.
TX	At least one frame was transmitted during the current second in the current interface. Transmitted frames may come from the second port receiver but they can also be internally generated (by means a frame duplication event, for example).
FCS	At least one frame with FCS errors have been found during the current second. A frame with a FCS error is a frame with a legal size which contains an invalid FCS field. FCS errors are caused by transmission errors. An optical Ethernet link with a poor power budget may experience FCS errors
Jabber	At least one jabber was received during the current second. Jabbers are defined as frames greater than 1518 bytes with a bad CRC.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Table 3.3: LED Indications

Metric	Description
UnderS	At least one undersized frame was received during the current second. An undersized frame is a frame which has a size smaller than 64 bytes.
OverS	At least one oversized frame was received during the current second. An oversized frame is a frame which has a size larger than the configured MTU.
Overflo	The *Overflo* event applies to the shaping filter only. It indicates that, within the current second, the filter has been unable to apply the correct delay to at least one frame. If there are no transmission tokens available, the shaping filter delays the traffic to ensure that the outgoing bit rate will not exceed the filter rate. However, the delay could never exceed 60 seconds. The tester applies the maximum delay to all frames affected by the *Overflo* condition. The *Overflo* event is a condition that may arise when the in coming rate and the shaping rate are small enough to generate very large delays (larger than 60 s) without filling completely the temporary storage space (and therefore generating a *Drop* event). *Overflo* events are fault conditions that should never be registered if there is no event insertion.
Late	The *Late* event indicates that, within the current second, at least one frame has abandoned the equipment after expected. This event is related with congestion of the outgoing interface. If the departure time for a frame is scheduled for an specific time but the outgoing interface is busy during this specific time, the departure will have to be delayed, thus generating a *Late* event. *Late* is a fault condition that is only registered under heavy traffic load but it should never happen under normal operating conditions.

Table 3.3: LED Indications

Metric	Description
Drop	The *Drop* event indicates that, within the current second, at least one frame has been discarded for forwarding and subsequent transmission. *Drop* events are related with congestion in the internal Net.Storm storage space. Packets are discarded if there is storage available

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Chapter 4
Multi-stream Analysis

Net.Storm is capable of processing and computing statistics over fractions of the Ethernet traffic meeting specific conditions. The process of selecting a fraction of traffic is called filtering. The result of the filtering process is one or several traffic streams called flows.

This chapter describes how to configure Net.Storm for packet filtering and how to get basic flow statistics. Information about inserting impairments on Ethernet flows is explained in a dedicated chapter.

4.1. Enabling and Disabling Filters

Traffic selection or filtering is configured by first enabling one or several filtering blocks and after that setting the filtering rule. Net.Storm supports Ethernet, VLAN, IPv4 and TCP / UDP filters.

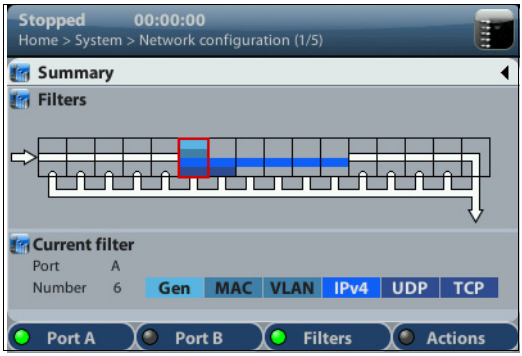

Figure 4.1: Filter setup panels. Filter status can be checked from this panel. It is also possible

5. The ALBEDO Telecom Net.Storm is equipped with 15 filters plus one special filter for background traffic (*Default* filter). Each filter has a priority number. If one frame is selected by an specific filter it will not be processed by any lower priority filters. The Default filter as the lowest priority of all filters to ensure that it will only process traffic not accepted by any other filter.

Current status of all filters can be checked at any moment with the help of the filter summary panel by pressing the SUM key and enabling Filters for *Port A* or *Port B.*

4.2. Configuring Filters

If a filter is left with its default configuration, it will not accept any frame. To allow the filter to accept and process frames, a correct filtering rule must be configured before.

To configure the correct filtering rule two decisions must be taken. First, it is necessary to know which frame fields are going to be matched and after that, which are the value or values to be matched. The first decision involves choosing whether the filtering is going to be done at MAC, IP or transport layer and which specific frame field or fields are going to be used for filtering (MAC addresses, IP addresses, Ethertype field, protocol or any other). The second is carried out by configuring the field value and sometimes a mask. The mask selects which field bits are taken into account when a frame is matched. Matching masks are not related to IP subnet masks even if they can be applied to IP addresses. Specifically, the binary representation of a matching mask does not need to be a sequence of '1' followed by a sequence of '0' like IP network masks are.

The generic procedure to configure one or several matching rules with Net.Storm is the following:

1. From the *Home* panel, go to *Setup*,
   The test port settings panel is displayed.
2. Select either *Port A or Port B* to enter in the port specific configuration.
3. Select one of the filtering menus labelled as *Filter 1*, *Filter 2*, etc.
4. Enable the filter by setting the *Block* field to the value *No*.
   Different types of filtering rule families are enabled for that filter: *Generic selection*, *MAC selection*, *VLAN selection IPv4* selection, *TCP selection*, *UDP selection*.
   Select the matching rule family.
5. Choose a matching field and configure de matching mode for this field. Most of the matching fields have at least two matching modes. The *Equal* mode selects frames matching the configured value or values for the field and *Ignore* does not match any frame by the current field. Other matching modes may be available in specific fields.
6. Configure the field value to be matched by the filter.
7. If the matching field has this capability, enter the mask value. To select a single value, set of the mask bit values to all ones.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

8. Optionally, configure more matching rules for the current filter by repeating steps 3, 4, 5, 6 and 7 as many times as necessary.

Quick information about currently matching rules for each filter is available in the *Filter setup* panel. The Default filter does not accept the same configuration than the other 15 filters. Specifically, the *Default* filter is a permanent filter that it does not accept the configuration of filtering rules based on the values of any frame field.

4.2.1. MAC Selection

MAC frames are envelopes in which the Ethernet frames are sent and received. MAC frame format is currently specified by the standard IEEE 802.3. This format is shared by all existing Ethernet interfaces thus making Ethernet the most scalable transmission technology currently available.

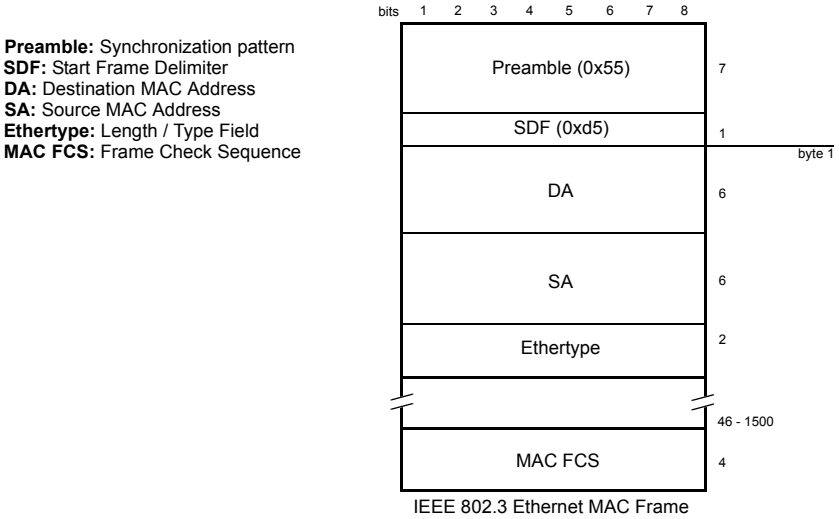

Figure 4.2: IEEE 802.3 frame structure

The ALBEDO Telecom Net.Storm provides frame selection based on the MAC address source and destination and Ethertype value. It is possible to configure a matching mask for all three fields to select a value set rather than a single value.

Table 4.1: MAC Selection

Metric	Description
Source address selection	Enables selection by source MAC address in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: The source MAC address is ignored and not taken into account for the purpose of the filter. All frames are allowed to pass through the filter when *Ignore* is configured if they are not blocked by other selection rule. • *Equal with mask*: All frames matching a user configurable pattern are allowed to pass through the filter. The matching pattern is configured with the help of the *Source address* and *Source address mask* fields.
Source address	This is a 48-bit MAC address in the standard hexadecimal-digit format *XX:XX:XX:XX:XX:XX*. Source addresses matching some or all bits of the address configured here will be allowed to pass through the filter. Bits used for matching frames to this filter are configured in the *Source address mask*.
Source address mask	This is the mask for the source MAC address filter selection rule. Before comparing the *Source address* field with the frame addresses, bit wise AND operations are carried out between the value configured here and the *Source address* field so that only the values surviving the AND are taken into account for matching the filter.
Destination address selection	Enables selection by destination MAC address in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source address selection* setting.
Destination address	This is a 48-bit MAC address in the standard hexadecimal-digit format *XX:XX:XX:XX:XX:XX*. Destination addresses matching some or all bits of the address configured here will be allowed to pass through the filter. Bits used for matching frames to this filter are configured in the *Destination address mask*.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Table 4.1: MAC Selection

Metric	Description
Destination address mask	This is the mask for the destination MAC address filter selection rule. Before comparing the *Destination address* field with the frame addresses, bit wise AND operations are carried out between the value configured here and the *Destination address* field so that only the values surviving the AND are taken into account for matching the filter.
Ethertype selection	Enables selection by Ethertype value in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source address selection* and *Destination address selection* settings.
Ethertype	This setting contains a 2-byte field that constitutes the Ethertype value to be matched in the incoming traffic. Ethertypes matching some or all bytes of the value configured here will be allowed to pass through the filter. Bits used for matching frames to this filter are configured by means the *Ethertype mask*.
Ethertype mask	This is the mask for the Ethertype filter selection rule. Before comparing the *Ethertype* field with the frame Ethertype, bit wise AND operations are carried out between the value configured here and the *Ethertype* field so that only the values surviving the AND are taken into account for matching the filter.

4.2.2. VLAN Selection

Within enterprise networks, VLANs are important because they enable network segmentation on an organisational basis, by functions, project teams or applications, rather than on a physical or a geographical basis. The network can be reconfigured through software, instead of physically unplugging and moving devices or wires.

VLANs are an important contribution to scalable Ethernet networks, because they limit broadcast traffic inherent to the bridging mechanism. Large amounts of broadcast traffic may damage performance and even collapse network equipment, which is why it must be controlled.

Standard IEEE 802.1Q specifies the most popular VLAN frame format. VLAN frames carry a 16-bit header which specifies the VLAN Identifier (VID) and the frame priority within the VLAN. Many carrier Ethernet networks use the VID for segmentation just like enterprises. The VID in carrier Ethernet networks is used by service providers as

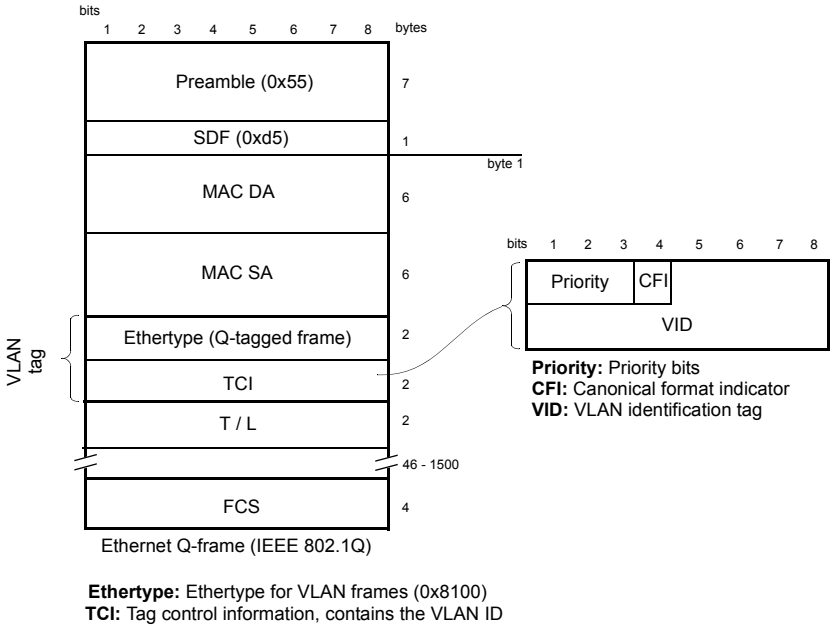

Figure 4.3: IEEE 802.1Q frame structure

general purpose identifiers. They can be associated to an specific service, customer, node or several of them at the same time.

Net.Storm provides frame selection based on the VLAN tag based either in the VID or the priority bits.

Table 4.2: VLAN Selection

Metric	Description
VID selection	Enables selection by VID in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: The VID is ignored and not taken into account for the purpose of the filter. All frames are allowed to pass through the filter when *Ignore* is configured if they are not blocked by other selection rule. • *Equal*: All frames matching a user configurable pattern are allowed to pass through the filter. The matching pattern is configured with the help of the *VID* field.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Table 4.2: VLAN Selection

Metric	Description
VID	This setting contains a 10-bit identifier that constitutes the VID value to be matched in the incoming traffic.
Priority bits selection	Enables selection by IEEE 802.1Q/p priority bits in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *VID selection* field.
Priority bits	This setting contains a 3-bit identifier that constitutes the priority value to be matched in the incoming traffic.

4.2.3. IPv4 Selection

The Internet Protocol version 4 (IPv4) was conceived by the U.S. *Department of Defence* (DoD) to facilitate communication between dissimilar computer systems and is a reliable technology. The IPv4 constitutes the most important protocol of the Internet and it is today widely used to connect heterogeneous packet networks everywhere.

IP is based on variable length data packets called datagrams. The datagram header includes two 32-bit addresses that identify the datagram source and destination and other fields with miscellaneous purposes.

Net.Storm filtering capabilities can be programmed to match fields within the IPv4 datagram. It is currently supported IP datagram matching based on source IP address, destination IP address, protocol and DSCP. Source and destination IP addresses can be matched by means selection masks.

Table 4.3: IPv4 Selection

Metric	Description
Source address selection	Enables selection by source IPv4 address in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: The source IP address is ignored and not taken into account for the purpose of the filter. All frames are allowed to pass through the filter when *Ignore* is configured if they are not blocked by other selection rule. • *Equal with mask*: All frames matching a user configurable pattern are allowed to pass through the filter. The matching pattern is configured with the help of the *Source address* and *Source address mask* fields.

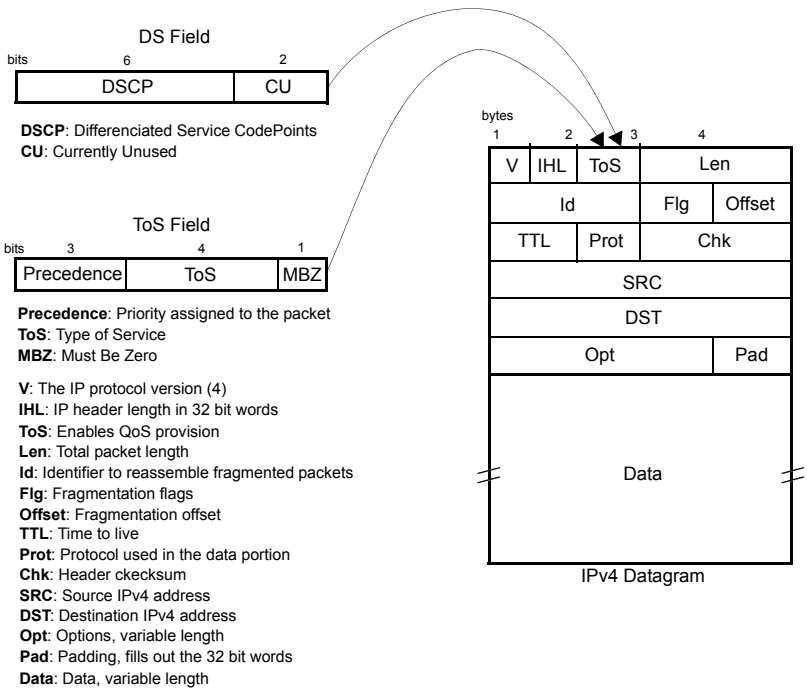

Figure 4.4: IPv4 Datagram structure

Table 4.3: IPv4 Selection

Metric	Description
Source address	This is a 32-bit IPv4 address in the standard four-dotted decimal format *A.B.C.D*. Source addresses matching some or all bits of the address configured here will be allowed to pass through the filter. Bits used for matching frames to this filter are configured in the *Source address mask*.
Source address mask	This is the mask for the source IPv4 address filter selection rule. Before comparing the *Source address* field with the frame addresses, bit wise AND operations are carried out between the value configured here and the *Source address* field so that only the values surviving the AND are taken into account for matching the filter.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Table 4.3: IPv4 Selection

Metric	Description
Destination address selection	Enables selection by destination IPv4 address in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source address selection* setting.
Destination address	This is a 32-bit IPv4 address in the standard four-dotted decimal format *A.B.C.D*. Destination addresses matching some or all bits of the address configured here will be allowed to pass through the filter. Bits used for matching frames to this filter are configured in the *Destination address mask*.
Destination address mask	This is the mask for the source IPv4 address filter selection rule. Before comparing the *Source address* field with the frame addresses, bit wise AND operations are carried out between the value configured here and the *Source address* field so that only the values surviving the AND are taken into account for matching the filter.
Protocol selection	Enables selection by the 1-byte IPv4 protocol field in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: The *Protocol* field is ignored and not taken into account for the purpose of the filter. All frames are allowed to pass through the filter when *Ignore* is configured if they are not blocked by other selection rule. • *Equal*: All frames matching a user configurable pattern are allowed to pass through the filter. The matching pattern is configured with the help of the *Standard protocol selection* field and *Protocol* fields.

Table 4.3: IPv4 Selection

Metric	Description
Standard protocol selection	Configures the protocol to be filtered when protocol selection is enabled. The available configuration values are the following: • *UDP*: Matches traffic with a *User Datagram Protocol (UDP)* envelope. Traffic commonly transported over UDP includes IP voice, IP video and DNS. • *TCP*: Matches traffic carried over the Transfer Control Protocol (TCP). Most data applications (web, file transfer, e-mail...) ere normally based on TCP transport. • *ICMP*: *Matches Internet Control Message Protocol* packets. IP operation and maintenance traffic like ping use ICMP. • *Numeric*: Use this control if the traffic to be matched is different of UDP, TCP and ICMP and it has an specific protocol identifier assigned by the IANA.
Protocol	This setting contains an 8-bit word that constitutes the protocol identifier to be matched in the incoming traffic. Configuring this field to 17 is equivalent of setting the *Standard protocol selection* to UDP. TCP uses 6 as the protocol number and ICMP uses number 1. This control is enabled only if Standard protocol selection has been previously set to *Numeric*.
DSCP selection	Enables selection by the 6-bit DSCP field in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source address selection* field.
DSCP	This setting contains a 6-bit word in decimal format that constitutes the DSCP to be matched in the incoming traffic.

4.2.4. TCP Selection

The IP protocol does not offer reliable end-to-end communications. This capability is one of the attributions of the transport layer that operates above the IP layer. The

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Transfer Control Protocol offers error recovery mechanisms that enable reliable data transmission over IP.

Table 4.4: TCP Selection

Metric	Description
Source port selection	Enables selection by source TCP port in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: The sourceport is ignored and not taken into account for the purpose of the filter. All frames are allowed to pass through the filter when *Ignore* is configured if they are not blocked by other selection rule. • *In range*: All frames with a destination port in an specified range are allowed to pass through the filter. The port range is specified with the help of the *Minimum source port* and *Maximum source port* fields.
Minimum source port	This is the minimum 16-bit TCP source port allowed to pass through the Source port selection filter. The port is configured and displayed in decimal format.
Maximum source port	This is the maximum 16-bit TCP source port allowed to pass through the Source port selection filter. The port is configured and displayed in decimal format.
Destination port selection	Enables selection by the 2-byte TCP protocol field in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are the same that for the *Source address selection* field.
Minimum destination port	This is the minimum 16-bit TCP destination port allowed to pass through the Destination port selection filter. The port is configured and displayed in decimal format.
Maximum destination port	This is the maximum 16-bit TCP destination port allowed to pass through the Destination port selection filter. The port is configured and displayed in decimal format.

TCP also offers a communication channel for IP applications. Applications speak through special 16-bit identifiers called ports in the same way that hosts use IP addresses. Net.Storm filtering capabilities include matching of TCP source and destination ports in each of the filtering blocks.

4.2.5. UDP Selection

Some applications do not require reliable transmission at the transport layer either because they implement their own error control mechanisms or because the mechanisms used by TCP are too slow for them. These applications can use the light weight User Datagram Protocol (UDP). Like TCP, UDP provides communications through ports to applications but it doesn't have any error recovery capability.

Net.Storm features related with UDP are equivalent to the TCP capabilities, including matching of the source and destination UDP ports.

4.2.6. Generic Selection

Generic selection is the matching mode to be used when the Ethernet frames carry uncommon protocols or if inspection beyond the UDP and TCP transport protocols is required. This selection mode defines an offset and a mask. Frames matching the specified mask in the configured offset are selected.

Table 4.5: Generic Selection

Metric	Description
Filter mode	Enables generic selection in the current filter. The value configured here is used to determine which frames are allowed to pass through the filter and which ones are blocked. The available configuration values for this field are: • *Ignore*: Generic matching is ignored and not taken into account for the purpose of the filter. All frames are allowed to pass through the filter when *Ignore* is configured if they are not blocked by other selection rule. • *Equal with mask*: All frames matching a user configurable pattern are allowed to pass through the filter. The matching pattern is configured with the help of the *Frame start*, *Offset (bytes)* and *Match code* fields.
Frame start	Defines the payload type and the reference point within the frame to start counting the filter offset. The reference can be the beginning of the MAC, IPv4, UDP or TCP payload depending on the chosen value. It is also possible to set the reference to the beginning of the Ethernet frame (first byte immediately after the SDF) by configuring *Start* in this field. The frame start field is shared by all the port A or port B filters. If the *Frame start* field is modified for one specific filter, the remaining filters will be set to the same value.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Table 4.5: Generic Selection

Metric	Description
Offset (bytes)	This field defines the offset expressed in bytes from the reference point defined with the *Frame start* control. The value 0 corresponds with the first byte of the MAC, IPv4, UDP or TCP payload (or the first frame byte, if *Frame start* is set to *Start*). If due to the limited frame size, some or all the byte positions defined by the *Offset (bytes)* field, do not exist in the corresponding payload, the equipment will consider that the frame does not match the filtering rule. The offset field is shared by all the port A or port B filters. If the *Offset (bytes)* field is modified for one specific filter, the remaining filters will be set to the same value.
Match code	16-bit code expressed with four hexadecimal digits used to match frames.in the current filter.
Mask	This is a mask for the generic filter match code. Before comparing the *Match code* with the selected bytes in the Ethernet frame, bit wise AND operations are carried out between the value configured here and the *Match code* field so that only the values surviving the AND are taken into account for matching the filter.

4.3. Getting Statistics about Filters

Once the filter has been configured, it is usually desirable to know how many matching frames have been found for each filter. In case some action as been set for the filters it is desirable to know how many frames have been affected.

To get statistics about filtered frames follow this procedure:

1. From the *Home* panel, go to *Results*,
   The test port results panel is displayed.
2. Select Filter statistics.
   Matched and Accepted frame counts are displayed for each filter (including the BG filter).

Table 4.6: Filter statistics

Metric	Description
Matches A / Matches B	Count of all frames matching the selection rules for the current filter in Port A or Port B.

Table 4.6: Filter statistics

Metric	Description
Accepted A / Accepted B	Number of frames accepted by the filter in Port A or Port B. If there are no actions defined for the filter, the number of accepted frames is always the same that the number of matched frames. If there are frame loss impairments enabled in the filter, the number of accepted frames could be smaller than the number of matched frames. If there is frame duplication, the accepted frames count could be larger than the matched frames count. Delay impairments do not modify the number of frames in the flow but they may affect the time they are registered by the *Accepted frames* counter.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Chapter 5
Inserting Events

Current Metro Ethernet networks are QoS-capable Ethernet network that offers services beyond the classical best-effort LAN Ethernet services. These services can be, for instance, Time-Division Multiplexing (TDM) circuit emulation, Voice over IP (VoIP) or Video on Demand (VoD).

Native Ethernet, however, as a best-effort technology, does not provide customized QoS. To maintain QoS, it is necessary to carry out a number of operations, such as traffic marking, traffic conditioning and congestion avoidance.

It is essential to check that network nodes and software will operate as expected under non-ideal network operation circumstances. ALBEDO Telecom Net.Storm has the ability to generate the impairments that are commonly found in packet-switched networks like Ethernet / IP networks. Net.Storm is able to generate delay, frame loss and other network impairments using both deterministic or random insertion modes.

Despite being based on random impairment generation, the events inserted by Net.Storm are always strictly controlled. This is the essential difference between a Net.Storm simulation and the real network.

5.1. Introduction to Performance Metrics for Ethernet

The first step in offering QoS is to find a set of parameters to quantify and compare the performance of the network. QoS is provided by the network infrastructure, but experienced by the users. This is the reason why QoS is specified by means of end-to-end parameters.

5.1.1. One-way Delay

The end-to-end one-way delay experienced by a frame when it crosses a path in a network is the time it takes to deliver the frame from source to destination. This delay is the sum of delays on each link and node crossed by the frame.

The Round Trip Delay (RTD), is a parameter related to one-way delay. It is the delay of a frame on its way from the source to the destination and back. RTD is easier to

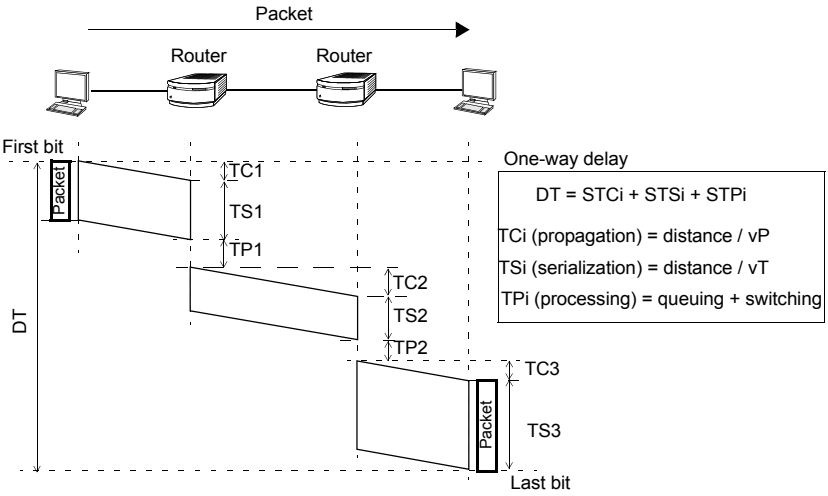

Figure 5.1: One-way delay is the sum of delays on each link and node crossed by a frame.

evaluate than other delay parameters, because it can be measured from one end with a single device. Frame timestamping is not required, but a marking mechanism of some kind is needed for frame recognition. The one popular RTD tool is Ping. This tool sends Internet Control Message Protocol (ICMP) echo request messages to a remote host, and receives ICMP echo reply messages from the same host.

There are three types of one-way delay:

- *Processing delay* is the time needed by the switch to process a frame.
- *Serialization delay* is the delay between the transmission time of the first and the last bit of a frame. It depends on the size of the frame.
- *Propagation delay* is the delay between the time the last bit is transmitted at the transmitting node and received at the receiving node. It is constant, and it depends on the physical properties of the transmission channel.

5.1.2. One-way Delay Variation

The one-way delay variation of two consecutively transmitted frames is the one-way delay experienced by the last transmitted frame, minus the one-way delay of the first frame. The one-way delay variation is sometimes referred to as frame jitter.

In packet-switched networks, the main sources of delay variation are: variable queuing times in the intermediate network elements, variable serialization and processing time of frames with variable length, and variable route delay when the network implements load-balancing techniques to improve utilization.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

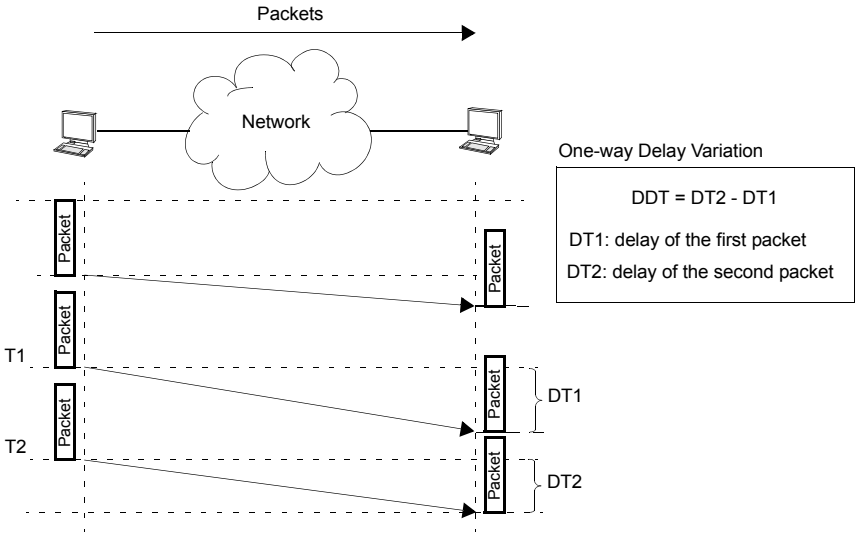

Figure 5.2: One-way delay variation: measurement and impact on data periodicity

5.1.3. Frame Loss

A frame is said to be lost if it does not arrive to its destination. It can be considered that frames that contain errors or arrive too late are also lost.

Frame loss may occur when transmission errors are registered, but the main reason behind these events is network congestion. Intermediate nodes react to high traffic load conditions by dropping frames and thus generating frame loss. Congestion tends to group loss events, and this harms voice and video decoders optimised to work with uniformly distributed loss events.

5.1.4. Frame Corruption and Duplication

The most important and potentially harmful events in packet-switched networks are the frame loss and (variable or fixed) delay. However, there are other events that must be studied and considered. This section provides some information about corrupted frames and duplicated frames:

- *Errored and corrupted frames*: Like it happens in any other digital signal, the Ethernet frame flow is made up of bits. As they are transmitted through the network, Ethernet frame content may be altered by noise, interferences and other effects. Frames are protected with an error detection code carried in the FCS field. As a result of the FCS, bit errors caused by noise are detected by network elements. Frames with errors are discarded and for this reason, frame loss is closely

related with frame errors in Ethernet networks. Sometimes, due to different reasons, the Ethernet payload may carry errors but the FCS is correct. These corrupted frames are not detected by Ethernet equipment and they are passed to the higher levels of the protocol stack like the IP layer.

- *Duplicated frames*. Duplicated frames are caused due to some wrong configurations in routers. Miss-connected Ethernet bridges are likely to cause frame multiplication too. Receivers usually have the means to discard duplicated frames but duplicated frames still waste bandwidth and may even consume large amounts of transmission capacity.

5.2. Adding Impairments to Ethernet Traffic

With the help of Net.Storm you can add impairments such as frame delay, frame delay variation and frame loss to Ethernet frames as they pass through the equipment.

Impairments can be added to all Ethernet frames or a fraction of the traffic. This section explains how to add impairments to every frame and the next one explains how to use filters to add impairments to some part of the traffic meeting one or several conditions.

5.2.1. Frame Loss

Net.Storm provides several frame loss insertion mode. Some of them are very simple like the insertion of single frame loss event. Some others are more sophisticated. For example, the random insertion with to states with different frame loss probabilities.

Table 5.1: Frame Loss Insertion

Metric	Description
Mode	Specifies to the test unit the way the frame loss events are inserted into the traffic flow. The available choices are the following: • *None*: Disables frame loss insertion. No frame loss will be inserted if this mode is selected. • *Single*: One single frame loss is inserted in the first insertion opportunity after pressing the EVENT button. • *Timed burst*: Drops a sequence of consecutive frames within a configurable time period after pressing the EVENT button. • *Frame burst*: Drops a configurable number of consecutive frames after pressing the EVENT button. • *Timed periodic burst*: Drops periodic frame bursts. The time periods corresponding to frames to be dropped and frames to be transmitted are configurable.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Table 5.1: Frame Loss Insertion

Metric	Description
Mode	• *Frame periodic burst*: Drops periodic frame bursts. The number of frames that makes up each loss burst and the separation between loss bursts specified in frames are configurable. • *Random*: Packets are randomly dropped with a configurable constant probability. • *Two-state random*: This simulates a transmission channel with two different loss probabilities. This is useful for modelling channels experiencing temporary or periodic interferences.
Burst length (s)	Frames received during the time interval specified in this field are all dropped. If no frame is received within the specified period then no frame is dropped. This parameter makes sense if the frame loss insertion *Mode* is set to *Burst (s)* or *Periodic burst (s)*. If the current mode is *Burst (s)* the frame drop interval starts just after the EVENT key is pressed. If the mode is Periodic burst (s), drop events are periodically inserted after pressing EVENT. The separation between frame drop events is specified with the *Burst separation (s)* parameter.
Burst length (fr)	Specifies how many frames make up a loss burst in the *Burst (fr)* and *Periodic burst (fr)* insertion modes. If the current mode is *Burst (fr)* then the next *Burst length (fr)* frames ready to be transmitted after pressing EVENT will be dropped. If the mode is *Periodic burst (fr)* then loss bursts will be periodically inserted. Separation (specified in number of frames) between consecutive loss bursts is specified with the help of the *Burst separation (fr)* parameter.
Burst separation (s)	Specifies the separation in time units between consecutive loss bursts when the current insertion mode is *Periodic burst (s)*.
Burst separation (fr)	Specifies the separation in number of frames between consecutive loss bursts when the current insertion mode is *Periodic burst (fr)*.
Loss probability	If the insertion mode is set to *Random,* this is the probability of a single packet loss event. This parameter also has a meaning when the mode is *Two-state random*. In this case it sets the loss probability of one of the two possible states defined for this insertion mode.

Table 5.1: Frame Loss Insertion

Metric	Description
Alternative loss prob.	Configures the loss probability of the second state when the mode is set to *Two-state random*. The fists state loss probability is configured with the *Loss probability* field
Mean length (fr)	Configures the average length in number of frames of the first state in *Two-state random* insertion mode. The loss probability for this state is configured with the *Loss probability* field.
Mean alt. length (fr)	Configures the average length in number of frames of the second state in *Two-state random* insertion mode. The loss probability for this state is configured with the *Alternative Loss prob.* field.

Before configuring the tester for frame loss insertion, make sure that no filters are enabled but the *Default* filter (see Chapter 4). To enable frame loss insertion proceed as follows:

1. From the *Home* panel, go to *Test Setup*,
   The *Test* configuration panel is displayed.
2. Select *Action*
   The event insertion menu is displayed.
3. Go to Port A or Port B depending on the traffic direction you want to impair.
   Note: If Port A and Port B are coupled, you will get the same configuration by setting either Port A or Port B.
4. Select *Default*
   Frame loss is going to be inserted in the background traffic. Background traffic is made up of all frames not previously selected by any other filter.
5. Select *Loss* to insert frame loss.
   Note: Frame loss insertion is not compatible with traffic policing (Bandwidth control filter). Some packed duplication modes and loss insertion modes are not compatible.
6. Select the insertion mode for the event selected in the previous step with the help of the *Mode* menu item. Available insertion modes *Single*, *Burst (s)*, *Burst (fr)*, *Periodic burst (s)*, *Periodic burst (fr)*, *Policing*, *Random* and *Two-state random*.
7. Configure the insertion parameters with the help of the *Burst length (s)*, *Burst length (fr)*, *Burst separation (s)*, *Burst separation (fr)*, *Rate (fr/s)*, *Queue length (fr)*, *Loss probability*, *Alternative loss prob.*, *Mean length (fr)* and *Mean alt. length (fr)* menu items.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

8. Start insertion by pressing the EVENT button.
   Note: Depending on the insertion mode, event insertion will finish automatically or you will need to press EVENT a second time to stop.

5.2.2. Delay & Jitter

Net.Storm generates delay on Ethernet frames following deterministic or random laws. The procedure for delay insertion is equivalent to the frame loss insertion setup. However, the insertion modes for delay and frame loss are different. Currently, there are four different insertion modes for delay: *Deterministic*, *Shaping*, *Random (uniform)*, *Random (exponential)*.

Table 5.2: Delay & Jitter Insertion

Metric	Description
Mode	Specifies the way the frame delay events will be added to frames. The available delay insertion modes are: • *None*: Disables delay / jitter insertion • *Deterministic*: Adds a constant configurable delay (specified in ms) to all matching frames. • *Random (uniform):* Adds a random delay to each matching frame. The probability density function in this delay insertion mode is uniform. • *Random (exponential):* Adds a random delay to each matching frame. The probability density function in this delay insertion mode is exponential.
Delay	Deterministic delay expressed in ms to be applied to all matching frames if the delay insertion mode is set to Deterministic.
Maximum delay)	Specifies the maximum delay expressed in ms to be applied to Ethernet frames by the *Random (uniform)* insertion mode.
Minimum delay	Specifies the minimum delay expressed in ms to be applied to Ethernet frames by the *Random (uniform)* insertion mode.
Average delay	Sets the average delay to be applied to Ethernet frames by the *Random (exponential)* insertion mode. Delay is not bounded when the delay insertion mode is set to *Random (exponential)*. For this reason it makes no sense to configure the maximum delay in this case.

Table 5.2: Delay & Jitter Insertion

Metric	Description
Allow reordering	This parameter enables the user to decide which the priority when generating random delay: to preserve the transmission order or the preserve the shape of the delay probability density function at the price of altering the transmission packet ordering. This parameter makes sense only if the inter-frame time is of the same order or smaller than the inserted jitter. Not allowing reordering preserves the transmission order but in this case the equipment may be unable to add delay to the traffic with uniform / random probability distributions. In this case the configured probability distributions are replaced by a new much more complex one with correlation between consecutive and non consecutive frames.

Random delay insertion can be used for jitter generation. Exponential or uniform delay modes can be used for this purpose. For the uniform distribution, the maximum and minimum delay are bounded and therefore the delay variation is bounded as well. The maximum delay is unbounded when the distribution is exponential and the jitter is also unbounded in this case.

Delay insertion capabilities depend on the incoming bit rate and frame size. Maximum delay is 20 ms with worst case transmission (64 kb/s frames, 100% of traffic load). Under lighter traffic load or longer frames, the maximum delay available increases but it can never exceed 60 s in any case.

Table 5.3: Maximum Delay for Different Traffic Loads and Frame Lengths

	100 kb/s	10 Mb/s	500 Mb/s	1 Gb/s
64 bytes	60.00 s	2.20 s	40 ms	20 ms
128 bytes	60.00 s	3.88 s	80 ms	40 ms
512 byes	60.00 s	13.95 s	280 ms	140 ms
1518 bytes	60 00 s	40.32 s	810 ms	400 ms
10000 bytes	60.00 s	60.00 s	2.00 s	1.00 s

5.2.3. Bandwidth

Bandwidth control filters are useful in case the user is interested in simulating links of custom bandwidth smaller than the nominal channel capacity (10 Mb/s, 100 Mb/s, 1000 Mb/s).

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Users have at their disposal two different bandwidth control modes. Bandwidth control by means a policing filter preserves data stream timing but not-conforming packets are lost. Usually, policing is considered best in delay sensitive applications like VoIP. On the other hand bandwidth control by means a shaping filter tends to preserve the information but it may alter the timing of the original data stream. Shaping uses to be the preferred bandwidth control mechanism in data networks.

Table 5.4: Bandwidth Control

Metric	Description
Mode	Specifies the way the bandwidth control mode to be used by the filter. The available modes are: • *None*: Disables bandwidth control. • *Shaping*: Simulates a shaping filter. The shaping filter is allowed to transmit one frame per each 'token' stored in its 'token bucket'. The bucket is filled with new tokens at a constant rate to replace the ones spent in transmitted frames. If one packet finds no token in the bucket then it waits in a temporary buffer until a token is available. • *Policing*: Simulates a policing filter. A policing filter is allowed to transmit one frame per each 'token' stored in a virtual buffer known as 'token bucket'. The bucket is filled with new tokens at a constant rate to replace the ones spent in transmitted frames. If one frame finds no token in the bucket when is going to be transmitted then it is automatically dropped.
Rate (fr/s)	It is the rate at which new tokens fill the bandwidth control filter (policing or shaping) 'token bucket'. The *Rate (f/s)* value corresponds to the sustainable rate supported by the bandwidth control filter which does not add extra delay or drops any frame.
Maximum burst size (fr)	Configures the buffer size ('token bucket' size) if the insertion mode is set to *Policing* or *Shaping*. The *Maximum bust size (fr)* enables the user to add flexibility to the decision about whether one frame is conforming or not when the incoming rate is larger than the configured filtering rate.

5.2.4. Frame Duplication

Net.Storm supports frame duplication of Ethernet traffic. If duplication is used, the equipment will generate duplicated traffic for some incoming frames. If duplication is enabled, the resulting outgoing traffic could be higher than the incoming traffic. That means that for very high traffic load the outgoing traffic could become higher than the

nominal line capacity. For this reason, duplication has to be used with care. If the delay block is disabled, duplicated frames are immediately transmitted after the original ones. If there is delay insertion, timing of duplicated frames is controlled by the delay block.

Net.Storm has two frame duplication modes. One of them is deterministic (*Single* event insertion) and the other one is random (*Random* event insertion).

Table 5.5: Frame Duplication Insertion

Metric	Description
Mode	Specifies to the test unit the way the frame duplication events are inserted into the traffic flow. The available choices are the following: • *None*: Disables frame duplication insertion. No frame will be duplicated if this mode is selected. • *Single*: One single frame duplicated in the first duplication opportunity after pressing the EVENT button. • *Random*: Packets are randomly duplicated with a configurable constant probability.
Duplication prob. (%)	If the insertion mode is set to *Random,* this is the probability of a frame duplication event.

5.2.5. Frame Errors

Net.Storm currently supports error insertion without FCS regeneration. Specifically, the, Net.Storm error insertion capability modifies the FCS field of selected Ethernet frames. These frames are detected as frames containing bit errors by network elements.

Net.Storm has two frame error insertion modes. One of them is deterministic (*Single* event insertion) and the other one is random (*Random* event insertion)

Table 5.6: Frame Error Insertion

Metric	Description
Mode	Specifies to the test unit the way the frame errors are inserted into the traffic flow. The available choices are the following: • *None*: Disables frame error insertion. No frame with errors will be inserted if this mode is selected. • *Single*: One error is added in the first duplication opportunity after pressing the EVENT button. • *Random*: Errored frames are randomly inserted with a configurable constant probability.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Table 5.6: Frame Error Insertion

Metric	Description
Frame error prob. (%)	If the insertion mode is set to *Random,* this is the probability of an errored frame event.

5.3. Adding Impairments to Selected Traffic Flows

Sometimes it is required to impair some protocol or some traffic class leaving all other frames unaltered. Some networks process different traffic classes in different ways and they produce different service performance in traffic belonging to each class. Net.Storm can be used to model these environments by using the filtering capabilities available for Net.Storm.

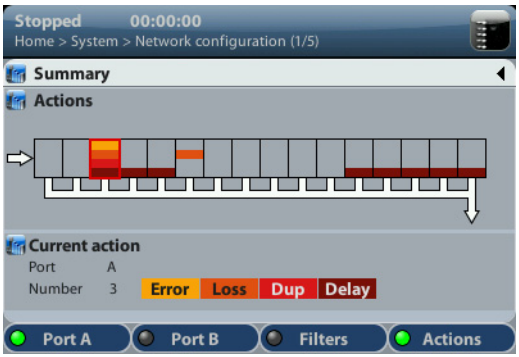

Figure 5.3: The event summary panel displays information regarding which events are being added to each filter

The sequence of frames meeting some filteringrule set by Net.Storm constitute one flow. Net.Storm can add impairments to one or several flows rather than the general traffic sequence. Users can define up to 15 flows and set specific delay and loss patters for each of them.

The procedure to add frame loss, delay or any other impairment to selected traffic flows described below.

1. Enable one or more filters and configure the matching rule for all of them (see Chapter 4)
2. From the *Home* panel, go to *Test Setup*,
   The *Test* configuration panel is displayed.
3. Select *Action*
   The event insertion menu is displayed.

4. Select either *Port A* or *Port B* to enter the port specific action menu.
5. Select *Flow 1*, *Flow 2*,..., *Flow 3*
   The impairment is going to be inserted in the flow you select. *Flow N* traffic is made up of all frames matching the filtering criteria configured for *Filter N*.
6. Select *Loss* to insert frame loss, *Delay & Jitter* to insert delay, *Bandwidth* to add a traffic control filter to the flow, *Duplication* to add frame duplication or *Bit errors* to add errored bits.
7. Select the insertion mode for the event selected in the previous step with the help of the *Mode* menu item.
8. Configure the insertion parameters with the help of the configuration parameters available for the selected insertion block.
   Note: Some insertion modes, like *Single*, do not require further configuration.
9. Repeat the previous steps over the remaining flows until all of them have been configured.
10. Start insertion by pressing the EVENT button.
    Note: Depending on the insertion mode, event insertion will finish automatically or you will need to press EVENT a second time to stop.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Chapter 6
Test Management

This chapter describes all those features available in your test unit that are not directly related with configuring your tester or reading measurement results but they are important for proper test management. Specifically, configuration and result management, report generation and test platform settings are covered in the following sections.

6.1. Generating Reports

Users may want to generate reports based on their measurements. Reports are important to save results for later reference. Reports can be used to share a test result or to include results in documents.

Depending on the purpose of the report, users have different ways to generate and store them. Net.Storm offers maximum flexibility and at the same time simplicity when configuring reports. Follow these steps to configure and generate a report:

1. From the *Home* panel, go to *File*,
   The tester file manager base menu is displayed.
2. Select *Report files* to go to the report file settings
3. Enable report generation by means the *Generate reports* control.
4. Set the *Report format*, *Report named after* and *Report header* fields.
5. If you have set *Report named after* to *User ref.+sequence*, configure the *User reference* field to the desired sequence.
6. Optionally, if you have configured *Report named after* to *User ref.+sequence* or *Serial no.+sequence*, enter the *Next sequence number* to be applied to the next report.
7. Set the correct action to be carried out when the internal storage is full.

If report generation is enabled, a new report is generated each time a test finishes either by pressing the run button or automatically. Reports are available as standard

text or PDF files from the USB slave connector and they can be exported through the USB master port, the SD card reader or the web interface.

Table 6.1: System Settings Panel

Setting	Description
Internal memory	Displays report files stored in the internal tester memory. Net.Storm can store up to 50 report files.
External devices	Displays report files stored in external devices (SD memory card, USB memories or drives) connected to the tester. The amount of files stored in an external device is only limited by the device capacity.
Generate reports	Enables / Disables report generation.
Report format	Selects the report format for future reports. • *PDF*: Reports are generated using the portable document format (PDF). Use this configuration if you want to make difficult for anyone to modify the report. • *Plain text*: Reports are text documents which can be edited with any text editor. Use this configuration if you want to modify the report or include it in a wider document.
Report named after	This control enables the user to choose between different templates for the report name. There are three different templates to choose: • *Start time*: The report is identified by a time stamp that contains both data and time with the following format: yyyy-MM-dd-hhmmss. • *User ref. + sequence*: The report name is set to a user configurable string plus a sequence number that is incremented for each new test. • *Serial no. + sequence*: The report name is set to the tester serial number plus a sequence number that is incremented for each new test.
User reference	This could be any alphanumeric string containing upper case letters, lower case letters and numeric digits. This field makes sense only if the report name format is *User ref. + sequence*.
Next sequence	Displays and configures the sequence number that will be assigned to the next report to be generated. This field makes sense only if the report name format is *User ref. + sequence* or *Serial no. + sequence*.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Table 6.1: System Settings Panel

Setting	Description
Report header	This menu item enables you to configure report data that will be stored with the test result. These data identify the report, customer, and also includes some other relevant information. • *Customer*: Field that can be used to set the company where the test report applies. • *Department*: This field can be used to identify the department where the user that has carried out the tester. belongs. • *Company*: This is the field that identifies the company that carries out the test. • *Location*: This describes where the test results from the network were recorded. • *Operator*: This field may contain the name of the operator that owns the network infrastructure where the test was run.
Maximum reports	Displays the maximum number of reports that can be stored within the tester internal memory. Currently this number is limited to 50 files.
Action when disk full	Action to be carried out when the maximum reports limit is reached. There are three possible choices here: • *Block measurements*: No new measurements can be run when the internal memory is full • *Stop report generation*: New measurements are run even if the internal memory is full but no reports are generated for them. • *Delete oldest reports*: When the maximum available capacity is reached, new files replace the older ones. Use this action with care. No warning is displayed when old reports are deleted.

6.2. File Management

Net.Storm stores configurations and reports in files. These files can be deleted, renamed or exported to an external USB memory or SD card. Configurations can be shared between different Net.Storm units by means compatible storage devices. Report files can be included to documents, sent by e-mail or printed.

6.2.1. Saving Configurations

To store the current configuration follow these steps:

1. From the *Home* panel, go to *File*,
   The tester file manager base menu is displayed.
2. Select *Configuration files* to go to the configuration file settings.
3. Select the location to save the configuration: *Internal memory*, or *External devices*.
   Note: If you select E*xternal devices*, you will be asked to choose the specific storage device (USB device or SD card).
   Note: If there is no external device connected to the Net.Storm unit, a *No devices present* popup panel is displayed.
4. Press the *Save* (F2) contextual button.
5. Enter a file name for the configuration file that is going to be saved and confirm with the *Done* (F4) contextual button.

6.2.2. Renaming Files

Both configuration and report files can be renamed after they are created. To rename files follow these sequence:

1. From the *Home* panel, go to *File*,
   The tester file manager base menu is displayed.
2. Select *Configuration files* or *Report files*.
3. Select the location of the file you want to rename: *Internal memory*, or *External devices*.
   Note: If you select E*xternal devices*, you will be asked to choose the specific storage device (USB device or SD card).
   Note: If there is no external device connected to the Net.Storm unit, a *No devices present* popup panel is displayed.
4. Select the file you want to rename with the help of the cursors and the ENTER button.
   Note: You can select several files in the list, but renaming of many files at the same time is not allowed.
5. Press the *Rename* contextual button.
6. Enter the new file name for the selected configuration or report file with the alphanumeric keyboard. Confirm with the *Done* (F4) contextual button.

6.2.3. Deleting Files

With the file manager you can delete files that are not needed anymore. To do that follow these steps:

1. From the *Home* panel, go to *File*,
   The tester file manager base menu is displayed.
2. Select *Configuration files* or *Report files*.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

3. Select the location of the file you want to delete: *Internal memory*, or *External devices*.
   Note: If you select E*xternal devices*, you will be asked to choose the specific storage device (USB device or SD card).
   Note: If there is no external device connected to the Net.Storm unit, a *No devices present* popup panel is displayed.
4. Select the file you want to delete with the help of the cursors and the ENTER button.
   Note: You can select several files in the list at the same time.
5. Press the *Delete* contextual button.
6. Enter the new file name for the selected configuration or report file with the alphanumeric keyboard. Confirm with the *Done* (F4) contextual button.

6.2.4. Exporting Files to External Devices

Configuration and report files can be exported to external devices like USB memories or SD cards. The procedure is as follows:

1. From the *Home* panel, go to *File*,
   The tester file manager base menu is displayed.
2. Select *Configuration files* or *Report files*.
3. Select *Internal memory*, to list the files currently stored in the Net.Storm unit.
4. Select the files you want to export with the help of the cursors and the ENTER button.
5. Press the *Export* contextual button.
   A popup menu to select the external device where the files will be exported is opened.
   Note: If there is no external device connected to Net.Storm, a *No devices present* popup panel is displayed.
6. Select an external device, confirm, and wait for the files to be copied.
7. Remove the USB storage device or SD card from the unit.

6.2.5. Importing Configurations

If you have a configuration file from a compatible tester you can import and load this file in your unit to reproduce similar measurements. This is the procedure you have to follow:

1. From the *Home* panel, go to *File*,
   The tester file manager base menu is displayed.
2. Select *Configuration files* to go to the configuration file settings.
3. Select *External devices* to list the files currently stored in the external device.
   A popup menu to select the source external device is opened.
   Note: If there is no external device connected to the Net.Storm unit, a *No devices present* popup panel is displayed.

4. Select the configuration files you want to import with the help of the cursors and the ENTER button.
5. Press the *Import* contextual button, confirm, and wait for the files to be copied from the internal memory.
6. Remove the USB storage device or SD card from the unit.

6.2.6. Using the Embedded Web Server

As an alternative of using a USB external storage device or an SD card for file management, Net.Storm has a web interface that can be used for the same purpose.

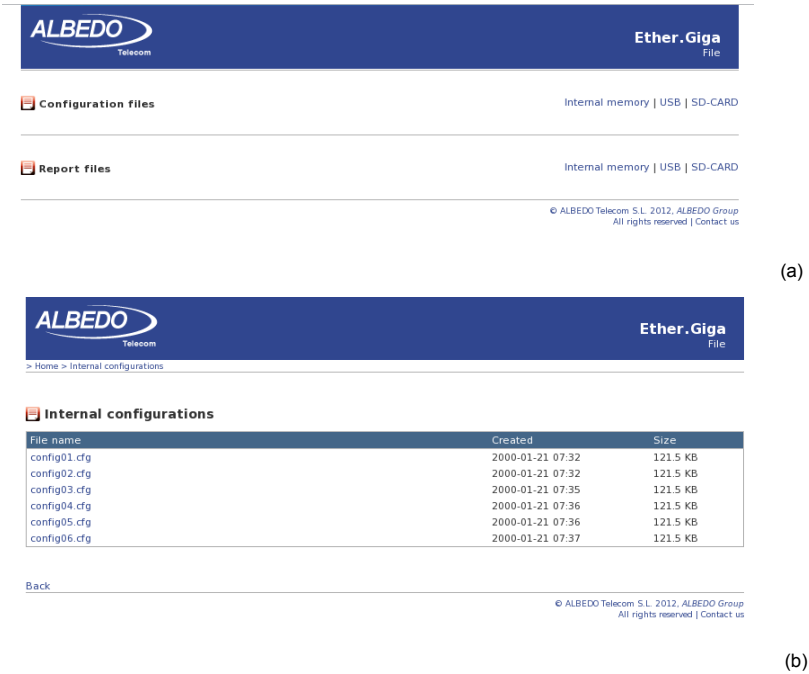

Figure 6.1: Net.Storm web interface: (a) Home panel (b) Configuration management panel.

The web interface can be used for downloading configurations and reports from a remote computer without using any accessory other than an standard network connection. Currently, the web interface does not support file uploading but for this purpose, the USB and SD interfaces are still available.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

To use the web interface you need to connect the platform network connector to the management network and configure the management Ethernet interface (See section 6.4.1). Once you have done this, follow this procedure:

1. Open a browser in a computer with network connection.
2. Type the IP address you have assigned to the tester in the browser destination URL.
   The web interface home panel is displayed in the Internet browser.
3. Choose the files you want to display (*Configuration flies*, *Report files* or any other if available) and the location of these files (*Internal memory*, *USB*, *SD-CARD*) and press to the correct hyper link.
   A list with the available files for the selected category is displayed in the web browser.
4. Select the file you want to download it to the local computer.
   The web browser displays a dialogue that requests your configuration to download the selected file. If you accept, the file will be downloaded.

6.3. Programming Tests

Net.Storm is able to start and finish tests without direct user intervention. All automatic testing features are included within the *Autostart/stop* menu

Follow these steps to program an automatic measurement in the test unit.

1. From the *Home* panel, go to *Test*,
   The test configuration panel is displayed.
2. Select *Autostart/stop* to enter in the automatic test programming menu.
3. If you want the automatic test to start at a specific date and time set *Start mode* to *Auto* and enter the start date and time in *Start time*.
   Note: Manual start has precedence over autostart. That means that if a tester is started by pressing RUN but there is an automatic test programmed the manual test will start anyway.
4. If you want the automatic test to stop at a specific time after it has started set *Stop mode* to *Auto* and enter test duration with the help of the *Duration* and *User duration* controls.
   Note: Manual stop has precedence over autostop. That means that if a tester is

stopped by pressing RUN but there is an automatic test programmed the manual test will stop anyway.

Table 6.2: System Settings Panel

Setting	Description
Start mode	Configures the start test mode. There are two different choices here: • *Manual*: The test starts when there is not an ongoing test and the RUN key is pressed. • *Auto*: The test starts at a configured date and time without the need of pressing any key.
Start time	Enter the start date and time for the next automatic measurement with the following format: *dd/MM/yyyy hh:mm:ss*. To configure Start time, you have to set *Start* mode to *Auto* before.
Stop mode	Configures the stop test mode. There are two possibilities: • *Manual*: The test finishes when there is an ongoing test and the RUN key is pressed. • *Auto*: The test finishes when a configurable test duration is reached. This mode does not require user intervention once the duration has been set and the measurement has started.
Duration	Sets the duration of the next measurement. The available test durations are: 15 minutes, 1 hour, 1 day, 7 days, 30 days or user configurable duration. Setting up *Duration* requires previous configuration of *Stop Mode* to *Auto*.
User duration	Sets the duration of the next measurement when *Stop mode* has been configured to *Auto* and *Duration* to *User*. The duration has to be entered in a *hh:mm:ss* format.
Last started on	Displays the date and time when the last measurement was started.
Last stopped on	Displays the date and time when the last measurement was stopped. If there is an ongoing test, the value of this field is empty.
Last power down on	Displays the date and time when the tester was powered down for last time.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

6.4. Using the System Menu

The System menu includes platform wide settings organized in four different submenus:

- *General settings*: This menu includes controls to manage the way the user interface behaves and how the information is presented.
- *Network configuration*: Includes the IP configuration corresponding with the platform NIC.
- *System information*: This menu has the test unit model name and serial number and software, firmware and hardware versions.
- *Licensed options*: This is a menu that displays the software versions installed in the tester and enables their management.

Table 6.3: System Settings Panel

Setting	Description
Brightness (%)	Sets the screen brightness from 10% to 100%. Within the *Brightness* panel, the left and right cursors are used to set the correct value and a contextual key (*Done*) is used to confirm selection.
Keyclick	Enables or disables the keyclick. The keyclick is a sound that is played each time a key is pressed.
Language	Selects the user interface language. Menus, selection lists and results are presented in the language selected here. The languages currently available are English and Spanish.
Date	This is used to configure the current date. The date is used for the *Autostart/stop* features and other purposes. The date has to be entered with the following format: *dd/MM/yyyy*.
Time	This is used to configure the current time. The time is used for the *Autostart/stop* features and other purposes. The time has to be entered with the following format: *hh:mm:ss*.
Time display	Select the way the time is displayed in the graphical user interface. One of the following has to be selected: • *Elapsed*: Time from the beginning of the test is displayed with the following format *hh:mm:ss*. If there is not an ongoing test, then the duration of the last test is shown • *Absolute*: The current date and time is displayed with the following format: *dd/MM/yyyy hh:mm:ss*.
Screensaver	Sets or unsets the screensaver. The screensaver reduces power consumption and increases operation time under battery operation.

Table 6.3: System Settings Panel

Setting	Description
Screensaver delay	Configures the delay to switch the screensaver on. The backlight brightness is set to a low value once the time configured here has finished. The display backlight is switched off after twice the screensaver delay. The available configuration values for this item are: 10s, 30s, 1min, 2min, 5min, 10min, 20min.
Remote control	Enables or disables the Ethernet / IP remote control. The remote control is an optional feature that enables remote users to use the tester from a computer running VNC.
Remote control password	Configures a password for the remote control. Any alphanumeric string should be accepted. Use the same password in the remote VNC client to access to the tester user interface.

This section supplies a description of the *General settings* menu and *System information* menu. To learn how to configure and use the network interface or how to install licenses for new software options go to the sections specifically dedicated to these topics.

Table 6.4: System information panel

Setting	Description
Model Name	Shows the test unit model name: Net.Storm.
Serial number	Displays the test unit serial number. It is a 8 character alphanumeric string
Software release	Displays the current software release.
Hardware release	Displays the current hardware release.
Firmware release	Displays the current firmware release.
PM release	Displays the current power management release.

6.4.1. Using the Network

The platform network interface is currently user for three different purposes:

- The *Ethernet / IP remote control*. This feature enables any user to access to the equipment form a remote location, configure a test, run it and display the results.
- The *Web interface*: This is used to retrieve reports configurations or any other file available in the tester internal memory or attached storage device.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

- *Maintenance and factory configuration*: The ALBEDO Telecom staff use the Ethernet interface to configure or verify the equipment in the factory. This feature is not available to ordinary users.

Table 6.5: Network Configuration Panel

Setting	Description
Ethernet interface	Configuration menu for the platform network interface. This menu can be used to configure the interface IP address and mask either automatically (DHCP) or statically.
Wireless interface	Configuration menu for the platform wireless network interface. This menu is used to set the radio parameters for the interface such as the SSID and the network parameters like the IP address and mask. The wireless interface requires a compatible WiFi adapter for the USB port. This adapter is supplied by ALBEDO as an optional accessory.
Gateway address	IP address corresponding to the IP default gateway in four dotted format. There is only one default gateway for all the network interfaces (wired and wireless). By setting up this field, the user decides which management port is used by the system to reach remote networks. It is possible to configure the gateway address automatically if either the wired or the wireless interfaces are configured to get an IP profile through the DHCP protocol.
DNS address	DNS server address used by the platform management ports to resolve domain names. It is possible to configure the DNS address automatically if either the wired or the wireless interfaces are configured to get an IP profile through the DHCP protocol.

To configure and use the Ethernet platform interface follow these steps:

1. From the *Home* panel, go to *System*,
   The general system menu is displayed in the screen.
2. Select *Network configuration* to display the network configuration and management menu.
3. Go to the *Ethernet interface*.
4. Enable the platform network interface with the *Enable interface* control.
5. Enable DHCP with the *Use DHCP* control if you want to let DHCP to configure your IP settings automatically or disable it to configure an static IP profile.

6. If you are not using DHCP, enter correct values for the *Static IP address* and *Static network mask*.
7. Leave the *Ethernet interface* panel with the ESC key.
8. If you are not using DHCP, configure the *Gateway address* and *DNS address*.
9. Connect the platform Ethernet connector (platform panel, RJ-45 connector with the *Ethernet* label) to the management network.
10. Optionally, check from a remote computer that the equipment is responding to ping requests.

Table 6.6: Ethernet Interface Configuration

Setting	Description
Enable interface	Enables or disables the network interface. Note that the link led placed in the Ethernet platform connector is lit even if the interface is not enabled.
Use DHCP	Configures the mechanism used to set the interface IP address and mask (and also other system-wide settings like the gateway address and the DNS server). If *Use DHCP* is enabled, the IP profile is configured automatically using a DHCP server installed in the network. Otherwise, the user has to enter the IP address, mask, default gateway and DNS address by hand.
Static IP address	Static IP address assigned to the interface in a decimal four dotted format. This setting makes sense only if *Use DHCP* is not enabled.
Static network mask	Static network mask in a decimal four dotted format. This setting makes sense only if *Use DHCP* is not enabled.
Leased IP address	Current DHCP-assigned IP address in a decimal four dotted format. This is a read-only field that cannot be directly configured by users This setting makes sense only if *Use DHCP* is enabled.
Leased network mask	Current DHCP-assigned network mask in a decimal four dotted format. This is a read-only field that cannot be directly configured by users This setting makes sense only if *Use DHCP* is enabled.
Ethernet address	48-bit physical address of the NIC attached to the test unit. This address is assigned to the NIC when it is manufactured and it cannot be changed later.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

6.4.2. Installing Software Options

New software for Net.Storm can be licensed after the unit as been purchased when new testing needs arise. To install new software options for your unit follow this procedure.

Table 6.7: Licensing

Setting	Description
Licensed options	Shows a list with all the software options currently available in your test unit.
License number	8-digit hexadecimal number provided by ALBEDO Telecom that identifies the software options to be added to your unit. Enter your license number in this field before adding the new software options to your test unit.
License key	8-digit hexadecimal number provided by ALBEDO Telecom that enables secure management of the software options installed in your test unit. Enter the license key in this field before adding the new software options to your test unit.
Activate	Set this field to Yes to add new software options to your tester. You have to enter the *License number* and the *License key* before adding new options.
Status	Displays the result of the software option activation operation performed by enabling the *Activate* field.

1. Contact with your local sales representative to purchase software options for your test units.
   You will receive one license number and one license key for each tester you want to upgrade.
2. From the *Home* panel, go to *System*,
   The system configuration panel is displayed.
3. Select *Licensing* to enter in the software upgrade menu.
4. Enter the number and key supplied by your ALBEDO Telecom representative in *License number* and *License key*.
5. Enable the new software options with the *Activate* control.
6. Check that the upgrade has been successful with the help of the *Status* control.

6.5. Using the Remote Control

The remote control application constitutes a remote graphical user interface that reproduces pixel by pixel the tester screen in virtually any remote device supporting the VNC protocol. This includes not only computers but also smartphones or tablets. The only requirements for the controlling devices are:

- IP connectivity with the tester. Any IP connection including Ethernet, WiFi and 3G should work.
- They must have a VNC client installed. Currently, there are VNC clients for most OS in the market. Some of them are free.

The remote control is an optional feature for Net.Storm that is supplied by ALBEDO Telecom with an special license.

Before using the remote control you need to configure the platform Ethernet interface and connect the equipment to the management network (See section 6.4.1). Once this is done, follow this procedure to use the remote control:

1. From the *Home* panel, go to *System*,
   The system configuration panel is displayed.
2. Select *General settings* to display miscellaneous system-wide settings, including the ones referred to the remote control.
3. Enable the remote control with the help of *Remote control*.
4. Optionally, supply a password with *Remote control password*. The password you configure here will be requested in all incoming VNC connections.
5. In the controlling device, run the VNC client and enter the password you have configured in *Remote control password* if you are requested to do so.
6. Use the keyboard (navigation through the mouse is not available in the remote control) to browse the instrument panels, start measurements, insert events or any other action.

Table 6.8: Remote Control Keys

Key	Description
Up, Down, Left, Right	These keys are equivalent to the cursor keys in the tester local interface. They move the focus through the different fields available in the current panel and they also help with the navigation through different panels.
Home	It is equivalent to the HOME key. It displays the *Home* panel.
Esc	It is equivalent to the Esc key. It leaves the current panel and displays the previous one in the panel hierarchy.
Enter	It is equivalent to the ENTER key. It confirms settings.
Ctrl+L	It is equivalent to LEDS. It displays the *Leds* panel.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Table 6.8: Remote Control Keys

Key	Description
Ctrl+S	It is equivalent to SUM. it displays the *Summary* screen
Ctrl+R	It is equivalent to RUN. It starts / stops a measurement
Ctrl+E	It is equivalent to EVENT. It starts / stops event insertion
F1, F2, F3, F4	They are equivalent to the F1, F2, F3, F4 contextual keys. The purpose of these keys depend on the current screen.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

Appendix A
Technical Specification

A.1. Ports and Interfaces

- Dual RJ-45 port for electrical connection 10/100/1000BASE-T.
- Dual optical and electrical SFPs ports operating up to 1 Gb/s.
- SFP interfaces including: 10BASE-T, 100BASE-TX, 100BASE-FX, 1000BASE-T, 1000BASE-SX, 1000BASE-LX.

A.2. Formats and Protocols

- Ethernet frame: IEEE 802.3, IEEE 802.1Q.
- IP packet: IPv4 (IETF RFC 791).
- Jumbo frames: up to 10 kB MTU (Maximum Transmission Unit).
- Throughput between measurement ports: 1 Gb/s or 1,500,000 frames/s in each direction.

A.3. Configuration

- Configurable MTU size.

A.4. Results

- Auto-negotiation results including current bit rate, duplex mode, Ethernet interface.
- SFP presence, vendor, and part number.
- Separate traffic statistics for each port.
- Separate statistics for transmit and receive directions.
- Frame counts: Ethernet, and IEEE 802.1Q (VLAN), control frames.
- Frame counts: unicast, multicast and broadcast.

- Basic error analysis: FCS errors, undersized frames, oversized frames, fragments, jabbers.
- Frame size counts: 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 bytes.
- Byte counts: Port A (Tx / Rx) and Port B (Tx / Rx).
- Traffic counters follow RFC 2819.

A.5. Filters

- One filter for background traffic processing and up to 15 fully configurable and independent filters.
- User-configurable filters defined by field contents on Ethernet, IP, UDP and TCP headers.
- Agnostic filters defined by 16-bit masks and user defined offset.

A.5.1. Ethernet filters

- MAC address: source, destination.
- MAC address group: subset of addresses filtered by a mask.
- Ethertype field with selection mask.
- VLANs field.
- CoS field.

A.5.2. IP filters

- IPv4 address: source, destination.
- IPv4 address group: subset of addresses filtered by masks.
- Protocol encapsulated in the IP packet (TCP, UDP, Telnet, FTP, etc.).
- DSCP field.
- TCP / UDP port.

A.5.3. Statistics

- Accepted and dropped frame counters for each configured filter.

A.6. Event Insertion

- Events are implemented at Ethernet layer.
- Independent event insertion in every single flow identified in the main stream.
- Events: Frame loss, delay, frame duplication, errored frames.
- Maximum process time caused by event insertion: 10 μs

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

A.6.1. Frame Delay and Jitter

- Deterministic delays: defined as a single Delay (ms).
- Random delays with uniform distribution: defined with a Minimum and a Maximum delay (ms).
- Random delays with exponential distribution: defined with a Mean (ms) and a Minimum delay (ms).
- Shaping filter for bandwidth control. Based on a token bucket algorithm is defined with two parameters (a) *sustainable rate* (frames/s), and (b) *depth* (frames) that determines the traffic allowed to pass-through when the rate is above sustainable. Not conforming frames are delayed.
- Worst case maximum delay (1 Gb/s traffic load and 64 byte frame): 20 ms

Table A.1: Accepted Ranges for Delay Event Parameters

Metric	Minimum	Maximum
Delay	0 ms	60 s
Minimum Delay	0 ms	60 ms
Maximum Delay	0 ms	60 ms
Average Delay	0 ms	60 ms
Rate	0 frames/s	1,500,000 frames/s
Maximum burst size	0 frames	32767 frames

A.6.2. Packet Loss

- Single loss insertion.
- Constant loss defined by a probability.
- Random loss defined by a probability.
- Random loss defined by the two-state model of Gilbert-Elliot which is configured by (a) the probability of packet loss during a period of high losses, (b) probability of packet loss during a period of low losses, (c) average length of high losses (in frames), and (d) the average separation between high-loss events in frames.
- Burst loss: defined as event duration, and number of packets affected.
- Periodic burst loss: defined with a burst duration, and the separation between two consecutive bursts. Both parameters can be defined using as units either the number of frames or time duration.
- Policing filter for bandwidth control. Based on a token bucket which is defined with two parameters a) *sustainable rate* (frames/s), and b) *depth* (frames) or how much

traffic is allowed to pass through when the rate is above sustainable. Not conforming frames are dropped.

Table A.2: Accepted Ranges for Frame Loss Event Parameters

Metric	Minimum	Maximum
Burst length	0 minutes	30 minutes
Burst length	0 frames	32737 frames
Burst separation	0 minutes	30 minutes
Burst separation	0 minutes	30 minutes
Rate	0 frames/s	1,500,000 frames/s
Maximum burst size	0 frames	32767 frames
Loss probability	0%	99.99%
Alternative loss prob.	0%	99.99%
Mean length	1 frame	16383 frames
Mean alt. length	1 frame	16383 frames

A.6.3. Frame Duplication

- Single duplication event insertion.
- Random duplication defined by a probability.

Table A.3: Accepted Ranges for Duplication Event Parameters

Metric	Minimum	Maximum
Duplication prob.	0 %	99.99 %

A.6.4. Errored Frames

- Single errored frame event insertion.
- Random errored frames defined by a probability.

Table A.4: Accepted Ranges for Frame Error Event Parameters

Metric	Minimum	Maximum
Frame error prob.	0 %	99.99 %

A.7. User Interface

- Direct configuration and management in graphical mode using the keyboard and display of the instrument.

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz

- Remote access for configuration and management in graphical mode from remote IP site thought the Ethernet interface of the control panel.

A.8. General

- Operation time with batteries: 3.5 hours (minimum, two battery packs).
- Configuration and report storage and export through attached USB port.
- TFT colour screen (480 x 272 pixels).
- Dimensions: 223 mm x 144 mm x 65 mm.
- Weight: 1.0 kg (with rubber boot, one battery pack).

ALBEDO Telecom - B6523022 - Joan d'Àustria, 112 - Barcelona - 08018 - www.telecom.albedo.biz