DATACOM

WISE Indústria de Telecomunicações

TSW900ETH

PRODUCT MANUAL

204.0233.04 Date: 21/11/2014

WARRANTY

This product is warranted against material and workmanship defects for the period specified in the sales invoice.

The warranty includes the repair and replacement of defective components and parts only without any resulting burden to the customer. Defects resulting from the following are not covered: improper use of device, faulty electrical power network, nature-related events (lightning discharges, for instance), failure in devices connected to this product, installations with improper grounding or repairs made by personnel not authorized by Wise or DATACOM.

This warranty does not cover repairs at the customer's facilities. Devices should be sent for repair at Wise Indústria de Telecomunicações.

Quality Management System

Certified by DQS in compliance with

ISO9001 Registration No. (287097 QM)

ISO9001:2008 Registration No. (FM544846)

Although every precaution has been taken in the preparation of this document, the Company takes no responsibility for possible errors or omissions, and it will accept no obligation for damages resulting from the use of the information contained in this manual. The specifications provided in this manual are subject to changes without notice, and they will not be recognized as any kind of contract.

CONTACTS

TSW900ETH is a product that resulted from a partnership between Wise Indústria de Telecomunicações and DATACOM.

To contact technical support or sales department:

- Support:
  - E-mail: wise@wi.com.br
  - Phone: +55 61 3486-9100
  - Fax: +55 61 3486-9109
- Sales:
  - E-mail: comercial@wi.com.br
  - Phone: +55 61 3486-9100
  - Fax: +55 61 3486-9109
- Internet:
  - www.wi.com.br
- Address:
  - **WISE**
  - Setor de Indústria Bernardo Sayão
  - SIBS quadra 01 conjunto D lote 12
  - Núcleo Bandeirante | DF | Brazil
  - ZIP CODE: 71736-104

- Support:
  - E-mail: support@datacom.ind.br
  - Phone: +55 51 3933-3122
  - Fax: +55 51 3933-3003
- Sales:
  - E-mail: sales@datacom.ind.br
  - Phone: +55 51 3933-3000
  - Fax: +55 51 3933-3003
- Internet:
  - www.datacom.ind.br
- Address:
  - **DATACOM**
  - Rua América, 1000
  - Eldorado do Sul, RS - Brazil
  - ZIP CODE: 92990-000

CONVENTIONS

In order to facilitate comprehension, throughout this manual the following keys have been adopted:

Hyperlink – Indicates an internet address or e-mail address.

Command or Button – Whenever a command, button or menu of a piece of software is mentioned, it will be identified in italics.

```
# Terminal screen commands and messages are presented as unformatted text,
  preceded by # (sharp).
```

The notes provide a better explanation of certain details presented in the text.

This format indicates that the text contained here is very important and there are risks of damage. It must be read carefully and may prevent a series of difficulties.

Indicates that a risk of electric shock exists, should the procedures not be followed correctly

Indicates the presence of laser radiation. If the instructions are not followed and if direct exposure to skin and eyes is not avoided, the skin and vision may be damaged.

Indicates equipment or parts sensitive to static electricity. It should not be handled without the proper care, using antistatic wrist straps or the equivalent, for example.

Indicates the emission of non-ionizing radiation.

Symbol of WEEE directive (Applicable to the European Union and other countries with selective waste collection systems). This symbol on the product or packaging indicates that the product cannot be discarded with domestic trash. However, it is your responsibility to take the equipment for disposal at a designated collection point for electric and electronic equipment recycling. Separate collection and recycling of equipment at the time of disposal helps conserve natural resources and ensures that the equipment is recycled in a manner that protects the health of people and the environment. For more information on where to dispose of equipment for recycling, contact your local retailer from where the product was purchased.

INDEX

FIGURE INDEX

TABLE INDEX

1. GENERAL RECOMMENDATIONS

Prior to installation, carefully read the whole manual.

The installation of any electric equipment must be in compliance with existing local legislation for where the equipment will be installed, including suitable protection devices, dimensioning and protection of its capacity.

Always pay attention to the safety instructions during installation, operation or maintenance of this product. Adaptation or maintenance may only be conducted by authorized and qualified personnel with the suitable training.

Carefully follow all guidelines in this manual. In case of doubt, please contact authorized technical support.

The equipment described in this manual includes an optical interface that emits a laser. Avoid laser exposure to the eyes and skin.

2. INTRODUCTION

2.1. Ethernet Tests

Ethernet tests are of great importance to the installation, activation and maintenance of Ethernet services and equipment. As with any other service, the activation and maintenance of Ethernet networks is critical to confirming that the service is operating as specified or agreed upon between the provider and its client.

The only way of checking the Ethernet service is by generating data traffic and gauging the parameters and characteristics of this traffic. This brief introduction to Ethernet tests covers the types of traffic and parameters that need to be configured and generated, as well as the measures and analyses that need to be implemented, in order to obtain reliable information regarding the operation and performance of the Ethernet service.

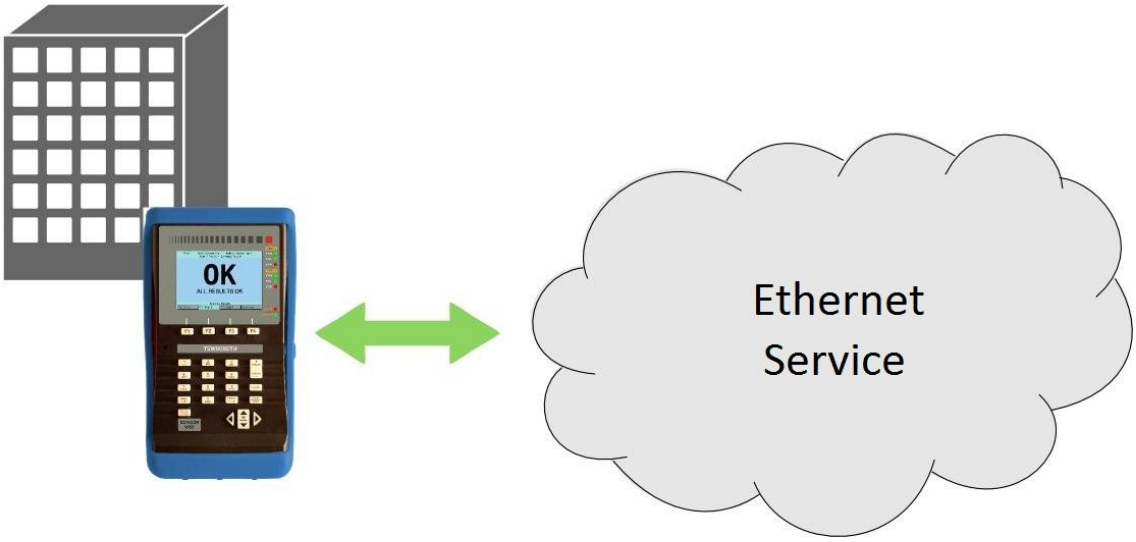


Figure 1. Ethernet service test

2.1.1. Traffic Generation Test

An Ethernet service can be seen as a channel offered by a provider to a client so that the latter can transmit traffic from one point to another. So as to confirm that the channel is clean and will transmit the client's traffic, technicians must generate traffic and confirm that all this traffic crosses the network without being corrupted.

When configuring test equipment to generate traffic, there are a number of parameters that must be specified, among them the band use rate, the size of frames and the traffic profile.

The use, or use rate, is the most critical parameter. Depending on the service, the Ethernet channel can transmit a rate equal to or less than the Line rate (10, 100 or 1000 Mbps). Thus, in many cases, it is vitally important to be able to accurately generate traffic at the maximum rate supported by the channel and to confirm that the traffic was not corrupted.

Tests involving a variation of frame sizes are also important. Differing frame sizes may affect a number of Ethernet network elements. Smaller frames make the device to work more intensely than larger frames, due to there being less time to process the frame before the next one arrives. Depending on the use rate, this may cause a device in the network to discard or corrupt frames.

The real traffic, of a client, always presents a variety of frame sizes due to differing applications and requirements. Generating different frames sizes in real time, a piece of test equipment can more efficiently emulate client data. The TSW900ETH Test Set can be configured to generate many frame sizes, with the additional possibility of configuring traffic with random frame sizes or even different types of lows, for quality of service (QoS) tests.

Another important parameter is the frame content, or payload. In the majority of cases, this portion is irrelevant to the Ethernet service. However, from the client's point of view, this is the most critical part of the service. Thus, the ability to edit, personalize and analyze the frame payload can be a requirement in some Ethernet service tests.

The traffic profile is another parameter to be considered in the generation of Ethernet traffic, and one that can be of great importance when analyzing specific features of an Ethernet service or device. To follow are descriptions of the leading traffic profiles: Constant Band, Ramp, Time and Bursts

- Transmission – Constant Band

  When activating a circuit, generating constant traffic at the maximum rate supported is the only way to confirm that the circuit is able to transmit client data at the guaranteed rate, without errors. The constant traffic test, with the use of maximum band, should ideally run without errors and offer the client proof that the circuit offered will transmit traffic correctly.

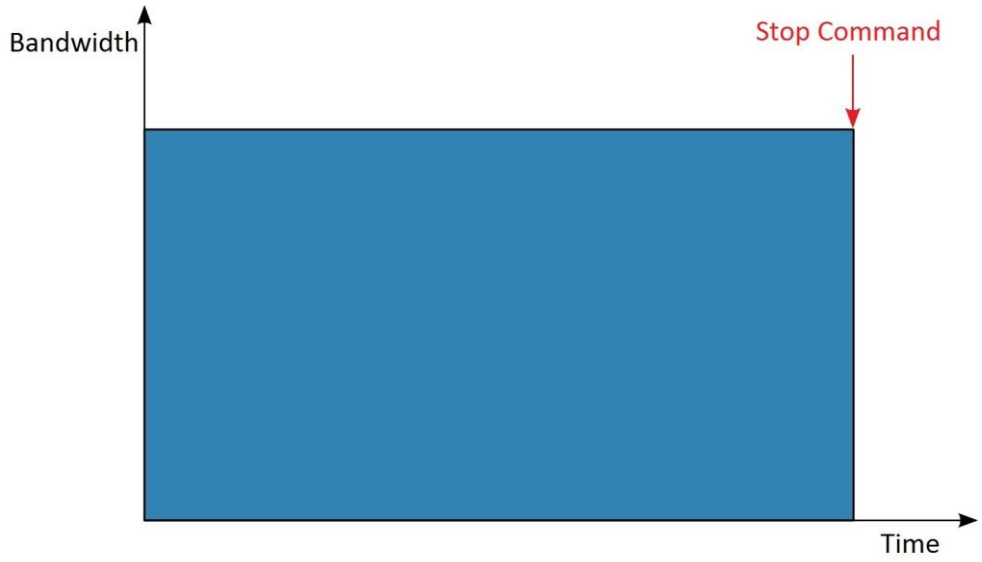


Figure 2. Constant bandwidth traffic

- Transmission – Ramp

  Another option for generating traffic is increasing the rate, step by step, over time, that is, in the form of a ramp. This test involves configuring a constant rate, waiting a short period of time, and recommencing the transmission at a higher rate. The easiest way of running this test is by having a piece of test equipment that does this automatically.

  Through this increase in ramp, it is possible to prove that the service is free of errors at a series of rates, not only at the maximum rate offered. If there are errors in the circuit, the ramp steps help identify the rate at which the errors occur, while it also being a fast method to obtain the maximum reachable rate.

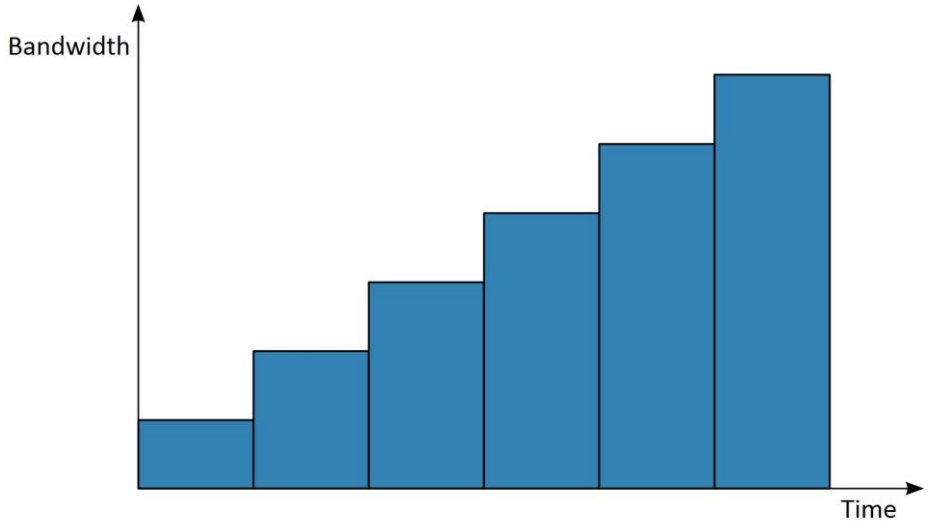


Figure 3. Ramp Traffic

- Transmission – Bursts

  The generation of traffic in bursts is a manner of boosting client data traffic in a more realistic manner. By adjusting the test equipment to generate this type of traffic, different band and frame sizes can be configured.

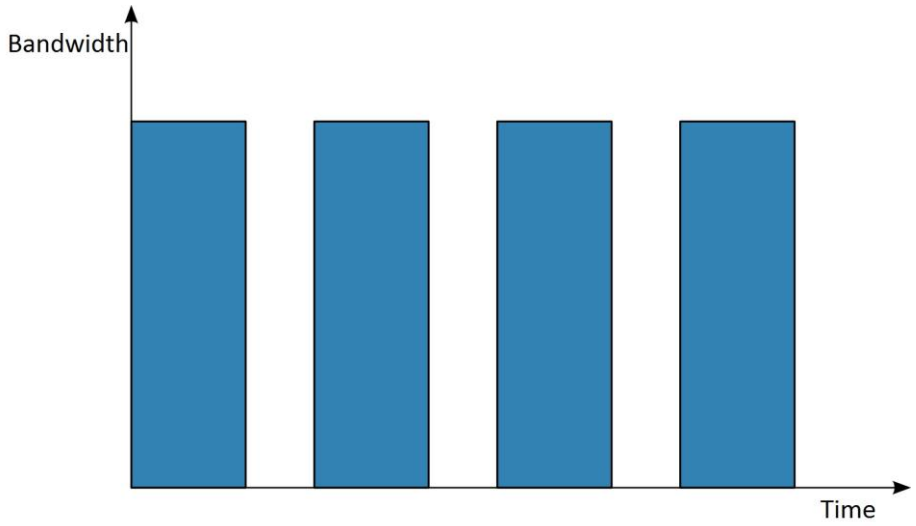


Figure 4. Traffic in bursts

- Transmission – Time

  Similar to constant traffic, traffic by time can transmit at the maximum supported rate, but for a pre-determined period of time. By configuring the test equipment for this type of traffic, the rate and time for running the test can be configured.

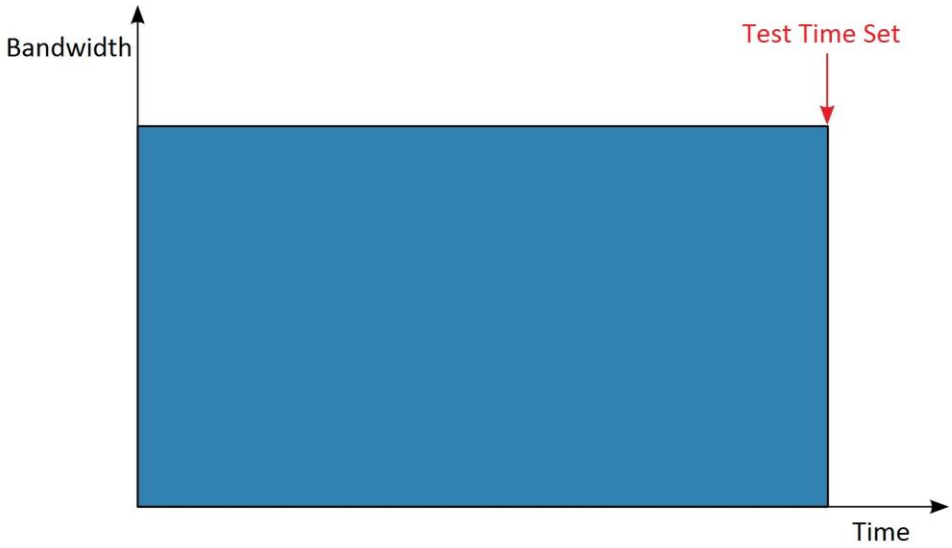


Figure 5. Traffic by time

2.1.2. Test results

After configuring and generating traffic, the results of the tests must be analyzed, in order to confirm if the service is operating according with the contract or not (this contract, or agreement, is commonly called an SLA – Service Level Agreement).

- Interpreting errors

  By generating traffic, any error received is indication of a problem. Errors chiefly include frames with CRC errors, Runts (frames smaller than the minimum size, with CRC errors) and Jabbers (frames larger than the maximum size, with CRC errors). These frames are usually discarded either by the client or the actual service network.

  In the TSW900ETH Test Set, two payload types can be configured: Timestamp and BERT. The information included in these payloads allows for a Test Set analysis, in addition to errors mentioned previously, other specific characteristics. The Timestamp type payload contains a sequence number and a time label, allowing the gauging of package loss, frames out of sequence and transmission delays. When setting the BERT type payload, a pseudorandom sequence of bits is included in the Ethernet frames. With this data, the Test Set is able to gauge and count bit errors within the frame payload.

- Interpreting link statistics

  Regardless of whether the link presents errors or is operating normally, there are a number of statistics that the technician can use to confirm that the traffic being transmitted is correctly received by the Test Set.

  In TSW900ETH a great range of counters and statistics are available and are presented in detail in this manual.

2.1.3. RFC 2544 Tests

The tests most often used in the installation and maintenance of Ethernet circuits are RFC 2544 tests. RFC 2544 is a specification that was initially developed to qualify Ethernet switches and their capacities. These tests were later adopted to characterize Ethernet services prior to them being delivered to the user. In the version with support for the TSW900ETH IPv6 it is also possible to apply the RFC 5180 tests; this specification was created with the same purpose as RFC 2544, though applied to IPv6.

There are four tests that are part of the RFC 2544 specification and are very important in characterizing Ethernet circuits. They are:

- Throughput

  The Throughput test identifies the maximum rate the circuit can operate at. This value must be in accordance with the bandwidth provided to the client.

- Latency

  The result of the latency test is a measurement of time for the departure and return of frames and is typically offered in milliseconds.

  There are two principle factors that create latency: network architecture and network traffic.

  While the architecture adds a fixed amount of latency in the network, the total amount of traffic that passes through an element (router or switch) can add a variable latency to the circuit being tested.

- Frame Loss Rate

  The RFC 2544 Frame Loss Rate test is aimed at determining the percentage of frames lost in a range of rates. The tests begin at the maximum configured rate and are decreased, according to the time and granularity configured until no losses are found. The correct result should be zero, that is, no frames are lost in the throughput rate.

- Back-to-back Frames

  This test is chiefly used in the area of development and manufacture of Ethernet equipment, when determining buffer capacities in elements. When activating an Ethernet circuit, this test is very often not a requirement.

  The test generates a number of frames in the minimum rate (a long burst). The Test Set then continues reducing the number of sent frames until the element being tested stops losing frames.

2.2. TSW900ETH Test Set

The TSW900ETH is a portable piece of test equipment, which can be used in installation, certification, development and maintenance of Ethernet circuits and equipment. The TSW900ETH Test Set conducts physical diagnosis tests (for electric cables and optical signals) and different tests with configurable data traffic, in addition to automatically conducting tests foreseen in RFC 2455 (Throughput, Latency, Frame Loss Rate e Back-to-back Frames). Additionally, the TSW900ETH can be configured to operate in Loopback mode and operates at the point of scenario of test, retransmitting the received data. All the tests mentioned can be conducted in layer 2 (Ethernet) or also in layer 3 (IP packages encapsulated in Ethernet frames), containing the Test Set with a number of specific IP layer functions and tests, such as Ping and Trace Route.

With two completely independent ports, the TSW900ETH is a piece of equipment of great use in different applications. Each of the ports can be used via an electric interface (RJ-45 connectors for 10/100/1000 Base-T) or optical interface (SFP – Small Form Factor Pluggable – module connections). This, for example, allows field technicians to conduct simultaneous test on two circuits, which can be from completely different customers/networks, or can also represent two routers from the same network (see the example of the illustrated application Figure 6).

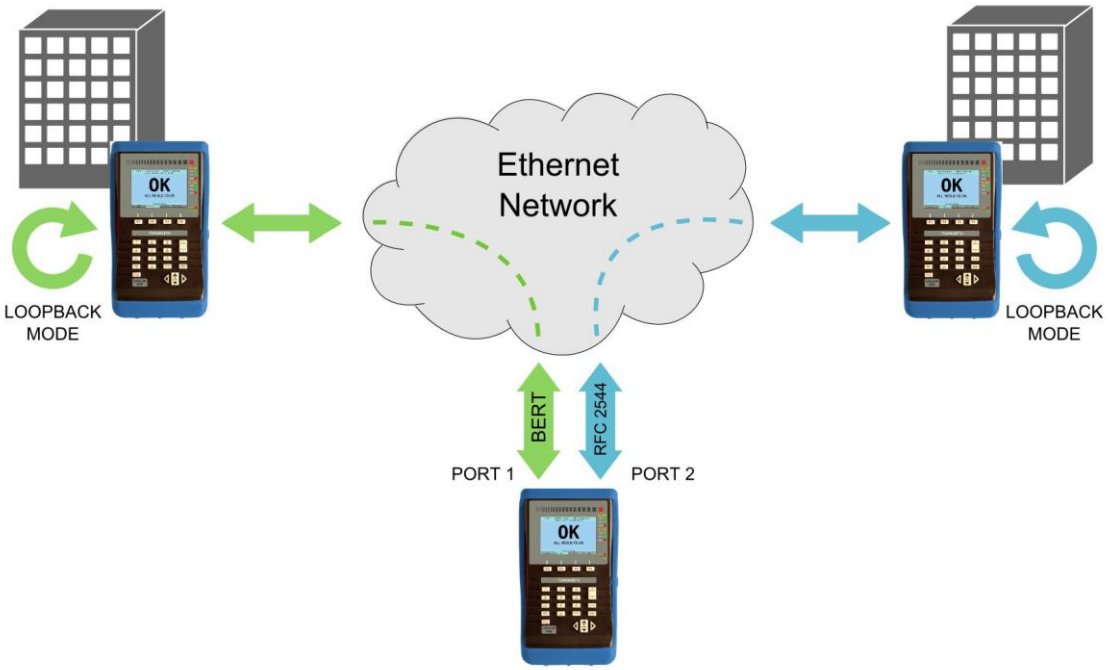


Figure 6. TSW900ETH Application Scenario

2.2.1. Functional Characteristics

To follow is a brief list of the leading functions of equipment in Ethernet tests.

- Generation and monitoring of traffic in layers 2 and 3 at 10/100/1000 Mbps for electric interface (10/100/1000 Base-T) or 100/1000 for the optical interface (100/1000BaseX).
- VLAN and Q-in-Q Configuration.
- Configuration of traffic in different profiles (constant, burst, ramp or time).
- Traffic generation rate configurable from 0.001 to 100%, with accuracy up to 0.001%.
- Physical layer test: cable diagnosis and optical signal test.
- Timestamp or BERT Payload type (with a range of patterns and customization options).
- Generation of NCITS TR-25:1999: CJPAT, CRPAT and CSPAT patterns.
- Filter for Ethernet, IPv4 and IPv6 headers.
- Traffic counters and statistics of received and transmitted frames.
- Loopback mode.
- Ping and Trace Route Tests.
- ARP and DHCP Support.
- Remote Loopback commands (capacity to place another TSW900ETH Test Set into Loopback mode, remotely, via an Ethernet network).
- Generation and transmission of up to 18 data streams per port, with each flow configured and analyzed independently (optional functionality).
- Creation of a number of user profiles, by means of the possibility of saving and loading configurations easily.
- Graphic visualization of the results of RFC 2544 tests on the Test Set screen and Web Interface.

- Generation of scripts for personalized tests, for specific and automated tests.
- Quality of Service (QoS) verifications.

2.2.2. Applicable Regulations:

- RFC 2544.
- IEEE 802.3.
- IEEE 802.1q.
- NCITS TR-25-1999.
- RFC 5180.
- ITU-T Y.1564.

2.2.3. Test Options:

- Automatic RFC 2544 Tests:
    - Throughput
    - Latency
    - Frame Loss Rate
    - Back-to-back Frames
- Configurable traffic test.
- Ping test.
- Trace Route test.
- Loopback mode.
- Cable diagnosis test.
- Optical signal test.

2.2.4. Traffic Monitoring and Analysis:

- General Counters:
    - Received/transmitted frames.
    - Received frames separated by size range, in bytes.
    - Received/transmitted bytes.
    - Unicast, Multicast and Broadcast Frames.
    - Received valid frames.
    - Pause Frames.
    - Frames received with VLAN.
    - Frames received with Q-in-Q.
    - The VLAN/SVLAN ID, VLAN/SVLAN Priority and SVLAN DEI fields of the last frame with a VLAN tag.
- General Statistics:
    - Frame Reception and Transmission rates (average, current, maximum and minimum).
    - Frame Reception and Transmission rates (average, current, maximum and minimum).

    - Delay (average, maximum and minimum).
    - Jitter (average, maximum and minimum).
- Error counters:
    - FCS, Runt and Jabber Error.
    - Lost frames and OoS (out of sequence).
    - Collisions.
    - Checksum and Length (IP packages) Errors.
- BERT Statistics:
    - Bit errors in frames.
    - Seconds with errors, seconds without errors, total time for BERT generation.
    - Total analyzed frames, total analyzed bits, and bit error rate.

2.2.5. NiMH Battery:

- Estimated duration: 4h.
- Estimated load time: 3h.
- Battery charger (Entrance: 90-240 V AC, 50-60Hz / Output: 15 V DC, 2 A).

2.2.6. General Specifications:

- Size (Height x Width x Depth): 246 mm x 132 mm x 61.8 mm.
- Approximate weight: 1.3 kg.
- Operating Temperature: 0 °C to 50 ºC.
- Storing Temperature: -20 °C to 70 ºC.
- Humidity: 5% to 95% (non-condensing).

2.2.7. Connectors:

- RJ-45 10/100Base-T.
- 2 RJ-45 10/100/1000Base-T, MDI/MIDI-X autonegotiation.
- 2 optional ports to connect SFP 100/1000Base-X modules for optical circuits.
- Mini USB.

2.2.8. Additional Characteristics:

- Color display: 480x272 pixels.
- Alphanumeric keyboard with 23 keys, including function keys.
- Memory for storing over 1000 results.

Under no hypothesis whatsoever look at the SFP while uncovered or at the fiber optic ends with the equipment turned on. Invisible laser beams could harm your vision!

Do not short circuit the AC adaptor terminal/charger and batteries. High currents may cause accidents due to the production of smoke, electric shock or equipment damage.

Do not operate the equipment close to hot objects, nor in environments with high temperatures, excessive dust or high moisture levels. This may result in electric shock, poor product operation or hampered performance.

2.3. Models

The TSW900ETH can be provided in different functional combinations. The different models are identified in accordance with product licensing, which must be defined at acquisitions, in accordance with the desired optional features. Insertion of new licenses can be implemented later.

2.3.1. Licenses

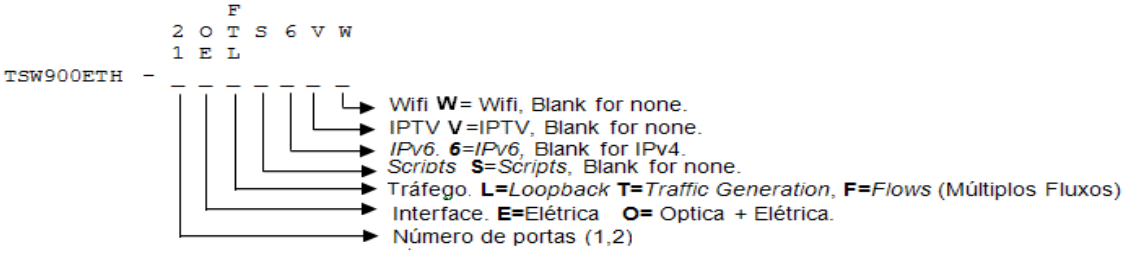
The table below shows the different licenses that are possible to add:

Identifying Character	Description
(**1**) Single port	TSW900ETH Single Port License
(**2**) Dual port	TSW900ETH Dual Port License
(**O**) Optical Interface	TSW900ETH Optical Interface License
(**E**) Electrical Interface	TSW900ETH Electrical Interface License
(**U**) Unlocked All	TSW900ETH Unlocked All (Electrical + Any SFP) License
(**L**) Loopback	TSW900ETH Loopback License
(**T**) Traffic Generation	TSW900ETH Traffic Generation License
(**F**) Flows (Multiple Streams)	TSW900ETH Flows (Multiple Flows) License
(**S**) Scripts	TSW900ETH Scripts License
(**6**) IPv6	TSW900ETH IPv6 License
(**V**) IPTV	TSW900ETH IPTV License
(**W**) Wifi	TSW900ETH WiFi License

Table 1. Licenses

2.3.2. Nomenclature

To assemble the desired configuration, one number and three letters follow the name of the product. In accord with the present license, as shown below:



The licenses in the same column are always added, without losing the previous characteristic below, which is a requirement for being able to rise to the next.

For example, to have license (**F**) Flows, it is necessary to have license (**T**) Traffic Generation.

Option / Code	Licenses
TSW900ETH–1EL.	Basic, no license required
TSW900ETH–1OL	**O**ptic Interface
TSW900ETH–1UL	**U**nlocked All – accepts any SFP.
TSW900ETH–1ET	**T**raffic Generation
TSW900ETH–1OT	**O**ptic Interface + **T**raffic Generation
TSW900ETH–2OT	**D**ual Port + **O**ptic Interface + **T**raffic Generation
TSW900ETH–1OF	**O**ptic Interface + **F**lows
TSW900ETH–2OF	**D**ual Port + **O**ptic Interface + **F**lows
TSW900ETH–1OFS	**O**ptic Interface + **F**lows + **S**cript
TSW900ETH–2OFS	**D**ual Port + **O**ptic Interface + **F**lows + **S**cript
TSW900ETH–2OFS6	**D**ual Port + **O**ptic Interface + **F**lows + **S**cript + IPv**6**
TSW900ETH–2OFS6-V	**D**ual Port + **O**ptic Interface + **F**lows + **S**cript + IPv**6 +** IPT**V**
TSW900ETH–2OFS6-VW	**D**ual Port + **O**ptic Interface + **F**lows + **S**cript + IPv**6 +** IPT**V + W**ifi
TSW900ETH–2UFS6-VW	**D**ual Port + **U**nlocked All + **F**lows + **S**cript + IPv**6 +** IPT**V + W**ifi

Table 2. Example of TSW900ETH models according to licenses

3. INITIAL EQUIPMENT OPERATION

3.1. Learning about the TSW900ETH

The TSW900ETH is operated via a keyboard and a liquid crystal display. Furthermore, a set of LEDs help verify the status of connections and tests.

The equipment is powered by an internal battery set that must be charged using a power source supplied with the product. The Figure 7 shows each of the items that make up the piece of equipment.

Figure 7. General view of the TSW900ETH

3.2. External Connections

- POWER SUPPLY: A switch mode power supply, for charging the battery, is provided with the equipment. The connection is located on the side of the TSW900ETH. The use of a power supply different from that provided may damage the equipment or result in the battery no charging.

The upper connectors, described as follows, can be seen in Figure 8.

- ETH MNG – RJ45 10/100 Base-T Connector Used for IPTV functions and equipment management, with access to reports, version updates and remote access.
- ETH1 – RJ45 10/100/1000 Base-T Connector. Used for a range of Ethernet test functions. This connector is a test interface, called Port 1, in the case of choosing to use an electric link.
- ETH2 – RJ45 10/100/1000 Base-T Connector. Used for a range of Ethernet test functions. This connector is a test interface, called Port 2, in the case of choosing to use an electric link.
- SFP1 – SFP 100/1000 Base-X module input. Used for Ethernet connections via optical cable. This input is a test interface, called Port 1, in the case of choosing to use an electric link.
- SFP2 – SFP 100/1000 Base-X module entry. Used for Ethernet connections via optical cable. This input is a test interface, called Port 2, in the case of choosing to use an optical link.
- USB – mini USB connector, used for maintenance.

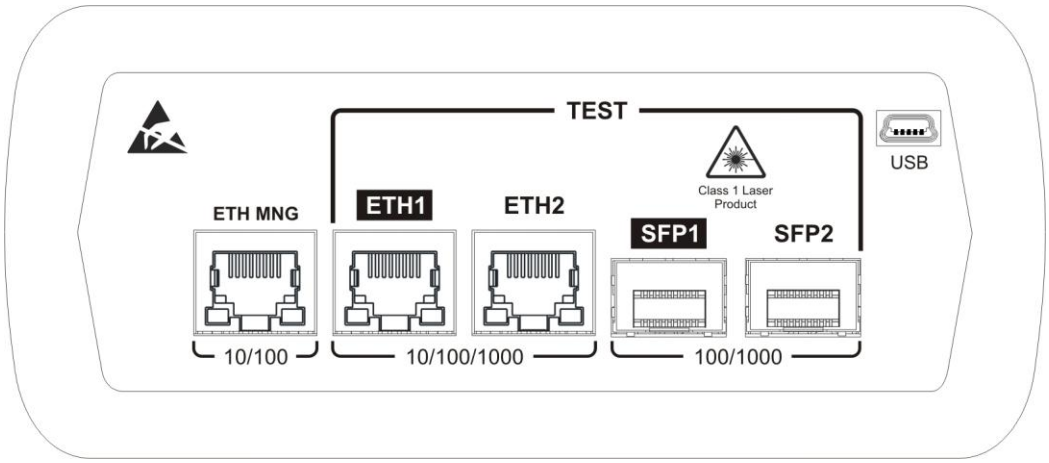


Figure 8. Interfaces of the upper part of the TSW900ETH

3.3. LEDs

Figure 9 illustrates the equipment's front panel, which includes LEDs, described as follows.

- BATT – Flashes when the battery reaches a power level insufficient to operate the equipment, warning the user that it is necessary to charge the equipment.
- IN CHARGE – ON when connected to the battery charger. Red while the battery is charging and green when the battery is fully charged.

The LEDs listed below are present in both port 1 and 2.

- FRM – Frame LED, ON when the equipment receives a frame from a specific port.
- SYN – Synchronism LED, ON when the port in question is synchronized with the equipment/network being tested (active link).
- ERR – ON when there is an error during the test of the port in question.

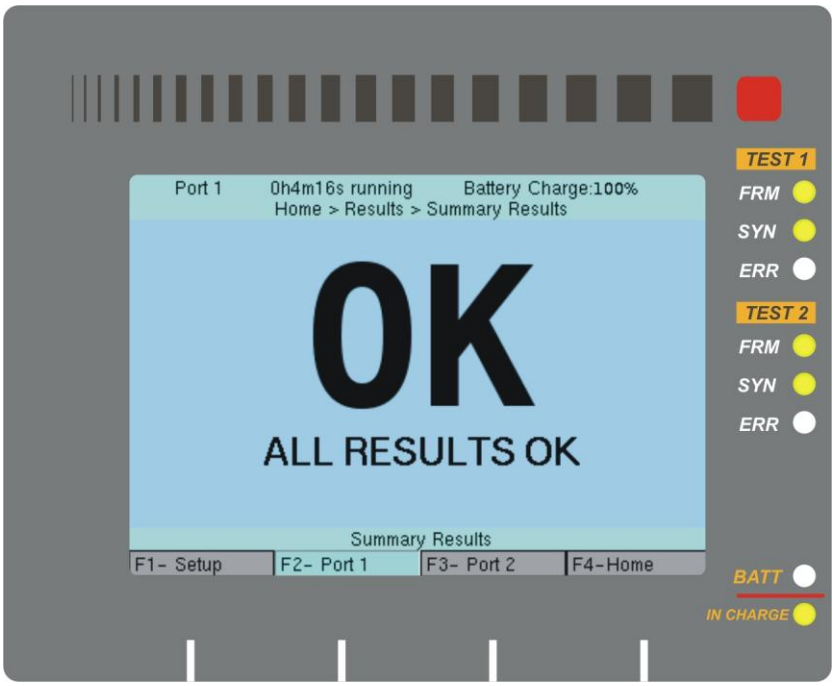


Figure 9. TSW900ETH LEDs illustration

3.4. Keyboard

The TSW900ETH keyboard, which can be seen in Figure 10 offers a range of keyboards to facilitate its operation.

The function keys allow navigation between application tabs, among other things (as detailed in section 3.5).

- F1 – Can be used as a shortcut key for the Setup tab. In editing fields, it is used to confirm the typed value.
- F2 – Its main function is to be used as a shortcut key for the tab with Port 1 configurations and tests. In editing fields, it is used to cancel modifications.
- F3 – Serves as a shortcut key to use the tab with Port 2 configurations and tests.
- F4 – When in the Home Menu (Home), the F4 shortcut key access the tab that presents the saved test results. When leaving the Home Menu, entering any menu, key F4 begins working as a shortcut return to the Home Menu. The tab corresponding to key F4 of the display, changes its description according to the case, able to exhibit the F4 text - Home or F4 – Results.

Besides these 4 function keys, an alphanumeric key can be used in editing. The keys can assume numeric values or texts, depending on the editing format. When in the numeric editing, it has the value of the written number. When in text editing, it has the value of one of the letters present on the button, depending on the number of times it is pressed. The types of fields and the form of browsing and editing them will be detailed in the section 3.5.

Other keys present in the TSW900ETH keyboard are:

- (↑ and ↓) – Shortcut Keys, which make navigability possible among the menu items.
- (→) – Enter the item or run the action selected in the menu.
- (←) – Shortcut key that allows you to return to the previous screen.
- CLEAR – Allows the last digit entered to be cleared. It is also used to clean the counter if in any one of the result screen.

- PRINT – Can be used as a key to type “.” and “*”.
- ERROR – Allows for the forced insertion of CRC or BERT errors, depending on the type of traffic being generated.
- ON/OFF – Key used to turn the device on/off.
- START/STOP – Through one of the ports (keys F2 or F3), it can be used to open a quick Menu, as a shortcut key to start or stop tests. Furthermore, it can serve to confirm the completion of a field.
- VOLUME (+/-) – Allows a quick change among the item options chosen on the menu.

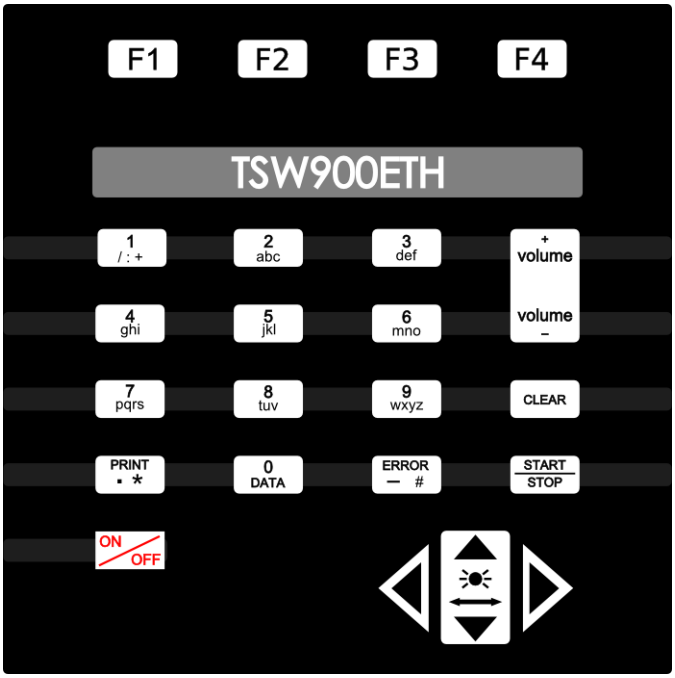


Figure 10. TSW900ETH Keyboard

3.5. Interface with the User

Interface with the user is achieved through a simple and intuitive application, using the colored display graphic on the Test Set. To follow are examples of some of the application keys, describing how to navigate and use each of the functions.

3.5.1. Tab Division

The TSW900ETH Application is divided into four main screens, access through four tabs that appear in the lower part of the display. Each of the tabs corresponds to a function key (F1, F2, F3 and F4).

The four tabs can be seen in Figure 11, which shows the initial screen of the equipment.

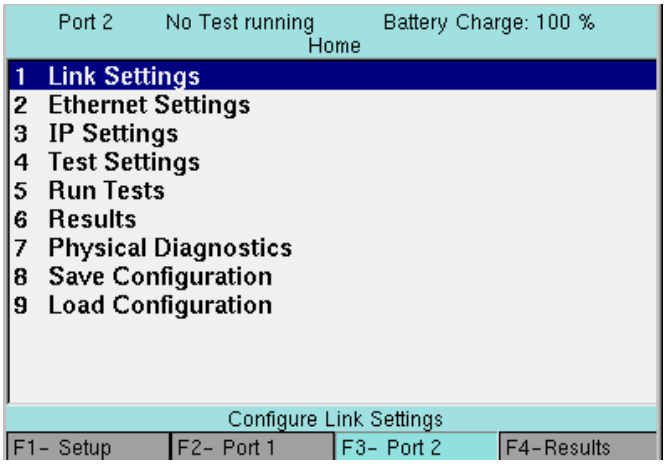


Figure 11. Test Set User Interface

The tabs shown in Figure 11:

- F1 – Setup: Instrument configuration
- F2 – Port 1: Port 1 Configuration and Tests.
- F3 – Port 2: Port 2 Configuration and Tests.
- F4 – Results: Management of Saved Results / Shortcut to Home Menu.

When turning the equipment on with fully charged battery, the display shows a screen with the last port accessed by the user (tab F2 or F3). From that point, keys F1/F2/F3/F4 can be used to change the tab.

3.5.2. Menus

Figure 11besides illustrating the division of the tabs in the upper part of the screen, it also shows the Home Menu of one of the Test ports. The Test Set Menu keys are formed by a list of numerated options.

The directional keys (↑) or (↓) can be used to alternate among the items, (→) to enter one of the menu options. The (←) key returns to the previous screen, when possible.

On the menu screens, the numerical keys can be used to choose between one of the offered options. This is achieved using the key with the number corresponding to the option on the menu (for example, on Figure 11screen, key 4 serves to enter the item Test Settings).

The same is true for a sequence of screens. To access the Link Counters screen, for example, it is possible to choose to navigate among the menus or type the corresponding keys as in the sequence below:

- Navigating with the (↑), (↓), (→) or (←) keys.

  Home > Results > Link Counters

- Navigating by menu numeric sequence

  (F4-Home), (6), (6)

3.5.3. Editing Fields

The editing fields are those in which the user needs to write the desired value. Some examples of editing fields are MAC or IP addresses, VLAN ID value, frame size or number of frames to be sent in a burst.

Figure 12 shows an example of an editing screen.

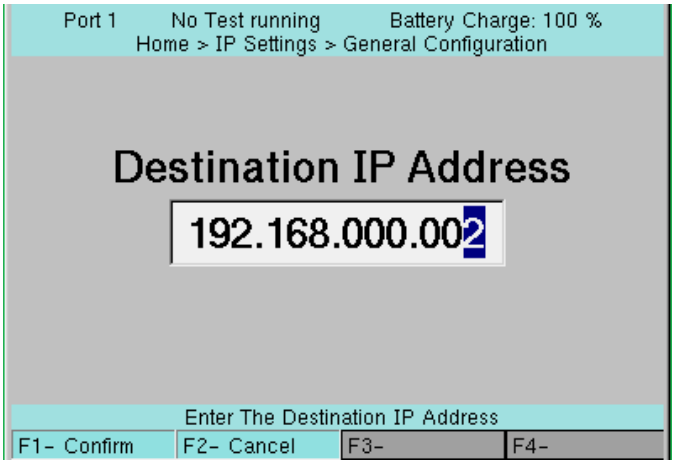


Figure 12. Field editing example screen

Note that, in these cases, the four tabs change functions, no longer providing access to the options explained in section 3.5.1, rather showing the Confirm and Cancel options, selected by keys F1 and F2, respectively.

To configure values in fields of this type, the user must use the alphanumeric keys on the keyboard to write the desired value (text or number) and the F1 or F2 keys to confirm or cancel the edit.

Warning 5 – 2 or More Streams Configured With the Same Source MAC/IP Address

"When configuring multiple stream IPs, it is possible to attribute the same IP to a stream. Thus, different MACs can be configured for the same IP. An IP cannot have more than one MAC associated with it and a MAC cannot be associated with more than one IP. Invalid configuration situation. Only use this option if you are sure you want to force a situation that may result in an error.".

3.5.4. Selection Fields

The selection fields are those where the Application offers a limited number of options, among which the user selects the desired one. Some examples of selection fields are: priority of a VLAN tag, number of flows to be generated in a Multiple Flow test, Link speed and the type of Ethernet Frames.

Figure 13shows two examples of screens with selection fields. Note that when selecting the Speed option, the column on the right displays the options that can be selected: 10, 100 or 1000.

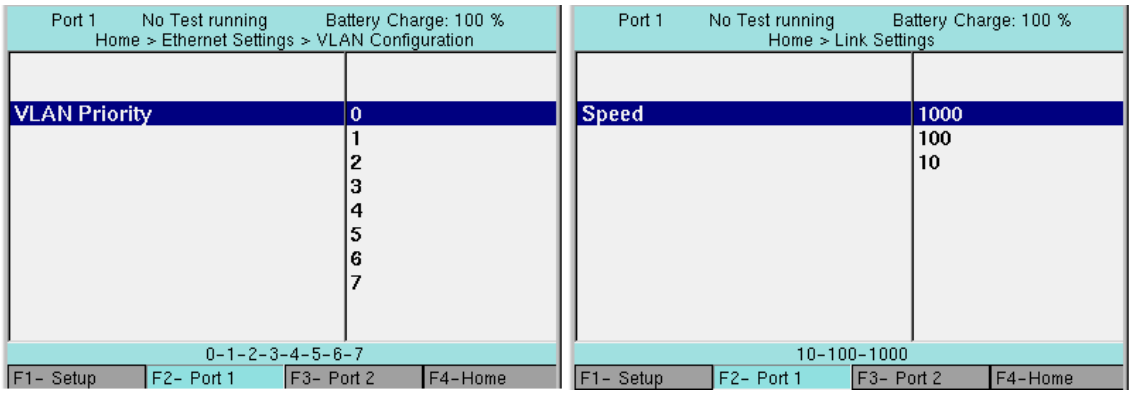


Figure 13. Fields selection example screens

The selection, in this type of configuration field, is made using the navigation keys (↑), (↓), (→) and (←).

3.5.5. Result Screens

States the results of tests conducted or that are running. They are counters or records of test results like RFC 2544, Link Counters/Statistics, errors and indications of tests running. The results of the finalized RFC 2544 are displayed in graphs or tables, as detailed in section 5.7.3. The remaining results, that is, the status of the Link, frame counters, traffic stats and error counters, are displayed according to the example of Figure 14.

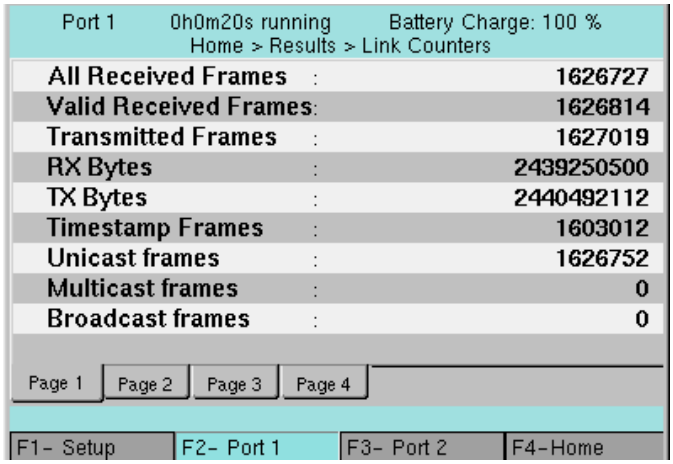


Figure 14. Result screen – Link Counters

On this type of screen, when the number of counters/statistics cannot be shown on a single screen, these counters are divided into pages, as can be seen in Figure 14. To run through the pages, simply use the navigation keys (↑) and (↓).

3.5.6. Help Bar

On all the screens for Menus, Selection Fields, or Editing Fields, a small guideline is provided regarding the selected option. On the lower part of the screen, just above the four tabs, this help bar can be seen, containing more information about the option highlighted by the cursor. When the cursor is over a selection field, the text in the help bar will show all the available options for that field.

Below, two examples of guidelines provided in the help bar (note the text shown in the lower part of the screen).

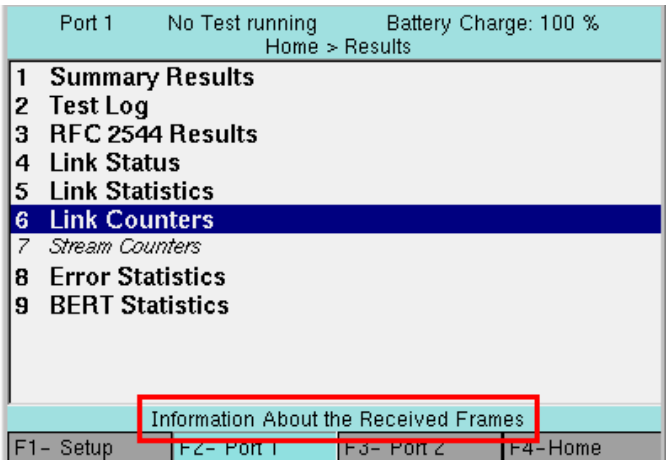


Figure 15. Help Bar in Menu

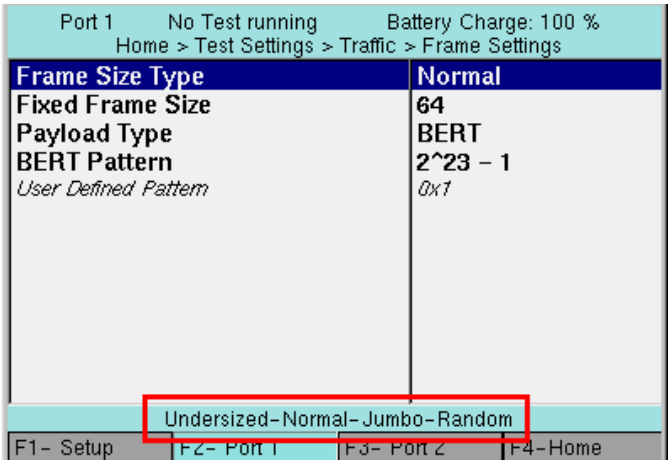


Figure 16. Help Bar in Selection Field

3.5.7. Additional Information

In the range of interface Menus, when an item is in bold, it means that it is available. Items in bold cannot be added due to the equipment configurations or conditions. For instance: a traffic test in Port 1 cannot be run without the port having an active link (SYN LED on).

If an item appears in red or shows the message “Feature not licensed”, this option belongs to a test module not acquired by the user. These options can be enabled if acquired and licensed, after the sale of the unit. Contact the sales sector to acquire optional modules.

3.6. Battery

The TSW900ETH is powered by NiMH batteries. Due to the characteristics of the batteries, in order to achieve the best performance, it is recommended that, once charged, the battery is used up to the minimum limit prior to recharging. This procedure, besides ensuring the battery is fully charged, ensures the useful life specified by the manufacturer.

When the batteries inside the TSW900ETH require recharging, the equipment must be connected to a source (Input: 90 to 240 VAC / 60 Hz and output 15VDC 2 A) by means of the battery charger input, located on the side of the device.

While the battery is charging, the user can find out if the maximum load has been achieved by means of an LED with an “IN CHARGE” indication on the front of the TSW900ETH panel, which can be seen at Figure 9. While this LED is red, the battery is charging. If the LED turns green, the battery is fully charged. If the battery is not fully charged, in the event of disconnecting the charger or a blackout, the operating time of the TSW900ETH will also be reduced.

To avoid electricity network interferences from altering test results, it is recommended that the battery charger for the TSW900ETH is not connected or disconnected while the test is running.

The TSW900ETH has a battery manager that shows the charge status in the form of a percentage. It is shown in the upper right corner of the screen. When the battery reaches the minimum level, the LED indicated as BATT begins to flash. Following the amount of time that the BATT LED flashes (around 3 minutes), the equipment turns off. If the battery level is normal, the LED will remain off.

The TSW900ETH must only be charged with the source provide with the equipment. On the contrary, the manufacturer is not liable for possible damage caused to the equipment and for the reduction in performance and useful life of the batteries.

3.7. Optical Transceivers

TSW900ETH has optical ports for 100Base-FX/1000Base-X Ethernet tests. The optical port is of the SFP type with a LC connector. The use of the SFP transceiver is optional, and is not included in the basic package. Table 3. lists some of the compatible SFPs that can be ordered with the TSW900ETH.

SFP Module	Type of Optical Fiber	Typical reach
100 BASE-LX	Single mode	2 km
1000 BASE-SX	Multimode	550 m
1000 BASE-LX	Single mode	10 km
1000 BASE-LH	Single mode	70 km
1000 BASE-ZX	Single mode	110 km

Table 3. SFPs compatible with the TSW900ETH

DATACOM SFP and XFP modules are tested to fulfill norm IEC60825-1. Unratified modules do not ensure correct operation of the equipment and may damage the interface cards. DATACOM equipment software checks whether the modules used are ratified prior to their use and block those that are unratified. Contact the technical support team about the risks of using unratified modules and the possibility of unlocking them.

If necessary, contact our technical support sector for more information and detailed specifications.

3.7.1. Installing SFP Modules

The installation is conducted by simply fitting the module into the SFP slot of the equipment and pushing it until it is firmly held. The correct position of the attachment can be seen in Figure 17.

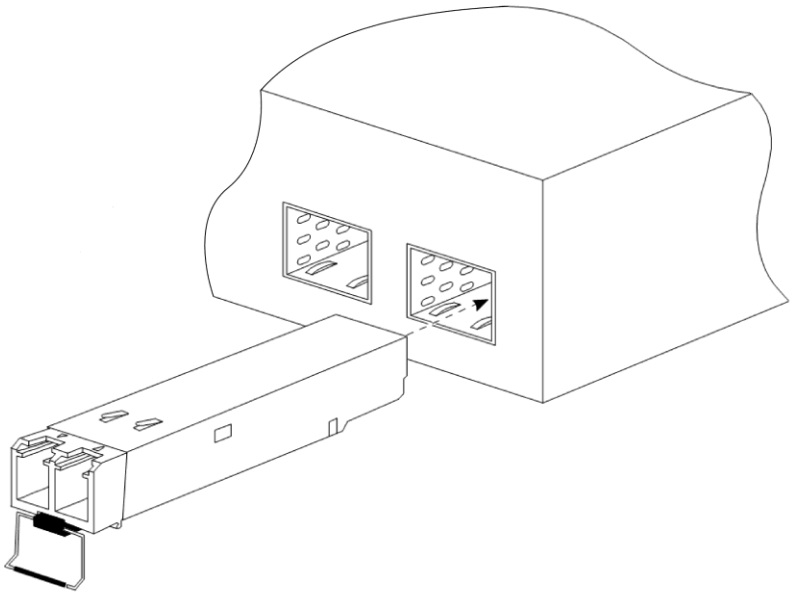


Figure 17. SFP Module install

After attaching the module, it is necessary to secure the securing handle as shown in Figure 18, as it serves as a lock for the optical cables when these are connected.

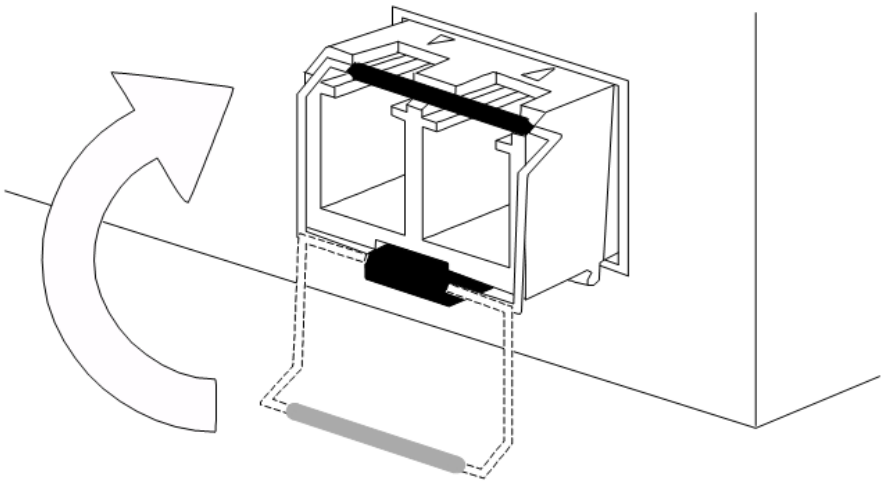


Figure 18. Securing Handle

After positioning the handle simply connect the optical cables.

3.7.2. Removing SFP Modules

To remove the modules, simply follow the installation instructions in reverse:

- Remove the optical cables.
- Lower the securing handle.
- Pull the module by the handle, as shown in Figure 19.

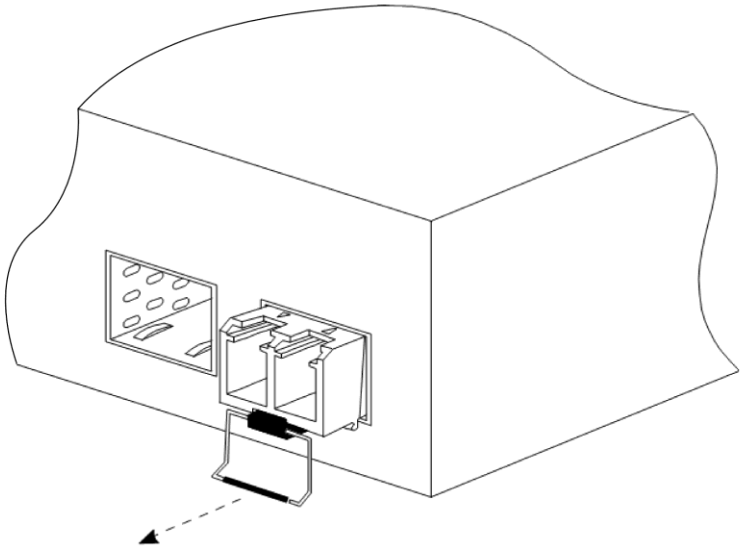


Figure 19. SFP Module removal

4. INTRUMENT CONFIGURATION

By pressing key F1, the Setup screen is presented:

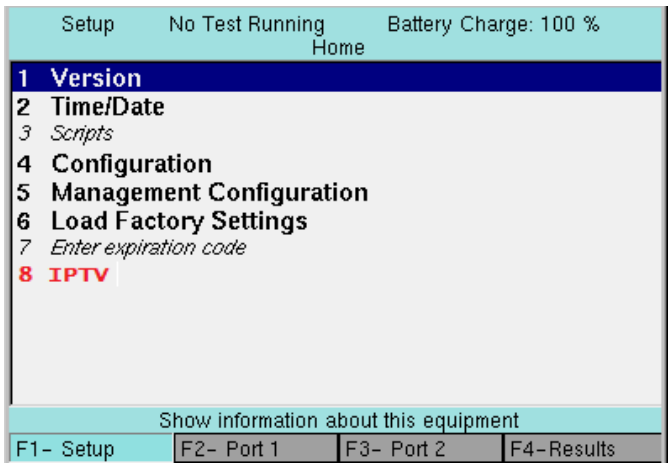


Figure 20. TSW900ETH Setup Screen

The Setup screen presents general information about the product, date/time configuration/ battery alarm, backlighting, TSW900ETH management and factory setting restoration. Other configuration options are also accessed on this screen, such as the option to enter a code for expiry – release for use for a specific period and script use mode (disabled, remote or embedded), if applicable.

4.1. Version

Shows information about product version. The following items are presented on this screen:

- **Product ID** – Shows the unit identity number.
- **Product Revision** – Shows the version of the unit hardware.
- **Software Version** – Shows the version of the software used in the unit.
- **Firmware Version** – Shows the version of the unit's auxiliary processor software.

4.2. Time/Date

Allows the date and time to be viewed and set. The following options are presented on the Menu:

- **Hours** – Allows the clock hours to be viewed/changed.
- **Minutes** – Allows the clock minutes to be viewed/changed.
- **Seconds** – Allows the clock seconds to the viewed/changed.
- **Month** – Allows the month of the set date to be viewed/changed.
- **Day** – Allows the day of the set date to be viewed/changed.
- **Year** – Allows the year of the set date to be viewed/changed.

4.3. Scripts

This is an optional product function. The TSW900ETH, by means of the management port 'ETH AUX' – provides support o scripts, which have two functions:

- Remote and interactive use.
- Test automation.

By means of commands that permit all the functions for the generation of traffic and counter reading to be configured and implemented, scripts can be developed for use on PC or embedded in the product. Personalized tests and access from a distance for configuration and remote use of all the product functionalities are some of the benefits of using scripts. Contact your local representative for further information.

4.4. Configuration

Permits access to general TSW900ETH information and configurations, such as backlight time and activating/deactivating the alarm that indicates a weak battery. The following options are presented:

4.4.1. Backlight Time

Configure the display backlight time. The following options are available:

- **20** – 20 second duration.
- **30** – 30 second duration.
- **40** – 40 second duration.
- **Always On –** Backlight always on.

4.4.2. Keyboard Buzzer

Enable/disable the “beep” that sounds when a key is pressed. The following options are available:

- **On** – Enable
- **Off** – Disable.

4.4.3. Battery Alarm

Enable/Disable the alarm that indicates a weak battery. The following options are available:

- **On** – Enable.
- **Off** – Disable.

4.4.4. Script Mode

Set the device script options (function for generating remote access and personalized tests by means of scripts). The following options are available:

- **Disabled** – Use of the scripts function is disabled.
- **Remote** – Permits remote access to a PC.
- **Embedded** – Permits the use of embedded Scripts. Personalized tests can be inserted and run when accessed in the Scripts Menu on the Setup screen.

4.4.5. Space Left on Device (KB)

This is merely a reading parameter. It states the amount of space available in the TSW900ETH memory, in kilobytes. This information is useful in assisting the management of files and data stored on the equipment.

4.5. Management Configuration

In this menu the configurations for access to the equipment management interface are accessed. To create a connection, link the ETH AUX port to a local network point or directly to a PC (with an Ethernet crossover cable). In the Management Configuration Menu, the IP Address, IP Mask and IP Gateway of the management port are configured, as described below and, then, the IP Address configured as a URL address can be used in an Internet browser or connection via Telnet, with the equipment requiring a specific license for the latter option. A Web page with a range of options will be opened in the browser, such as access to results for reports, parameter configurations, Software and License Updates, among others.

In the Configuration Management Menu the following configurations are presented:

- **IP Address** – Allows the management port IP address to be viewed and edited.
- **IP Mask** – Allows the management port IP mask to be viewed and edited.
- **IP Gateway** – Allows the Gateway to be viewed and edited in the case of using an intermediary computer for access to different networks.

Warning 1 – Management port Gateway out of range

"The IP configured in the management port is out of this Gateway's reach. The Gateway must be configured for an address able to reach the desired IP."

4.6. Load Factory Settings

This option allows for the restoration of all the TSW900ETH factory settings. To enable this action, press (→), in Load Factory Settings Menu and then confirm the operation by selecting with the (←) and (→) keys, press F1 to confirm.

Prior to confirming the restoration of factory settings, make sure there are no tests running.

4.7. Enter expiration code

This option, when available, allows to enter a key code which renews, if needed, TSW900ETH license.

In case TSW900ETH license expires, contact WISE technical support team, through the following ways:

- Support WISE:
  - E-mail: wise@wi.com.br
  - Phone: +55 61 3486-9100
  - Fax: +55 61 3486-9109

After providing sales code and expiration date, displayed in TSW900ETH screen, support team can provide liberation code, with new expiration date.

4.8. IPTV

This option, when available, allows to access IPTV feature configuration, which are detailed on section 5.11.

5. GENERAL TEST SET OPERATION

This section presents the general equipment operation, detailing the configurations related to the Ethernet tests (for example, Link, Ethernet, IP, Traffic, and RFC 2544 configurations, among others). All these configurations are set through the Port 1 and 2 tabs (accessed by function keys F2 and F3).

The F2 – Port 1 and F3 – Port 2 tabs are identical, each one corresponding to an independent port, (Port 1 and Port 2, respectively, with each one able to use optical or electrical interfaces).

If the Port 2 tab is not accessible, it is possible that your product is only licensed to use a single port. If necessary, contact our sales sector for more information on options and licenses.

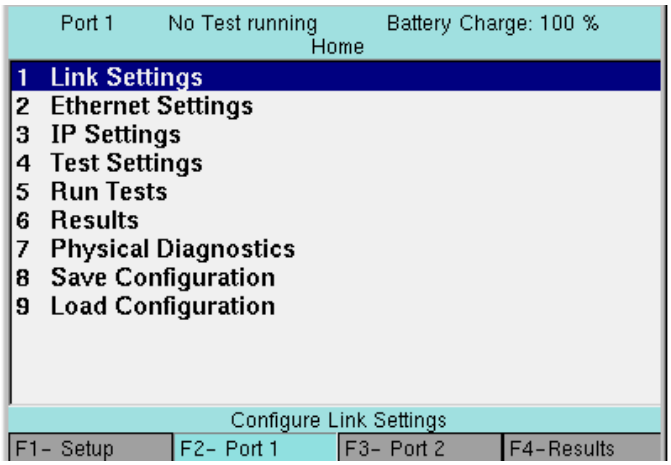


Figure 21. Port 1 initial screen (Tab F2)

Using the port tabs, it is possible to configure and run different tests for each of the ports. A simplified scheme of some available tests will be presented later.

5.1. Link Settings

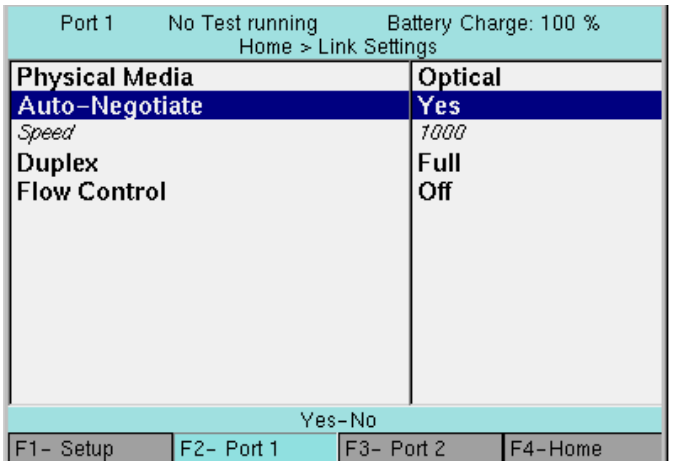


Figure 22. Link Settings

To configure the Ethernet Link, access the Link Settings option in the Home Menu. This option provides access to the following Link settings. Physical Media, Auto-Negotiate, Speed, Duplex mode and Flow Control.

The parameters of the link setting are described below:

5.1.1. Physical Media

This command allows you to configure the Link physical media. The following options are available:

- **Electrical** – Link through an electrical interface.
- **Optical** – Link through an optical interface.

5.1.2. Auto-Negotiate

Allows Auto-Negotiate to be enabled/disabled. The following options are available:

- **Yes** – Link with Auto-Negotiate.[1]
- **No** – Link without Auto-Negotiate.[2]

5.1.3. Speed

Set the Speed of the link or the maximum Auto-Negotiate limit. The following options are available:

- **10** – Speed of 10 Mbps.
- **100** – Speed of 100 Mbps.
- **1000** – Speed of 1000 Mbps.

[1] *If link partner is not autonegotiating, the link will be stablished on half-duplex mode.*

[2] *The behavior of a 1000Mbps link without autonegotiation in undetermined. It can present unspecified problems of all sorts. This option should only be used by experts on very particular test scenarios.*

Warning 12 - Stream rate higher than Speed

"The total Stream rate must be at most equal to the speed of the link. For example, in a link of 1000 Mbps, the rate of Streams can be a maximum of 1000 Mbps. This configuration does not permit tests to be started."

5.1.4. Duplex

Allows the Duplex mode to be selected. The following options are available:

- **Half** – Half Duplex link.
- **Full** – Full Duplex link.

5.1.5. Flow Control

Allows the Control Flow to be enabled/disabled, by means of identifying and treating pause frames. The following options are available:

- **Off** – pause frame processing disabled.
- **On** – pause frame processing enabled.

5.2. Ethernet option settings

Selecting the Ethernet Settings option in the Home Menu, it is possible to set general Ethernet configurations and apply different filters. The options presented in this menu are:

5.2.1. General Configuration

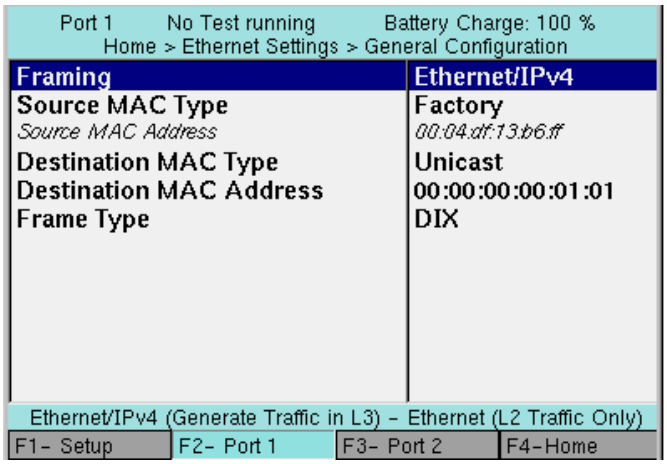


Figure 23. General Ethernet Configuration

Allows the type of frame and MAC address from the source and destination to be selected. The following options are available:

- **Framing** – Allows a choice between the Ethernet frame (only layer 2), Ethernet/IPv4 and Ethernet/IPv6 (enabling layer 3 to be processed).
- **Source MAC Type** – Allows the type of TSW900ETH source MAC address to be chosen. The following options are available:
  - **Factory** – Maintains the product's factory MAC address.
  - **Custom** – Enables the option of entering an MAC address for a device on the configuration screen.

- **Random** – The frames are sent randomly alternating the source MAC address.

- **Source MAC Address** – If the customized MAC address option is selected, it allows the source MAC address to be defined.
- **Destination MAC Type** – Allows the type of TSW900ETH source MAC address to be chosen. The following options are available:
  - **Unicast** – The frames are sent with the Unicast destination address,
  - **Broadcast** – The frames are sent with the Broadcast destination address;
  - **Multicast** – The frames are sent with the Multicast destination address,
  - **Random** – The frames are sent randomly alternating the destination MAC address.
- **Destination MAC Address** – Depending on the type of destination selected, it allows a destination MAC address to be defined.
- **Frame Type** – Allows the Ethernet frame type to be chosen. The following options are included:
  - **802.3** – The fames are sent using the IEEE 802.3 pattern.
  - **DIX** – The frames are sent in the Ethernet II, or DIX, format.

Warning 2 - Src and Dst MAC addresses are equal
"Two cards with the same MAC address should never exist in an Ethernet network. Invalid configuration situation. Only use this option if you are sure you want to force a situation that may result in an error."

5.2.2. VLAN Configuration

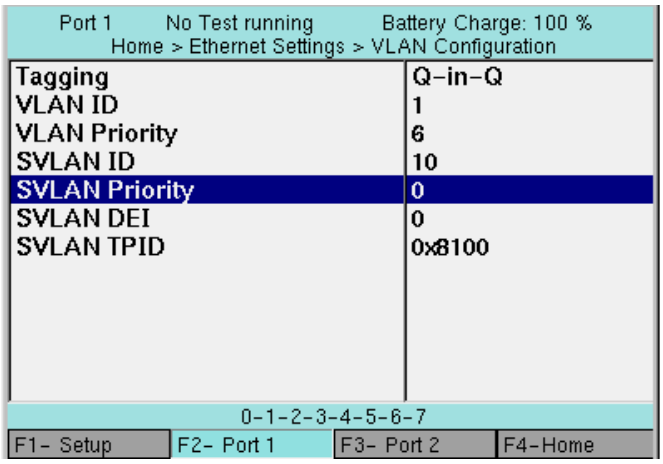


Figure 24. VLAN Configuration

Allows VLAN and Q-in-Q parameters to be configured. The following options are included:

- **Tagging** – Allows VLAN tag options to be enabled/disabled. The following options are included:
  - **VLAN** – Frames using a VLAN tag.
  - **Q-in-Q** – Frames using a VLAN tag encapsulated in another VLAN.
  - **Non-Tagged** – Frames without a VLAN tag insertion.
- **VLAN ID** – VLAN Identifier (VID) allows the ID of the VLAN to be defined. An editing field is opened (F1 confirms and F2 cancels the editing). The value 0 indicates that the frame does not belong to any VLAN, and the value 4095 is reserved and, thus, cannot be used.
- **VLAN Priority** – Defines the frame priority of 0 (lowest) to 7 (highest). It can be used to prioritize different types of traffic.

- **SVLAN ID** – Defines the most external tag ID, when configured for inserting two tags, (Q-in-Q). An editing field is opened for the SVLAN ID (F1 confirms and F2 cancels the editing).
- **SVLAN Priority** – Defines the priority of most external tag, when configured for inserting two tags, (Q-in-Q).
- **SVLAN DEI** – Defines the value of the most external tag Drop Eligible bit, when configured for inserting two tags, (Q-in-Q).
- **SVLAN TPID** – Allows the Tag Protocol Identifier (TPID) to be defined for use in the Q-in-Q tag. Options: 0x8100, 0x88A8, 0x9100, 0x9200 and 0x9300.

Warning 8 - VLAN ID or SVLAN ID defined as '0' or '4095'
"When the selected Tagging is VLAN or Q-in-Q, and the VLAN or SVLAN ID is defined as '0' or '4095', this message will appear. This occurs as the values of '0' and '4095' are reserved values.".

5.2.3. Ethernet Filter

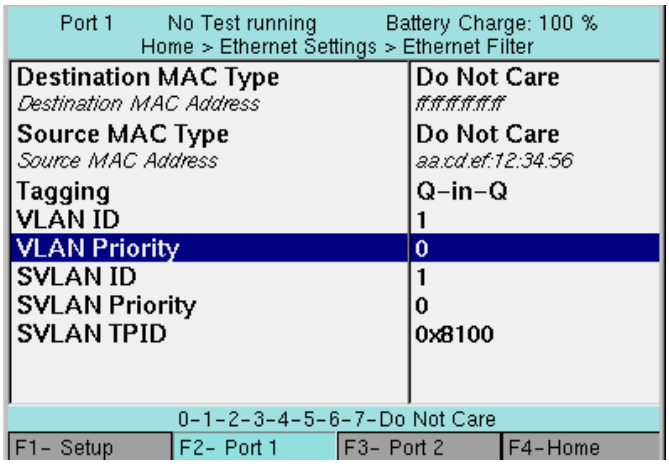


Figure 25. Ethernet Filters

Allows for the creation of filters according to origin/destination MAC addresses and VLAN and Q-in-Q tag parameters, similar to the Ethernet settings Menu. When a filter is defined as 'Do Not Care', this filter will be disabled for the parameter in question. Thus, the Test Set will continue to analyze a frame, regardless of this parameter. When a filter is enabled for a specific parameter, only the frames that pass through the configured filter (that is, they have a parameter equal to that defined in the filter) will be analyzed and counted. The following options are available:

- **Destination MAC Type** – Allows for the creation of frame filters for a specific type of destination MAC: Unicast, Broadcast, Multicast or Do Not Care.
- **Destination MAC Address** – When a Unicast or Multicast filter is enabled, it is possible to edit the destination MAC you want to filter.
- **Source MAC Type** – Similar to Destination MAC Type for the Source MAC.

Source MAC Address – Similar to Destination MAC Address for the Source MAC.

- **Tagging** – Allows filters to be configured for the VLAN or Q-in-Q tag parameters.
- **VLAN ID** – Allows for the creation of a filter for the VLAN tag ID.
- **VLAN Priority** – Allows for the creation of a filter for VLAN tag priority.
- **SVLAN ID** – Allows for the creation of a filter for the external tag ID (Q-in-Q).
- **SVLAN Priority** – Allows for the creation of a filter for the external tag priority (Q-in-Q).

- **SVLAN DEI** – Allows for the creation of a filter for the external tag DEI (Q-in-Q).
- **SVLAN TPID** – Allows for the creation of a filter for the external tag TPID (Q-in-Q).

Warning 3 – Adjusted to Unicast

"The configuration set in the MAC is incorrect. The MAC must have been configured for Broadcast or Multicast, but the type selected is Unicast."

5.3. Configuring the IPv4 options

The IPv4 options, that is, the configurations related to layer 3, can be accessed via the IP Settings Menu, located in the Home Menu. In the IP Settings Menu, different IPv4 header fields can be configured, in addition to the application of filters. This menu is only enabled if the type of frame is defined as Ethernet/IPv4 (Framing configuration, located in the Ethernet Settings Menu). The IPv4 Menu has the following options:

5.3.1. General Configuration

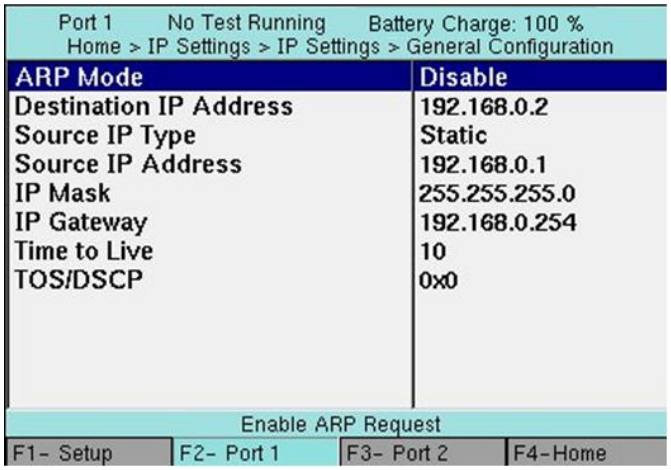


Figure 26. General IPv4 Configuration

Allows for general IPv4 layer configurations:

- **ARP Mode** – Allows for the ARP mode to be enabled/disabled (Enable/Disable, respectively). It is important to notice that the equipment does not respond to the ARP Solicitation when the Disable option is selected. In this case, if the TSW900ETH is being used as a Loopback, the equipment to be used to generate traffic must have the destination MAC address configured manually. Otherwise, leave the ARP option enabled.
- **Dst IP Address** – Allows the destination IPv4 address to be configured.
- **Src IP Type** – Allows the type of source IPv4 address to be configured, with this able to be static or obtained via DHCP (Static and DHCP, respectively).
- **Src IP Address** – Allows for the source IPv4 address to be configured, should the static Source IP Type have been selected.
- **IP Mask** – Allows for the configuration of the mask for the network to be used, should the static Src IP Type have been selected.
- **IP Gateway** – Allows the gateway to be used to be configured, should the static Source IP Type have been selected.
- **Time To Live** – Allows the Time to Live (TTL) value for IP packages to be configured.

- **TOS/DSCP** – Allows the configuration of the value of 6 ToS/DSCP bits, present in the header of the IPv4 packages.

Warning 6 - Src and Dst IP addresses are equal

"Equal IPs should not exist in a Ethernet network. Invalid configuration situation. Only use this option if you are sure you want to force a situation that may result in an error."

5.3.2. IP Header Filter

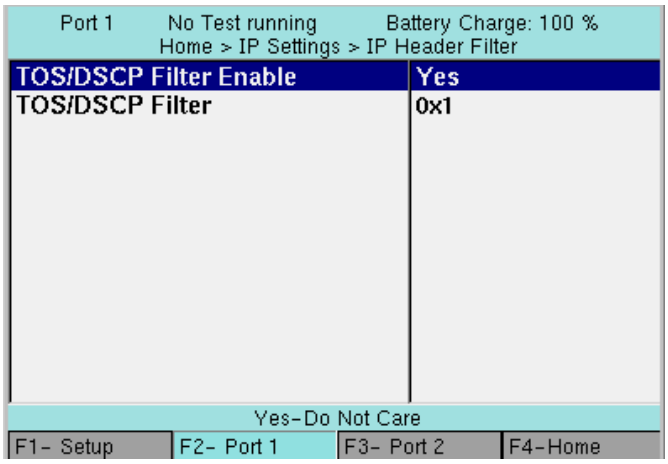


Figure 27. IP Header Filter

Filter configuration per ToS/DSCP and per TTL. When a filter is defined as 'Do Not Care', this filter will be disabled for the parameter in question. Thus, the Test Set will continue to analyze a frame, regardless of this parameter. When a filter is enabled for a specific parameter, only the frames that pass through the configured filter (that is, they have a parameter equal to that defined in the filter) will be analyzed and counted.

The filter descriptions are described below:

- **TOS/DSCP Filter Enable** – Allows the IPv4 package filter to be enabled/disabled per the ToS/DSCP value.
- **TOS/DSCP Filter** – Allows a filter to be created for a ToS/DSCP value.

5.3.3. IP Address Filter

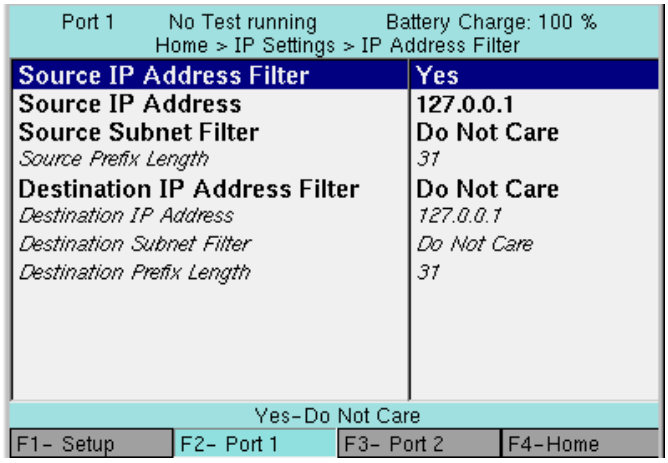


Figure 28. Address Filters

Allows filters to be configured through IPv4 addresses. When a filter is defined as 'Do Not Care', this filter will be disabled for the parameter in question. Thus, the Test Set will continue to analyze a frame, regardless of this parameter. When a filter is enabled for a specific parameter, only the frames that pass through the configured filter (that is, they have a parameter equal to that defined in the filter) will be analyzed and counted.

The filter descriptions are described below:

- **Source IP Address Filter** – Allows the filter to be enabled/disabled through the source IP address.
- **Source IP Address** – Allows a source IP address to be defined for filtering.
- **Source Subnet Filter** – Allows the mask to be enabled/disabled for the source IP address to be filtered. Disabled is equal to configuring the SRC Prefix Length to 32.
- **Source Prefix Length** – Allows for the definition of the size of the mask for the source IP to be filtered (example: 8 equals Src IP Address/8, thus it will filter all packages whose first 8 bits of the source IP are equal to IP Src Address). 1 to 31 are possible values;
- **Destination IP Address Filter** – Allows a filter to be enabled/disabled per destination IP address.
- **Destination IP Address** – Allows for the definition of a destination IP address for filtering.
- **Destination Subnet Filter** – Allows the mask to be enabled/disabled for the destination IP address to be filtered. Disabled is equal to configuring the Dst Prefix Length to 32.
- **Destination Prefix Length** – Allows for the definition of the size of the mask for the destination IP to be filtered (example: 8 equals Dst IP Address/8, thus it will filter all packages whose first 8 bits of the source IP are equal to IP Dst Address). 1 to 31 are possible values.

Warning 7 – Src and Dst IP Addresses are in different networks

"The configured source and destination IPs are in different networks. Thus, it will not be possible to reach the destination or the source. Invalid configuration situation. Only use this option if you are sure you want to force a situation that may result in an error."

5.4. Configuring the IPv6 options (optional)

The IPv6 options, that is, the settings related to layer 3, can be accessed through the IP Settings Menu, as with IPv4. In this menu it is possible to set configurations for the different IPv6 header fields, as well as filter applications. This menu is only enabled if the type of frame is defined as Ethernet/IPv6 (Framing options, located in the Ethernet Settings Menu). The IP Settings Menu has the following options:

5.4.1. General Configuration

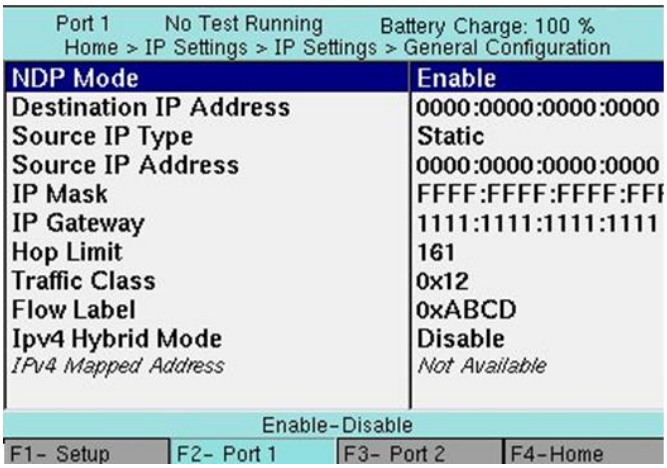


Figure 29. IPv6 Address Filters

Warning 10 - Invalid Frame Size. Change to 'n' bytes - IPv6

"When the size of the frame is defined for a value lower than 'n' bytes, with Ethernet/IPv6 Framing and, then, the extension header configurations, Tagging or UDP were altered, this minimum size must be adjusted to 'n' bytes. The value of 'n' varies according to the number of headers added and with the test options (example: active Q-in-Q and UDP), and will be calculated and presented through the application to the user. The application with automatically adjust this value."

Allows for general IPv6 header configurations:

- **NDP Mode –** Allows for the NDP mode to be enabled/disabled (Enable/Disable options, respectively). It is important to note that the equipment does not respond to the Neighbor Solicitation when the Disable option is selected. In this case, if the TSW900ETH is being used as a Loopback, the equipment to be used to generate traffic must have the destination MAC address configured manually, to the contrary leave the NDP option enabled.
- **Destination IP Address** – Allows the destination IP address to be configured.
- **Source IP Type** – Allows the type of source IP address to be configured, it possibly being static, obtained by DHCPv6 or obtained by Stateless.
- **Source IP Address** – Allows for the source IP address to be configured, should the static Source IP Type have been selected.
- **IP Mask** – Allows for the configuration of the mask for the network to be used, should the static Source IP Type have been selected.
- **IP Gateway** – Allows the gateway to be used to be configured, should the static Source IP Type have been selected.
- **Hop Limit** – Allows the Hop Limit value of the IPv6 package to be configured.
- **Traffic Class** – Allows the Traffic Class value of the IPv6 packages to be configured.
- **Flow Label** – Allows the Flow Label value of the IPv6 packages to be configured.
- **IPv4 Hybrid Mode** – Allows the hybrid mode to be enabled/disabled between the IPv6**/**IPv4**.** If the hybrid mode is enabled, the IPv4 function processing remains enabled, with responses to pings and ARPs.
- **IPv4 Mapped Address** – Allows the mapped IPv4 address to be configured to the IPv6 address.

5.4.2. IP Header Filter

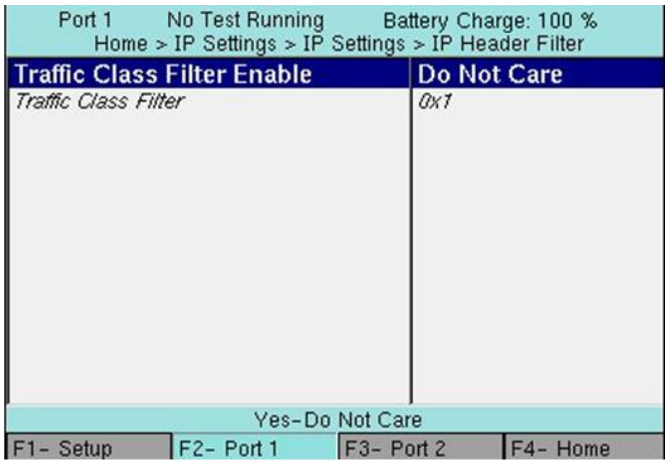


Figure 30. IPv6 Address Filters

Allows filter configuration by Traffic Class. When a filter is defined as 'Do Not Care', this filter will be disabled for the parameter in question. Thus, the Test Set will continue to evaluate a frame due to this parameter. When a filter is enabled for a specific parameter, only the frames that pass through the configured filter (that is, they have a parameter equal to that defined in the filter) will be analyzed and counted.

The filter descriptions are described below:

- **Traffic Class Filter Enable** – Allows the IPv6 filter to be enabled/disabled by the Traffic Class value.
- **Traffic Class Filter** – Allows a filter to be created for a Traffic Class value.

5.4.3. IP Header Filter

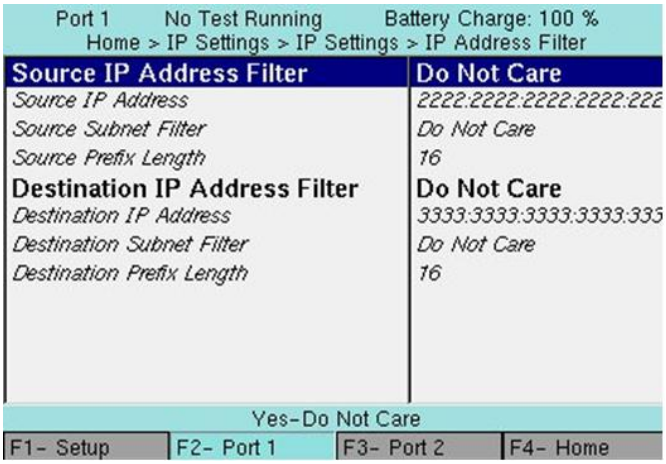


Figure 31. IPv6 Address Filters

Allows filters to be configured through IPv6 addresses. When a filter is defined as 'Do Not Care', this filter will be disabled for the parameter in question. Thus, the Test Set will continue to analyze a frame, regardless of this parameter. When a filter is enabled for a specific parameter, only the frames that pass through the configured filter (that is, they have a parameter equal to that defined in the filter) will be analyzed and counted.

The filter descriptions are described below:

- **Source IP Address Filter** – Allows the filter to be enabled/disabled through the source IPv6 address.

- **Source IP Address** – Allows a source IPv6 address to be defined for filtering.
- **Source Subnet Filter** – Allows the prefix for the source IP address to be filtered to be enabled/disabled. Disabled is equal to configuring the Source Prefix Length to 32.
- **Source Prefix Filter** – Allows for the definition of the size of the mask for the source IPv6 to be filtered (example: 8 equals Source IP Address/8, thus it will filter all packages whose first 8 bits of the source IP are equal to IP Source Address). 1 to 31 are possible values;
- **Destination IP Address Filter** – Allows a filter to be enabled/disabled per destination IPv6 address.
- **Destination IP Address** – Allows for the definition of a destination IPv6 address for filtering.
- **Destination Subnet Filter** – Allows the prefix to be enabled/disabled for the destination IPv6 address to be filtered. Disabled is equal to configuring the Destination Prefix Length to 32.
- **Destination Prefix Filter** – Allows for the definition of the size of the mask for the destination IPv6 to be filtered (example: 8 equals Destination IP Address/8, thus it will filter all packages whose first 8 bits of the destination IP are equal to IP Destination Address). 1 to 31 are possible values.

5.4.4. Extension Header

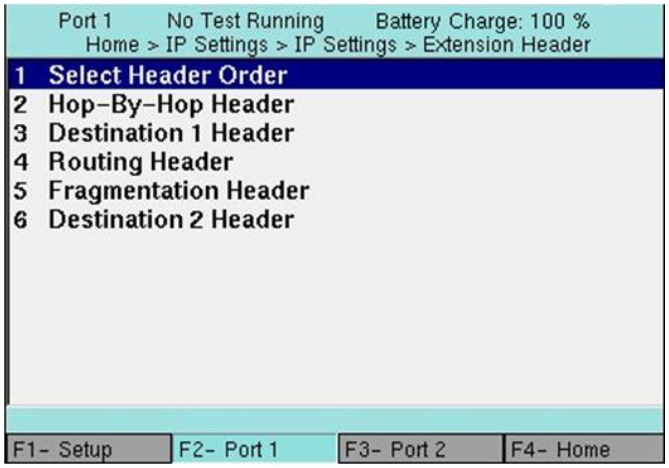


Figure 32. Extension Header

Allows for the configuration of the extension header in the IPv6 header.

Below is a description of the extension header options:

- **Select Header Oder** – Allows you to enable/disable the 5 extension headers available in the IPv6. It is possible to configure the following headers: Hop-by-Hop, Destination 1, Routing, Fragmentation and Destination 2. Note that an extension header cannot be selected more than once. The following options are presented:
    - **1st, 2nd, 3rd, 4th, 5th Header** – Allows you to enable/disable each IPv6 extension header. When the Disable option is selected, the header will not be used.
- **Hop-by-Hop Header** – Allows you to configure the Hop-by-Hop header options.
- **Destination 1** – Allows you to configure the Destination 1 header options.
- **Routing** – Allows you to configure the Routing header options.
    - **Type** – Identifies the type of package routing.
    - **Segments** – Number of intermediary nodes that must be inspected prior to the destination.

- **Data** – determined in accord with the routing algorithm. It must be a full value multiple of 64 bits.

- **Destination 2** – Allows you to configure the Destination 2 header options.
- **Fragmentation** – This header is used when a packed to be sent is bigger than the path MTU to the destination.
  - **Offset** – Indicates the position in the package at which this fragment must be inserted.
  - **ID** – Identification of the original package. This information must be unique in the network while the package is fragmented.

5.5. Setting Tests

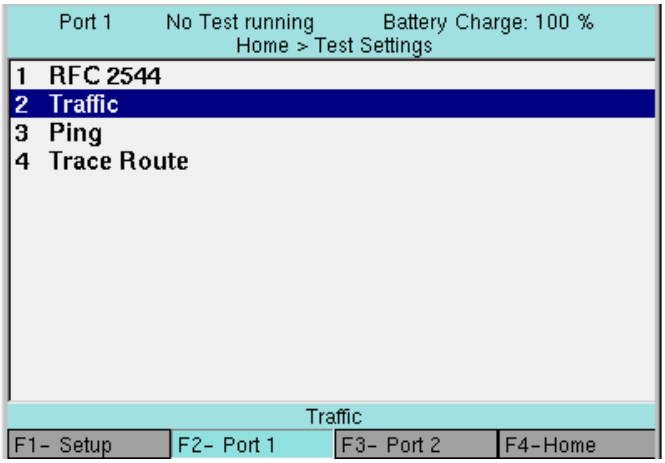


Figure 33. Test Settings Menu

The Test Settings Menu, accessible through the Home Menu, allows you to configure RFC 2544, traffic, Ping and Trace Route tests. The following options are available:

5.5.1. RFC 2544

Allows you to set configurations for RFC 2544 tests:

- **Enable Tests** – Allows you to enable/disable the available RFC 2544 tests. The following options are presented:
  - **Throughput** – a test used to determine the maximum rate of DUT (device Under Test) use, without any errors.
  - **Latency** – Round Trip Delay (RTD) test, used to check DUT transmission delay, that is, the time a frame takes to go and return when operating at the throughput rate (rate calculated in the Throughput test). As the maximum throughput value is required, this test cannot be executed without a Throughput test.
  - **Frame Loss Rate** – Frame loss test, used to check the overload point for equipment/network under test.
  - **Back-to-Back** – Burst tests, used to determine the capacity of the equipment/network being tested for retransmitting traffic without a time interval. The result of the test is the size of the largest burst that the DUT handles without any loss.
- **General Settings** – This allows one to configure, for all RFC 2544 tests, the maximum bandwidth and the frames sizes to be tested, as well as the size of the jumbo (oversized) frames, which can be enabled or not, in addition to configuring the dual stack (the dual stack option will only be available if the IPv6 license is activated). Options are:
  - **Frame Settings** – Configure frame options. The following options are included:

        - **Max Bandwidth** – Allows you to configure the maximum percentage of bandwidth used during the test. Minimum is 1% and maximum is 100%.
        - **64, 128, 256, 512, 1024, 1280, 1518** – Allows you to enable/disable the used of frames with the sizes shows (in bytes) in RFC 2544 tests.
        - **Jumbo Frames** – allows you to enable/disable the use of frames with a size larger than that cited by RFC 2544 IEEE802.3 (oversized/jumbo frames, with a size over 1518 bytes).
        - **Jumbo Size** – allows you to configure the frame size larger than the size listed by IEEE 802.3 (oversize/jumbo frames). Maximum size of 10k bytes.
    - **Rate Settings (IPv6 optional)** – Allows you to configure the dual stack in the RFC 2455, that is, it allows you to generate packages with IPv4 and IPv6 protocols in the hybrid manner. The following options are included:
        - **Max Bandwidth** – Allows you to configure the maximum percentage of bandwidth used during the test. Minimum is 1% and maximum is 100%.
        - **IPv4 100% - 0% IPv6** - Defines that all packages sent will use IPv4.
        - **IPv4 90% - 10% IPv6** - Defines that the packages will be sent, 90% using IPv4 and 10% using IPv6.
        - **IPv4 50% - 50% IPv6** - Defines that the packages will be sent, 50% using IPv4 and 50% using IPv6.
        - **IPv4 10% - 90% IPv6** - Defines that the packages will be sent, 10% using IPv4 and 90% using IPv6.
        - **IPv4 0% - 100% IPv6** - Defines that all packages sent will use IPv6.
- **Throughput Config** – Allows you to set the configurations for the flow test, if it is enabled. Include the following options:
    - **Durations (s)** – Allows you to configure the duration of each of the test attempts, from 3 to 1000 seconds.
    - **Bandwidth Granularity (%)** – Allows you to configure the accuracy of the obtained result (bandwidth precision). Contains the options 1, 0.1 and 0.01, which correspond to accuracies of 1, 0.1 and 0.01%.○
    - **Bandwidth Loss Tol (%) –** Allow to configure test acceptance limit, when configured “Pass Threshold” is not reached. For example: If “Pass Threshold” is 100% and “Bandwidth Loss Tol” is 5%, and the test reaches 95%~100% threshold, test will successfully executed.
    - **Pass Threshold (%)** – Allows you to configure a minimum limit for the approval of the Throughput test, like a bandwidth percentage in relation to the maximum bandwidth. This value must be equal to or less than the Max Bandwidth value and will be used in the report to indicate if the final test result passed or not.
- **Latency Config** – Allows you to set the configurations for the latency test, if it is enabled. Include the following options:
    - **Durations (s)** – Allows you to configure the duration of each of the test repetitions, from 1 to 1000 seconds.
    - **Number of Trials** – allows you to configure the number of test repetitions, between 1 and 100, for latency tests. Values lower than 20 are not in accordance with that specified by regulation RFC 2544.
    - **Pass Threshold (ms)** – Allows you to configure the maximum limit of time for frame return, for a latency test pass, from 0.001 to 5000 ms. It is used to indicate if the final result of the test passed or not.

- **Frame Loss Rate Config** – Allows you to set the configurations for the frame loss test, if it is enabled. Include the following options:
    - **Durations (s)** – Allows you to configure the duration of each of the test repetitions, from 1 to 1000 seconds.
    - **Bandwidth Granularity (%)** – Allows you to configure the bandwidth granularity for the Frame Loss test (decreasing value of the transmission rate for each repetition of the test, from 1 to 100%). Values set above 10% are not in compliance with regulation RFC 2544.
- **Back-to-Back Config** – Allows you to set the configurations for the Back-to-Back Frames test, if it is enabled. Include the following options:
    - **Duration (s)** – Contains an editing field to configure the duration of the first burst, from 1 to 1000 seconds. Values set above 2 seconds are not in compliance with regulation RFC 2544.
    - **Frame Granularity** – Allows you to configure burst granularity (decreasing value of the burst size for each test repetition, from 1 to 1000 frames).
    - **Number of Trails** – Allows you to configure the number of Back-to-Back Frames test attempts. The final results will be the average of the partial results for each size of the selected frame. Values lower than 50 will not be in compliance with regulation RFC 2544.
- **System Recovery** – Allows you to set configurations for the System Recovery test, if it is enabled. This test is not available in this version of the equipment. Include the following options:
    - **Duration (s)** – Allows you to configure the duration of the test in seconds.
    - **Number of Trails** – Allows you to configure the number of attempts.
- **Reset Config** – Allows you to set the configurations for the Reset test, if it is enabled. This test is not available in this version of the equipment. The following option is included:
    - **Number of Trials** – Allows you to configure the number of test repetitions, between 1 and 100.

5.5.2. Traffic

Allows you to set configurations for traffic tests: It includes the following items:

- **Traffic Test Type** – Allows you to configure the Traffic Type to be generated, with the following options:
    - **Single Stream** – A single stream of data.
    - **Multiple Streams** – Multiple stream of data configured independently (optional product functionality). When operating with protocol IPv6 (optional), it is possible to also generate dual stack streams in multiple flows. In this case the generated streams can by hybrid (IPv4 and IPv6 simultaneously).
    - **Promiscuous Timestamp**: (disable recommended). Use this function if you want to force the TSW900ETH to identify and count a Timestamp type frame from another TSW900ETH, without the use of loopback. To do so, both pieces of equipment (generator and receiver) must have the function enabled and the same “Timestamp ID” value configured. Only use this function if you are certain of your need, to the contrary, static data for time (delay and jitter), lost frames and test out of sequence are inconsistent. Function not available for Ramp type traffic and RFC 2544 tests.

Warning 13 – Not recommended configuration

“Warns the user that enabling Promiscuous Timestamp is not a recommended configuration”

- **Frame Setting** – allows you to configure the frame size or define it with a random size. It includes the following items:
    - **Frame Size Type** – Allows you to configure the type of frame per size. Includes options like Undersized (frames smaller than the normal size), Normal (frames from 64 to 1518 bytes)[3], Jumbo (frames above the normal size) and Random (randomly sized frames).
    - **Fixed Frame Size** – Allows you to configure the frame size, should you choose to use a fixed size for all the frames.
    - **Payload Type** – Allows you to choose what should be used as content in the frame, includes options like Timestamp (necessary for gauging Delay, Jitter, Lost Frames and OoS Frames) and BERT (necessary for BERT measurements).
    - **BERT Pattern** – If the BERT type payload is configured, it allows you to choose the pattern, bit sequence, what will be inserted into the payload, while at the same time conferring the payload received to learn if it is the same sequence sent. There are two ways of running the BERT test: with a single piece of equipment generating and checking the pattern and another in Loopback, and with two pieces of equipment generating and checking the pattern. In the second case both pieces of equipment must be configured with the same pattern. The following options are available:
        - **2^23-1** – Pseudo-random sequence with a size of 2^23-1.
        - **2^23-1 Inv** – The same sequence as before with inverted bits.
        - **2^31-1** – Pseudo-random sequence with a size of 2^31-1.
        - **2^31-1 Inv** – The same sequence as before with inverted bits.
        - **All Ones** – All the bits in 1.
        - **All Zeros** – All the bits in 0.
        - **User Defined** – Allows the user to define four bytes that will for the payload of the frames.
    - **User Defined Pattern** – Enabled when the BERT Patter is configured as User Defined. Allows you to set a personalized BERT pattern, entering the value, in hexadecimals, of the byte that will fill the payload.

For the correct analysis of the signal in BERT tests, both the port that is generating the traffic and the port receiving or in loopback mode must be configured with the same type of bit sequence pattern.

The minimum size permitted for the generation of traffic will depend on the configuration of certain header parameters and there payloads. Table 4. shows the minimum and maximum sizes that can be configured for the frames, depending on the layer (Ethernet, Ethernet/IPv4 or Ethernet/IPv6), the payload type configured (BERT or Timestamp) and the inclusion of VLAN tags.

[3] *If there is no tag (VLAN or SVLAN) configured, the maximum Normal frame size is 1518 bytes. But, if there is a VLAN tag, the maximum Normal frame size increases to 1522 bytes. If there is a SVLAN tag, the maximum Normal frame size increases to 1526 bytes.*

Type of Payload	Minimum Size (bytes)									Maximum Size (bytes)
	Ethernet			Ethernet/IPv4			Ethernet/IPv6			
	No VLAN	One VLAN	Two VLANs	No VLAN	One VLAN	Two VLANs	No VLAN	One VLAN	Two VLANs	
BERT	*40	44	48	*60	64	68	68	72	76	10000
Timestamp	64	68	72	64	68	72	76	80	84	10000

Table 4. Minimum and Maximum Frame sizes

***** When configured for the transmission of random frames, minimum size = 64 bytes.

Warning 10 - Invalid Frame Size. Change to 'n' bytes - IPv4

"When the size of the frame is defined for a value lower than 'n' bytes, with Ethernet/IPv4 Framing and, then, the Tagging and UDP configurations were altered, this minimum size must be adjusted to 'n' bytes. The value of 'n' varies according to the selected configurations (example: active Q-in-Q and UDP), and will be calculated and presented through the application to the user. The application with automatically adjust this value."

- **Traffic Settings** – Allows you to choose the type of traffic generated, as well as specific configurations of each type. Include the following options:
  - **Load Type**– allows you to choose the type of traffic generated, or traffic profile (see section 2.1.1 where the traffic generation profiles are presented and explained). Include the following options:
    - **Constant** – Constant band traffic. In the constant traffic option, if the TSW900ETH is configured to transmit a load of 100%, it will transmit a little less than 100% (99.99% for optical 100/1000 Mbps, 99.98% for electrical 10/100/1000 Mbps) as a form of security against network elements that would not be able to handle 100%. But if the option is Flood, it will transmit the real rate of 100%.
    - **Flood** – Constant traffic at real 100%. Use when you are sure all elements of the network being tested can handle this rate. To the contrary, set it as another type of traffic (Constant, Burst, Ramp or Time) and set the rate at 100%.
    - **Burst** – Traffic in bursts. When setting the Load Type equal to Burst, the TSW900ETH transmits a burst of N frames in accordance with the set transmission rate (up to 100%), according to the set Burst Size, then followed by a pause, without transmission. This step is repeated indefinitely if the Burst Type is configured to Continuous or repeats the number of times set in Burst Quantity, if configured to Fixed.

        - **Ramp** – Traffic in ramps. The ramp test is a quick method of finding the maximum rate of a link. When the Load Type is equal to Ramp, the TSW900ETH will initiate a transmission of 1% of the link rate, increasing at a rate of 1% every second, until detecting an error. For each increase, the TSW900ETH does not pause transmission, generating the traffic directly at the new rate instead, without interruptions.

        - **Time** –Traffic by time. In the traffic by time options, the TSW900ETH will transmit data at the rate set during the configured time, ending transmission at the end of this period.

    - **Load Units** – Allows you to define if the traffic generation rate to be used will be configured as a percentage, Percent option, or as a direct rate, Bit Rate option (configure the rate in Mbps).
    - **Load Bit Rate (Mbps)** – Allows you to set the traffic generation rate if the Load Units are configured to Bit Rate.
    - **Load Bit %** – Allows you to set the traffic generation rate as a percentage if the Load Units are configured to Percent.
    - **Burst Size (Frames)** – If the burst mode is selected, it allows the size of the generated frames to be chosen (options: 16, 64, 256, 1024 or User Defined – in the last, the user selects a personalized size).
    - **User Burst Size** – Allows you to edit the size of the generated frames, if the option User Defined is selected in Burst Size.
    - **Burst Type** – Allows you to select the type of burst as Fixed or Continuous.
    - **Burst Quantity** – Allows you to select the number of frames generated in the Burst mode, if Burst Type is configured as Fixed.
    - **Test Time** – Allows you to choose the duration of the test if Load Type is configured as Time.

- **Streams Settings** – Configuration of Multiple Streams, if this option is available. The following configuration options are available:
    - **General Settings** –General settings for Multiple Streams:

        - **Transmission Streams** – Defines the number of streams to be generated and transmitted by the Test Set, ranging from 2 to 8.

    - **Stream Rates** – Configuration of the rates that each configured stream should occupy in the total band transmitted. The configured values are a percent of the obtained link (the total sum of the rates of all the streams cannot exceed 100%).

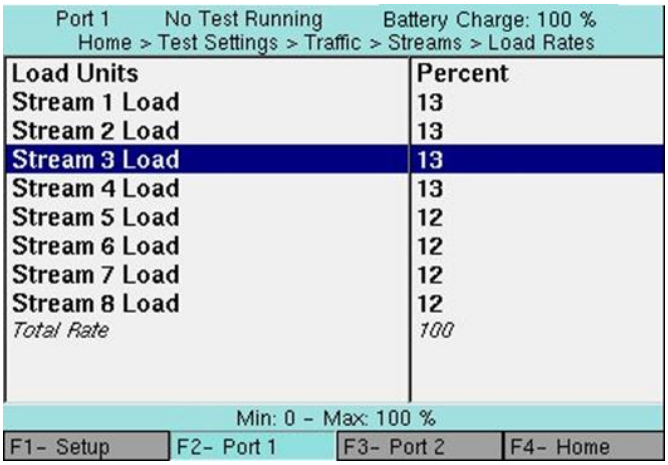


Figure 34. Streams Load Rates Menu

Warning 11 - Stream rate higher than 100%

"The total rate of Streams must be at most 100%. This configuration does not permit tests to be started."

- **Load Units** – Allows you to define if the traffic generation rate to be used will be configured as a percentage, Percent option, or as a direct rate, Bit Rate option (configure the rate in Mbps).
  - **Stream 1 Load** - Stream 1 transmission rate.
  - **Stream 2 Load** - Stream 2 transmission rate.
  - **Stream 3 Load** - Stream 3 transmission rate.
  - **Stream 4 Load** - Stream 4 transmission rate.
  - **Stream 5 Load** - Stream 5 transmission rate.
  - **Stream 6 Load** - Stream 6 transmission rate.
  - **Stream 7 Load** - Stream 7 transmission rate.
  - **Stream 8 Load** - Stream 8 transmission rate.
- **Total Rate** – States the total transmission rate used by the sum of the streams.
- **Stream Setup** – This menu holds the specific configurations of each stream to be generated, in accord with the table below:
  - **Stream 1** – The stream 1 configuration options are detailed below and are repeated for all 8 streams.
    - **Ethernet Settings** –Configuration of MAC addresses the frame type. Through this option it is possible to configure dual stack. Simply configure a stream for Ethernet/IPv4 and another stream for Ethernet/IPv6
    - **VLAN Configuration** – Configuration of VLAN tags
    - **IP Configuration** – Configuration of IP header parameters, when configured to operate in layer 3.
    - **Frame Settings** – Frame size settings
    - **Copy** – Option of copying the stream settings for all the other streams.

5.5.3. Ping

Allows you to set configurations for Ping tests. The following options are presented:

- **Number of Packets** – Allows you to set the number of ICMP request packets sent during the test. If the 0 value is selected, the packets will be sent indefinitely.
- **Ping Interval (ms)** – Allows you to configure the interval between each packet sent during the Ping test.
- **Timeouts to retry ARP** – Allows you to configure whether the TSW900ETH makes new ARP requests during Ping test errors (if the ARP mode is enabled). If the 0 value is chosen, no new ARP request will be made and the destination MAC address is maintained. Values different to 0 indicate that after this number of timeouts (Pings with no responses) the equipment assumes that the destination MAC address can be modified or lost, and a new ARP request will be made.
- **Ping Payload Size** – Allows you to configure ping packet payload size. Can be configured with any value between 32 and 1900 bytes.

5.5.4. Trace Route

Allows the configurations to be set for the Trace Route test. Running the Trace Route test can determine where problems in the network are occurring.

The only option available is:

- **Max hops** – Allows you to define the maximum number of packet hops until reaching the destination (maximum: 255).

Layer 3 tests are only enabled if Home > Ethernet Settings > General Configuration > Framing is configured as Ethernet/IPv4 or Ethernet/IPv6.

For tests with IP, remember to check the correct configuration of the source and destination IPs in the network and confirm if the generation of ARP or NDP is duly enabled or disabled.

5.5.5. ITU-T Y.1564 Script (Embedded Script)[4]

Allows to configure TSW900ETH to execute ITU-T Y.1564 test script.

The script has the following options:

- **Test Identifier** – Allows to configure test name to check saved results in WEB interface.
- **Enable test options** – Allows to enable test options: CIR, Color Aware, Policing Test, Performance and Loopback.
- **Number of services** – Configures number of streams used during test (in case color aware option is available, services can be configured up to 4. If not, services can be configured up to 8).

[4] *To execute Y.1564 embedded test script, it is mandatory that both ports are configured in Multiple Streams mode, with each stream source and destination addresses correctly configured, in order to avoid data transmission issues.*

- **CIR Test Time** – CIR test execution time.
- **Performance Test Time** – Performance test execution time.

For each service:

  - **CIR (Mbps)** – CIR load rate.
  - **EIR (Mbps)** – EIR load rate.
  - **FLR (%)** – Frame Loss Rate value (percentage).
  - **FTD (ms)** – Frame Transfer Delay time, in milliseconds (ms), which means TSW900ETH delay.
  - **FDV (ms)** – Frame Delay Variation time, in millisenconds (ms), which refers to TSW900ETH jitter.

5.6. Running Tests

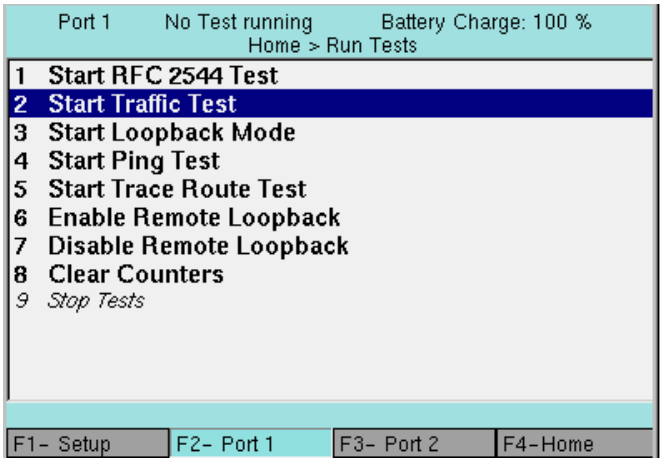


Figure 35. Run Tests Menu

The initiation/finalization of all available tests (RFC2544, Traffic and Loopback), can be implemented via the Run Test options, in the Home Menu. This option, besides initiating and finalizing tests, also includes the commands for reinitiating the counters and remote Loopback.

These options can also be obtained by pressing the Start/Stop shortcut key.

- **Start RFC 2544 Test** – Allows you to start the RFC 2544 test.
- **Start Traffic Test** – Allows you start the Traffic test.
- **Start Loopback Mode** – Allows you to start Loopback mode.
- **Start Ping Test** – Allows you to start the Ping test.
- **Start Trace Route Test** – Allows you to start the Trace Route test.
- **Enable Remote Loopback** – Allows you to start Loopback mode in a remote Test Set.
- **Disable Remote Loopback** – Allows you to disable Loopback in a remote Test Set.
- **Clear Counters** – Allows you to restart the counters.
- **Stop Test** – allows you to stop a test that is running.

5.7. Viewing Results

To view the results of a test that is running or the last test run, select Results, in the Home Menu. Accessing this option, it is possible to view the results of RFC 2544 tests, a range of statistics, counters (Link, BERT, etc.), among other information. The options are presented in detail below.

The counters are accumulative among the tests, and are only cleared in the following situations:

- The equipment is turned off.
- The Clear Counters function is used.
- There is an exchange between the generation tests and Loopback, or vice-versa.

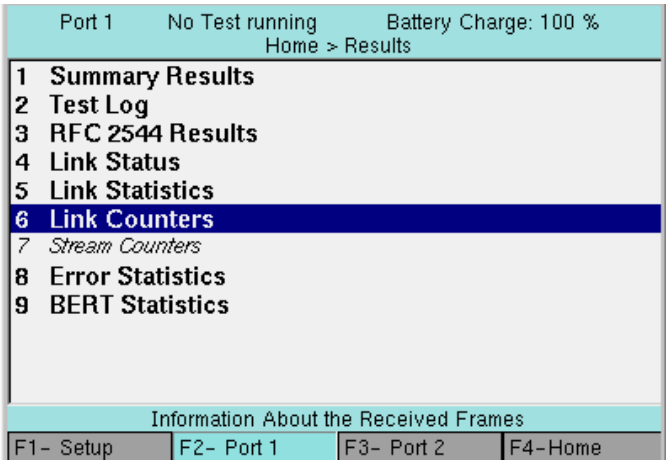


Figure 36. Results Menu

5.7.1. Summary Results

Presents a result summary of the last test ran or the status of a test that is running. If there are no errors, the message “ALL RESULTS OK” appears, to the contrary a summary of errors present is shown.

- **Errors Summary** – Shows a summary of the errors found. They are:
  - **Status** – Shows the status of the link, if active or not.
  - **Link Active** – Shows that the link is active during the test - Link Up, or if there is a break in connection during the test - Link Lost. Link Down indicates the connection remains inactive.
  - **Sync** – Indicates the status of BERT sequence synchrony (Up or Down).
  - **Errors** – Indicated if an error has occurred (Present).

5.7.2. Test Log

This present the log from the last test ran or the test that is running, if one exists.

5.7.3. RFC 2544 Results

The TSW900ETH screen presents the results from the last RFC 2544 test ran. The following options are shown:

- **Throughput –** Results of the last Throughput test. The following options are presented:

    - Chart – Graph with the results of the Frame Rate x Frame Size (ideal curve and curve obtained in test). See Figure 37.

    - Table – Table with the results of the Throughput test. See Figure 38.

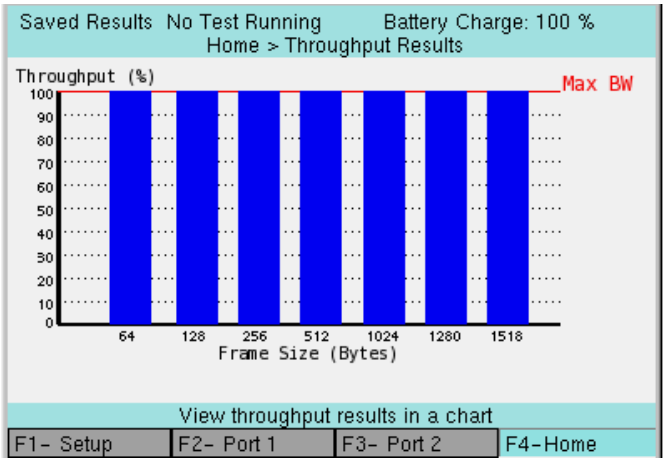


Figure 37. Chart result example (Throughput)

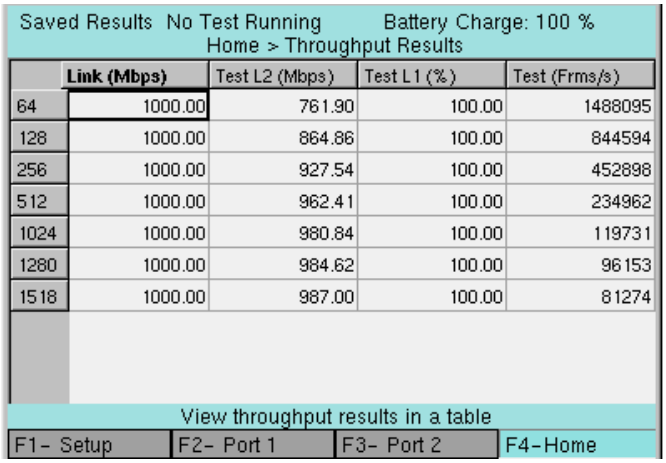


Figure 38. Table result example (Throughput)

- **Latency –** Presents a table with the results of the latency test.

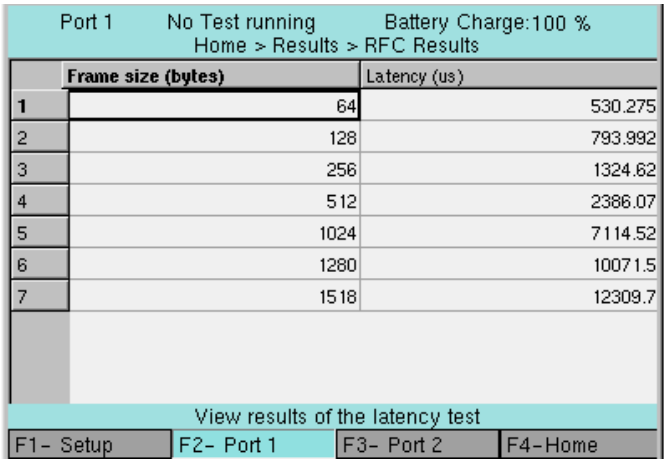


Figure 39. Latency test results

- **Frame Loss Rate** – Presents a graph representing Frame Loss Rate x Frame Rate, both in percent, showing the results of the Frame Loss test. A page is opened for each frame size tested.

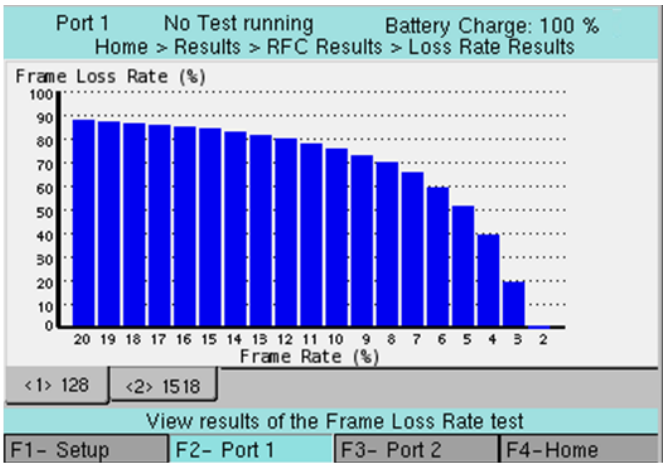


Figure 40. Frame Loss Test results

- **Back-to-Back** – Presents a table with the results of the Back-to-Back Frames test. The result for each size of the frame tested is the average of the number of frames returned without loss, for each attempt and the equivalent time of the burst in seconds.

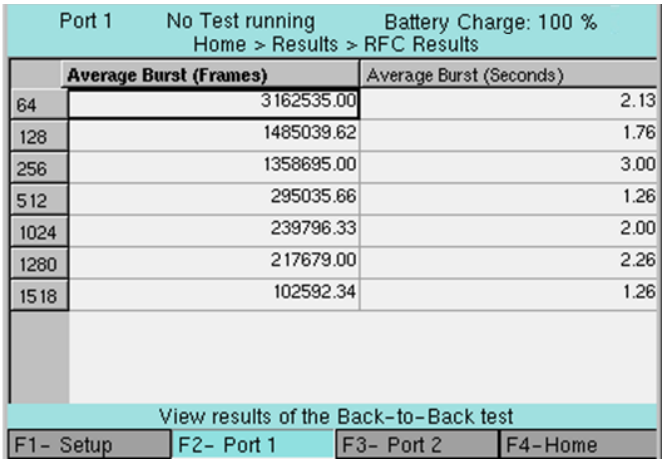


Figure 41. Back-to Back test results

- **Set Operator** – allows you to edit the name of the operator that ran the test (so that this name is presented with the results if it is saved).

- **Save Results** – Allows you to save the results of the last test run. These results can then be accessed later on the Results (tab F4) screen and in the Results option of the Web browser to view the reports.

5.7.4. Link Status

Presents the active link information: link status, speed, duplex mode and physical media.

5.7.5. Link Statistics

Presents a range of statistics obtained about the transmitted/received data, among them the delay and jitter (so that the two are obtained, it is necessary that the payload of the frame is Timestamp). The description of each counter is as follows:

- **RX Util %** – Shows the reception rate as a percent of the maximum possible rate considering frame size. The variations are to indicate the average vale (**Avg**), current (**Cur**), maximum (**Max**) and minimum (**Min**).

- **RX Frame Rate** – Shows the rate of frames received, in frames per second. The variations are to indicate the average **(Avg)**, current **(Cur),** maximum **(Max)** and minimum **(Min)** values.

- **RX/TX L1 Mbps** – Shows the theoretical data rate, in Mbps.

- **RX/TX L2 Mbps** – Shows the rate of data received/transmitted in layer 2 (Ethernet), ignoring the preamble and interval between frames.

- **Last Frame Size** – Size of the last frame received.

- **Delay µs** – Delay time, calculated in microseconds, taking between the sending and reception of the frame. Only available if the payload is Timestamp. The variations are to indicate the average vale **(Avg)**, maximum **(Max)** and minimum **(Min)**.

- **Pkt Jitter µs** – Gauges the delay variation between frames, in microseconds. Only available if the payload is Timestamp. The variations are to indicate the average vale **(Avg)**, maximum **(Max)** and minimum **(Min)**.

5.7.6. Link Counters

Presents TSW900ETH test counters. There are 4 different counter screens. First screen displays the following counters:

- **All Received Frames** – Total amount of received frames, regardless any error or applied filters.
- **Valid Received Frames** – Valid received frames include no errors frames and frames which have passed through filters.
- **Trasmitted Frames**.
- **RX Bytes** – Received bytes.
- **TX Bytes** – Transmitted bytes.
- **Timestamp Frames** – Frames with Timestamp payload type.
- **Unicast Frames**.
- **Multicast Frames**.
- **Broadcast Frames**.

Warning 4 – Adjusted to Multicast

"MAC configuration is incorrect. MAC may be configured as Unicast, but Multicast is selected."

Second screen displays counters splitted by frame sizes:

- **< 64 Bytes** – Less than 64 bytes sized frames.
- **64 Bytes** - 64 bytes sized frames.
- **65-127 Bytes** – From 67 to 127 bytes sized frames.
- **128-255 Bytes** – From 128 to 255 bytes sized frames.
- **256-511 Bytes** – From 256 to 511 bytes sized frames.
- **512-1023 Bytes** – From 512 to 1023 bytes sized frames.
- **1024-1518/1526 Bytes** – From 1024 to 1518/1526 bytes sized frames.
- **> 1518/1526** – More than 1518/1526 bytes sized frames.

Third screen displays VLAN and Pause Frames counters:

- **VLAN Frames** – One VLAN tagged frames.
- **Q-in-Q Frames** – Two VLANs tagged frames.
- **Last VLAN ID** – VLAN ID field from the last received VLAN tagged frame.
- **Last VLAN Priority** – VLAN Priority field from the last VLAN tagged frame.
- **Last SVLAN ID** – External tag VLAN ID (Service VLAN) from the last double tagged frame (Q-in-Q).

- **Last SVLAN Priority** – External tag VLAN priority (Service VLAN) from the last double tagged frame (Q-in-Q).
- **Last SVLAN DEI** – External tag VLAN DEI (Service VLAN) from the last double tagged frame (Q-in-Q).
- **Last SVLAN TPID** – External tag TPID (*Service* VLAN) from the last double tagged frame (Q-in-Q).
- **Pause Frames** – Received Pause Frames (flow control protocol).

Fourth and last screen displays layer 3 counters:

- **IPv4 Packets** – IPv4 received packets.
- **IPv6 Packets** – IPv6 received packets.
- **UDP Packets** – UDP received packets.
- **ARP/NDP/Ping/Remote Replies** – ARP, NDP, Ping and remote loopback replies.

Warning 9 – Invalid Frame Size. Change to 'n' Bytes

"When a frame size is configured under 'n' bytes, using Framing Ethernet and, after that, Tagging is changed, frame size must be adjusted to 'n' bytes. 'n' value varies according to selected Tagging (example: Q-in-Q), and will be calculated and displayed to user through application. The application will automatically adjust this value."

5.7.7. Stream Counters (optional)

This section presentes multiple flow statistics. This option is only enabled when TSW900ETH is configured to generate multiple data flow traffic. In a multiple flow test, general counter and statistics previously described, remain working the same way, but TSW900ETH analyzes each generated and received flow characteristics. Counters and statistics below are available and can be analyzed for each configured flow:

- **Timestamp Frames** - Frames with Timestamp payload type.
- **OoS Frames** – Out of sequence frames.
- **Lost Frames**.
- **Rx Frame Rate** – Received frames rate (frame/s).
- **Rx Data Rate** – Received data rate (Mbps).
- **Delay** – Delay measure, in microseconds (average, maximum and minimum).
- **Pkt Jitter** – Delay variation measure, in microseconds (average, maximum and minimum).

5.7.8. Error Statistics

Displays counters/statistics over errored frames/packets:

- **Total Errored Frames** – Total amount errored frames.
- **FCS Errored Frames** – FCS (CRC) errored frames.
- **Runts** – Less than 64 bytes sized frames, with FCS errors.
- **Jabbers** – More than 1518 bytes sized frames, with FCS errors.
- **OoS Frames** – Out of sequence frames.
- **Lost Frames.**
- **Frame Loss Ratio –** Lost frames rate.

- **Collisions –** Collisions total amount.
- **Checksum Error Packets –** Checksum errored packets.
- **Lenght Error Packets –** Lenght sized packets.

5.7.9. BERT Statistics

Displays BERT statistics:

- **BERT Pattern Sync** – BERT sequence synchronization indicator. It will only be synchronized if a valid sequence is received according to BERT standard configured in TSW900ETH.
- **BERT Frames** – BERT payload received frames.
- **Bit Error Rate (%)** – Percentage bit error rate.
- **Bit Errors** – Total amount errored bits received.
- **Total Bits** – Total amount bits sent.
- **Error Seconds** – Time, in seconds, with errors.
- **Error-free Seconds** – Time, in seconds, with no errors.
- **Total Seconds** – Taffic flow generation time, in seconds.

5.8. Physical Layer diagnostics

TSW900ETH allows to perform physical layer tests, electrical or optical. Different information can be obtained through Physical Diagnostics option, on main Menu. In this option, it is possible to access two different tests, depending on physical media configuration (*Link Settings* > *Phisycal Media*): electrical or optical.

5.8.1. Cable Diagnostic

Cable test is used to diagnose UTP twisted pair cables, up to category 6e/Class E.

Displays, for each four pairs from electrical link, cable test diagnostics result. The result shows cable length and current cable situation. Situations can be classified as:

- **OK** – When cable has no failure, so twisted pair is working.
- **Open** – When twisted pair is open, in other words, no signal, no short circuit, and no other twisted pair interference.
- **Crosstalk** – When twisted pair is suffering interference from another twisted pair.
- **Short** – When twisted pai ris in short circuit.
- **Unknown** – When there is no twisted pair, no identified signal or there is already one active cocnection (check if the specifications are attended).

TSW900ETH can check cable capabilities to send Ethernet circuits electrical data traffic up to 10/100/1000 Mbps. Note that only twisted pairs used on Ethernet signal are tested. In case of a 10 Base-T and 100 Base TX tests, twisted pairs 2 and 3 are tested. On a 1000 Base-T test, all four twisted pairs are tested.

If a connection is active, TSW900ETH consider that cable has no issues. For a more detailed level test, leave the other cable connector disconnected. In this situation Open status and cable length are displayed.

Cable wired standart used is T568A, as indicated in Figure 42. Note that, in case of a crossover cable usage, one connector follows T568A standard and the other follows T568B. In this situation, pairs 2 and 3 are in different positions.

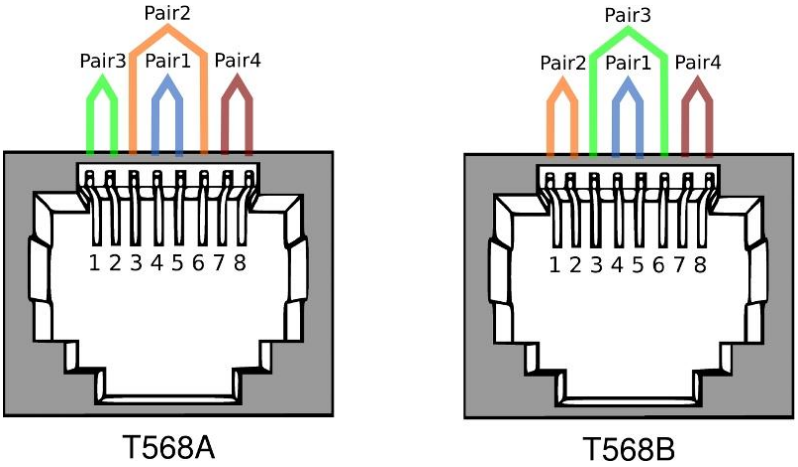


Figure 42. Cabling wire map, according to T568A and T568B standards

Cable Diagnostic specification: minimum cable lenght 3m. Handles Ethernet cables, categories 3/Class C, Category 4, Category 5, Category 5e/Class D, Category 6e/Class E.

5.8.2. Optical Signal Test

Displays optical signal test result (equivalent to cable diagnostic, for optical link scenario). A SFP with Digital Diagnostic is needed, in order to obtain all measures, otherwise, only part of results can be reached. Figure 43 shows ameasure sample.

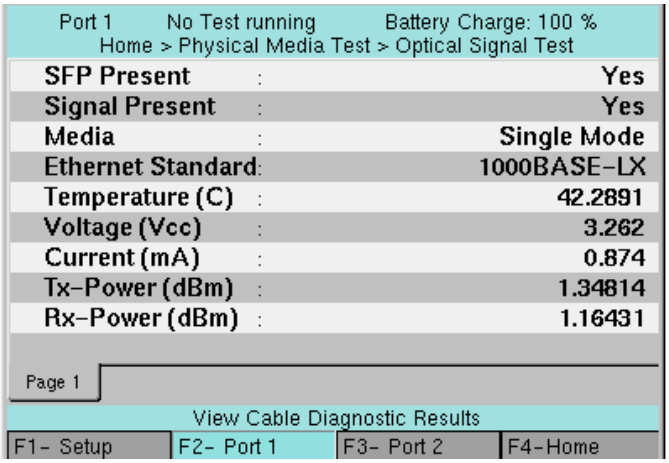


Figure 43. Optical Signal Test results example

Optical Signal Test is only available when testing por is set as optical interface link.

5.8.3. L2 Pattern CxPAT

Allows perform layer 2 tests, with specific optical Gigabit Ethernet interface standards. The goal is to stress all optical Gigabit Ethernet components or systems, through the following patterns transmission: CJPAT – Continuous Jitter Test Patterns, CRPAT – Continuous Random Test Patterns and CSPAT – Compliant Supply Noise Pattern.

- **CJPAT** – Starts special test pattern which creates a worst jitter condition scenario. Expose receivers (clocks and data recovery circuits) to instant phase hops, switching between repeated low density transition patterns and high density transition patterns.
- **CRPAT** – Starts special test pattern which creates a worst jitter condition scenario, by sending broad-spectrum frames.
- **CSPAT** - Starts special test pattern which emulates a noise power worst scenario, introduced by network transceivers.

L2 Pattern CxPAT só é habilitado se a porta de teste estiver configurada com *link* para interface óptica. O TSW900ETH ao ser utilizado neste teste em modo *loopback* também deve estar utilizando a interface óptica para retornar devidamente o sinal.

5.9. Managing Configuration

On tests Main menu, Save Configuration and Load Configuration options offer a solution to save a specific TSW900ETH user profile. Through these options, all settings can be saved and, later, loaded.

On a web browser, through management port connection, is also possible export saved settings to a PC. Later, is possible import saved settings to other TSW900ETH equipment. Settings are saved on an independent way, for each test port. Port 1 settings can be loaded in port 2, and vice-versa. Options are detailed below.

5.9.1. Save Configuration

Allows to save current settings from a specific port, in order to use custom settings later.

- **Details** – Allows user to change settings description and save it.
    - **Description** – Allows to edit settings name and save it.
- **Save** – Allows to save settings with a custom name, and with current timestamp.

5.9.2. Load Configuration

Lists all previously saved settings, and allows user to load them, by selecting the desired setting and pressing (→).

5.10. Shortcut to start tests

Inside F2 and F3 tabs it is possible to find a shortcut to start/stop tests for the selected port, triggered by START/STOP button. Pressing START/STOP, a shortcut window is opened and enables to start/stop tests, as in Figure 44.

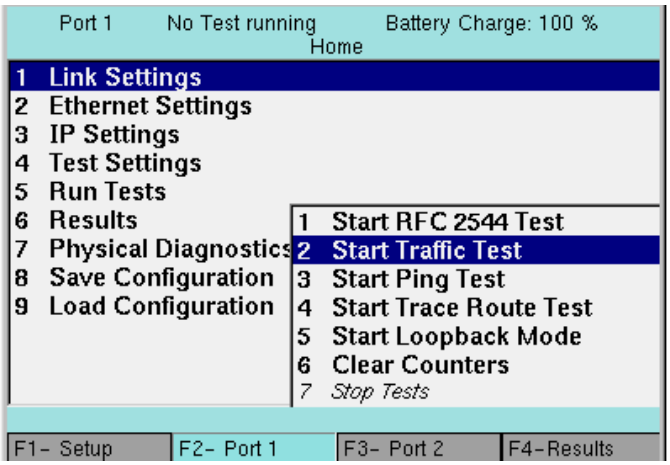


Figure 44. START/STOP key shortcut

To trigger any option listed in the shortcut, just press (→). START/STOP shortcut has the same functions described on Run Tests Menu (Figure 35), except for Remote Loopback commands.

After choosing to trigger one of these tests, start tests options become disabled, and only Stop, Test and Clear Counters options are displayed, as in Figure 45.

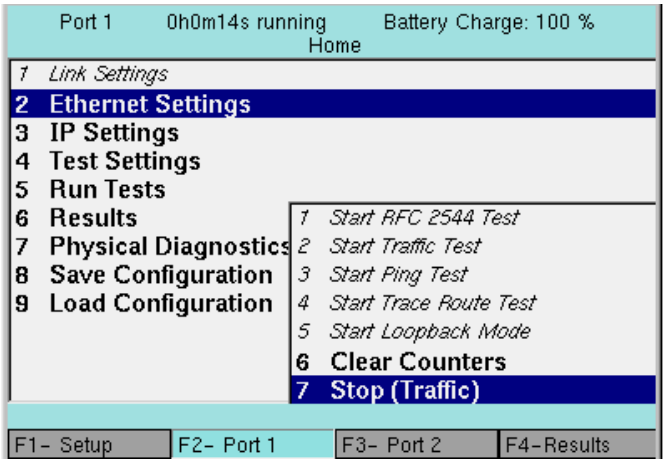


Figure 45. START/STOP shortcut after Loopback test triggered

5.11. IPTV

5.11.1. IPTV/Browser on TSW900ETH

TSW900ETH IPTV/Browser module was developed for installation, maintenance or fixes on IPTV (Internet Protocol TV) and VoD (Video on Demand) services. TSW900ETH allow to verify if vídeo stream sent from IPTV or VoD Server is reaching the equipment and measures signal power, to evaluate connection quality. Video, audio and data streams rates are separately measured, and so is the total amount of frames for each. Also many types of errors are counted, which turns easier to verify what is happening when service is not performing as expected. Lost frames, delay and jitter are also considered. Most important parameters are compared with pre-determined thresholds, which define quality of service (QoS). This module also has a browser for web pages visualization. The following information are analyzed by TSW900ETH:

- **Errors**
    - Continuity error
    - Error indicator

- Synchronization error
- RTP package lost
- RTP package out of sequence
- RTP package discontinuity

- **Jitter measures**
  - Package Jitter
  - PCR Jitter
  - Package and PCR Jitter histogram from last 5 minutes
- **Stream Statistics (TS)**
  - Total of video packets
  - Total of audio packets
  - Total of data packets
  - Total of unknown packets
- **Stream rates**
  - Video stream rate
  - Audio stream rate
  - Data stream rate
  - Unknown stream rate
- **Number of channels (PAT PIDS)**
  - Bandwidth usage percentage by channel
- **IGMP measures**
  - IGMP latency (time to request channel and receive stream)

5.11.2. IPTV test settings

5.11.2.1. IPTV Menu and Browser

Start screen contain Browser  and IPTV Test  options.

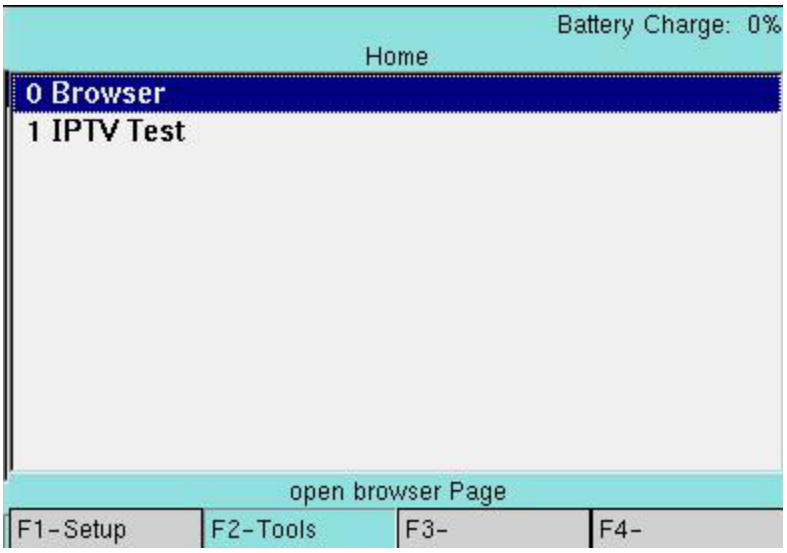


Figure 46. Start screen with browser and IPTV test options

5.11.2.2.IPTV Configurations

Press F1 to enter on equipment setup, where the following options are listed:

- **Tools Version** – Displays TSW900ETH version
- **IP Configuration** – Displays network settings
- **IP Status** – Displays TSW900ETH network status
- **Software Update** – Updates TSW900ETH software
- **Load Tools factory settings** – This item loads factory configuration
- **Exit** – Back to TSW900ETH main Page

5.11.2.3.IPTV tests

On first IPTV module screen, select IPTV test, pressing 1 key or using ▼ and ▲ keys and pressing ▶ to continue. On next screen, press key or move cursor to IPTV Config item, and press ▶ to advance to next screen.

On this screen is possible to choose a stream to configure by pressing ▶ on selected stream or pressing respective numerical key.

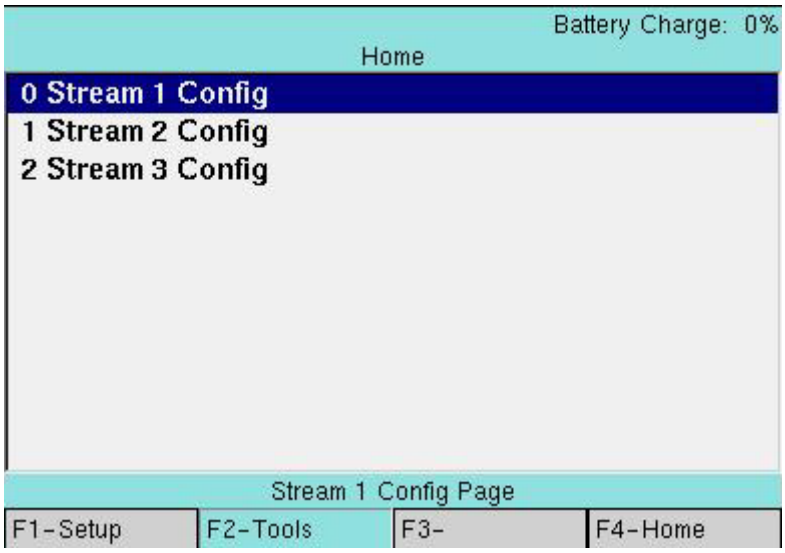


Figure 47. Stream configuration screen

5.11.2.4.IPTV configuration screens

This screen allows to select protocol, IP and port which will be used.

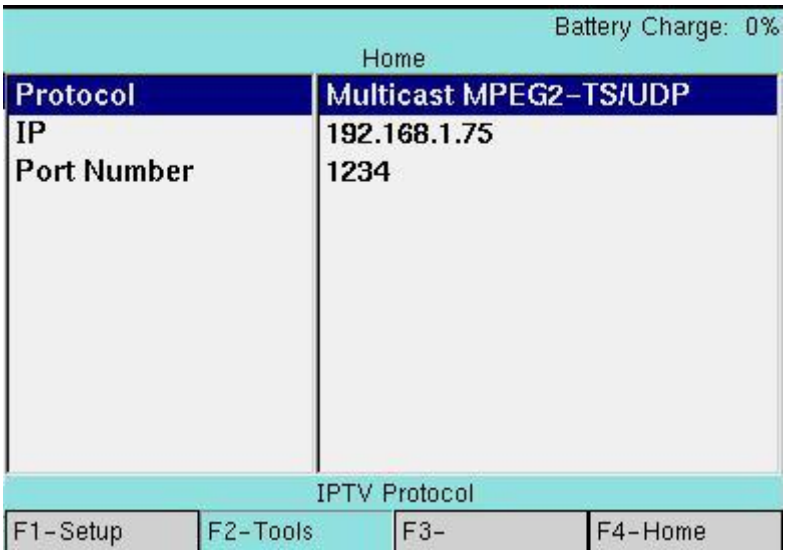


Figure 48. IPTV configuration screen

- **Protocol** – This parameter defines transport protocol type to be used. Although vídeo encoding protocol is MPEG-4, many providers use MPEG-2 encapsulation mode to transport. This way TS (Transport Stream) packets carry MPEG-4 encoded data. TS packets can be encapsulated in two different ways: UDP/IP and RTP/UDP/IP. Also, there is a difference between IPTV, which uses IGMP (Internet Group Management Protocol) protocol to be part of a multicast group, and VoD, which uses RTSP (Real Time Streaming Protocol) protocol to be parto f a unicast group.

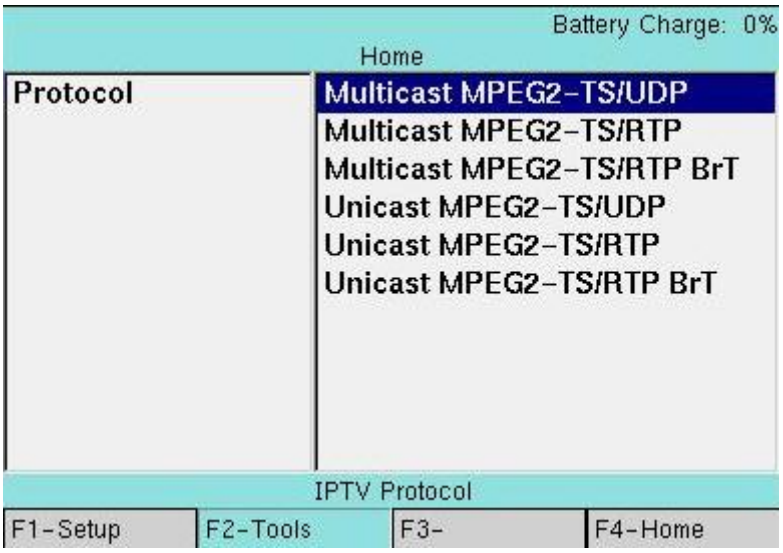


Figure 49. IPTV protocol selection screen

- **Multicast MPEG2-TS/UDP** – In this option, MPEG2 TS packets are encapsulated directly over UDP/IP. In Brazil, this is the way Telefônica and Oi selected for IPTV.
- **Multicast MPEG2-TS/RTP** – In this option, MPEG2 TS packets are encapsulated inside RTP packets, which are encapsulated inside UDP/IP.
- **Multicast MPEG2-TS/RTP BrT** – In this option, MPEG2 TS packets are encapsulated inside RTP packets, which are encapsulated inside UDP/IP. In Brazil, this is the way Brasil Telecom selected for IPTV.
- **Unicast MPEG2-TS/UDP** – In this option MPEG2 TS packets are encapsulated direclty over UDP/IP. In Brazil, this is the way Oi selected for VoD.
- **Unicast MPEG2-TS/RTP** – In this option, MPEG2 TS packets are encapsulated inside RTP packets, which are encapsulated inside UDP/IP.
- **Unicast MPEG2-TS/rTP BrT** – In this option, MPEG2 TS packets are encapsulated inside RTP packets, which are encapsulated inside UDP/IP. In Brazil, this is the way Brasil Telecom selected for VoD.

- **IP** – This parameter defines IPTV channel IP to be received. It is necessary to know this IP in order to send one IGMP packet, requesting to be part of multicast group that is receiving the channel. After this request is accepted, video stream starts to be sent by server. On unicast protocols, IP is not configured.
- **URL (RTSP)** – This parameter defines VoD server URL. It is necessary to know this URL in order to send one RTSP packet, requesting to enter on unicast mode, where only a specific user receives the vídeo. After request is accepted, vídeo stream starts to be sent by server. Only used on unicast protocols.
- **Port Number** – This parameter defines port number where IPTV communication Will work. Only used on multicas protocols.

5.11.3. IPTV tests

5.11.3.1. Test execution

In IPTV test screen, press 1 key or select Run Stream option and then press ▶. On this screen is possible to start stream test pressing respective numerical key or selecting and pressing ▶. It is possible to perform tests on each stream indiviadually or three streams simultaneously.

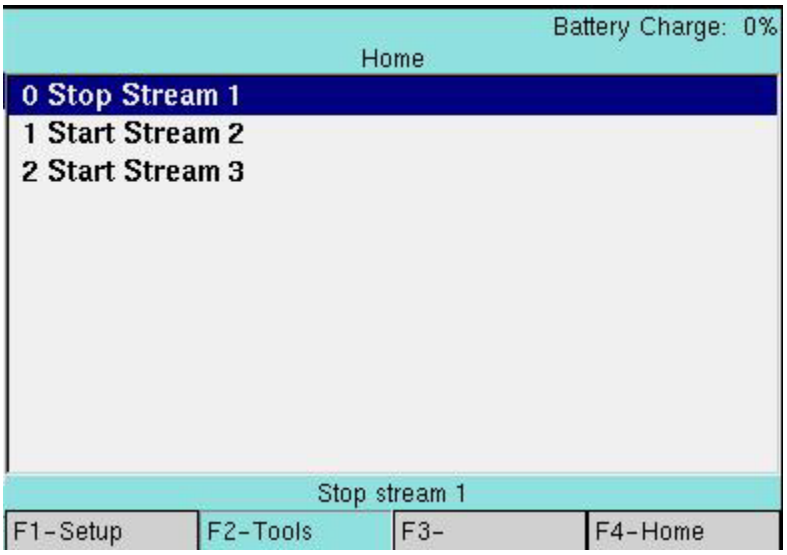


Figure 50. IPTV test execution screen

If protocol is IPTV (multicast) then an IGMP packet is sent. If protocol is VoD (unicast) then a RTSP packet is sent. After this, video flow starts, and so the measure.

Measure results can be verified on IPTV Results option.

5.11.3.2.Test data visualization

On IPTV test screen, press 2 key or select using ▼ and ▲ keys, then press ▶.

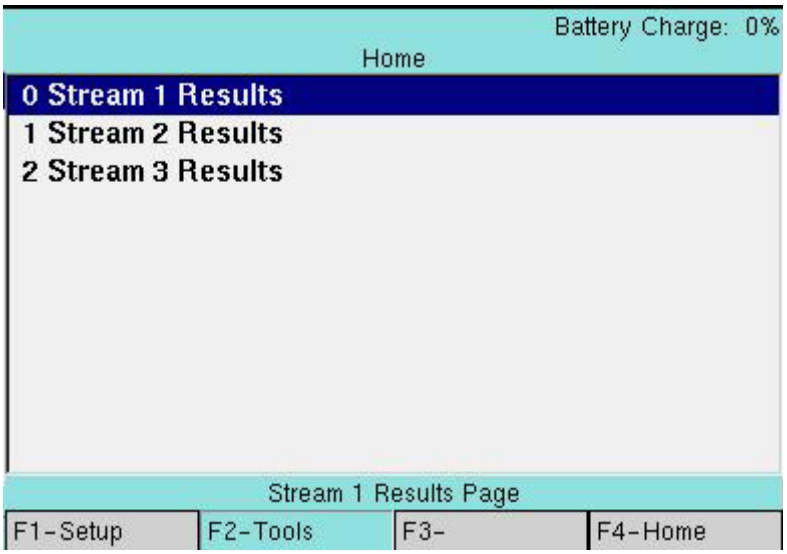


Figure 51. IPTV test results screen

Press respective numerical key to select a stream, or select it using ▼ and ▲ keys, the press ▶.

On the next screen, press respective numerical key, or select it using using ▼ and ▲ keys, the press ▶.

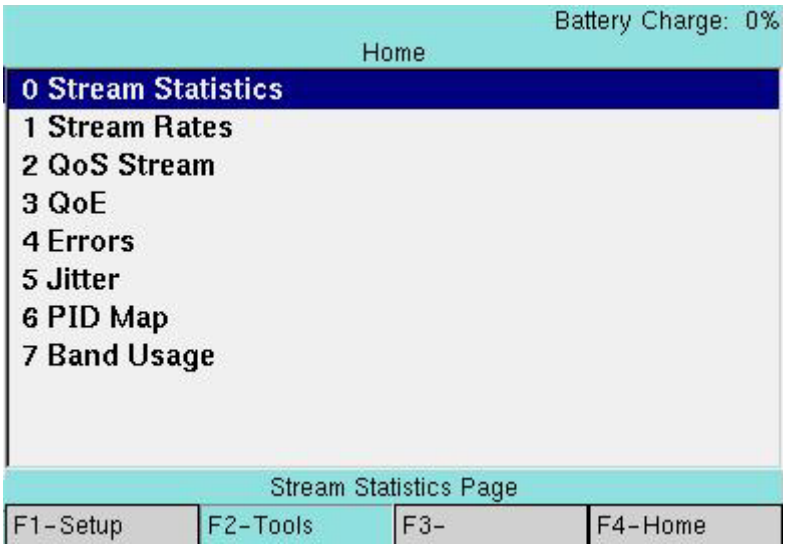


Figure 52. IPTV options screen

- **Stream statistics** – Displays total amount of TS packets (MPEG-2 transport packet with 184 bytes of data and 4 bytes of header). Also displays video, audio, data and unknown packets counts, besides total amount, in bytes.

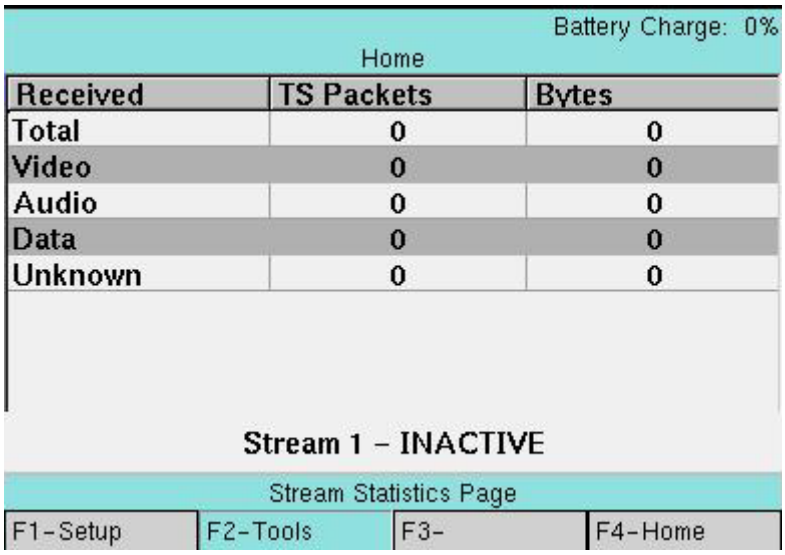


Figure 53. Stream Statisctics screen

- **Stream rates** – Displays video, audio, data and unknown packets rates in kbit/s.

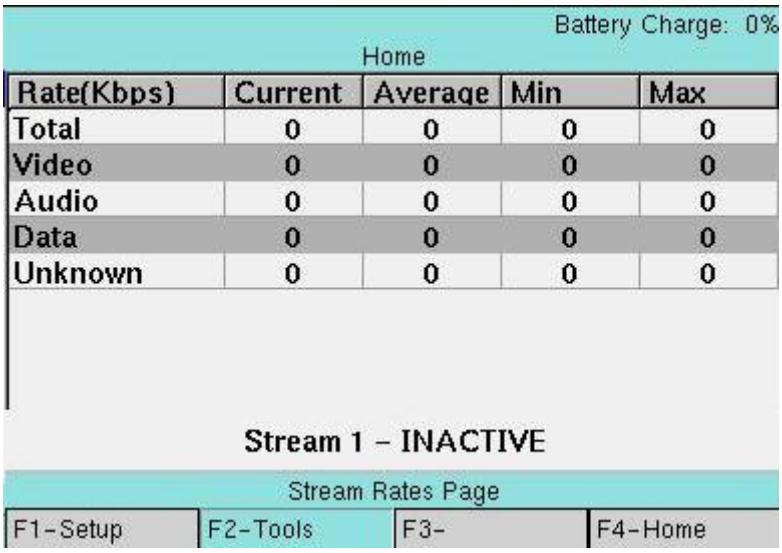


Figure 54. Stream Rates screen

- **QoS Stream** – Displays QoS parameters, current values, maximum values, and indicates if they are within pre-defined thresholds for quality of service.

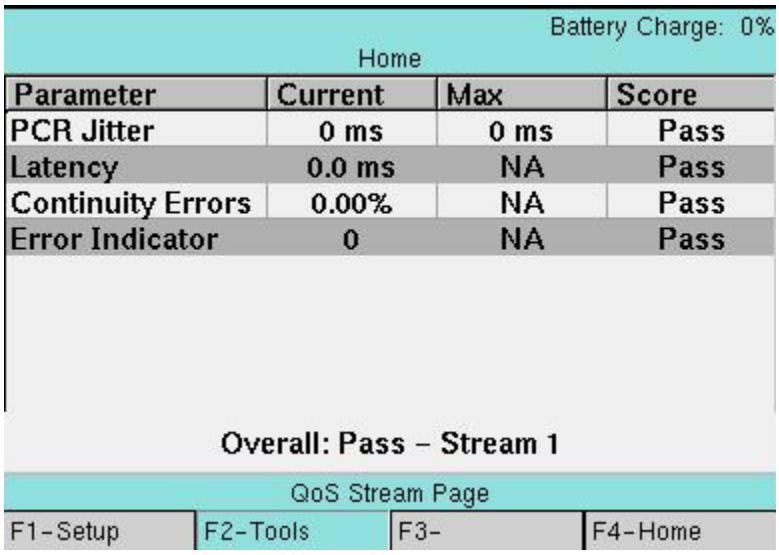


Figure 55. QoS Stream screen

  - **PCR Jitter** (Program Clock Reference) – Measures Jitter whne analyzes reference clock saved in some packets. Jitter is the time interval oscilation between packets receiving, comparing with it creation timestamp. This interval should be equal to the difference between timestamp recorded when they were created, but the encoder and network can cause delays in some packets. In case of a high oscilation, decoder problems may be caused. Maximum jitter to attend quality of service is 10 ms.
  - **Latency** – Measures the time between a request sent to receive a determined program (stream) and the moment when packets flow start to be received. Maximum latency to attend quality of service is 250ms.
  - **Continuity Error (Cont. Err.)** – Measures packet sequence lost. MPEG2 TS packets have a sequence counter, which allows the receptor to know when a packet was not received in the correct order. On qoS screen, this counter is percentage (total amount of continuity errors divided by total amount of MPEG2 TS packets). The maximum percentage to attend quality of service is 0.1.
  - **Error Indicator (Err. Ind.)** – Indicates if there was any problem with video packets. This indication is made by encoder, when realizes there are corrupted data. Only value zero attends quality of service for this item.

- **QoE (Qualit of Experience)** – This new term is being used to evaluate final user perception against deliver media quality. To measure IPTV QoE, MDI (Media Delivery Index) is used, defined by RFC4445. This index is made by two measures: DF (Delay Factor), Jitter and MLR (Media Loss Rate).
    - **DF Jitter** – indicates video time needed to be stored, considering current video rate, to eliminate jitter effect on final user delivered video. It is measured in milissenconds. This parameter is used to measure a Set Top Box buffer size for a current packets flow.
    - **MLR** – represents lost media packets total amount per second.

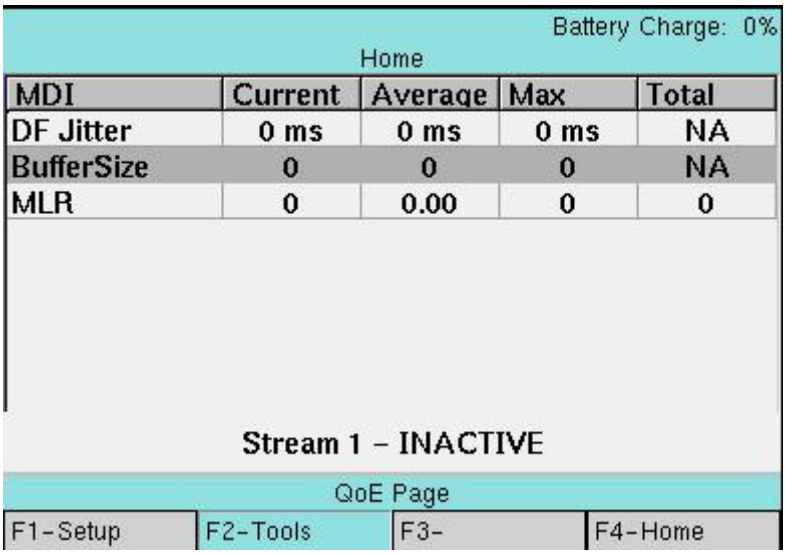


Figura 56. QoE screen

Buffer overflow lost, caused by network traffic jam or bad network devices configuration, may happen periodically, resulting many time intervals with positive and similar MLR values. Transient effects, perhaps because the electrical noise caused by variations, will result in fewer time intervals affected, in other words, MLR positive values are more random and more widely spaced.

- **Errors –** Various errors types and quantity

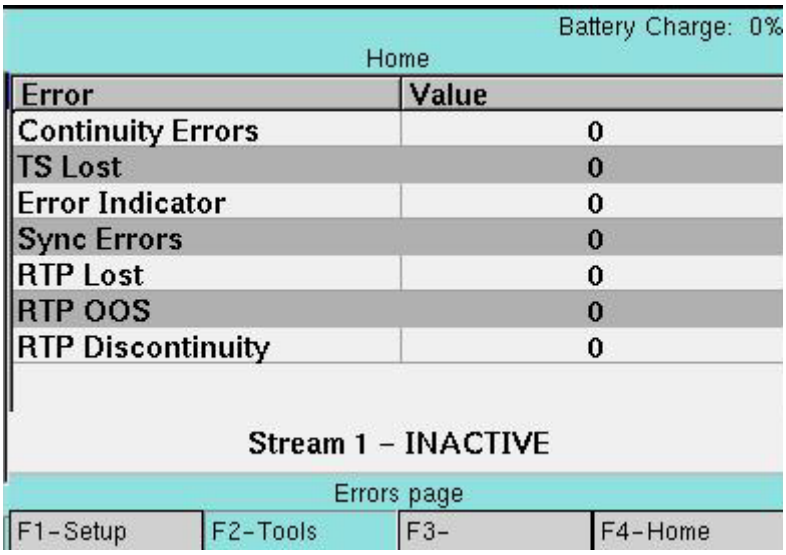


Figure 57. Errors page screen

- **Continuity Errors** – Packets sequence lost quantity.
- **TS Lost** – Lost TS (Transport Stream) units. Each single video packet, according to MPEG2-TS transport protocol, has seven TS units.

- **Error Indicator** – Total amount of packets received with active bit Error Indicator.
- **Sync Errors** – Amount of times when MPEG2 TS packet was not identified, on application layer.
- **RTP Lost** – Lost RTP frames when using MPEG2 Broadcast (RTP) protocol.
- **RTP OOS** – Out of sequence RTP frames when using MPEG2 Broadcast (RTP) protocol.
- **RTP Discontinuity** – RTP frames with broken sequence when using MPEG2 Broadcast (RTP) protocol.

- **Jitter –** PCR jitter and netowrk jitter counts. Maximum and instantaneous values are displayed. Network jitter is caused by network traffic. PCR jitter may be caused by encoder, network or reception. Values remain the same when using MPEG2 Broadcast (UDP) protocol. IGMP Latency is also displayed on this screen, and measures the time between a request is sent to some specific program, and the moment when packets flow reaches destination.

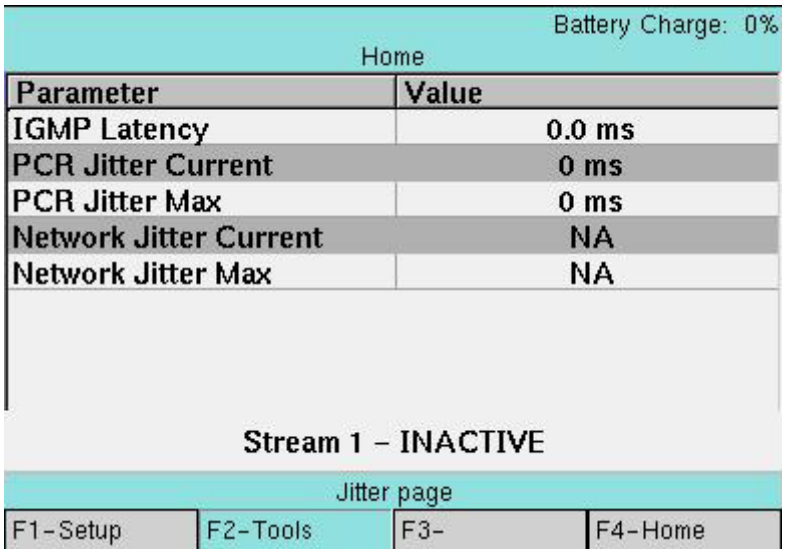


Figure 58. Jitter Page screen

- **PID Map –** Displays each received PID (Packet Identifier), type and description. PID identifies packets owner. If PID is 0, packet is PAT (Program Association Table), which consists on a table containing each PMT (Program Map Table) PID. There is one single PMT for each channel (program). This PMT consists on a table with video, audio and data packets PIDs fot this specific channel.

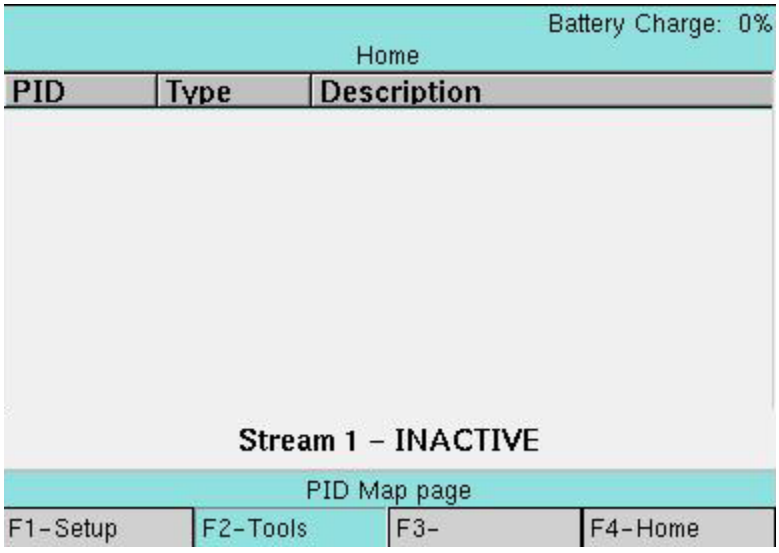


Figure 59. PID Map Page screen

- **Band Usage –** Bandwitdh usage status and percentage, by stream. Channel bandwidth percentage results from channel rate divided by the sum of all active channels rates.

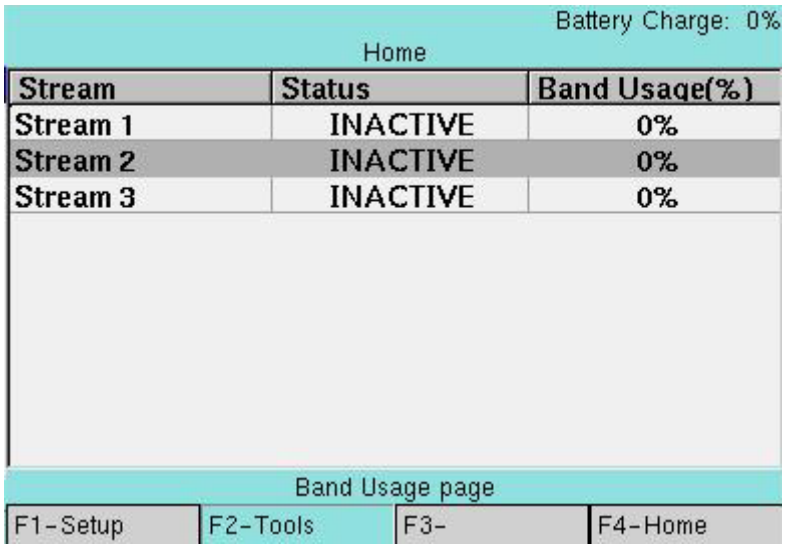


Figure 60. Band Usage Page screen

5.11.3.3. IPTV testing conclusion

On Run Stream screen, pressing respective numerical key or selecting specific stream using ▼ and ▲ keys and pressing ▶, it is possible to stop IPTV test.

5.11.4. Browser

Through Browser mode is possible to access an Internet page. To start it, on IPTV start menu, press 0 DATA key or select it using ▼ and ▲ keys, and pressing ▶ key. Selecting Browser option, the screen below is displayed, where it is possible to configure web page to be accessed or acces the web page already configured.

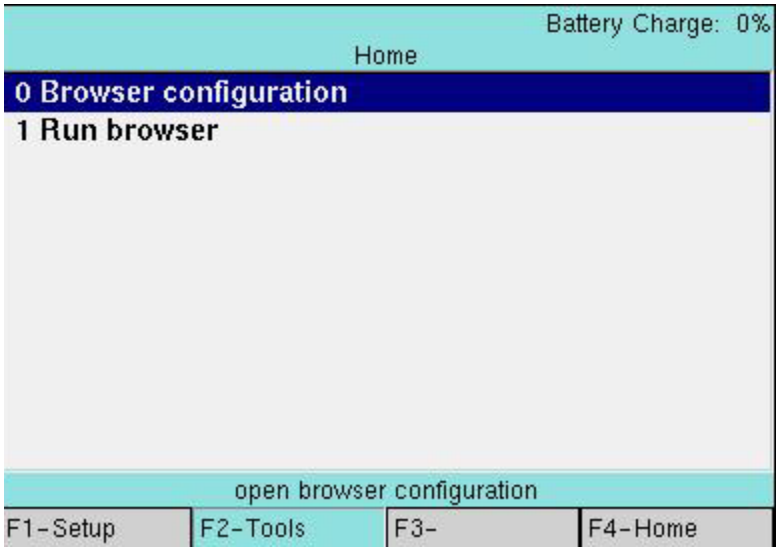


Figure 61. Open Browser configuration screen

Use alphanumerical keys to edit the address to be reached. Clear key cleans only the character where cursor currently is. Space and "@" characters can be found by pressing 0 DATA key twice and three times, respectively. "_" and "#" characters can be found by pressing Error - # key twice and three times, respectively. To change between lower and upper case, press F3 key. Press F1 key to confirm entered address or press F2 key to cancel.

When using browser, press ▼, ▲, ▶ and ◀ keys in order to move horizontal and vertical scroll bars. F1 key points cursor on address bar. F2 and F3 keys can be used to handle links selection (F2 selects previous link, and F3 selects next link). After selecting a link, press Start/Stop key to access it. This key returns to previous screen where Browser was accessed. + Volume and Volume - keys move forward and backward one page at a time, respectively.

It is possible to connect keyboard and mouse, using an USB adapter. These are optional parts, and are not included in TSW900ETH.

5.12. Wifi

5.12.1. Introduction

TSW900ETH Wifi module is userd to access management interface (Web and CLI).

For this purpose, a Wifi adapter needs to be connected to mini-USB port.

When Wireless mode is selected (Menu: Management Configuration > General Configuration > Management Type), ETH MNG port is disabled. If Wifi adapter is connected, Wifi module is automatically turned on. In other words, only one interface works at a time.

5.12.2. Wifi Settings

Remote access to Wifi is configured on Setup tab, Management Configuration menu. Figure 62 below displays Management Configuration menu. Besides that, Ethernet port configuration is placed inside this menu (“Cable” item).

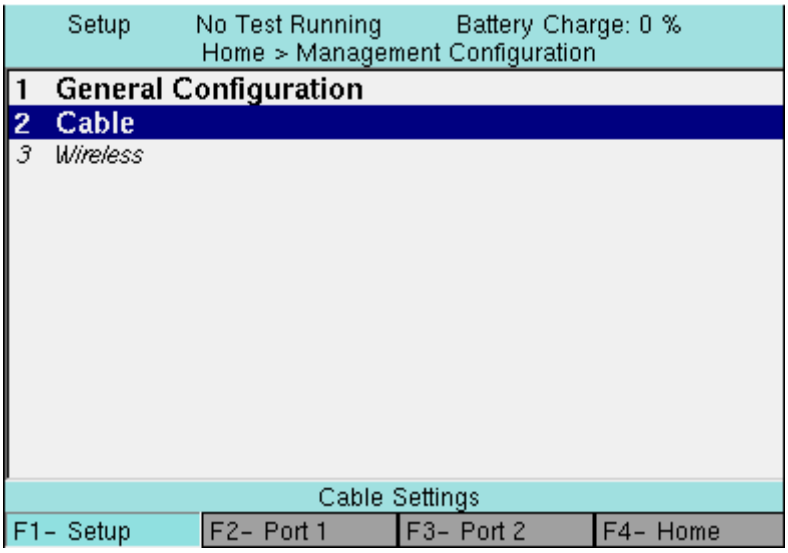


Figure 62. Management Configuration screen

General Configuration screen lists Ethernet (“Cable”) and WiFi (“Wireless”) options. Both can not operate simultaneously. An error message is displayed when selecting Wireless mode with no adapters connected on USB port.

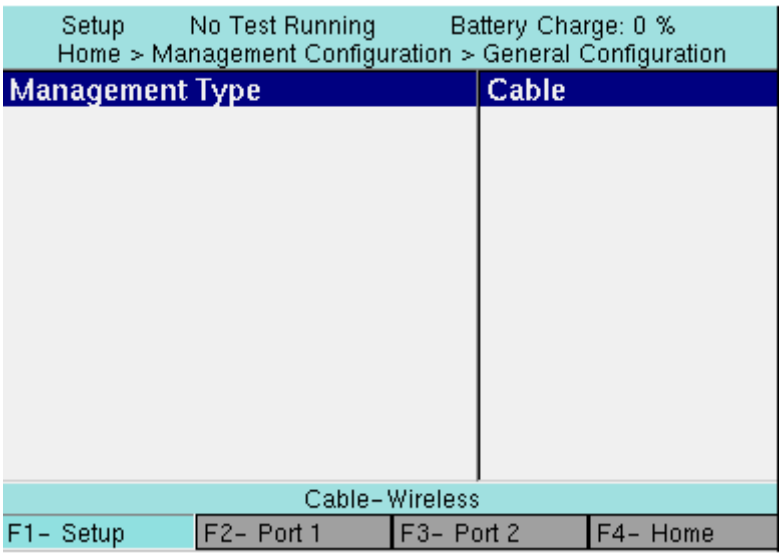


Figure 63. Management selection screen

Wireless interface configuration menu lists General Configuration, where interface is configured, and Networks, where network to be connected is selected.

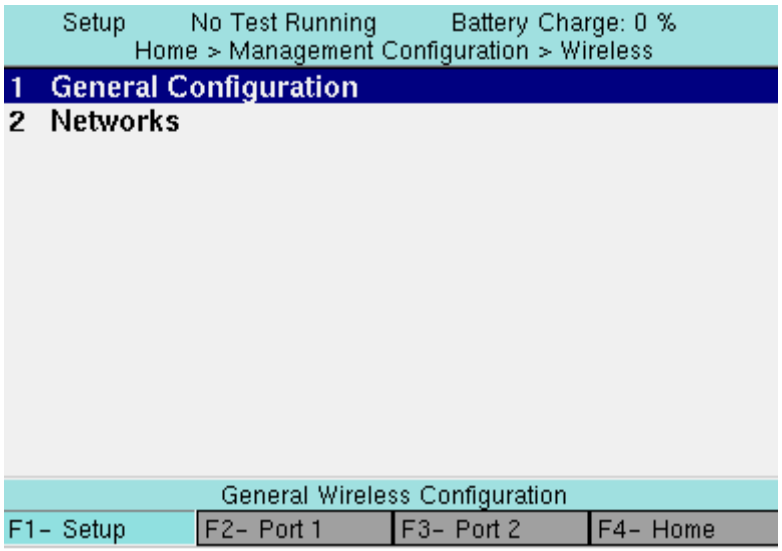


Figure 64. Wireless general configuration

General Configuration lists all necessary items to configure wireless interface, including IP, passwordd and encryption to connect.

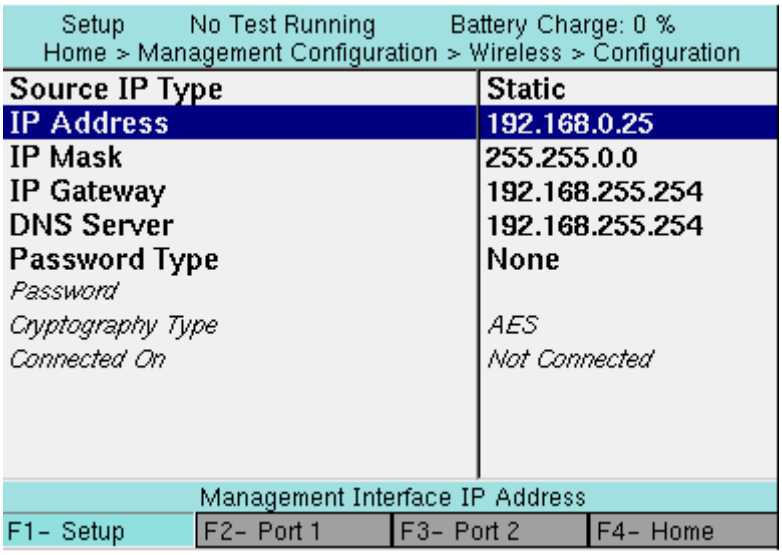


Figure 65. Wireless configuration screen

Selection fields list the following options:

- Source IP Type: Static, DHCP
- Password Type: None, WEP, WPA, WPA2
- Cryptography Type: AES, TKIP.

“Connected On” item displays the network where equipment is currently connected.

Networks menu lists available networks, which can be connected. Beside the name of each network, signal level is displayed. On the bottom screen, signal quality, operation mode and encryption information are listed.

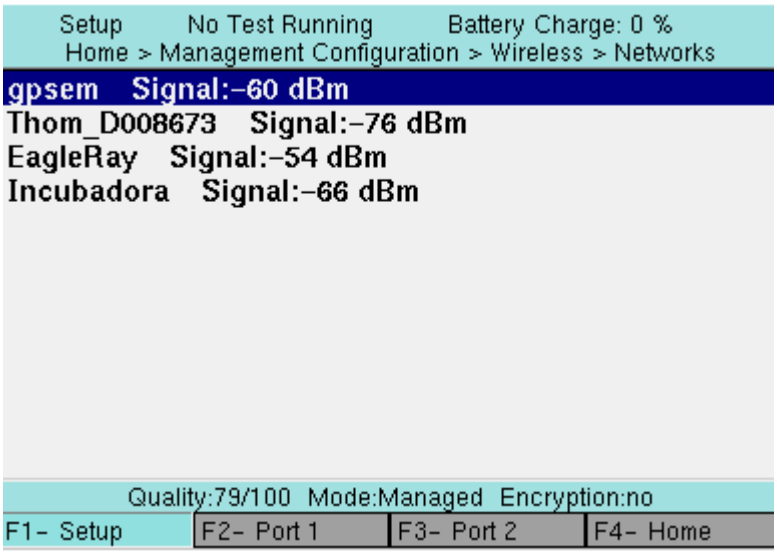


Figure 66. Wireless network selection screen

To connect a network, proceed the following steps:

1) Configure Password Type, Password and Cryptography Type. Obs.: IP configuration items (Source IP Type, IP Address, IP Mask, IP Gateway, DNS Server) can be configured after connected.

2) Access Networks menu, and select the network to be connected (Wait until full list of available networks loads).

3) Once connected, “Connected On” field displays the network (Can take few seconds to connect).

4) After connected, in case of DHCP mode, “Connected On” field displays “wait” message after the name. This means configuration still in progress. Besides that, IP Address, IP Mask, IP Gateway and DNS Server fields are disabled, showing DHCP status. In 40 seconds “wait” message desapears, otherwise, some connection issue may happened during configuration process, and then, “Not Connected” message displays.

5.13. Results management

By pressing F4-Results key, on HOME test screen, test results, saved by user, are displayed. To access results, press (→) on the selected option, as in Figure 67.

Some results are directly displayed in chart or table mode. Throughput result shows a new option before displays chart or table.

After select a result to visualize, it is possible to return to results menu, by pressing (←) key.

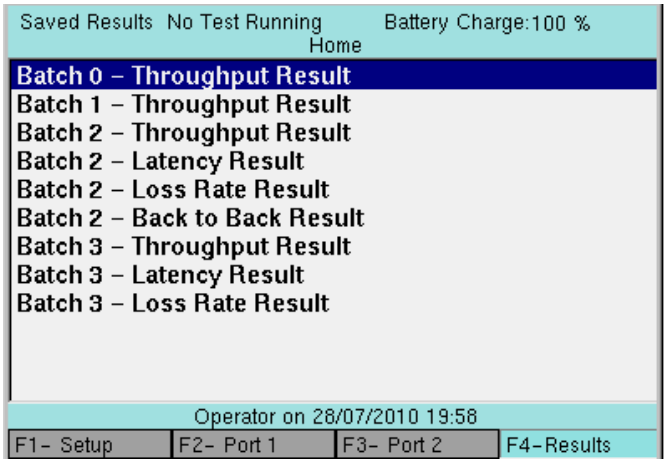


Figure 67. F4-Results screen with some saved results

In case F4 key is pressed and no there is no test result saved, TSW900ETH displays No Saved Results message.

These results can be loaded and visualized on a Web Browser, through management port connection, and saved on a PC or printed.

6. INTERFACE WEB

TSW900ETH allows user to access its configuration through Web interface, which can be access through a Web Browser. It is possible to configure all TSW900ETH features through Web interface. Besides that, it is also possible to visualize RFC2544 and traffic tests results. These results can be exported to PDF and XLS formats, or visualized in HTML format.

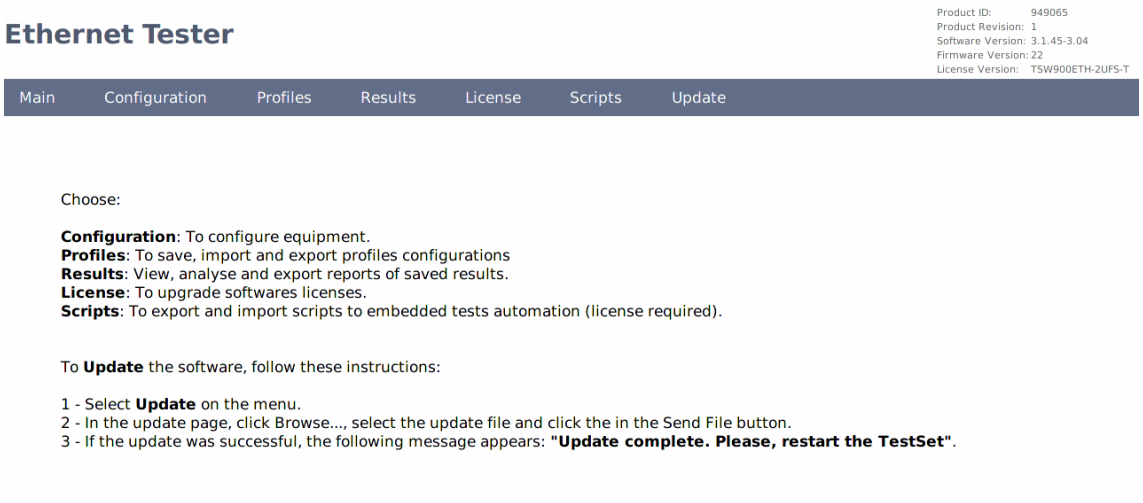


Figure 68. Web interface initial screen

6.1. Main

Main page. Displays all web interface functions brief information. Figure 68 shows main page initial screen.

6.2. Configuration

Configures TSW900ETH and shows results. Check first if the port to be tested is already running any test. It is not recommended to change configuration while running tests. Figure 69 shows “No Test Running” message, beside port selection dropdown menu, which means no tests executing at the moment. In case of test running, execution time displays instead of “No Test Running” message.

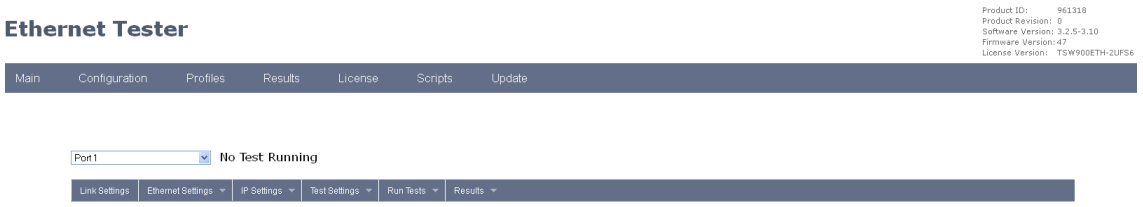


Figure 69. Web interface configuration

Web interface configuration menu, when selected, opens a new submenu, which lists selected port configuration options.

Configuration options are the same displayed when configuring TSW900ETH through keyboard and graphical interface, as detailed in chapter 5.

6.2.1. Link Settings

Allows to configure selected port connection parameters.

- Physical Media
- Speed
- Duplex
- Flow Control

6.2.2. Ethernet Settings

- General Configuration
- VLAN Configuration
- Ethernet Filter

6.2.3. IP Settings

- IPv4
- IPv6

6.2.4. Test Settings

Allows to configure TSW900ETH tests to be executed.

- Traffic
- Ping
- Trace Route

6.2.5. Run Tests

Allows to trigger a test execution through Web interface.

- Start RFC 2544 Test: Inicia teste de RFC2544.
- Start Traffic Test: Inicia um teste de tráfego.
- Start Loopback Mode
- Start Ping Test
- Start TRACE Route Test
- Enable Remote Loopback
- Disable Remote Loopback
- Clear Counters
- Stop Test

6.2.6. Results

Allows to visualize test results counters.

- RFC 2544 Results
- Link Statistics
- Link Counters
- Stream Counters

- Error Statistics
- BERT Statistics
- Save Results

Configuration through web uses the same process as in keyboard configuration. Therefore, if a specific parameter is not enabled to write, this also can not be changed through Web.

6.3. Profiles

Saves, imports and exports user profile configuration. TSW900ETH profile configuration can be made remote or locally. This feature has complete flexibility on field testing.

Figure 70. Web interface profiles management

Export Profile: Sends saved data from TSW900ETH to PC.

Import Profile: Sends saved data from PC to TSW900ETH.

Load Profile: Loads user profiles on TSW900ETH

Remove Profile: Removes user profiles from TSW900ETH.

Save Profile: Saves user profiles on TSW900ETH.

6.4. Results

Through this menu it is possible to visualize, analyze and export saved results reports.

After select this menu, saved results list is displayed. Click on selected result link and it shows up. Results, when opened, displays table or chart formats, as in Figure 71.

Test results can be exported to PDF or XLS format, and downloaded to PC.

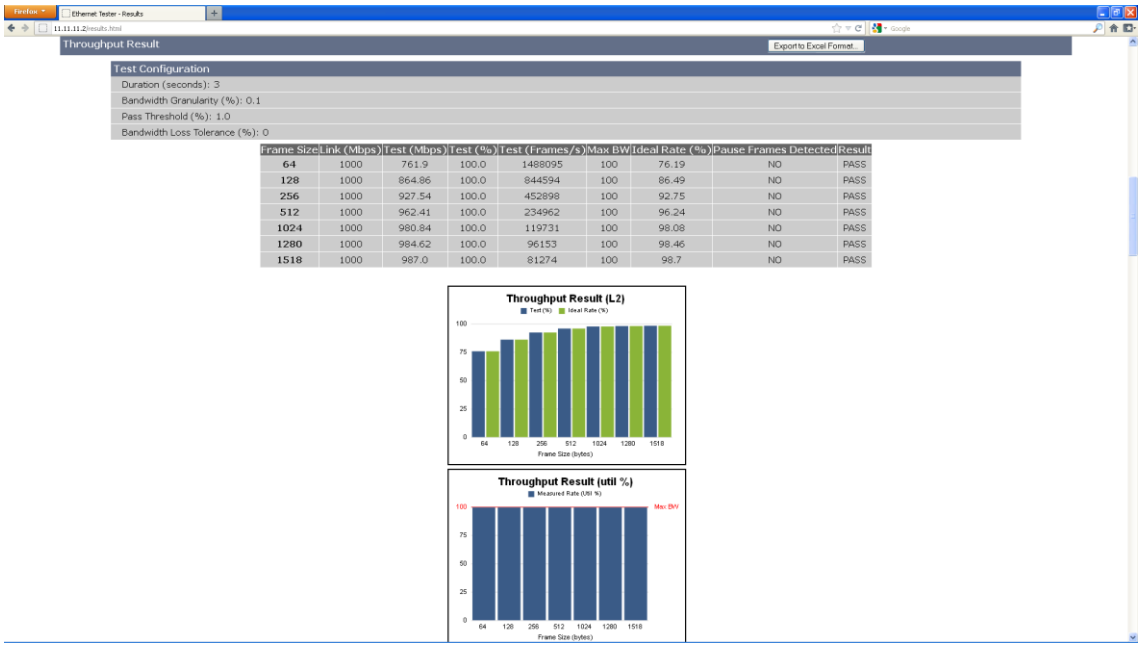


Figure 71. RFC2544 - Throughput test result

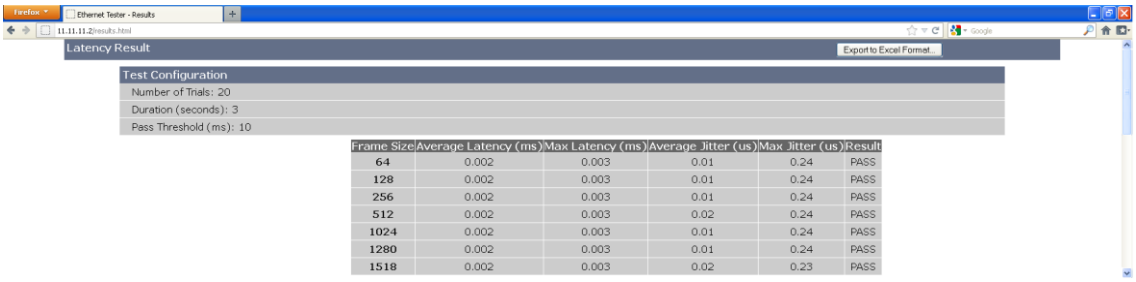


Figure 72. RFC2544 - Latency test result

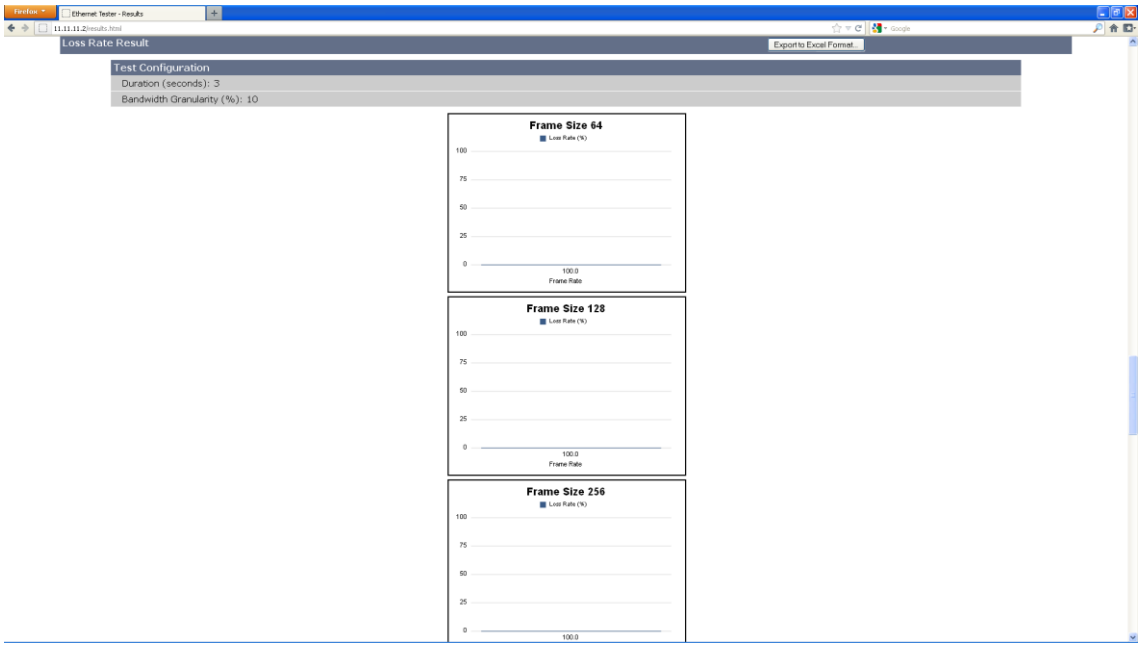


Figure 73. RFC2544 - Loss Rate test result

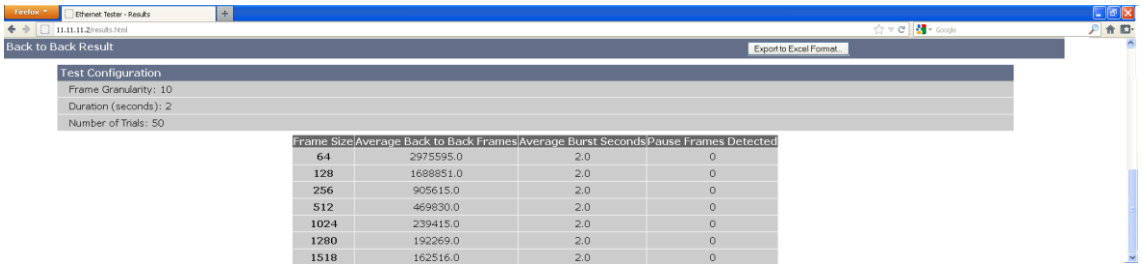


Figure 74. RFC2544 - Back to Back test result

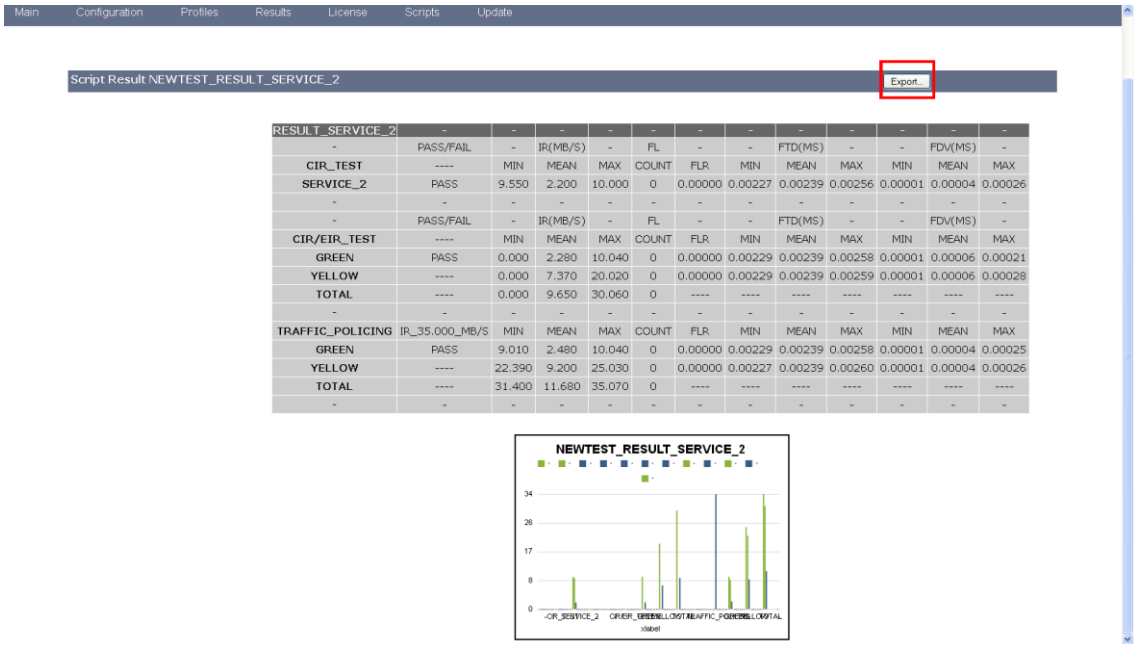


Figure 75. Web interface tests results

6.5. License

This menu is used to enable new option features to TSW900ETH. Software license is changed by typing a specific key code and clicking Send button. After sending correct key code, TSW900ETH must be restarted, in order to the new license start working.

6.6. Scripts

Export and import embedded scripts for automated tests (licensed required).

Select a script file, by clicking on “Select file” button and then, click on Send file, so it is sent to TSW900ETH.

After that, script is listed and can be selected on F1-Setup tab, Scripts option.

6.7. Update

To perform a software update, proceed the following steps:

1. Go to Update menu;
2. On Update page, click on “Select file” button, then select the new software image file, and then click Send File button.

3. In case of success, “Update complete. Please, restart the TestSet” message displays.

7. TESTES

Find bellow some examples of TSW900ETH tests usage. Scenarios and equipments configurations can vary. This document is not exploring total amount of scenarios and configurations.

7.1. Cable diagnostic test

Cable diagnostic test can be performed in TSW900ETH before traffic data. Usually, in out of service situations, in order to determine MDI or MDI-X twisted pair healthy, 1000Mbps links, or some issue with patch cords. In case link is inactive, this can be used to determine issue root cause and approximate patch cord issue distance.

To perform electrical cable diagnostics, follow steps below:

1. On Link Settings, set electrical link (according to the port where cable is connected).
2. Connect one cable end to a TSW900ETH port (ETH1/ETH2 interfaces), and the other cable end connected or disconnected, depending on what is being tested.
3. On selected port screen, select Physical Diagnostics > Cable Diagnostic.
4. Test result displays the four twisted pair current current state, and total length until some issue is detected.

Figure 76. Electrical cable test example

Cable Diagnostic menu is not enabled when TSW900ETH is configured to optical interface. Cable test requirements are:

- Minimum cable length: 3m
- Supported Ethernet cable categories: Category 3/Class C, Category 4, Category 5, Category 5e/Class D, Category 6e/Class E.

7.2. Optical test

To perfrom optical diagnostics, follow steps below:

1. Turn TSW900ETH off. Connect SFP modules to TSW900ETH and connect optical wire to SFP module.

Under no circumstances look into the uncapped or SFP fiber optic terminations with TSW900ETH connected. Invisible laser beam may damage your vision!

2. On Link Settings, set optical link (according to the port where cable is connected).
3. On selected port screen, select Physical Diagnostics > Optical Signal Test.

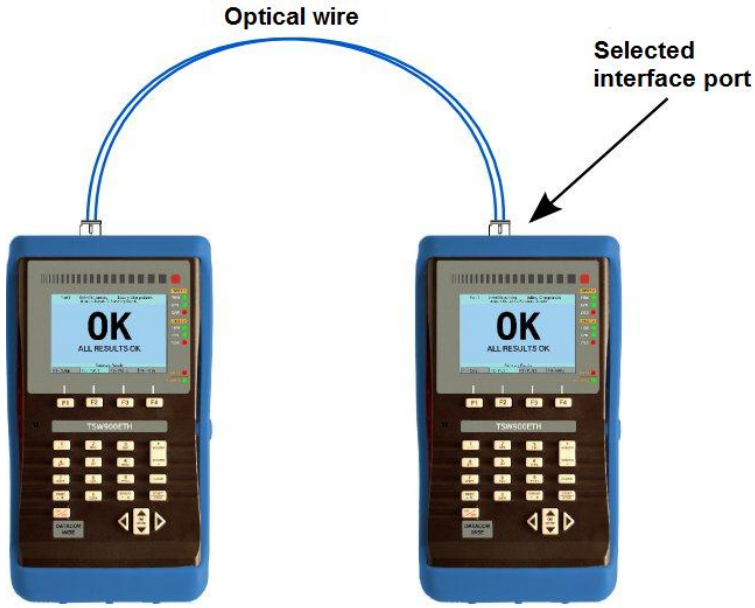


Figure 77. Optical wire test example

Optical Signal menu is not enabled when TSW900ETH is configures to electrical interface.

7.3. Loopback test

When configured in Loopback mode, TSW900ETH sends back to source destination all received frames. With electrical configuration, either ETH1 or ETH2 ports can be set as Loopback. With optical configuration, either SFP1 or SFP2 ports can be set as Loopback. To set Loopback mode in TSW900ETH, follow the steps below:

1. Configure links, accordind to section 5.1.
2. Proceed with Ethernet configurations, mainly source and destination MAC addresses. Case needed, perform filter configurations, according to section 5.2.
3. Back to main screen, go to Run Tests > Start Loopback Mode.

When in loopback mode, TSW900ETH returns all received frames in the following situations:

1. When operating in layer 2 (Framin = Ethernet), only returns frames if received frame destination MAC address is the same as TSW900ETH loopback port source MAC address. Retransmitted frames have source MAC addresses and destination reversed.

2. When operating in layer 3 (Framing = Ethernet/IPv4), only returns frames with destination MAC address and destination IP same as source MAC address and source IP as TSW900ETH loopback port. In this layer, is possible to configure ARP in IP Settings > Configuration > ARP Mode = Enable. This way it is not necessary configure frame destination MAC address. Both ports (traffic generator and loopback ports) must be configured to operate in layer 3, with ARP mode enabled. Retransmitted frames have reversed source and destination MAC address, as well as source and destination IP addresses.

7.3.1. Remote Loopback

TSW900ETH can be configured in Loopback, remotely, by another TSW900ETH. This can be done through commands sent by Ethernet network. User can follow the steps below:

1. Configure destination address as the other TSW900ETH source addres, which will be remotely put in loopback mode. If both TSW900ETH are configured to operate in layer 2, destination MAC address must be configured. If both are operating in layer 3, destination IP and MAC addresses must be configured (check sections 5.2 and 5.3).
2. On Run Tests menu, execute Enable Remote Loopback option.

If after Remote Loopback option is enabled and needs to be disabled, option Disable Remote Loopback option, on Run Tests menu must be executed.

7.4. Layer 2 tests

For tests described in this document, TSW900ETH is connected to network/equipment to be tested and, in this network/equipment another equipment is connected, but in Loopback mode (this can be from one TSW900ETH port to the other port, to other TSW900ETH or to another equipment which returns transmitted traffic). This way, Loopback equipment receives transmitted frames and send them back to TSW900ETH, which analyzes traffic or executes RFC2544 tests, as in Figure 78

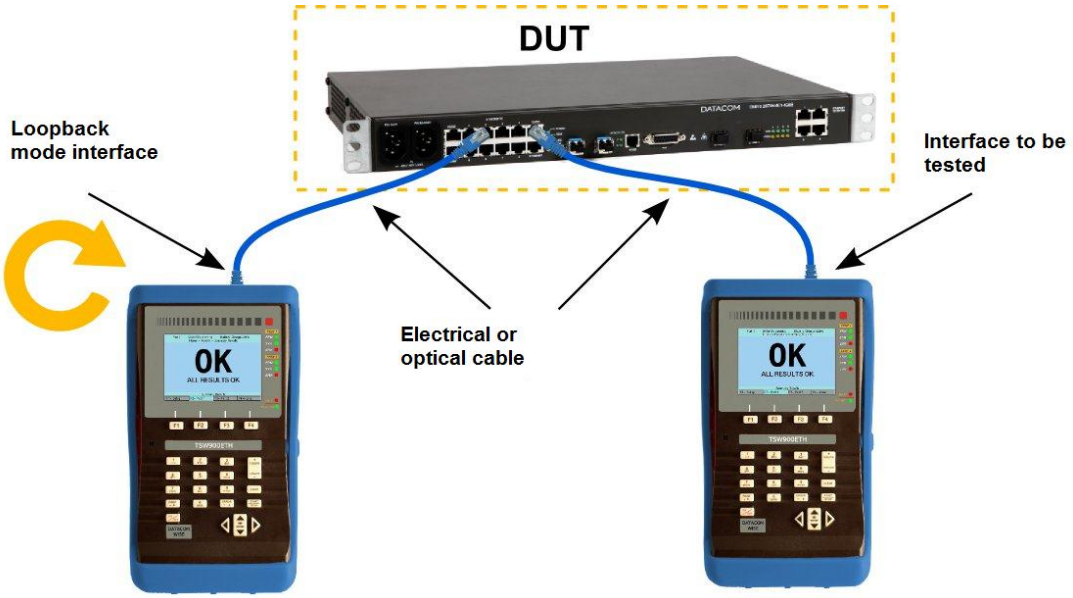


Figure 78. RFC2544 and traffic tests scenario

Before execute tests below, it is highly recommended to clear ports counters: on selected port tab (F2/F3 keys), select Run Tests > Clear Counter, since counters are cumulative between tests.

7.4.1. Traffic test

The purpose of traffic test is to verify bit and CRC errors, or some specific DUT capability. In this test, TSW900ETH sends permanent or variable traffic and checks DUT behavior. Bandwidth percentage can be Constant, Ramp, Burst, Time or permanent in 100% Flood, which generates an overflow, because channel, by specification, can not be full used (100% real usage). Payload can be used to load a Timestamp or a sequence to be used in BERT test. This sequence can be fixed or pseudo-random. In order to measure delay and jitter, payload Timestamp must be configured. To verify pauload bit errors, BERT paulod must be configured. To perform ordinary traffic test, Figure 78 setup must be in place and then, follow the steps below:

1. Configure Loopback TSW900ETH, according to section 7.3.
2. Select port to start the test and follow the steps below:
    2.1. Configure link, according to section **Erro! Fonte de referência não encontrada.**
    2.2. Configure Ethernet, according to section 5.2, select source and destination MAC addresses and filters configuration, in case nedded.
    2.3. Make test configurations in the selected port, in Test Settings > Traffic Test, according to section 5.5.2.
    2.4. Start the test in Run Tests > Start Traffic Test.

During tests, it is possible to check desired counters and statistics, on results screen.

7.4.2. RFC2544 tests

RFC2544 tests make available some DUT information. Below, available RFC 2544 tests operation and purpose are described.

- **Throughput**
    - **Purpose:** Reach DUT working limit rate, with no lost.
    - **Operation:** Send data according to configured Frame Size and Max Bandwidth, during timeframe configured in *Throughput Config* > *Duration*. In case of no lost frames (Lost frame is the sent frame that was not received), it is considered that DUT can transmit up to this rate. In case maximum configured rate is 100%, this is the DUT Throughput rate. In case any frame is lost, a test algorith verifies other rates, until find maximum rate without frames lost.
- **Latency**
    - **Purpose:** Verify frame round trip delay in DUT, with maximum throughput rate.
    - **Operation:** Calculates latency for each frame. Each attempt data traffic is sent according to configured throughtput rate, during timeframe configured in *Latency Config* > *Duration* and during transmission, calculates delay between sending and retunring a frame.
- **Frame Loss Rate**
    - **Purpose:** Find DUT overflow value, in other words, where DUT starts to lose frames more often.
    - **Operation:** Send data according to configured Max Bandwidth, calculates lost percentage (calculated by the difference between total transmitted and received frame amount, divided by total transmitted amount). After this, in case of lost frames, decreases transmission rates in Bandwidth Granularity and test it again, If a specific transmission rate can not identify frame lost in 2 sequential attempts, test is finished. A chart is built, displaying calculated lost rates and transmission rates from 0 to 100% of maximum theoretical value for tested frame size.
- **Back-to-back frames**

- Purpose: Determine highest burst DUT can attend with no losts.
- Operation: Send a frame burst using highest possible rate during timeframe configured in *Back-to-Back Config* > *Duration*. In case of frames lost, decreases burst rates according to *Back-to-Back Config* > *Frame Granularity*, until find burst rate which causes no lost. When burst rate causes no lost, this is the final Back-to-Back Frames test value.

To execute any RFC 2544 tests, it is mandatory to set up a scenario similar to Figure 78, following the steps below:

1. Configure link, according to section 5.1.
2. Configure Ethernet, according to section 5.2, select source and destination MAC addresses and configure filters, if needed.
3. Configure tests settings, in the selected port, in *Test Settings* > *RFC 2544*, according to section 5.5.1.
4. Execute *Run Tests* > *Start RFC2544 Test* to start RFC 2544 test.
5. TSW900ETH automatically opens log screen, where each test step can be verified during test execution.

7.5. Layer 3 tests (IPv4)

TSW900ETH uses same tests described in section 7.4, but destination IP address must be configured on tested port as Loopback source IP address and enable ARP (*IP Settings* > *Configuration* > *ARP Mode*) or configure destination MAC address same way as layer 2 test.

This layer also contains Ping and Trace Route test available, detailed below.

7.5.1. :Ping

Ping funtion can be used to verify conectivity and RTT (Round-Trip Time) against other layer 3 equipment which is able to respond ICMP request. During ping test TSW900ETH sends ICMP packets requests and wait its responses.

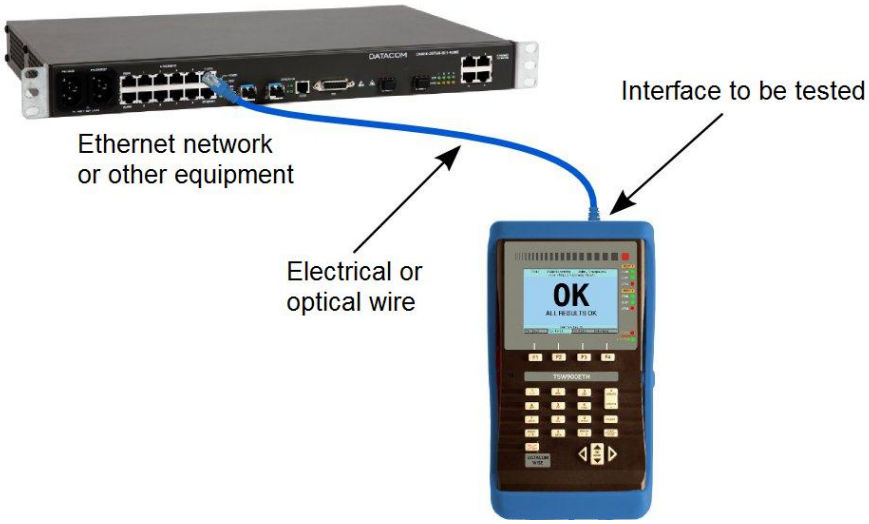


Figure 79. Ping and Trace Route test scenario

To execute Ping test, it is mandatory to set up a scenario similar to Figure 79, selecting optical ports (SFP1/SFP1) or electrical ports (ETH1/ETH2) as TSW900ETH interfaces, and following the steps below:

1. Configure link, according to section 5.1.

2. Configure Ethernet Settings, according to section 5.2. Select Ethernet/IPv4 in *Ethernet Settings* > *Configuration* > *Framing*.
3. Configure *IP Settings* > *Configuration* according to section 5.3.
4. It is recommended select Enable in *IP Settings* > *Configuration* > *ARP Mode*. Otherwise, destination MAC address needs to be configured.
5. Configure *Test Settings* > *Ping Test*. Number of Packets option determines total amount of packets during test. Value '0' determines unlimited packets.
6. Ping Interval (ms) option configures an interval between each packet transmission. Timeouts to Retry ARP is configured with '0' value, in case it is not necessary to send a new ARP packet when ping errors occurs. Ping Payload Size option configures a different size for ping packet payload, in bytes.
7. *Run Tests* > *Start Ping Test* to execute Ping test.
8. TSW900ETH automatically opens log screen, where each test step can be verified during test execution.
9. At the end of Ping test, TSW900ETH generates and displays on the screen ping statistics, showing minimum, average and maximum transmitted packets response time.

7.5.2. Trace Route

Trace Route test obtains IP packet path through network until reaches destination. Trace Route also helps detecting where network bottlenecks are, since it describes RTT (Round-Trip Time) for each network device.

To execute Trace Route test, it is mandatory to set up a scenario similar to Figure 79, and follow the steps below:

1. Configure link, according to section 5.1.
2. Configure Ethernet Settings, according to section 5.2. Select Ethernet/IPv4 in *Ethernet Settings* > *Configuration* > *Framing*.
3. Configure *IP Settings* > *Configuration* according to section 5.3.
4. It is recommended select Enable in *IP Settings* > *Configuration* > *ARP Mode*. Otherwise, destination MAC address needs to be configured.
5. Configure Max Hops (TTL) option from Trace Route test in Test Settings > Trace Route Test.
6. *Run Tests* > *Start Trace Route Test* to execute Trace Route test.
7. TSW900ETH automatically opens log screen, where each test step can be verified during test execution.

7.6. Embedded Tests (Scripts)

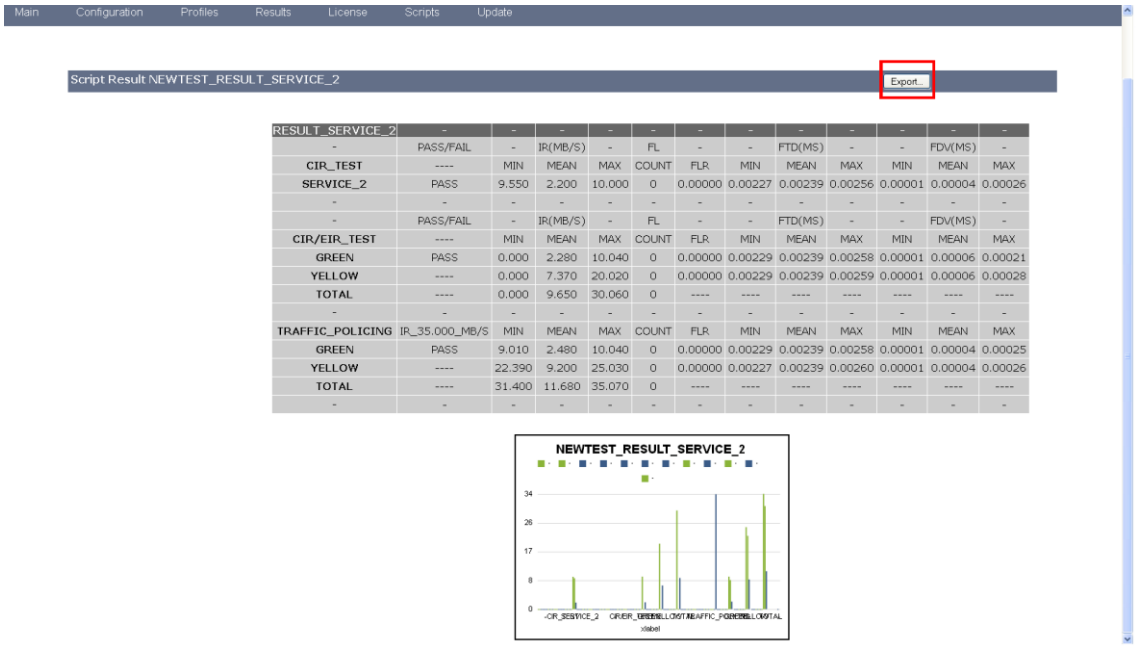
7.6.1. ITU-T Y.1564

ITU-T Y.1564 script defines a set of tests, which verify each quality of service (QoS) from each configured stream.

To execute test using ITU-T Y.1564 script, TSW900ETH needs to be configured and after that, some extra configuration need to be perfomed during test execution:

1. Configure data traffic on *Test Settings* > *Traffic* > *Traffic Test Type*. Select Multiple Streams.
2. Configure each stream on *Traffic Settings* > *Traffic* > *Streams Settings* > *Stream Setup*.
3. Execute the script, *F1-Setup* > *Scripts* > *Y1564.lic*.

4. TSW900ETH automatically opens log screen, where each test step can be verified during test execution. After test finishes, results are availble through TSW900ETH Web interface, Results menu (see Figure 80).



RESULT_SERVICE_2	-	-	-	-	-	-	-	-	-	-	-	-
-	PASS/FAIL	-	IR(MB/S)	-	FL	-	-	FTD(MS)	-	-	FDV(MS)	-
CIR_TEST	----	MIN	MEAN	MAX	COUNT	FLR	MIN	MEAN	MAX	MIN	MEAN	MAX
SERVICE_2	PASS	9.550	2.200	10.000	0	0.00000	0.00227	0.00239	0.00256	0.00001	0.00004	0.00026
-	-	-	-	-	-	-	-	-	-	-	-	-
-	PASS/FAIL	-	IR(MB/S)	-	FL	-	-	FTD(MS)	-	-	FDV(MS)	-
CIR/EIR_TEST	----	MIN	MEAN	MAX	COUNT	FLR	MIN	MEAN	MAX	MIN	MEAN	MAX
GREEN	PASS	0.000	2.280	10.040	0	0.00000	0.00229	0.00239	0.00258	0.00001	0.00006	0.00021
YELLOW	----	0.000	7.370	20.020	0	0.00000	0.00229	0.00239	0.00259	0.00001	0.00006	0.00028
TOTAL	----	0.000	9.650	30.060	0	----	----	----	----	----	----	----
-	-	-	-	-	-	-	-	-	-	-	-	-
TRAFFIC_POLICING	IR_35.000_MB/S	MIN	MEAN	MAX	COUNT	FLR	MIN	MEAN	MAX	MIN	MEAN	MAX
GREEN	PASS	9.010	2.480	10.040	0	0.00000	0.00229	0.00239	0.00258	0.00001	0.00004	0.00025
YELLOW	----	22.390	9.200	25.030	0	0.00000	0.00227	0.00239	0.00260	0.00001	0.00004	0.00026
TOTAL	----	31.400	11.680	35.070	0	----	----	----	----	----	----	----
-	-	-	-	-	-	-	-	-	-	-	-	-

Figure 80. ITU-T Y.1564 saved result - Web interface

8. APPENDIX

8.1. Warnings

During TSW900ETH handling, according to settings, warnings are displayed in some specific situations, in order to help user.

Messages are displayed for few seconds, according to the example in Figure 81.

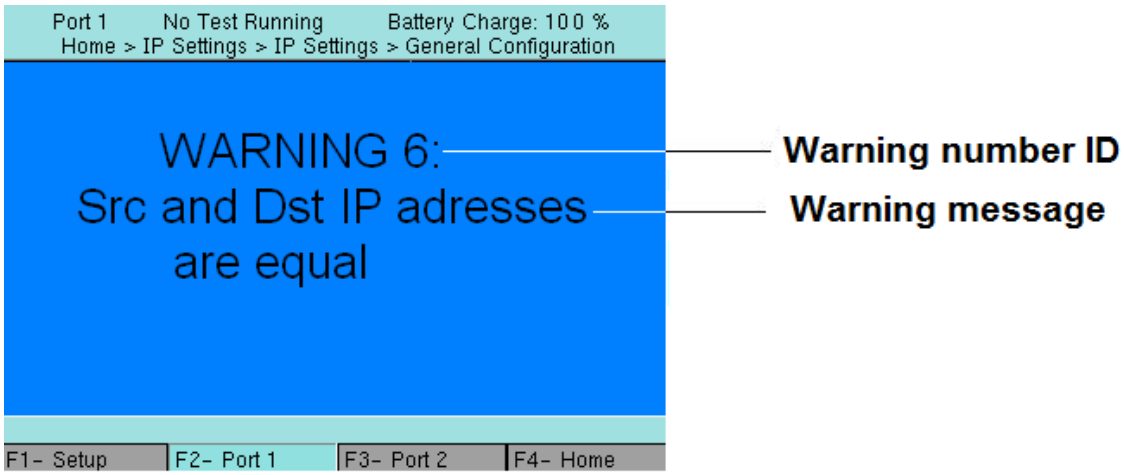


Figure 81. Warning example

Check on the warning number ID and message, to get more information about warning. Below there is a description for each possible warning.

ID	Warning	Description
1	Management port Gateway out of range	IP configured in management por tis out of Gateway range. Gateway must be configured with an address which can reach destination IP.
2	Src and Dst MAC addresses are equal	On the same Ethernet network exist two Ethernet cards with the same MAC address. Invalid configuration. Use this option only if sure to force situation like this.
3	Adjusted to Unicast	MAC configuration is incorrect. Maybe MAC is configured as Broadcast or Multicast, but selected type is Unicast.
4	Adjusted to Multicast	MAC configuration is incorrect. Maybe MAC is configured as Unicast, mas selected type is Multicast.
5	2 or More Streams Configured With the Same Source MAC/IP Address	When configuring multiple streams IPs, it is possible to set same IP on more than one stream. This way, it is possible to configure different MAC addresses with only one IP. One IP can not be associated to more than one MAC address and one MAC address can not be associated to more than one IP. Invalid configuration. Use this option only if sure to force situation like this.

6	Src and Dst IP addresses are equal	On the same Ethernet network exist two Ethernet cards with the same IP address. Invalid configuration. Use this option only if sure to force situation like this.
7	Src and Dst IP Addresses are in different networks	Source and destination IP addresses are configured in different networks. This way, is not possible to reach soruce or destination.. Invalid configuration. Use this option only if sure to force situation like this.
8	VLAN ID or SVLAN ID defined as '0' or '4095'	When Tagging is VLAN or Q-in-Q, and VLANID or SVLAN is ‘0’ or ‘4095’, this message is displayed. This occurs because ‘0’ and ‘4095’ values are reserved.
9	Invalid Frame Size. Change to 'n' Bytes	When frame size is configured less then ‘n’ bytes, using Framing Ethernet and after that Tagging is changed, minimum size must be adjusted to ‘n’ bytes. ‘n’ value vary according to configured Tagging (example: Q-in-Q), and is calculated and displayed for user by software. It is automatically adjusted.
10	Invalid Frame Size. Change to 'n' bytes - IPv4/IPV6	When frame size is configured less then ‘n’ bytes, using Framing Ethernet/IPv4 or Ethernet/IPv6 and after that Tagging is changed (plus UDP and Extension Headers, in case of IPv6), minimum size must be adjusted to ‘n’ bytes. ‘n’ value vary according to configured Tagging (example: Q-in-Q and UDP), and is calculated and displayed for user by software. It is automatically adjusted.
11	Stream rate higher than 100%	Total Streams rate must be up to 100%. It is not possible to start testing using this configuration.
12	Stream rate higher than Speed	Total Streams rate must be up to link speed. For example, if a link is configured as 1000 Mbps, stream rate only can be up to 1000 Mbps. It is not possible to start testing using this configuration.
13	Not recommended configuration	Informs user that Promiscuous Timestamp is not a recommended configuration.
14	Pass Threshold Adjusted	When configuring RFC Max Bandwidth with a value under Throughput Pass Threshold, Pass Threshold is automatically adjusted.
15	Frame Size of Stream(s) 'n' Adjusted	Multiple Streams IPv6 test can not have less than 100 bytes frames. Frame size is automatically adjusted.
16	Frame Size of 64 Bytes Can't be Tested. Changed to 'n'	When configuring RFC test with IPv6, 64 bytes frame sized can not be processed because its header is bigger than this size.
17	All Timestamps Will be Considered	If Timestamp ID field is configured as ‘0x0’ any Timestamp ID frame is accepted.
18	Stream(s) With L2, But Only L3 Packets Will be Considered	Informs user that when loopback starts with global framing configured as IPv4 or IPv6 (layer 3) and, even any flow is configured as Ethernet (layer 2), only IP packets (layer 3) are treated by loopback. In other words, global framing configuration handles loopback behavior.
19	Stream(s) With L3, But L3 Packets Will be Treated as L2	Informs user that when loopback starts with global framing configured as Ethernet (layer 2) and, even any flow is configured as Ethernet IPV4 or IPV6 (layer 3), every IP packets (layer 3) are treated by loopback as Layer 2 (loopback only evaluates MAC

		addresses). In other words, global framing configuration handles loopback behavior.

Table 5 Warning messages

Telephone: +55 61 3486-9100
Support: +55 61 3486-9100
Fax: +55 61 3486-9109
www.wi.com.br

DATACOM

Telephone: +55 51 3933-3000
Support: +55 51 3933-3122
www.datacom.ind.br