

Bercut-MMT
Ethernet 10/100 and Gigabit Ethernet Analysis

Operation Manual
1.2.7, 2009

Metrotek

© Metrotek, 2006-2009

No part of this document may be reproduced in any form or by any means without the express written permission of Metrotek. Metrotek retains the right to make changes to the hardware, software of **10/100/1000 Mbit/s Ethernet Networks Testing Module** , and to this document at any time, without notice.

Contents

1	Introduction	7
1.1	General	7
1.2	Documentation Set	8
1.3	Modifications Notice	8
2	General Information	9
2.1	Testing Procedure	9
2.2	RFC 2544 Method	9
2.3	B4-GBE: Ethernet Network Analysis Card	10
3	Starting Up	13
3.1	Device Connection Diagrams	13
3.2	Operation Mode Selection	14
3.3	Connection to Network Interfaces	14
3.4	Network Interfaces State Indication	14
4	RFC 2544. Parameters Configuration	17
4.1	Topology	19
4.2	Frame	20
4.3	Throughput	24
4.4	Latency	25
4.4.1	Theoretical Maximum Throughput Value	26
4.5	Frame Loss	27
4.6	Back-to-Back	28
5	RFC 2544. Measurements	29
5.1	Throughput	31
5.1.1	Plot	32
5.1.2	Table	33
5.2	Latency	33
5.2.1	Plot	34
5.2.2	Table	35
5.2.3	Latency over Time	36
5.3	Frame Loss	36

5.3.1	Plot	37
5.3.2	Table	38
5.4	Back-to-Back	38
5.4.1	Plot	39
5.4.2	Table	40
5.5	Measurements Processing	40
5.5.1	Saving Results	40
5.5.2	Previously Saved Results Display	41
6	TCP/IP: Basic Testing	43
6.1	Ping	44
6.2	Traceroute	45
6.3	ARP	46
6.4	Arping	47
6.5	Ftp/http	48
7	IPX Protocol	49
7.1	IPX Protocol Analysis	49
8	SNMP Protocol	53
8.1	SNMP Data Display	53
8.1.1	Advanced Settings Dialogue	54
9	PPPoE Protocol	57
9.1	PPPoE Connection Display	57
10	Network Interfaces Information	59
10.1	Interface Status	59
10.2	SFP Information	60
10.3	Cable test	61
11	Loopback	63
11.1	Loopback Modes in Ethernet Networks	63
11.1.1	First Layer Loopback	63
11.1.2	Second Layer Loopback	63
11.1.3	Third Layer Loopback	64
11.2	Loopback Configuration	64
A	Remote Testing	69
A.1	Connection Setup	69
A.2	Parameters Configuration	71

B	Traffic Types and Priorities	73
B.1	VLAN Tags	73
B.2	Type of Service	73
C	System Technical Specifications	75
D	Glossary	77
E	Technical support	81
E.1	Contact Information	81
F	Troubleshooting	83
	Bibliography	85

1. Introduction

1.1 General

Bercut-MMT Analyzer is a measurement device designed on the basis of a modular platform. It supports measurements in different segments of modern multi-technology telecommunication networks.

The analyzer's modular design provides its user with virtually unlimited testing and measuring capabilities for both traditional interface parameters and for working out long term diagnostics solutions for the communication network.

Figure 1.1 presents an external view of the device.



Figure 1.1. External view

The **Bercut-MMT** device consists of the system unit and two pluggable modules (cards¹), that provide an interface to such testing objects as PCM E1 streams, data transmission interfaces (Datacom) or Gigabit Ethernet.

The System Unit provides for the basic device functionality, i.e.: control of **Bercut-MMT** platform components, an interface to peripheral devices, power supply monitoring, a user interface and specialized computation, states and measurement modes indication.

¹ Terms *Pluggable Cards* and *Pluggable Modules* are convertible terms in the present manual and will be used interchangeably with equal meaning.

The **Bercut-MMT** System Unit consists of the following main components:

- Processor Module with a preinstalled operation system and nonvolatile data storage devices;
- LCD display with a sensor panel;
- number of multipurpose indication LEDs;
- keyboard;
- batteries;
- connectors for peripheral devices (serial port, USB interfaces, 10/100BaseT LAN interfaces, SD/MMC card connectors and connectors for headphones and an external power supply);
- connectors for specialized pluggable cards (modules) installation.

Cards usually contain a powerful processor that performs computations typical for a certain measurements mode. Computation results are transferred to the platform central processor that displays them to a user.

Various pluggable cards have different sets of hardware interfaces and programmable options. Each card has a unique serial number and provides information about a manufacturer, types of interfaces, allowed measurement options, etc.

1.2 Documentation Set

Depending on the ordered options, the following operations guides are delivered with the device:

- **Bercut-MMT**. Telecommunication Networks Analyzer Universal Platform.
- **Bercut-MMT**. E1 Interfaces Analysis.
- **Bercut-MMT**. Signalling Protocol Analysis.
- **Bercut-MMT**. Data transmission Interfaces Testing.
- **Bercut-MMT**. Ethernet 10/100 and Gigabit Ethernet Analysis.
- **Bercut-MMT**. OPIE Graphical Environment.

1.3 Modifications Notice

The manufacturer reserves the right to make any modifications that do not affect operability of the analyzer **Bercut-MMT** to the device hardware and software and to operation manuals without further notice and at its sole discretion.

2. General Information

10/100/1000 Mbit/s Ethernet Networks Analysis Subsystem based on the **Bercut-MMT** platform enables measurements and diagnostics of network equipment according to RFC 2544 methods (for a brief description please refer to par. 2.2, page 9 of the Manual) and basic IP testing.

2.1 Testing Procedure

In order to perform testing according to RFC 2544 methods, the following should be arranged:

- The Gigabit Ethernet analysis module, 10/100M Ethernet — B4-GBE should be installed (brief information about module can be found in section 2.3, page 10) according to procedure in section 3.3, page 73;
- the device should be connected to network under testing according to diagrams in section 3.1, page 13 ; the loopback for traffic redirection should be implemented, loopback description can be found in section 11, page 73;
- RFC 2544 parameters basic configuration should be performed, according to section 4, page 17 (interface configuration — IP and MAC addresses, frame size configuration, adding VLAN tags, frame priority, load and test duration setting for throughput, frame loss level, latency, back-to-back measurements);
- to measure throughput, frame loss, latency, back-to-back, following procedure in section 5, page 73;

Other types of diagnostics include:

- basic IP testing (ping, traceroute, arp, arping, ftp/http) — section 6, page 43;
- copper cable diagnostics and getting information about network interfaces status and SFP module — section 10, page 59;

2.2 RFC 2544 Method

This testing method is designed to determine characteristics of network interconnection devices. RCF 2544 is a standard method of Ethernet networks

performance evaluation.

For testing, typical frame sizes are used: 64, 128, 256, 512, 1024, 1280 and 1518 bytes, also it is possible to configure arbitrary frame size in the range from 64 to 1518 bytes inclusive; minimum duration of each test step; frame format (IP/UDP) and other parameters:

- Throughput measurement allows to determine the maximum rate at which there are no losses. Using previously obtained maximum rate value, it is possible to determine available channel bandwidth.
- Frame loss measurement allows to determine the percent of frames, that were not transmitted by network element at constant load due to the lack of hardware resources. This measurement may be useful to get information about network element behavior in case of abnormal network loading, for example, during broadcast storm.
- Latency measurement allows to determine a time period that starts from a moment when the last frame bit leaves transmitting side, passes through DUT/NUT, and finishes at a moment when first bit of a frame reaches receiving side. So this is a time required for a frame to be transferred over network and back. Delay deviations may be a problem in some cases, because for such protocols as VoIP, latency deviations or its increase may result in lower voice transmission quality.
- Back-to-back (marginal load) measurements. This test is transmission of frames of maximum length at maximum speed, which corresponds to minimal possible gap between frames during certain time period, starting from idle state. Test result is quantity of frames at the longest transmission, at which device or network under testing does not loose any frame.

2.3 B4-GBE: Ethernet Network Analysis Card

10/100/1000 Mbit/s Ethernet network transmission parameters analysis card (B4-GBE Card hereinafter) extends **Bercut-MMT** capabilities with functions of network testing on compliance to the norms, defined in RFC 2544 method and described in section 2.2, p. 9 .

The **Bercut-MMT** universal analyzer supports two B4-GBE cards simultaneously; each of them has two ports to connect to the network under testing. Connection may be either unidirectional (for example, one port works for data transmission (Tx), another — for data reception (Rx), Half-duplex), or bidirectional (Tx/Rx, Full-duplex mode).

The card supports either optical or standard copper cable connection. An SFP (Small Form Pluggable) adapter is used to connect to network interfaces; it is plugged into B4-GBE card.

The B4-GBE card layout is shown at Figure 2.1.



Figure 2.1. B4-GBE Card

3. Connection and Starting Up

3.1 Device Connection Diagrams

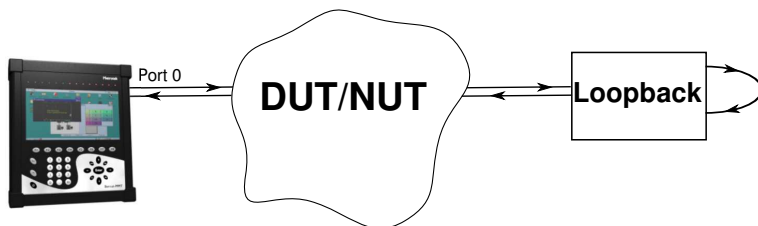


Figure 3.1. Connection Diagram 1

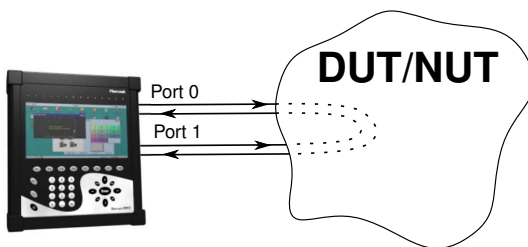


Figure 3.2. Connection Diagram 2

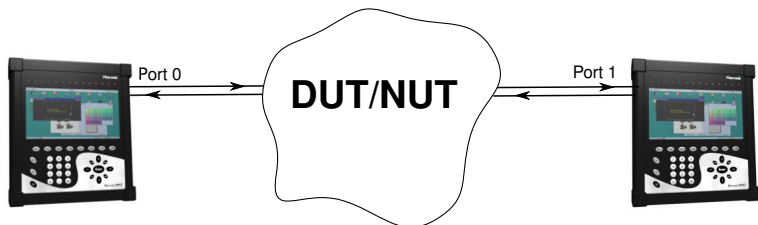


Figure 3.3. Connection Diagram 3

Device connection to the network or device under testing (NUT/DUT) using one port is schematically shown at figure 3.1. In this case, traffic generated by testing device should be redirected back by means of loopback.

In case networks or devices under testing are able to redirect traffic from one port of B4-GBE card to its another port, a connection scheme is used that is shown at Figure 3.2.

When two **Bercut-MMT** devices are used for remote testing of networks or devices, (refer to Figure 3.3), it is necessary to perform configuration, described in Annex A, p. 69.

3.2 Operation Mode Selection

The mode of operation of data transmission interface analysis card can be configured with the help of **Firmware Update utility** application: **O-Menu** ⇒ **Settings** ⇒ **Firmware Update utility** (for detailed description of operation mode configuration for pluggable modules refer to *Bercut-MMT operations manual. Telecommunication Systems Universal Analyzer Platform*).

3.3 Connection device to Network Interfaces

- Install the B4-GBE card according to description in *Operations Manual*.
- Install SFP modules in the card interface ports, up to click.¹
- Connect device to the network equipment to be tested according to Connection diagrams shown above.

After the device is connected to equipment to be tested, it is necessary to configure measurement parameters, that are described in details in section 4, p. 17.

3.4 Network Interfaces State Indication

For B4-GBE cards, network interfaces state indication is provided by LEDs at the **Bercut-MMT** front panel. In the upper part of a screen there are LED labels.



Figure 3.4. Indicators

¹ Module type should comply with the type of connected equipment (optical or copper cable).

LED/indicators meaning for each interface (from left to right):

- Connection state. Green means: connection with equipment under test established, red: no connection. In case connection is established, the column shows established link rate.
- Testing state:
 - TEST — green colour means: RFC 2544 measurement mode is active, frame transmission and reception is active;
 - LB1 — green colour means: loopback mode is active; indicator corresponds to the loopback layer (LB1, LB2, LB3).
- RX — transmission state. Is green when a frame is sent.
- TX — reception state. Is green when a frame is received.

4. RFC 2544. Parameters Configuration

The **Ethernet: RFC2544 Parameters** application is used to configure measurement parameters prior to testing with RFC2544 method. This application is launched with corresponding icon on the desktop or via menu in the following sequence:

O-Menu ⇒ **Ethernet Testing** ⇒ **Ethernet testing config.**

Application main window layout is shown at Figure 4.1.

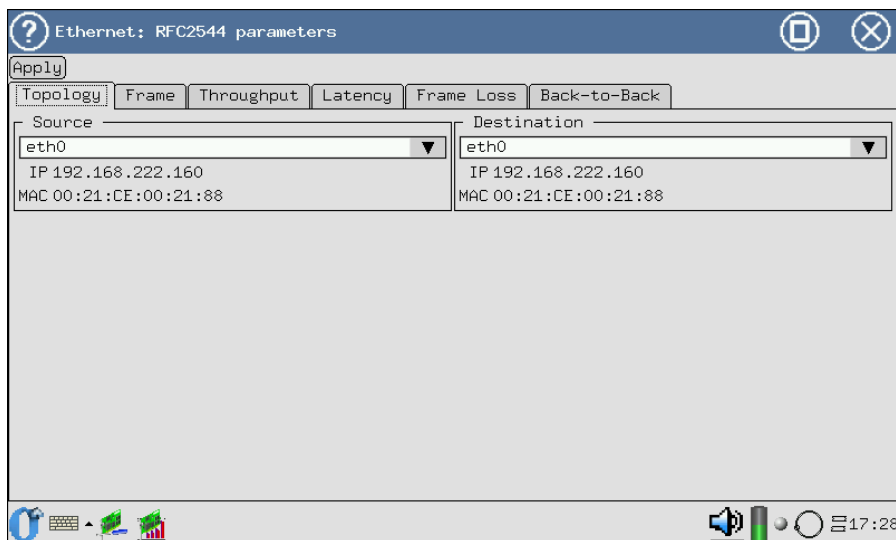


Figure 4.1. Ethernet: RFC2544 Parameters

The **Ethernet: RFC2544 Parameters** application window contains the following tabs:

- **Topology** — to choose source interface and destination interface from available in the list.

***Note:** in case source and destination interfaces are not configured (there are no IP- and MAC-addresses), measurement*

is not possible!

- **Frame** — contains B4-GBE module basic parameters needed for measurements.

Note: configuring this section parameters is mandatory!

- **Throughput** — configuration of tested equipment throughput measurement parameters.
- **Latency** — configuration of delay measurement parameters.
- **Frame loss** — configuration of frame loss level measurement parameters.
- **Back-to-Back** — configuration of maximum load measurement parameters.

Each of the mentioned application tabs is described in details in the following sections of this chapter.

Above all tabs there is **Apply** button. When it is pressed, previously configured parameters are activated.

To display F1 - F8 functional keys designation (refer to Figure 4.2), it is necessary to press the icon, located at the left of clock in the lower right corner of a screen, and to check **Fkey** item with a flag.

4.1 Topology

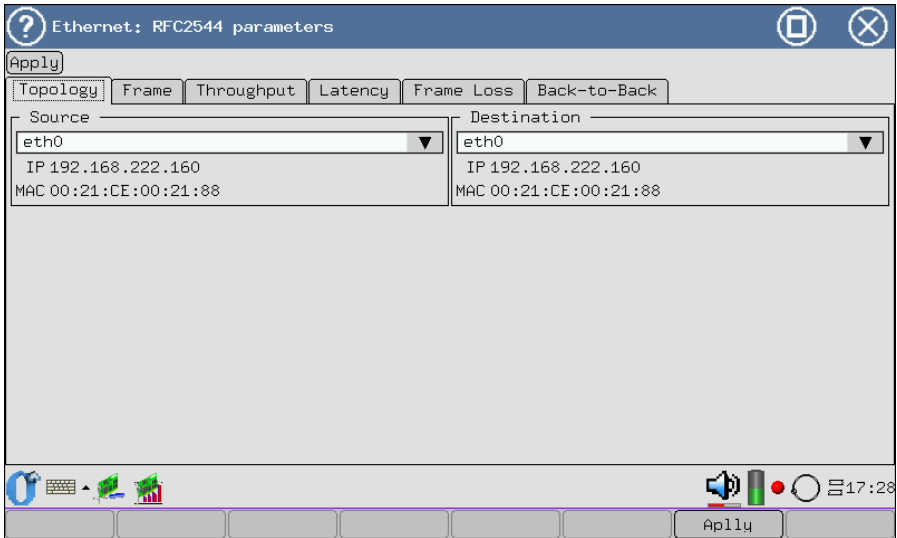


Figure 4.2. Basic Configuration Window

The **Topology** tab displays information about interfaces, connected according to various schemes from section 3.1, p. 13.

Before the work starts, it is necessary to define source interface and destination interface. Available local and/or remote interfaces - **Bercut-MMT** devices - are listed in the drop-down lists. When interfaces for testing are selected, reference information: IP and MAC addresses of corresponding interfaces is displayed below the chosen fields.

To save current configuration of this tab, it is necessary to press the **Apply** key, or F7 functional key with the same function.

4.2 Frame

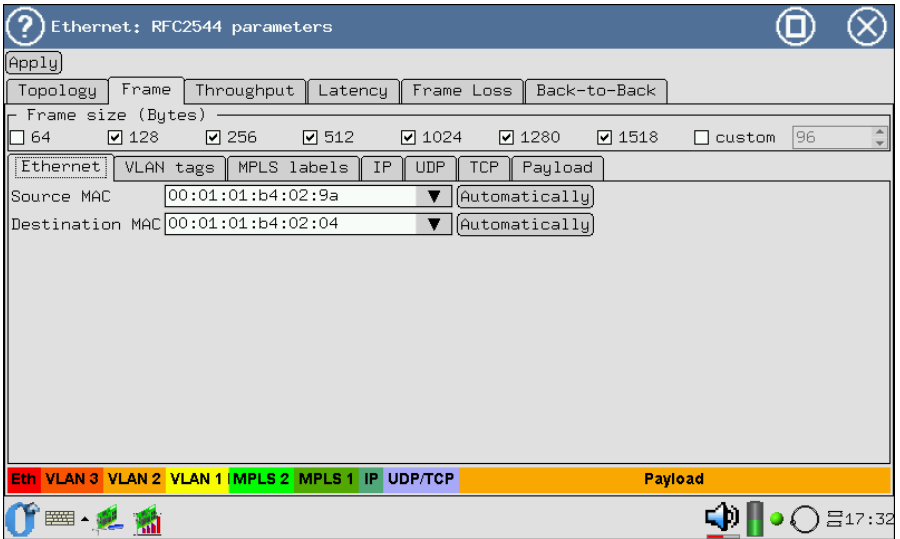


Figure 4.3. The *Frame* Tab Configuration Window

This tab allows to configure the following parameters.

- **Frame size (Bytes)** — size of the data packets used for testing purposes. Standard packets of 64, 128, 256, 512, 1024, 1280, 1518 bytes can be chosen, and any other value in the range from 64 to 1518 bytes inclusive, except currently selected.

Note: at least one value must be chosen.

- **Ethernet** — this tab contains fields to enter source and destination MAC addresses that will be inserted in the corresponding fields of the test packets. The **Automatically** tab is used to insert MAC addresses of source and destination interfaces that are chosen in the **Topology** tab.

MAC addresses may be configured using virtual keyboard. Virtual keyboard (refer to Figure 4.4) is displayed on pressing with a stylus to the MAC address input field, and has symbols (characters and digits) necessary to enter the MAC address.

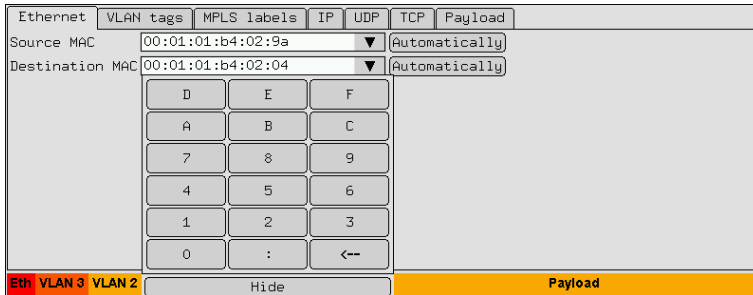
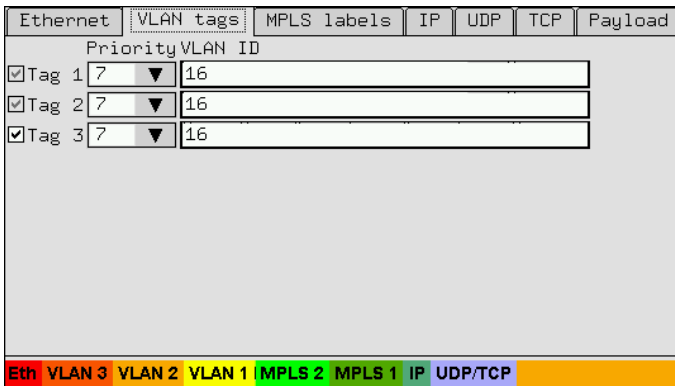


Figure 4.4. Virtual keyboard to enter MAC address

- **VLAN Tags** — this tab has **Tag** flags (marks added to Ethernet packets when device generates traffic). Flags are set in sequence in the ascending order.
 - **Priority** — this field set the priority with which a frame will be tagged (is significant when processing in network device is carried on).
Priority and traffic type mapping according to IEEE 802.1Q are shown at Figure 4.5 and are described in Table B.1 of Annex B, page 73.

Figure 4.5. The *VLAN-Tags* tab layout

- **VLAN ID** — a 12-bit VLAN identification, is a number from 0 to 4095, uniquely identifies the network a frame belongs to. VLAN ID zero value shows this given frame carries no information about VLAN and has only priority information.

- **MPLS labels** — this tab has flags to add MPLS labels to Ethernet frames, in order to increase transmission rate of IP traffic (refer to Figure 4.6). Up to three tags can be inserted, which may be needed when additional MPLS-based features are implemented. Following elements should be configured for this purpose:
 - **Label Value** — a 20-bits field with a tag code; is a number from 0 to 1048575; reserved tags with value from 0 to 15 do not depend on topological properties of the network and are defined by IETF committee;
 - **Time To Live** — analogous to IP TTL: this is a 8-bits field that specifies time of life of IP datagram; is used to avoid endless circulation of packets in the network (a number from 0 to 255 should be entered).

Ethernet	VLAN tags	MPLS labels	IP	UDP	TCP	Payload
		Label Value	TTL			
<input checked="" type="checkbox"/>	MPLS 1	0	0			
<input checked="" type="checkbox"/>	MPLS 2	0	0			
<input checked="" type="checkbox"/>	MPLS 3	0	0			

Figure 4.6. The *MPLS labels* tab layout

Ethernet	VLAN tags	MPLS labels	IP	UDP	TCP	Payload
Source IP	192.168.10.4	<input type="button" value="Automatically"/>	TTL	64		
Destination IP	192.168.10.3	<input type="button" value="Automatically"/>	TCP	<input type="button" value="▼"/>		
Precedence	000 (Routine)		ToS	0000 (all normal)		

Figure 4.7. The *IP* tab layout

- **IP** — this tab consists of a number of fields that have to be edited in order to generate outgoing traffic properly:
 - **Source IP** — is a field to enter sender’s IP address; is populated with virtual keyboard, that is displayed on pressing with a stylus in the address input field (the **Automatically** button is used for entering an IP address of sender’s interface that is chosen in the **Topology** tab);
 - **Destination IP** — this field is populated similar to the previous one;
 - **Time To Live** — 8-bit field representing time period of a packet’s life;
 - **UDP/TCP** — This field selects transport protocol to transfer data over IP networks:

Figure 4.8. Tab element: *IP*

- **Precedence** — this field sets frame priority, that will be present within IP packet structure when the device generates traffic; according to RFC 791, eight frame priority values are supported; sender can set in this field any value from Table B.2 of Annex B, page 73;
- **ToS (Type of Service)** — this field defines a type of serving IP packets; sender can set any value in this field, compliant to RFC 1349; in particular, values shown at Figure 4.9 and described in Table B.3 of Annex B, page 73 are possible.

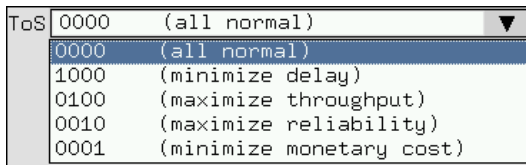


Figure 4.9. Type of Service

- **UDP** — with this tab a port is configured to send and receive data for a protocol selected under **IP** tab:

Figure 4.10. The *UDP* tab layout

- **TCP** — with this tab a port is configured to send and receive data for a protocol selected under **IP** tab.
- **Payload** — this field is used to select a type of payload which will be present in the datagram data field:

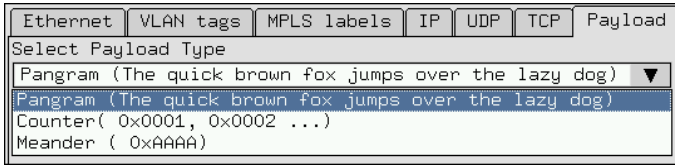


Figure 4.11. Payload Type Selection

- **Pangram** — is a check phrase that includes all alphabetic symbols. This device uses one of English pangrams: *The quick brown fox jumps over the lazy dog*.
- **Counter** — an incremental sequence of numbers (hexadecimal representation) in the form of 0x0001, 0x0002, etc.
- **Meander** — a sequence of alternating zeroes and ones.

Below all tabs there is a coloured scheme that corresponds to packet structure and includes all fields comprising the datagram.

4.3 Throughput

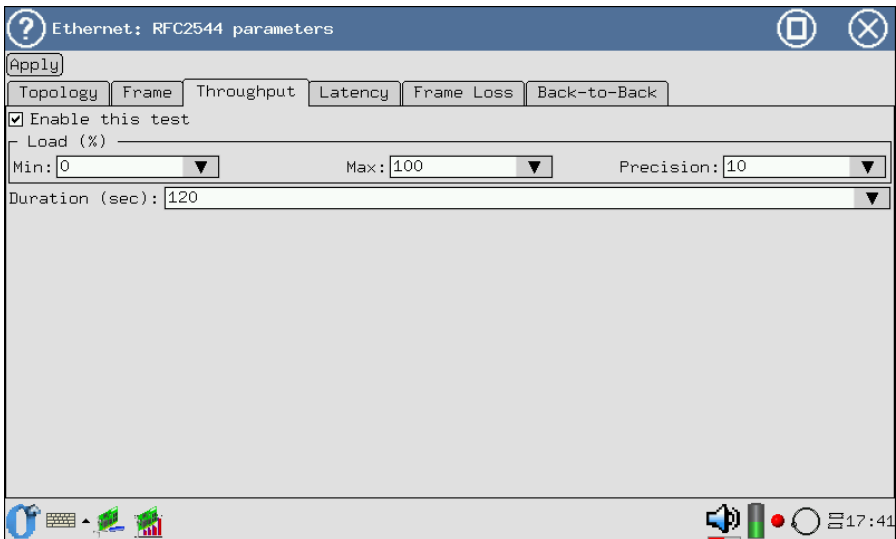


Figure 4.12. Throughput Measurements Configuration

- **Enable this test** — is a flag that turns throughput measurement on or off (the F2 functional key has the same meaning).

- **Load** — these are fields that allow to configure throughput value determination parameters.

This testing is based on dividing load in halves (binary determination algorithm). For example, in case testing starts with 10 percent channel payload (minimal load value, **Min**) and no packets were lost, then next testing step corresponds to 55%, then 77.5%, and so on up to 100% (maximum load, **Max**).

Testing will continue up to the moment when difference between maximum and minimum load values at current iteration is lower than a certain predefined **Precision** value.

Values are measured in percents of maximum connection throughput. Minimum resolution value corresponds to maximum test accuracy, but this increases measurements duration.

- **Duration (sec)** — time period of one measurement iteration for each frame size selected in the general frame size configuration (not more than 1200 s).

In order to obtain the most pictorial representation of the test results, it is recommended to choose the maximal value of this field.

4.4 Latency

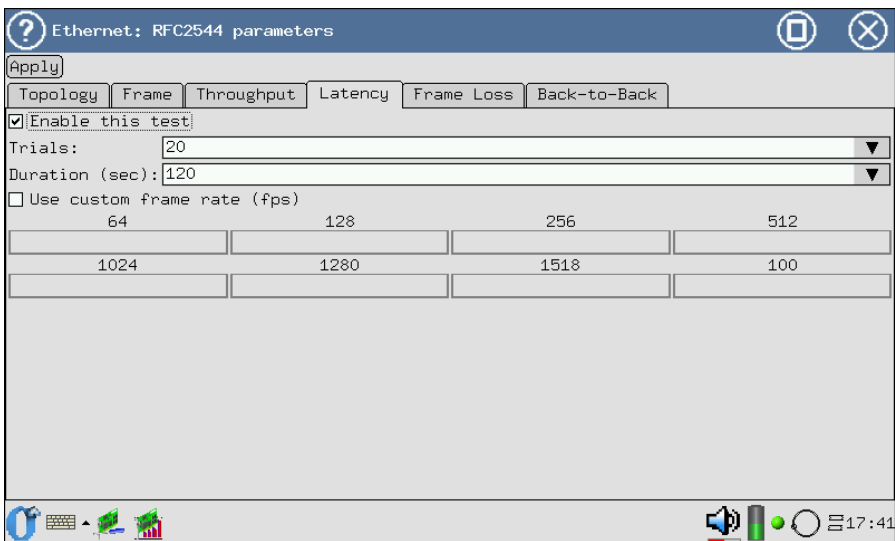


Figure 4.13. Latency Measurement Configuration

- **Enable this test** — is a flag that turns data transmission delay measurement on or off for equipment under testing (functional key F2 has the same meaning).
- **Trials** — quantity of delay measurements for each frame size configured.
- **Duration** — time period of one measurement iteration for each frame size selected in the general frame size configuration (not more than 1200 s).
- **Use custom frame rate (fps)** — a flag that allows to enter values manually. For each of frame sizes used, rate value is entered in the corresponding field (functional key F3 has the same meaning).
The **Configure** field allows to configure rate for arbitrary frame size, selected in the **Frame** ⇒ **custom** tab.

Note: if this test is selected, it is necessary to either select Throughput test (in this case Latency values will be calculated for determined throughput), or define desirable frames transmission rate. Frame transmission rate values (if configured manually) should not exceed theoretical maximum throughput value for current settings.

4.4.1 Theoretical Maximum Throughput Value

Theoretical maximum throughput value is calculated using minimal values of the following parameters:

- preamble = 8 bytes;
- frame size = 64 bytes;
- interframe interval = 12 bytes.

Theoretical value is calculated according to the following formula:

$$Max.throughp. = \frac{(Physical\ rate)}{(Preamble + Frame\ size + Interfr.\ interval)}$$

Maximum theoretical throughput values calculated using this formula are presented in the table below. Values are for standard frame sizes and physical interface rates allowed for testing purposes.

Table 4.1: Theoretical Throughput Values

Frame size, bytes	Maximum rate, frames/s		
	10 Mbit/s	100 Mbit/s	1000 Mbit/s

64	14880	148809	1488095
128	8445	84459	844594
256	4528	45289	452898
512	2349	23496	234962
1024	1197	11973	119731
1280	961	9615	96153
1518	812	8127	81274

4.5 Frame Loss

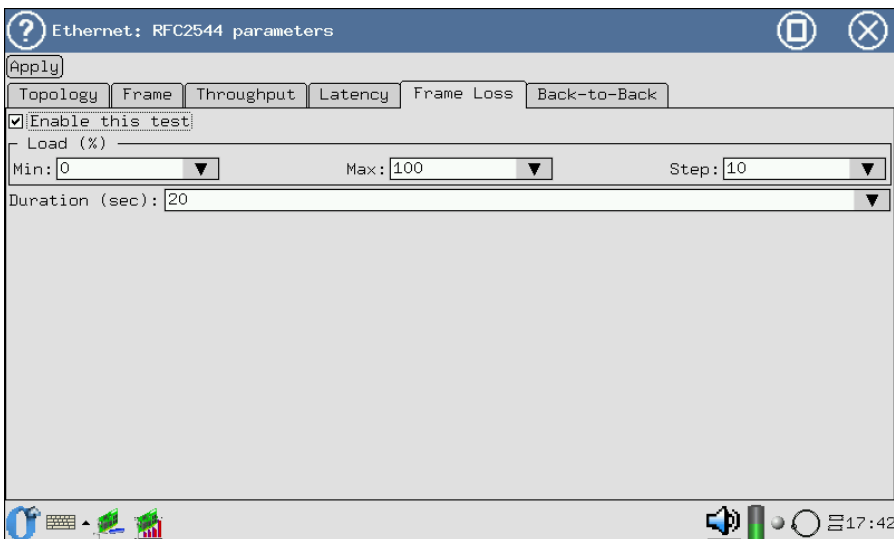


Figure 4.14. Frame Loss Measurements Configuration

- **Enable this test** — is a flag that turns transmission loss level measurements on or off (the F2 functional key has the same meaning).
- **Load** — these are fields that allow to configure load change parameters at loss level measurement: minimal (**Min**), maximal (**Max**) load values and **Step** parameter. **Step** — is a value by which a load is decreased on each iteration (maximum step is 10). Values are measured in percents of maximum connection throughput.
- **Duration** — time period of one measurement iteration for each frame size selected in the general frame size configuration (not more than

1200 s).

4.6 Back-to-Back

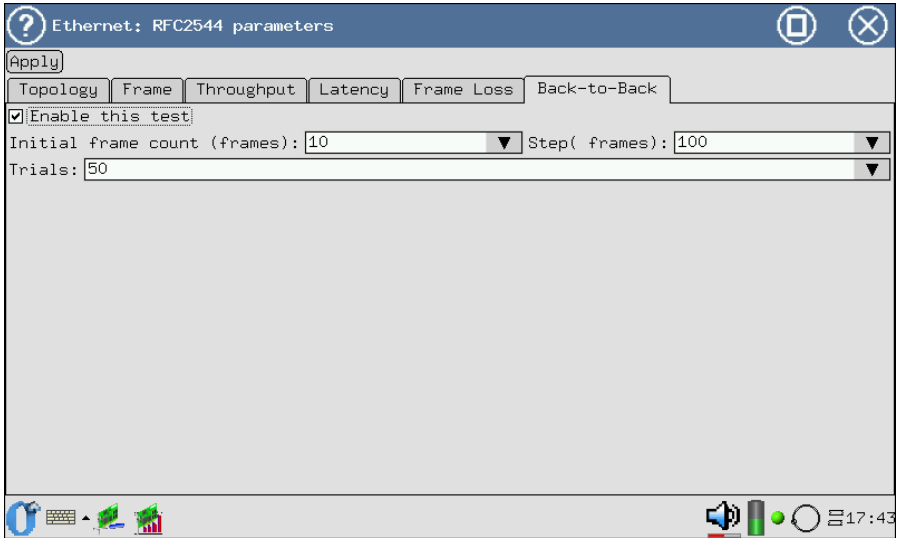


Figure 4.15. Back-to-Back Measurement Settings

- **Enable this test** — is a flag that turns Back-to-Back (maximum load) measurement on or off, F2 functional key has the same meaning.
- **Initial frame count (frames)** — the starting length of transmitted sequence.
- **Step (frames)** — is a step of frame quantity (sequence length) changing.
- **Trials** — quantity of measurements for each frame size configured.

5. RFC 2544. Measurements

The **Ethernet: RFC2544 Test** application is used to conduct Ethernet equipment testing according to RFC2544 method. This application is launched with corresponding icon at the desktop or with the device main menu, in the following sequence:

O-Menu ⇒ **Ethernet Testing** ⇒ **Ethernet testing**.

The application window is shown at Figure 5.1 .

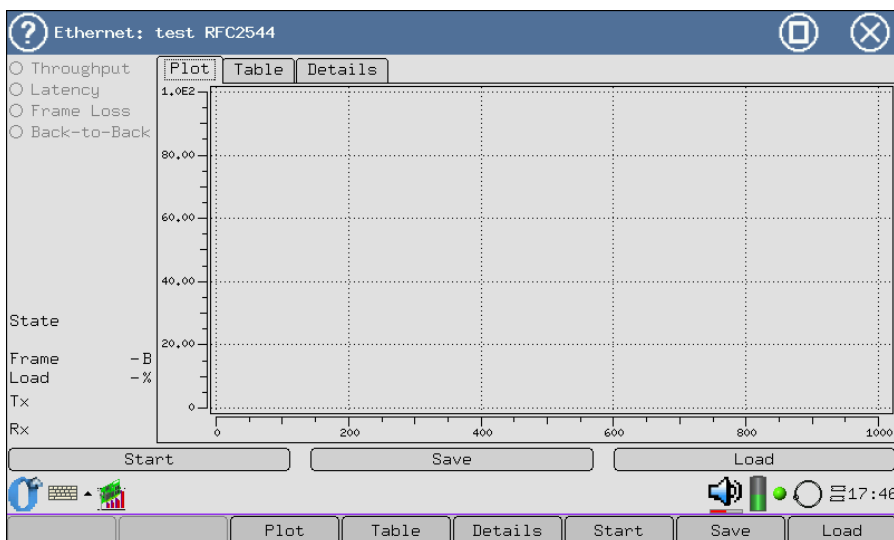


Figure 5.1. Measurements Window

The window consists of the following elements.

1. Dynamic list of measurements. Names colour is changed during measurements process. Initially, all tests names are unavailable and are of grey colour. The name of a test currently executed is highlighted by blue, completed test is shown in black.
2. Execution indication — the testing execution process for current card is displayed.

- **State** — state of the testing process. Possible states:
 - in progress — active state, frames sending and reception are being executed;
 - suspended — tests or test iterations are paused, frames are not sent or received;
 - completed — testing is completed automatically or is interrupted by user.
 - **Frame** — sent frames size.
 - **Load** — current load on a link.
 - **Tx** — frames sending process display for each test iteration.
 - **Rx** — frames receiving process display for each test iteration.
3. Right (main) window region (**Plot, Table, Details**, F3, F4 and F5 functional keys correspondingly) — measurement results. For each test, obtained results are displayed in three ways: graphical, table and textual. To switch between results display modes, just navigate to corresponding tab.
 4. Lower part of the window is occupied by toolbar with three buttons (refer to Figure 5.2).
 - **Start/Abort** — start and stop testing process (corresponds to F6 functional key). To stop the testing process, press the **Abort** button. In case the testing process is not aborted, system will automatically stop its execution after all necessary measurements are completed.
 - **Save** — save obtained results as a file (corresponds to F7 functional key **Save**), for more details refer to Par. 5.5.1, page 40;

Note: if current measurements results were not saved, with next start these data will be erased. On application closing, unsaved data will be also lost.
 - **Load** — loading of previously saved measurements, for more details refer to Par. 5.5.2, page 41;

Measurement results for each test are presented at three tabs:

- **Plot** — graphical representation of measurement results;
- **Table** — tabular representation of measurement results.
- **Details** — measurements log (this tab has the most detailed information about executed test, this is important for troubleshooting of equipment under testing).

Figure 5.2 shows an example of **Details** tab for **Throughput** test.

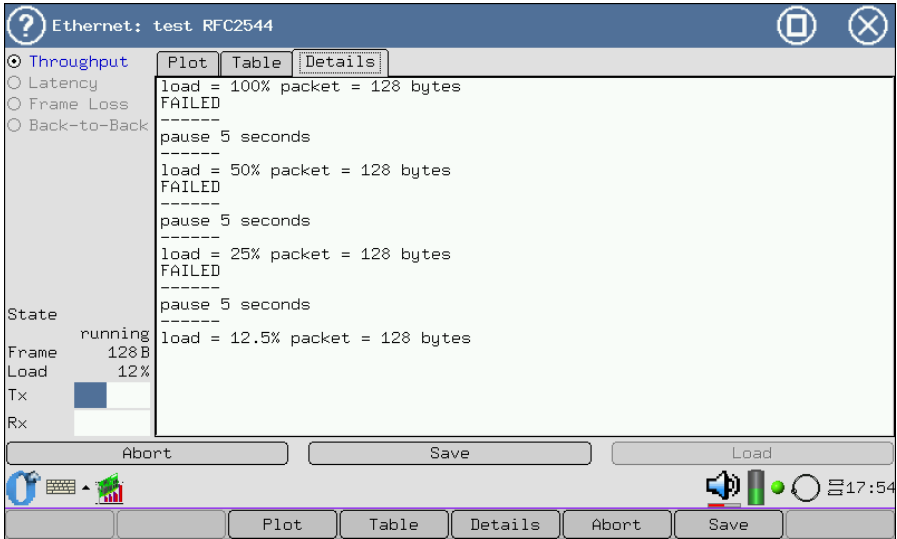


Figure 5.2. Throughput Test Results: details

Data representation structure for all other tests will be the same, that's why this tab for each test is not discussed in this Manual.

5.1 Throughput

Throughput measurements provide maximum rate value, at which there is no loss of frames transiting the system being tested. Using previously obtained maximum rate value, it is possible to determine available channel bandwidth.

5.1.1 Plot

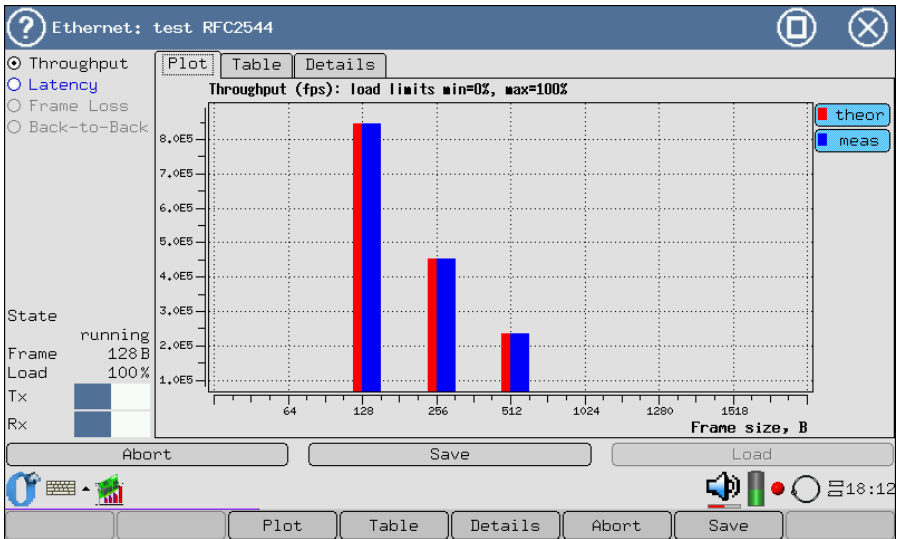


Figure 5.3. Throughput Test Results: Plot

This diagram shows measured and theoretical throughput values (fps) for each data packet, set in the configuration. Theoretical values are calculated for full (100%) load.

5.1.2 Table

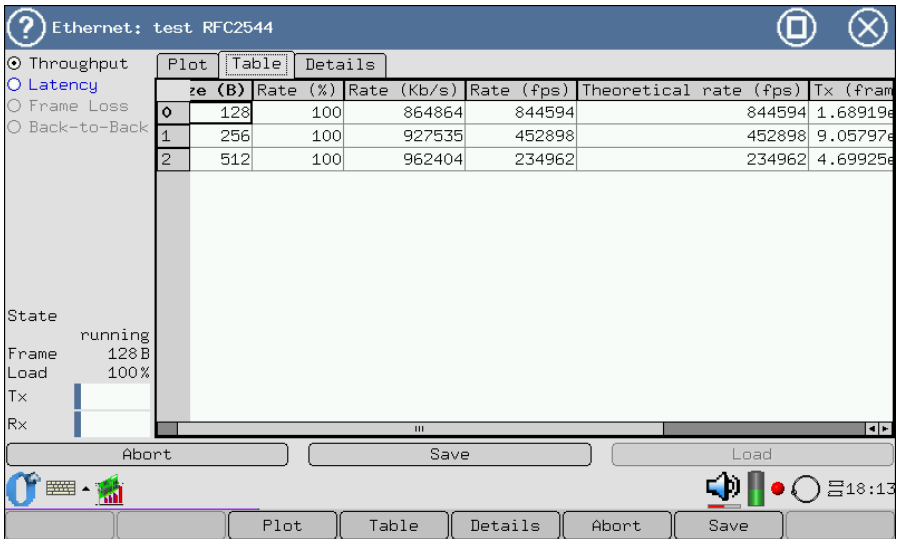


Figure 5.4. Throughput Test Results: Table

Test results are displayed as a table with following fields: frame size, load, throughput value (Kbit/s, fps) and theoretical value for frame size specified (fps), obtained as a result of measurements, quantity of packets transmitted (Tx) and received (Rx), and quantity of lost frames.

5.2 Latency

It is time that a frame needs to go through network and return back at network elements with buffering. This parameter allows to measure a time period that starts from a moment when last bit of outgoing frame leaves transmitting side, passes through DUT/NUT and finishes at a moment when first bit of a frame reaches receiving side.

5.2.1 Plot

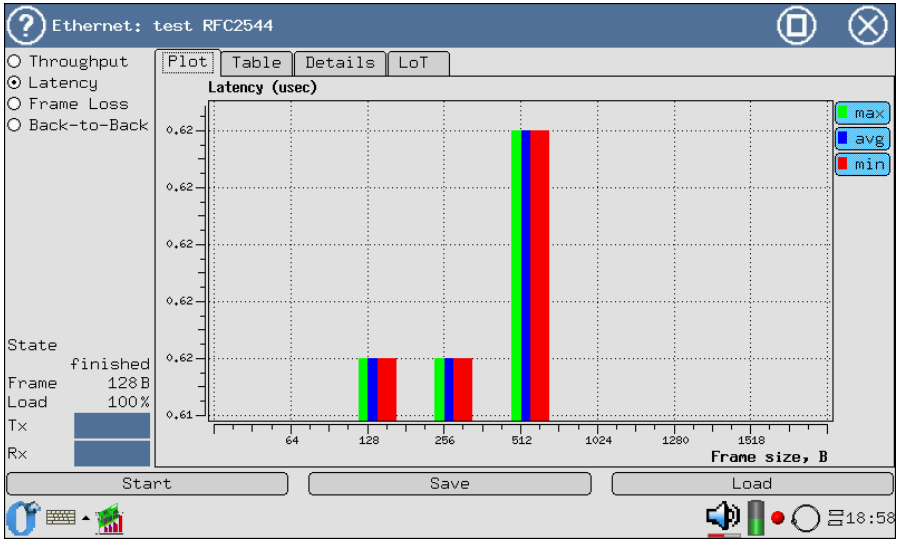


Figure 5.5. Latency Test Results: Plot

The diagram shows measured minimum/maximum/average delay value in microseconds, for each data frame size configured.

5.2.2 Table

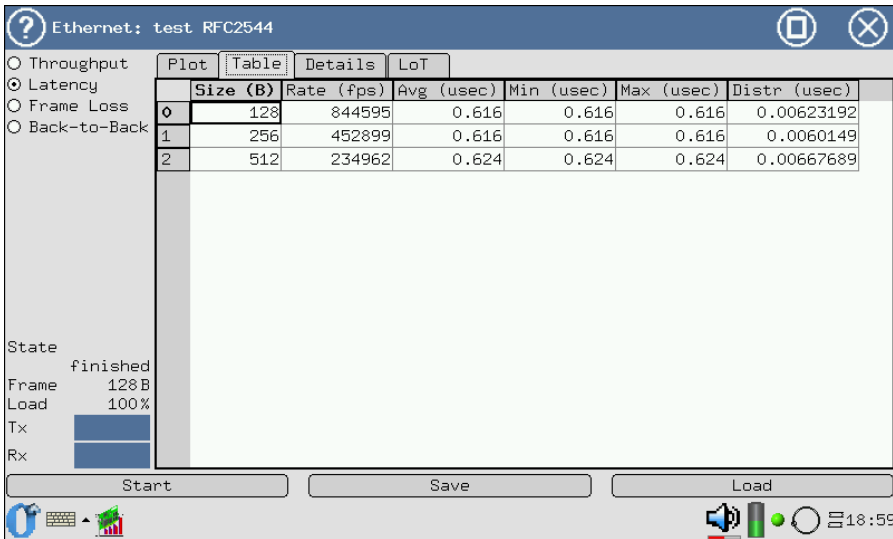


Figure 5.6. Latency Test Results: Table

The Table shows measured throughput value and average/minimum/maximum delay value in microseconds, for each frame size configured. The Distr (distribution) column shows by what value (on average) all delays differ from average value, in microseconds.

5.2.3 Latency over Time

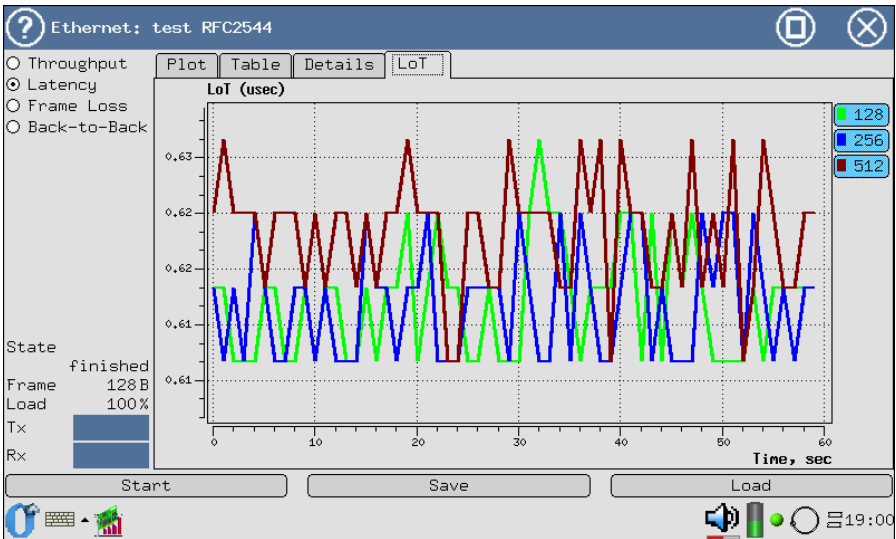


Figure 5.7. Latency over Time Test Results

Latency over time distribution is used to determine the ability of a device under testing (DUT) to effectively buffer the traffic.

In the best case, LoT will have small delay increase over short time period¹.

Quick LoT increase is a result of DUT buffer overflow, and problems may arise linked to its modes of operation. Smooth increase of LoT indicates that DUT is able to support the current frames flow.

The diagram shows delay changing during test execution. Horizontal axis corresponds to the last 60 seconds of a test.

5.3 Frame Loss

Frame loss measurement allows to calculate percent of frames, that were not transmitted by object under testing (network or device) at constant load, due to the lack of hardware resources. This measurement may be useful to get information about network element behavior in case of anomalous network loading conditions.

¹Measured LoT values depend on the tested equipment type and capabilities.

5.3.1 Plot

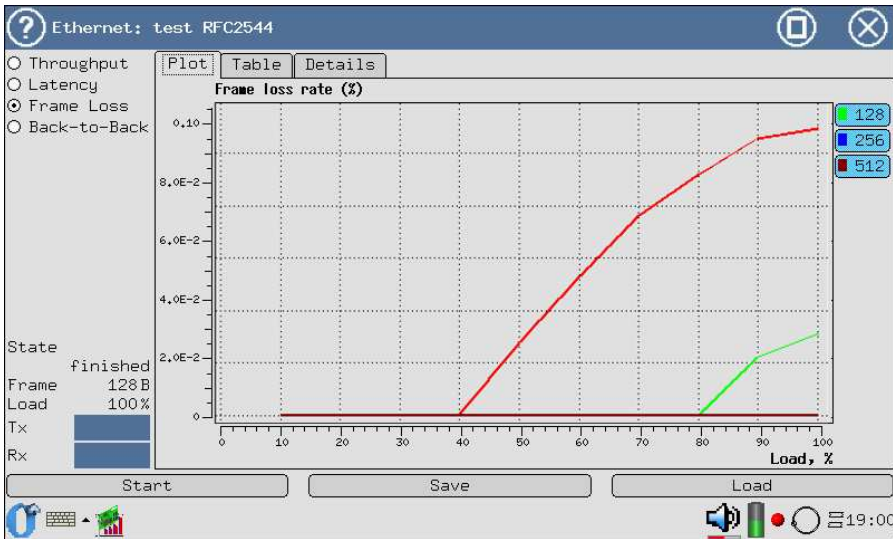


Figure 5.8. Frame Loss Test Results: Plot

The diagram for each configured frame size shows measured frame loss value (in %) dependency upon normalized value (in %), equal to ratio of input load to theoretical maximum throughput of equipment under testing.

Buttons at the left and right diagram sides are used to display frame size and its corresponding curve colour. These buttons allow to view the diagrams one by one or in together.

5.3.2 Table

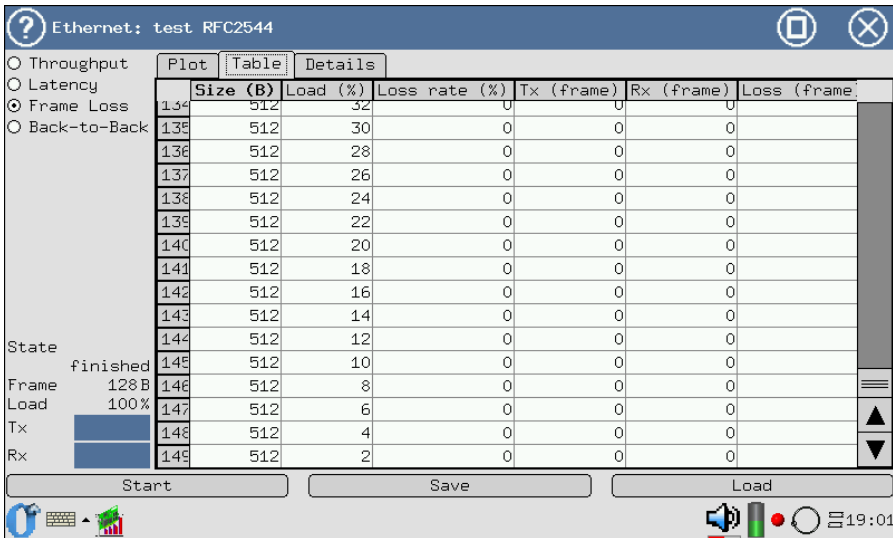


Figure 5.9. Frame Loss Test Results: Table

5.4 Back-to-Back

Marginal load measurement — back-to-back. This test is transmission of frames of maximum length at maximum speed, which corresponds to minimal possible gap between frames during certain time period, starting from idle state.

The result of the test is quantity of frames at most durable packet transmission, at which a device under testing or network does not loose any frame. This means that for equipment that supports transmission of any quantity of frames of certain size at maximum rate, testing will continue forever and result will not be obtained.

5.4.1 Plot

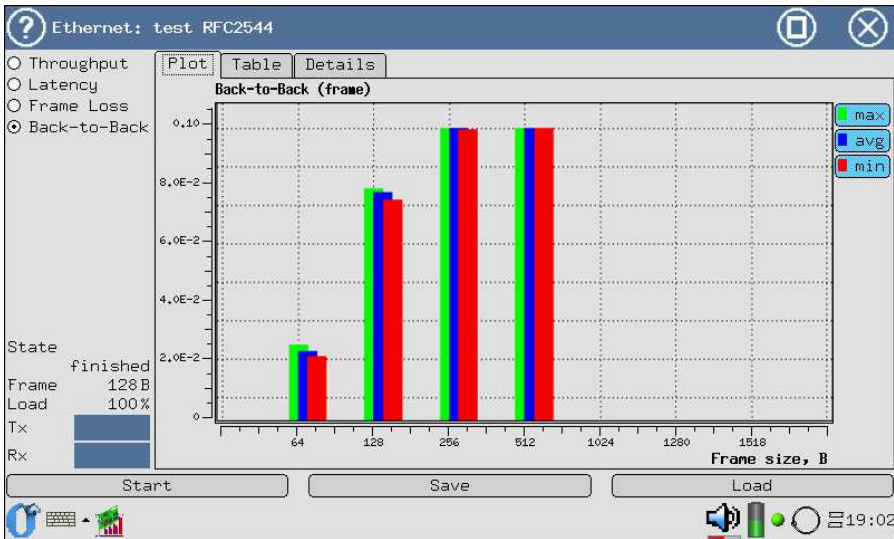


Figure 5.10. Back-To-Back Test Results: Plot

The diagram shows measured minimum/maximum/average quantity of frames transmitted without loss, for each frame size configured.

5.4.2 Table

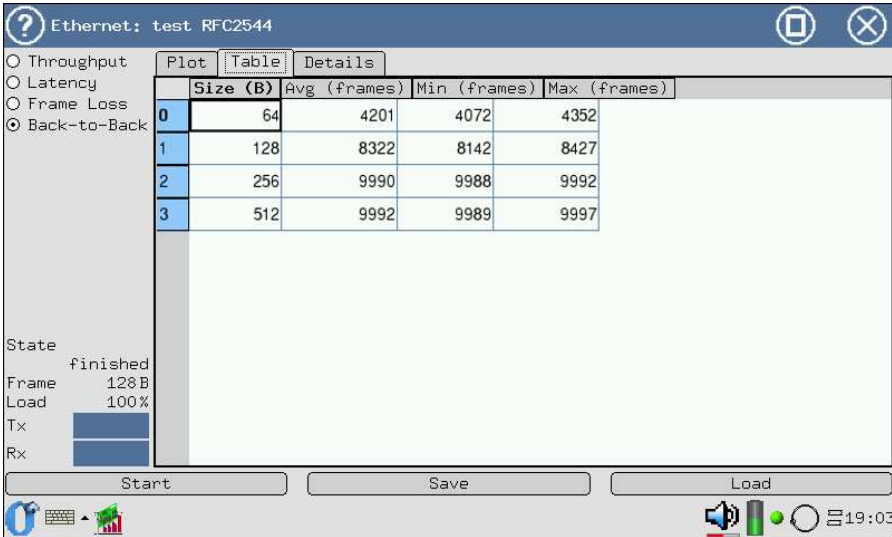


Figure 5.11. Back-To-Back Test Results: Table

5.5 Measurements Processing

Bercut-MMT enables saving of measurements results and reviewing of previously saved results.

These operations are performed by **Ethernet: test RFC2544** application.

5.5.1 Saving Results

The system supports saving to CSV and XML file formats. To the file, date and measurement results from the **Table** tab are saved. Information about measurements execution from the **Details** tab is not saved.

Results stored in CSV format can be viewed and edited on PC with any application that support electronic tables.

Results stored in XML format can be loaded for review into **Ethernet: RFC2544 test** application.

The **Save** button is used to save current measurement results. On pressing it, a dialogue window appears, shown at Figure 5.12. In the **Name** field of this window the saved file name is entered, or default name remains, that is built of measurement name, date and time.

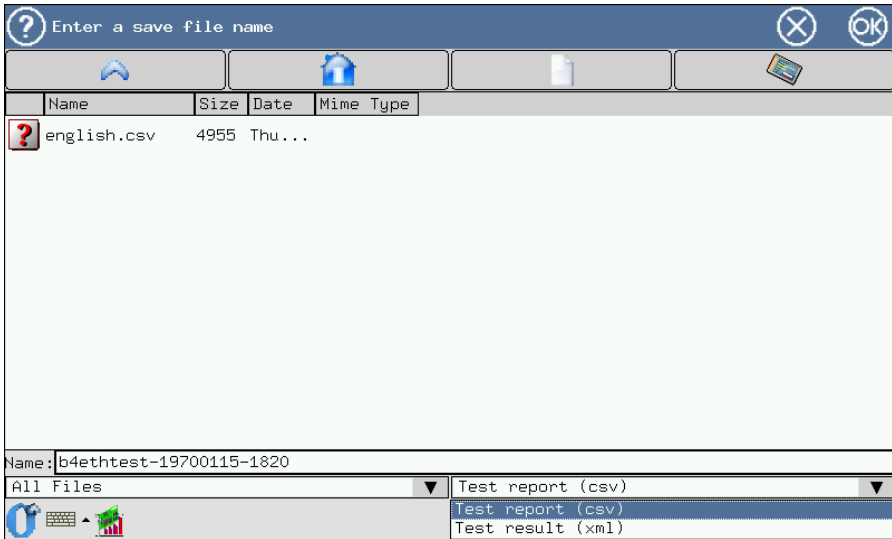


Figure 5.12. Results Saving Window

This window also has saved file format selection field, **OK** button to save and to cancel an action.

5.5.2 Previously Saved Results Display

Previously saved measurements loading function is available in case there are no active tests of **Ethernet: test RFC2544** application. The **Load** button (or F8 functional key) is used to open measurement results loading window, shown at Figure 5.13.

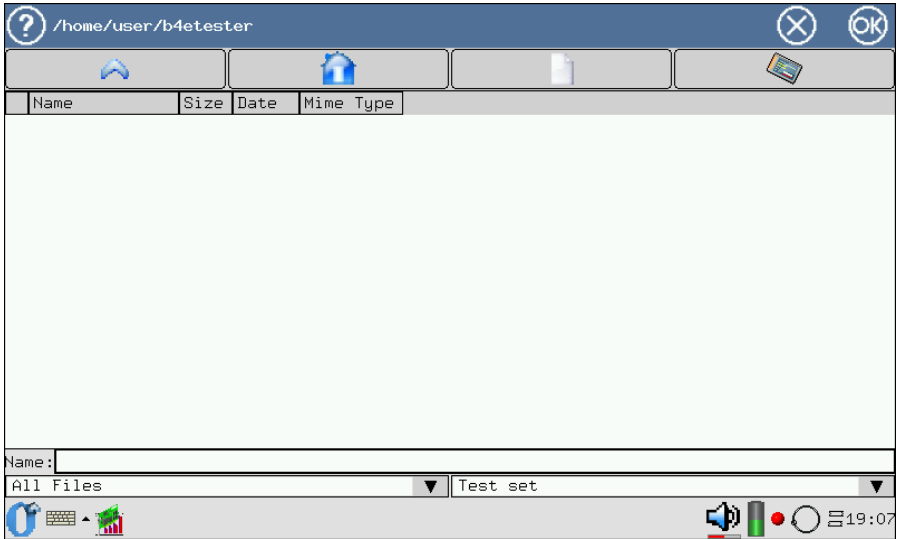


Figure 5.13. Measurements Loading Window

*Note: the **Ethernet: test RFC2544** application allows to review only the results that have been saved in XML format.*

The **Name** field of dialogue window allows to select a name of results file of interest. The window has **OK** button to load and to cancel an action.

6. TCP/IP: Basic Testing

Instruments and functions used for IP testing are main diagnostic tools in the TCP/IP networks [1] and enable detection of problems related to network configuration, network node reachability checking, data transmission route determination, data transmission channel availability checking.

To activate this application, the **IP tools** program is used (refer to Figure 6.1):

O-Menu \Rightarrow **Ethernet Testing** \Rightarrow **IP tools**.

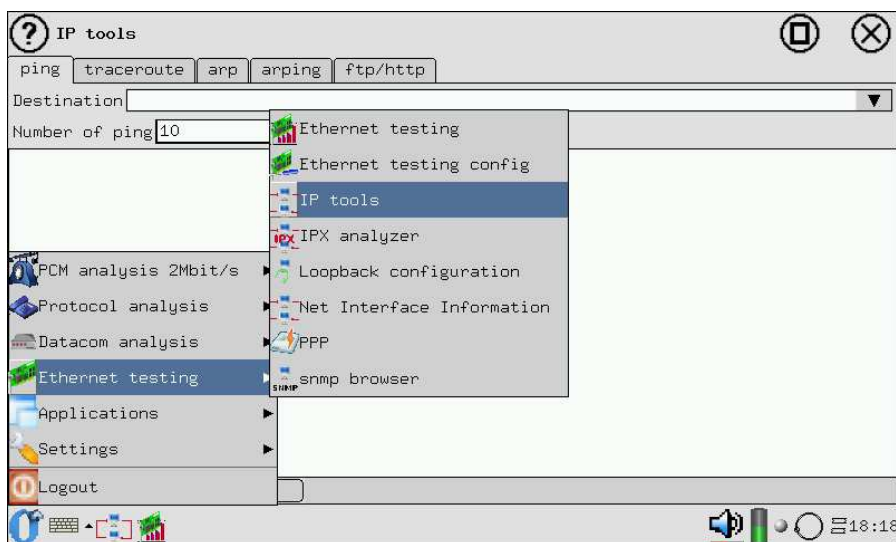


Figure 6.1. Navigation to the *IP tools* application

Note: all entered IP addresses and/or node names are stored in the drop-down lists of corresponding tabs after tests execution.

6.1 Ping

The ping tool (echo testing) is used to check a certain address reachability within or outside the subnetwork. The program sends requests to a certain network node and detects replies received. This procedure is based on IP and ICMP datagrams transmission protocols and allows to determine transmission links and intermediate devices availability [2].

Prior to start of testing, node name or IP address should be entered in the **Destination** field, for device that should be checked/reached (refer to Figure 6.2).

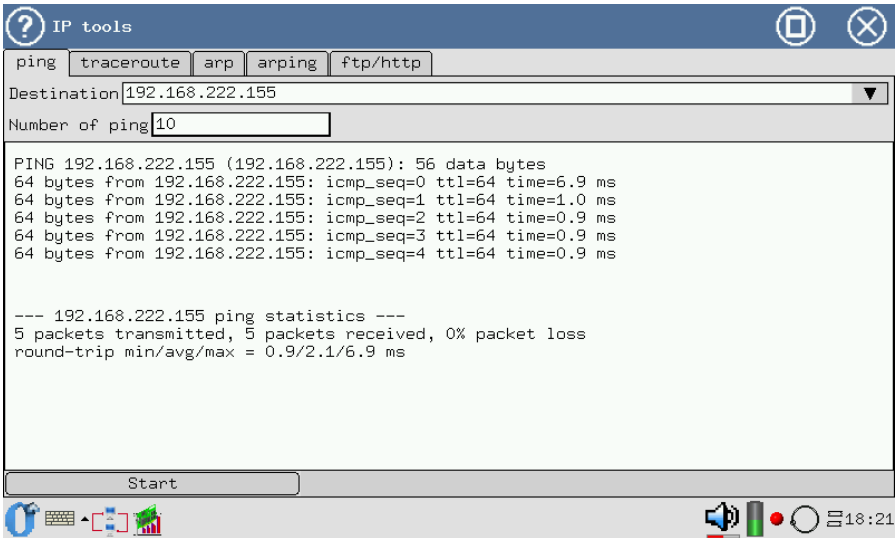


Figure 6.2. *Ping* Parameters Configuration

The **Number of ping** field is used to configure the required quantity of ICMP protocol requests. For more accuracy, more requests should be configured. The minimal value sufficient to check the connection is *1*. If this field is left blank, testing will be performed until **Stop** button or F6 functional key is pressed.

Test execution starts on pressing the **Start** button or F6 functional key.

Ping statistics displayed under information table provides data about amount of transmitted, received packets and percent of lost packets. The last row presents RTT measurement results (RTT stands for Round-Trip Time, a time between sending request and receiving reply, it represents two-way delays over route): Minimum/average/maximum values in milliseconds.

6.2 Traceroute

The Traceroute tool (route tracing in the network) is used to determine data transmission routes in the TCP/IP based networks. The program sends data-gram sequence to the specified network node and displays information about all intermediate routers thorough which data were relayed on the way to the end node [2]. In case of problems with data delivery to any node, the program allows to locate the hop where problems have arisen.

Test configuration is performed by filling out corresponding fields (refer to Figure 6.3).

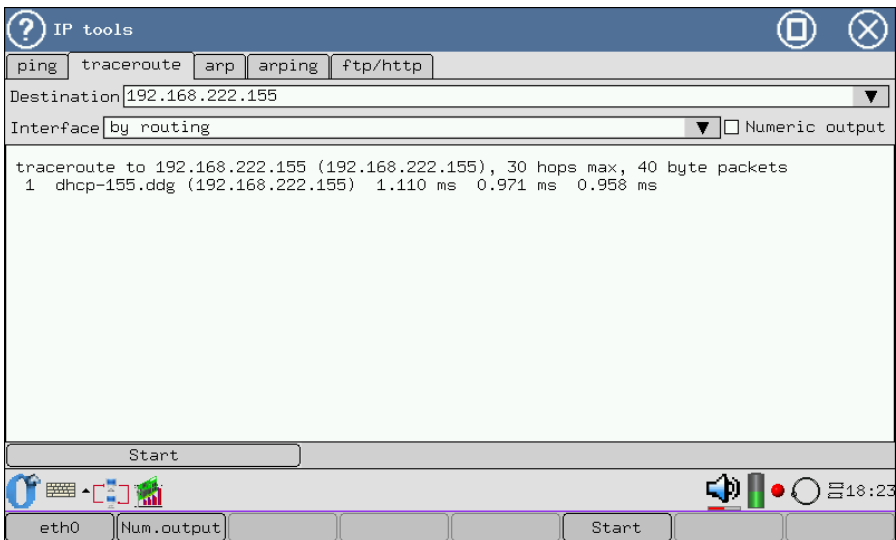


Figure 6.3. *Traceroute* Parameters Configuration

- **Destination** — target node IP address or name;
- **Interface** — name of the interface that will be used for data transmission/reception. Default interface is defined by routing configuration. To change an interface name, the line should be selected from the drop-down list, or F1 functional key should be used.

Test execution starts on pressing the **Start** button or F6 functional key.

The **Numeric output** flag is used to retrieve the information table with IP addresses of the nodes only (without nodes symbolic names), F2 functional key has the same meaning.

Data are displayed in information table in a form where each row contains node name and IP address (or just IP address), time between sending a packet

and receiving the reply.

6.3 ARP

Address Resolution Protocol allows to a network node for physical (MAC) address determination of recipient, that is connected to the same physical network; ARP uses just the IP address of recipient [3].

In order to determine Mac address, IP protocol performs ARP table lookup. This table stores all network level addresses known to the router, and MAC addressed (refer to Figure 6.4). This table generates device lists based on subnetworks routers and is updated periodically.

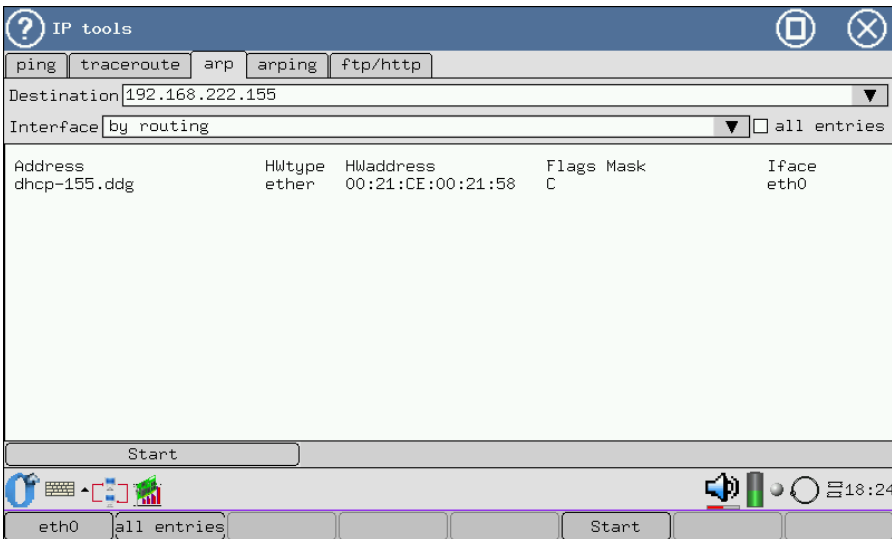


Figure 6.4. ARP Parameters Configuration

The ARP table is loaded on pressing the **Start** button or F6 functional key.

The **all entries** flag (F2 functional key has the same designation) is used to display network routers and their addresses. The **Destination** field value is ignored. To find certain IP address and corresponding information in the table, the **all entries** function should be deactivated and **Destination** field should be populated with name or IP address of a node in question.

6.4 Arping

ARP table displays information only for devices that were already addressed. In case it is necessary to connect to a network device not present in ARP table, the **Arping** program should be used (refer to Figure 6.5).

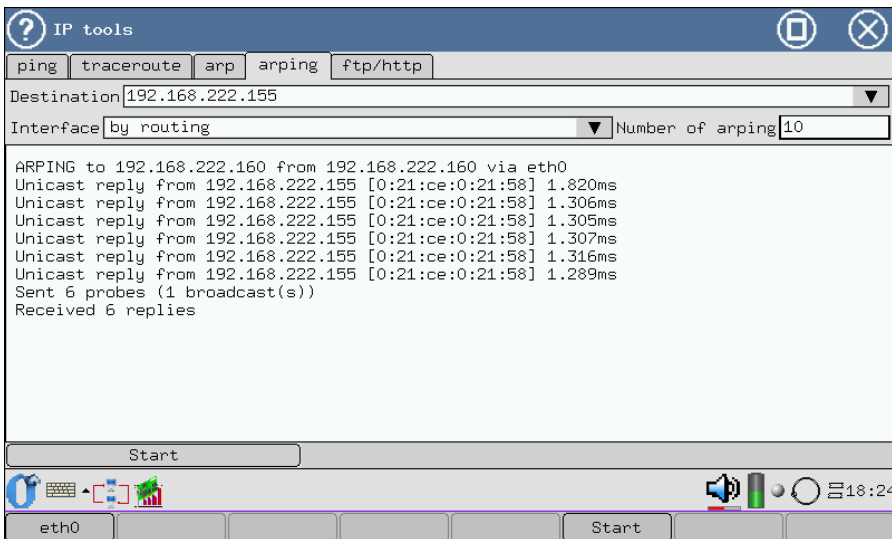


Figure 6.5. *Arping* Parameters Configuration

Arping — is a program to perform echo-request using recipient's IP address to determine its MAC address without ARP table [4]. This program uses ARP.

After the program execution is completed, on ARP table update (in the **ARP** tab), the information about the device in question will be displayed.

Test configuration is performed by filling out following fields:

- **Destination** — target node IP address for ARP request.
- **Number of arping** — is used to configure a certain quantity of ARP requests.
- **Interface** — displays interface name to work with. Default interface is defined by routing configuration. Changing of interface name is performed by selecting a row in the drop-down list or with the help of F1 functional key.

Test execution starts on pressing the **Start** button or F6 functional key.

Test results are put into information table with sender and recipient IP addresses, MAC address of a computer that answered to the broadcast request (is sent to all computers in the network), and response time.

6.5 Ftp/http

This function is used to check connection with a network resource by entering electronic address, valid for a given network. The **URL** field should be populated with URL of the needed resource¹. Test result is displayed in two information blocks: first has node name, its IP address and port (last two digits separated by colon from IP address). Below the first block, the second one is located, that contains downloaded page format and downloaded amount in percent, as shown at Figure 6.6.

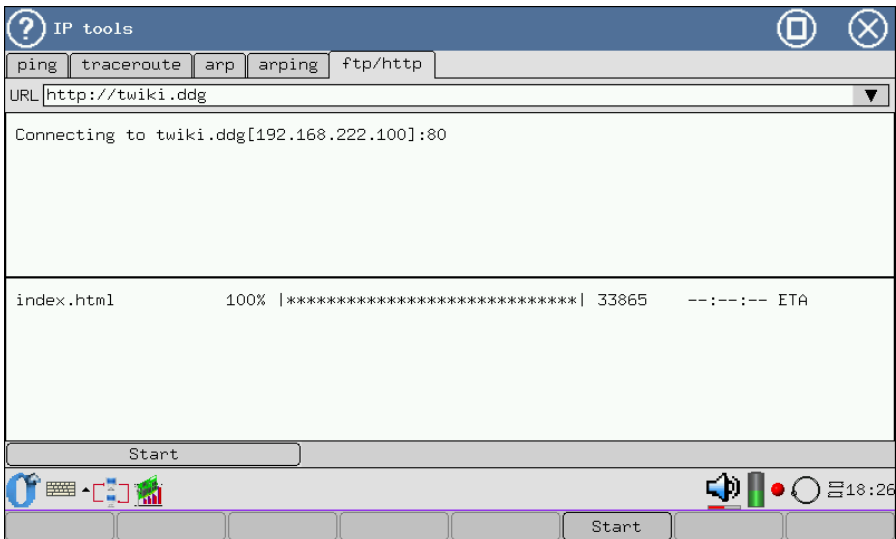


Figure 6.6. Results of connection using *ftp/http*

¹ Example of input electronic addresses: <http://linux.org> — for hypertext protocol [5]; <ftp://ftp.ru.debian.org> — for data transmission protocol [6].

7. IPX Protocol

The task of **IPX** (Internetwork Packet Exchange) protocol is to work in local area networks to transmit datagrams without establishing connection between data sender and recipient.

To activate this application, the **IPX Analysis** program should be used:
O-Menu ⇒ **Ethernet Testing** ⇒ **IPX Analysis**.

7.1 IPX Protocol Analysis

The "IPX Analysis" program collects IPX packets on the selected interface and displays the contents of their headers (first 64 bytes) at the device screen. Screen layout is shown at Figure 7.1.

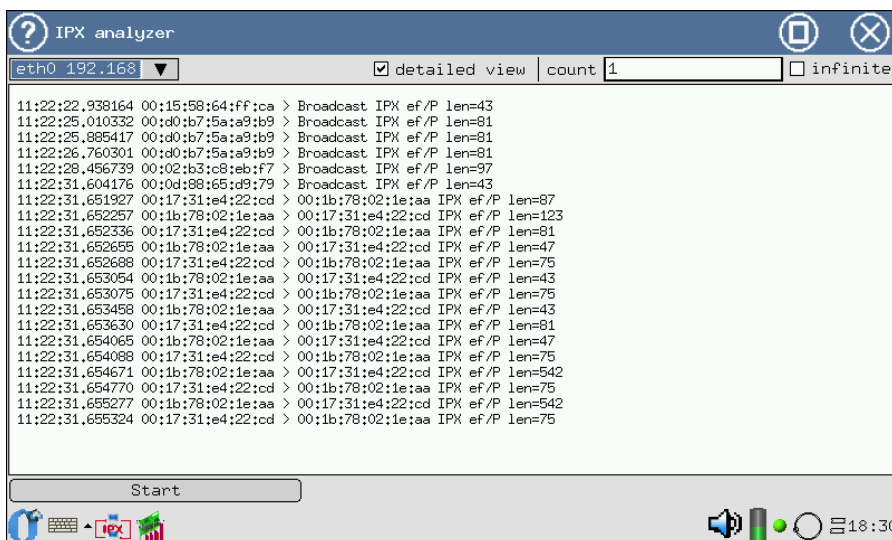


Figure 7.1. IPX Protocol Analysis Program

Program configuration window has the following elements:

- **Start/Stop** — testing process start and stop;

- field to select an interface where collection of IPX packets will be performed (refer to Figure 7.2, page 50);



Figure 7.2. Interface selection for IPX packets analysis

- **detailed view** — is a flag to switch detailed view of IPX packets on or off. When **detailed view** function is enabled, the screen shows first 64 bytes of IPX packet header and data;

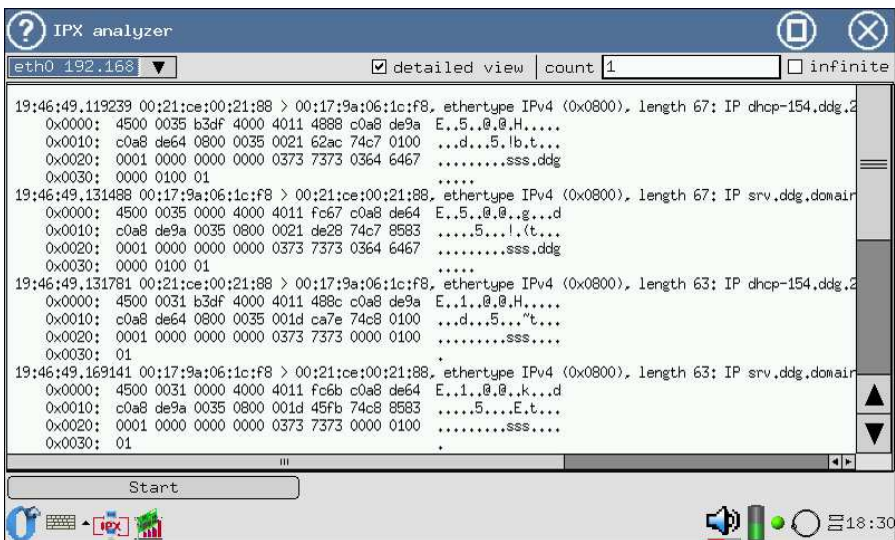


Figure 7.3. Detailed view of collected Packets

- **count** — is a field to configure IPX packets quantity;
- **infinite** — is a flag to turn infinite collection of packets on or off (is interrupted by pressing the **Start/Stop** button).

In order to work with the program, it is necessary to:

- select an interface where IPX packets are to be collected;
- select detailed view mode, if necessary;
- configure the quantity of packets, or switch on an infinite collection of packets;

- press the **Start** button and wait until packet collecting is finished, or stop the process by pressing the **Stop** button, when enough packets are collected.

*Note: on pressing the **Start** button any configuration changes are impossible; after packets collection is finished, fields become available for configuring again.*

IPX packets analysis results are put into information table with time of packet reception, packet sender MAC address, packet recipient MAC address, protocol type, etc.

8. SNMP Protocol

The **SNMP** (Simple Network Management Protocol) is designed to test network devices (routers, bridges, gateways, etc.) operability and to introduce necessary changes. To make this protocol operational, an agent and management system that collects information about agents status, are needed.

8.1 SNMP Data Display

The **SNMP** program (**O-Menu** ⇒ **Ethernet Testing** ⇒ **SNMP browser**) collects SNMP statistics from the specified agent.

Application window layout is presented at Figure 8.1.

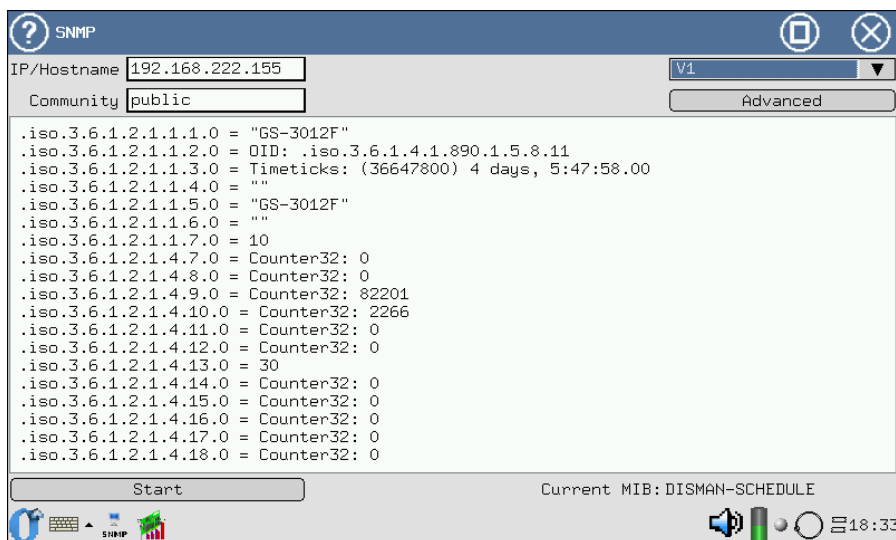


Figure 8.1. SNMP Program

Program configuration window has the following elements:

- **IP/Hostname** — IP address or name of a device where agent is running;
- **Community** — access group name (required for SNMP protocol versions v1, v2, v2c); allows for management system and agent interaction;
- **Select Protocol** — SNMP protocol version selection (available options are: v1, v2c, v3);
- **Advanced** — advanced settings dialogue;
- **Current MIB** — current MIB file¹, that is selected in the advanced settings dialogue;
- **Start** — data collection start.

8.1.1 Advanced Settings Dialogue

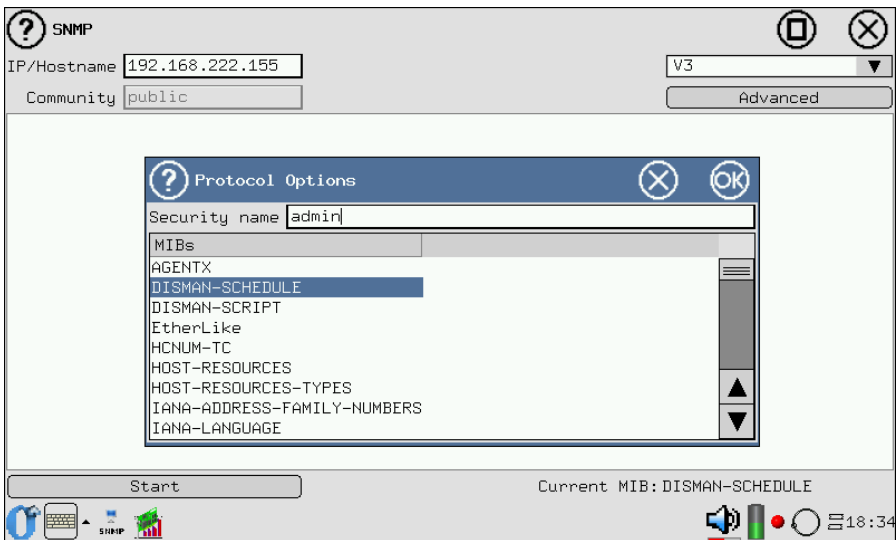



Figure 8.2. SNMP Program: Advanced Settings

Pressing the **Advanced** button allows to configure:

- **Security name** — user name for SNMP protocol versions v2c, v3 ;
- MIB file.

¹Management Information Base.

In order to work with the program, it is necessary to:

- enter IP address or name of a device where agent is running;
- in the **Select Protocol** field, choose the SNMP protocol version;
- in the **Community** field, enter community name, which data need to be reviewed;
- to select **MIB** file, navigate to advanced settings menu (**Advanced** button):
 - in case SNMP protocol versions **v2c/v3** is selected, the **Security name** field should be populated with user name;
 - select needed **MIB** file;
 - to terminate working with application and configuration saving, press the **OK** button or  (selected file will be shown in *Current MIB* field of the main application window).
- to execute testing, press the **Start** button.

When data collection has been started, application screen displays *Wait please* message. When data collection is completed, the **Start** button is active and data field is populated with statistics, collected from SNMP agent, containing information according to the MIB file selected (refer to Figure 8.1, page 53).

9. PPPoE Protocol

The PPPoE (Point-to-point protocol over Ethernet) has been designed to transfer PPP packets over Ethernet. Protocol functionality implies client and server, used for authentication, virtual channel creation and subsequent data exchange.

9.1 PPPoE Connection Display

The **PPPoE** program (**O-Menu** ⇒ **Ethernet Testing** ⇒ **PPP**) performs PPPoE connection testing for specified server. The **Bercut-MMT** device acts as a client.

Window layout is presented at the figure.

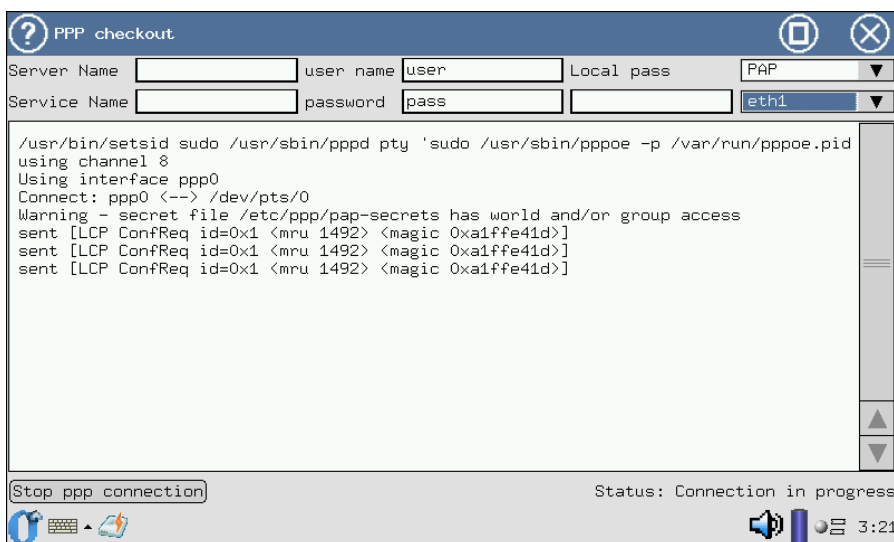


Figure 9.1. PPP Program

The application enables following parameters configuration:

- **Server name** — name of a server to setup a connection to;
- **Service name** — name of a PPPoE service at the server;
- **user name** — name of a user¹ when the **Bercut-MMT** device is authenticated against server;
- **password** — a password defined for a user;
- **Local pass** — local system password, in case of *bidirectional* CHAP authentication (**CHAP bidir**);
- **Auth Type** — authentication type (possible variants: **PAP**, **CHAP**, **CHAP bidir**);
- **Interface** — interface selection for connection;
- **Start/Stop** — testing process start and stop
- **Status** — connection current state; possible values: **Disconnected** (connection is not present), **Connection in progress** (connection is currently being setup), **Connected** (connection established).

In order to work with the program, it is necessary to:

- select authentication type: **PAP** , **CHAP** or **CHAP bidir** (**Auth Type** drop-down list);
- enter server name in the **Server Name** field;
- enter PPPoE service name at the server in the **Service Name** field;
- enter user name in the **user name** field;
- enter password in the **password** field;
- enter local system password in the **Local pass** field²;
- to execute testing, press the **Start** button.

When PPPoE connection is being setup (the **Status** field shows **Connection in progress**), information about the PPPoE connection will be output until user presses the **Stop** button (refer to Figure 9.1, page 57). In case connection is successful (the **Status** field shows **Connected**), PPP connection status information will be periodically displayed. Otherwise, the device screen will show possible reason of failed connection.

¹When **CHAP bidir** bidirectional authentication is used, the **Bercut-MMT** device name is used as user name (**O-Menu** ⇒ **Settings** ⇒ **Bercut-MMT Information**).

²This field is populated only at PPPoE connection testing for *bidirectional* **CHAP** authentication (**CHAP bidir**).

10. Network Interfaces Information

The **Network Interfaces Information** application enables data retrieval about port parameters, SFP modules parameters and copper cable characteristics. It is possible to retrieve for each Ethernet interface information about connection rate, data transfer modes, autonegotiation mode state.

This application is launched with corresponding icon at the desktop, or via main menu in the following order:

O-Menu ⇒ Ethernet Testing ⇒ Net Interfaces Information.

SFP module information includes following parameters: manufacturer name, model, operation modes supported.

Copper cable diagnostics supports standard faults detection (cable cut, short circuit), polarity, twisted pairs crossing detection, and also cable length measuring.

To retrieve network interfaces data, it is necessary to connect SFP module and to select interface from the drop-down list in upper left corner of a application (Figure10.1):

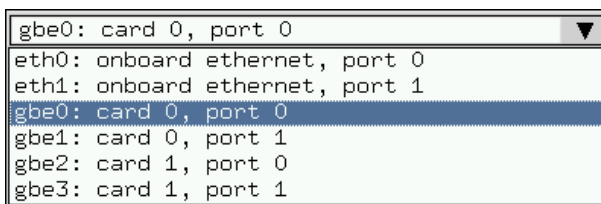


Figure 10.1. List of Interfaces

10.1 Interface Status

An application screen displays a table with information about interface state (Figure10.2):

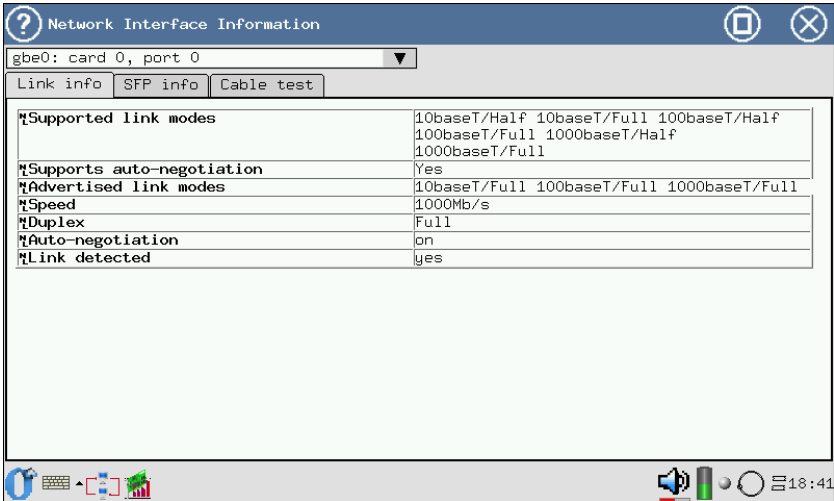


Figure 10.2. Interface Status

- **Supported link modes** — modes of operation, supported by this connection; possible transmission modes (half-duplex and duplex), data transmission rate (10Base-T, 100Base-T, 1000Base-T).
- **Supports auto-negotiation** — if auto-negotiation or network parameters automatic determination is supported.
- **Advertised link modes** — modes of operation, supported by connection when auto-negotiation is active.
- **Speed** — connection rate.
- **Duplex** — data transmission mode.
- **Auto-negotiation** — state of auto-negotiation mode.
- **Link detected** — presence of connection for selected interface.

Note: the table refreshes periodically, and in case SFP module is not present, applicable message is displayed.

For interfaces used to connect to local area network (eth0, eth1), connection rate will be 10/100 Mbit/s. Ports of the pluggable cards with installed SFP modules, purchased together with the device, support 10/100/1000 Mbit/s rates for copper cables and 1000 Mbit/s for optical cables.

10.2 SFP Information

SFP (Small Form-factor Pluggable) is a compact transceiver that interconnects Ethernet ports with the network by optical or copper cables.[8]

Screen layout is shown at Figure 10.3.

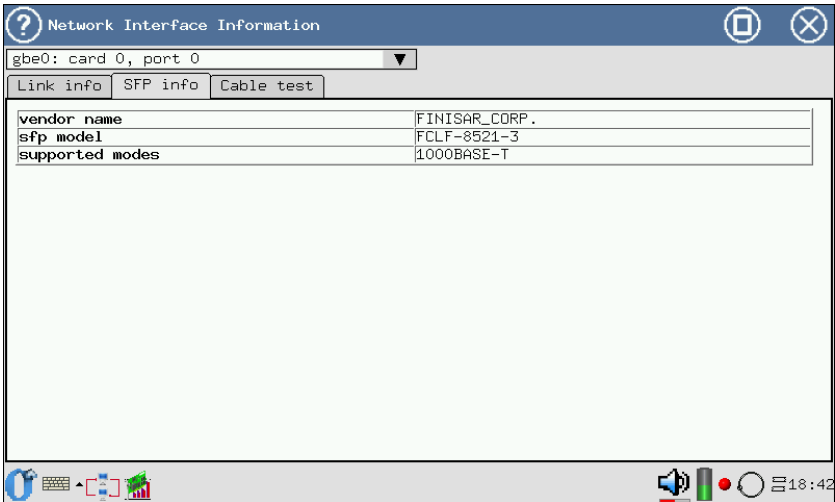


Figure 10.3. SFP Module Information

The following SFP information is displayed in the tab:

- **vendor name** — name of manufacturer;
- **sfp model** — name of SFP module;
- **supported modes** — modes of SFP module operation supported.

10.3 Cable test

Copper cable diagnostics is performed to obtain main parameters of interface under testing. Testing starts on pressing the **Run cable test** button.

Test results are displayed in the form of a table. Table columns contain information about each pair of cable wires.

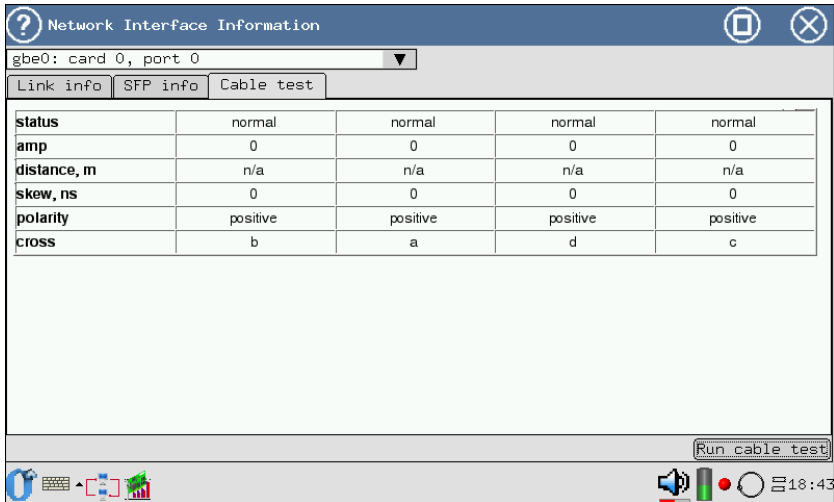


Figure 10.4. Copper Cable Diagnostics

The following data are present in the table:

- **status** — possible cable states:
 - normal — pair is OK;
 - short — short circuit;
 - open — beak (absence), i.e. cable is connected at one side only;
 - fiber — optical cable;
 - no-device — SFP module not present;
 - fail — cable test was not run;
- **amp** — amplitude of signal reflected from a defect; value range is from -1000 to 1000 mV;
- **distance** — cable length in meters; value range is from 0 to 255 (field is valid for *short* and *open* states only; in other modes it is *n/a*);
- **skew** — difference in transmission time over the longest and the shortest cable pair (phase distortion value), range of values is from 0 to 15 ns;
- **polarity** — twisted pairs polarity, can be negative/positive;
- **cross** — twisted pairs crossed connection (MDI/MDI-X); this field is valid for 1000BASE-T mode only and can have the following states:
 - a-b-c-d — connection is performed with straight cable;
 - a-b-c-d — connection is performed with crossed cable (cross-over).

Note: in case this field is not valid, *n/a* or — is displayed.

11. Loopback

In order to perform measurements and certification according to RFC 2544, **Bercut-MMT** supports loopback at different levels.

This mode can be used to check functioning of software components that are involved in TCP/IP family protocols implementation. Testing can be implemented at different OSI model layers.

11.1 Loopback Modes in Ethernet Networks

11.1.1 First Layer Loopback

At the physical layer (PHY), all incoming traffic including packets with errors¹, are redirected back without any changes (Figure 11.1).

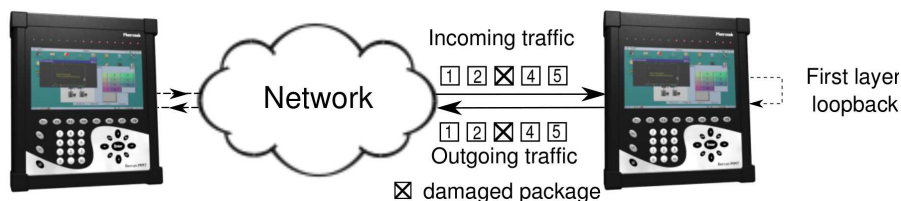


Figure 11.1. First Layer Loopback Connection

11.1.2 Second Layer Loopback

Incoming traffic is redirected back at the link layer (defective packets are not transmitted), with this sender and recipient MAC addresses are switched, VLAN tags can be replaced, other (user defined) MAC addresses may be inserted.

Figure 11.2, page 64 schematically shows device connection to the physical network using one port.

¹Packets with defective header, wrong CRC, oversized data field and other errors.

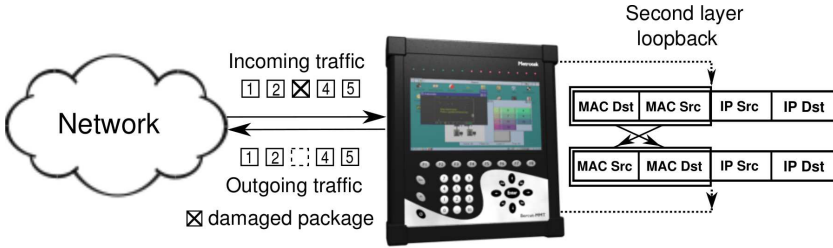


Figure 11.2. Second Layer Loopback Connection

Legend:

- MAC Dst — recipient's MAC address;
- MAC Src — sender's MAC address;
- IP Dst — recipient's IP address;
- IP Src — sender's IP address.

11.1.3 Third Layer Loopback

Incoming traffic is redirected back at the network layer (defective packets are not transmitted), with this, in addition to switching of MAC addresses, sender and recipient IP addresses are switched; another (user defined) MAC and IP addresses can be inserted, also ToS and VLAN tags can be changed.

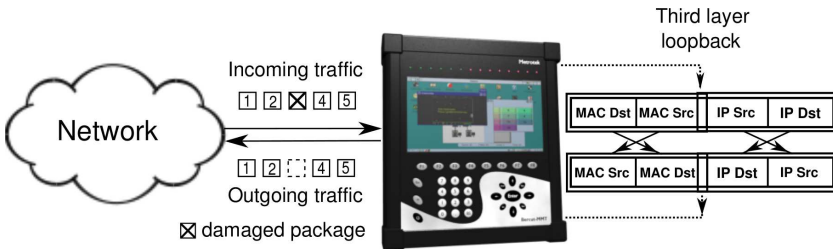


Figure 11.3. Third Layer Loopback Connection For One Port

11.2 Loopback Configuration

To activate this application, the **Loopback Configuration** program can be used (refer to Figure 11.4, page 65), through an access to

O-Menu ⇒ **Ethernet Testing** ⇒ **Loopback Configuration**.

Application main window layout is shown at the following Figure:

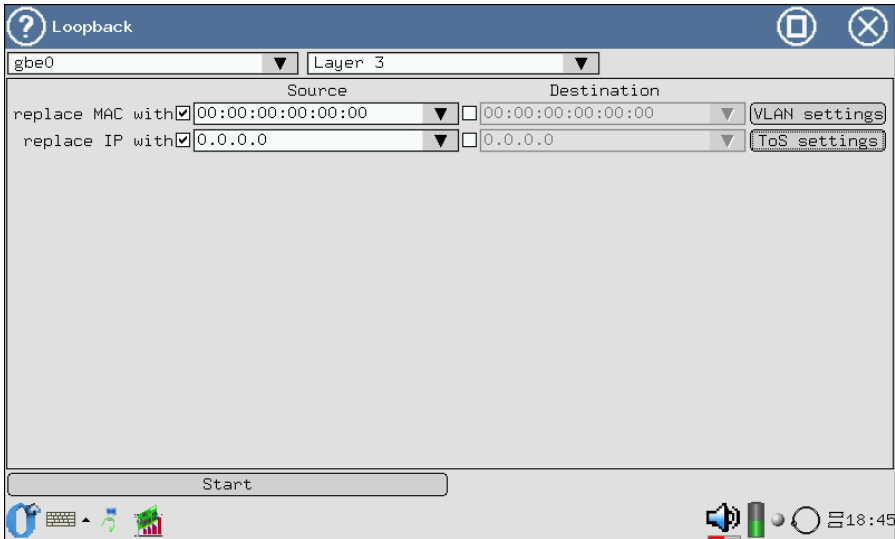


Figure 11.4. Loopback Configuration

Loopback configuration window has the following elements:

- Interface selection field to implement loopback:

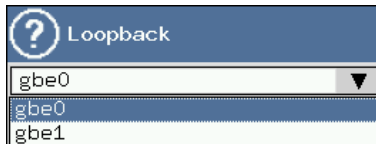


Figure 11.5. Interface selection for testing

Note: network interface with the loopback at any layer is unavailable for data packets transmission/reception. This means that conducting RFC 2544 testing, IP testing, cable testing is not possible.

- Loopback layer selection field:

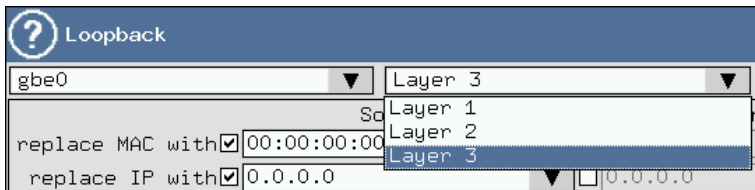


Figure 11.6. Loopback layer selection

- **Replace Source MAC** and/or **Replace Destination MAC** flags (or F3 and F4 functional keys) in corresponding fields are used to change MAC address in the redirected traffic packets. MAC addresses may be configured using virtual keyboard. Virtual keyboard (Figure 11.7) is displayed on pressing with a stylus to the MAC address field, and has symbols (characters and digits) necessary to enter the MAC address.

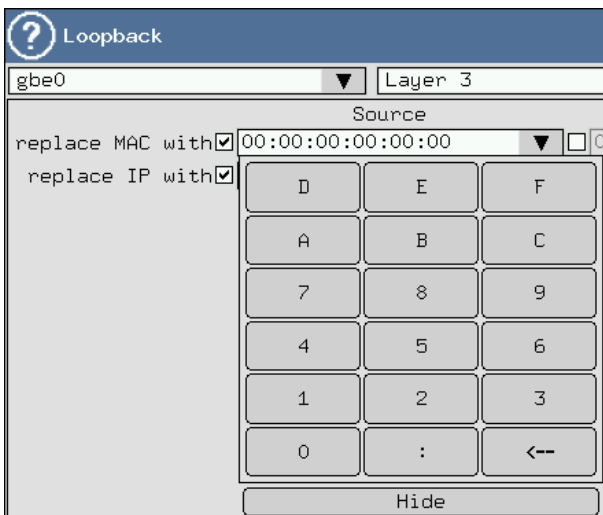


Figure 11.7. Virtual Keyboard to Enter MAC Address

***Note:** in case the selected loopback layer is Layer 2, the **replace IP with** field and **TOS Settings** menu are deactivated.*

- The **VLAN Settings** menu has **Tag** flags (a mark within Ethernet packet structure). When a flag is set, VLAN ID and VLAN priority in incoming packets are replaced by user defined values. If incoming

packets do not have VLAN tags, they are sent unchanged (even there are user defined tags).

- **VLAN ID** — a 12-bit VLAN identification, is a number from 0 to 4095, uniquely identifies the network a frame belongs to. VLAN ID zero value shows this given frame carries no information about VLAN and has only priority information.

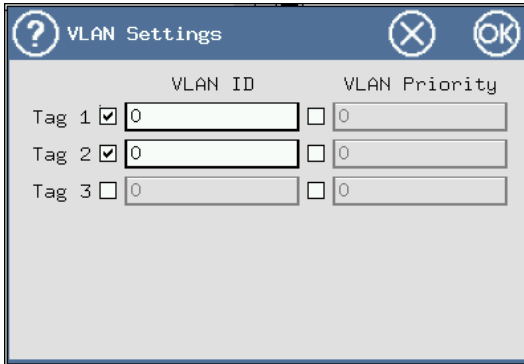


Figure 11.8. VLAN Settings Menu

- **VLAN Priority** set a priority, which a frame will be tagged with (is considered on processing in the network device). Priority and traffic type mapping according to IEEE 802.1Q is presented in Table B.1 of Annex B, page 73.

If *Layer 3* is selected as loopback layer, both source and destination MAC addresses and IP addresses will be switched.

To change MAC and IP addresses, it is necessary to set corresponding flags (F3, F4, F5, F6 functional keys) and use virtual keyboard (refer to Figure 11.9, page 68), that is displayed on pressing with a stylus at address input field.

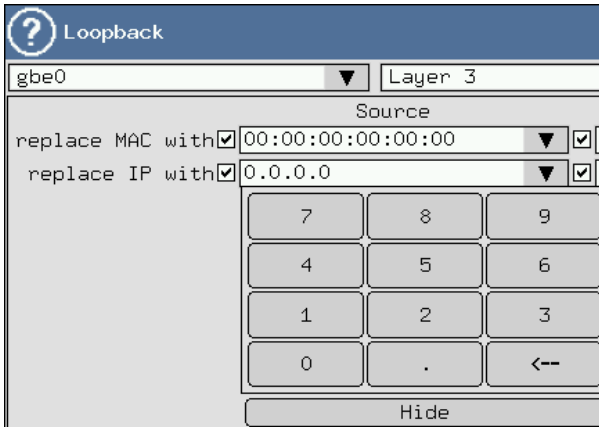


Figure 11.9. Virtual keyboard to enter IP address

- The **ToS Settings** menu is used to replace following TOS (Type of Service) parameters in redirected IP packets (for detailed information about possible values refer to Table B.2 and B.3, Annex B, page 73):
 - **ToS Precedence** (refer to Figure 11.10);
 - **ToS Value**.

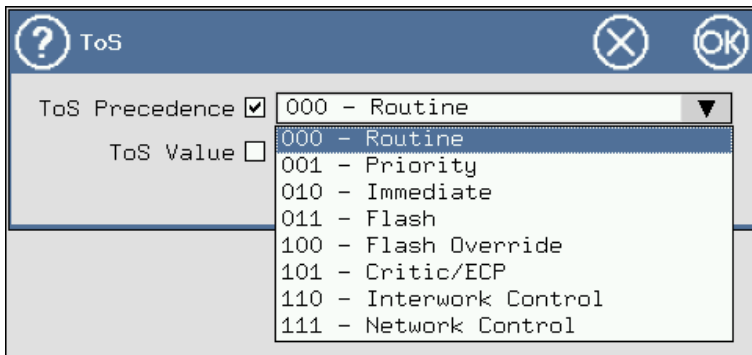


Figure 11.10. ToS Precedence Selection

Traffic loopback starts on pressing the **Start** button (or F7 functional key) and is active until the **Stop** button is pressed.

A. Remote Testing

A.1 Connection Setup

On conducting RFC 2544 remote testing, it is necessary to use two **Bercut-MMT** devices. These interfaces should be fully configured to work with the network, i.e. should be configured to transmit data over different network protocols, including ssh [7].

Connection with a remote device should be established using **Connection manager** program:

O-Menu ⇒ **Settings** ⇒ **Connection manager**.

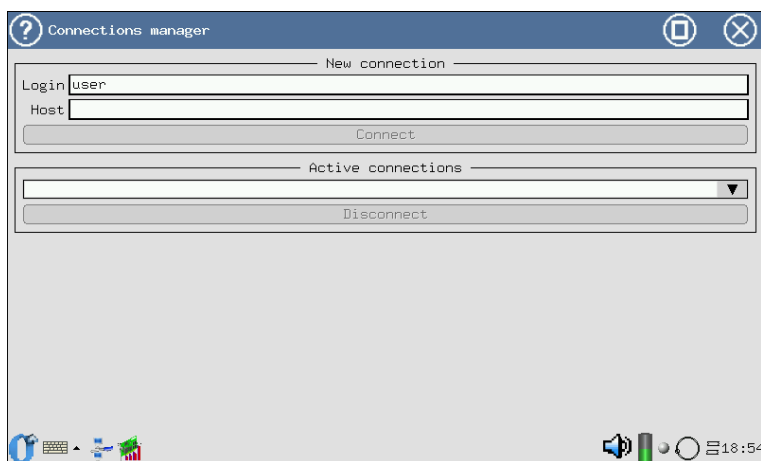


Figure A.1. Connection Setup

The **Login** field should be populated with the user name that is registered at the remote device (Figure A.1). The **Host** field should be populated with IP address (host) or remote **Bercut-MMT** name (hostname). Connection setup is performed by pressing the **Connect** button. When connection with remote **Bercut-MMT** is established for the first time (for specified user name at remote **Bercut-MMT**), a message will be displayed with public key and request to confirm proceeding with connection setup (answers are *yes*, *no*),

Figure A.2. For connection to be established, it is necessary to enter *yes* from virtual keyboard.

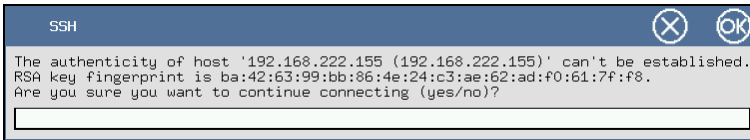


Figure A.2. First ssh connection confirmation

In case first connection setup is successful, a line similar to this one: *user@192.168.222.205*¹, (Figure A.3) will appear. Otherwise, a notification will appear. with possible reasons of connection failure. List of active connections is presented in Annex 4.1.

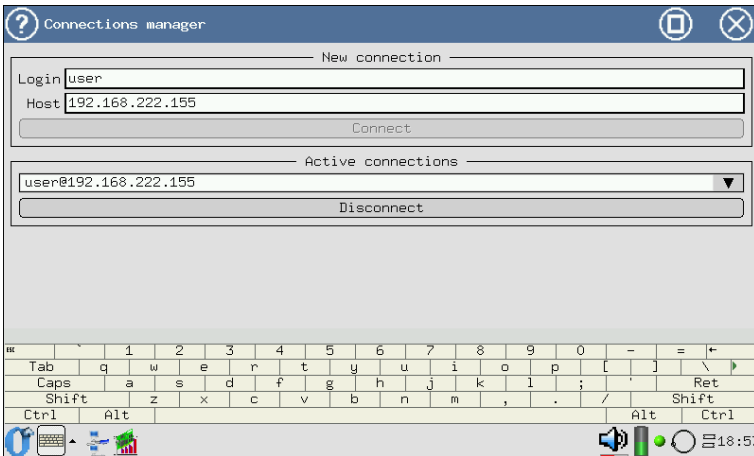


Figure A.3. Active Connections

¹Actual view of active connection will differ from this example, it depends on user connection parameters (user name and IP address).

A.2 Parameters Configuration

After connection setup, described in the previous paragraph, it is necessary to configure connection parameters as stated in section 4 *RFC 2544. Parameters Configuration*.

B. Traffic Types and Priorities

B.1 VLAN Tags

Table B.1: Traffic Types and Priorities

Value	Description
0 (Default)	Best Effort
1	Background
2	Excellent Effort
3	Critical Application
5	Voice
6	Internetwork Control
7	Network Control

Network Control and Internetwork Control are reserved for network management messages. This traffic type is considered as high priority. Priorities 4 and 5 can be used for delay sensitive traffic, such as video and voice. Traffic priorities from 3 to 1 are used for different tasks: from streaming applications to FTP traffic that is able to overcome possible losses. Class 0 (*best effort delivery rate*) is assigned to a traffic with lowest priority and is used when no other class is assigned [9].

B.2 Type of Service

According to RFC 791, eight frame priority values are supported [10].

Table B.2: Values of the Field **Precedence**

Value	Name	Description
000	Routine	Normal priority
001	Priority	Preferred priority
010	Immediate	Immediate priority

011	Flash	Expedited priority
100	Flash Override	Urgent priority
101	CRITIC/ECP	Critical priority
110	Internetwork Control	Internetwork Control
111	Network Control	Network Control

IP Packets type of service is defined by RFC 1349 [11] and can have values from the table:

Table B.3: ToS Field Values.

Value	Name	Description
1000	Minimize delay	To minimize delay. Is used when packet delivery time from source network device to destination (waiting time) is most critical and has to be minimal.
0100	Maximize throughput	Maximum throughput.. Denotes a packet should be redirected through a channel with maximum throughput.
0010	Maximize reliability	Maximum reliability. Is used when it is important to be sure that data will reach destination without retransmission.
0001	Minimize monetary cost	Minimize cost. Is used when it is necessary to minimize data transmission cost.
0000	All normal	Everything is OK. In this case packet is routed according to provider decision.

C. System Technical Specifications

Table C.1: Platform Specifications **Bercut-MMT**

Processor	Intel XScale PXA270 520MHz (312 or 416 MHz modifications available)
Memory	128 megabytes
Flash memory	32 megabytes
CF (non-volatile)	1(internal, non-removable, from 512 megabytes to 4 gigabytes)
Display	TFT 7 inches, 800x480 pixels, 65536 colours, sensor panel
Keyboard	cursor control, numeric and functional keys
Computer connection interface	RS-232, Ethernet 10/100 BaseT, USB client and USB host.
Power voltage	9-15 VDC
input current	not more than 3A
Batteries	Two Ni-Mh batteries with nominal voltage of 7.2 V and capacity of 4500 mAh each. Batteries are replaced by manufacturer
AC adapter	100-240V 50-60Hz input current not more than 1.5A
Power line protection	Internal fuse 7A

Table C.2: B4-GBE Module Specifications

Ethernet interfaces	two on-board ports 10/100/1000Base-T SFP connector IEEE 802.3 compatible
Ethernet functions	Autonegotiation Full and half duplex Flow control
Operation mode	Terminal
RFC 2544 compliance check	Automatic check with configurable constraints and maximum transmission rate Throughput, latency, frame loss, back-to-back testing Frame size: 64, 128, 256, 512, 1024, 1280 and 1518 bytes
IP utilities	Ping, traceroute, ARP, arping, ftp/http
Loopback implementation	At physical (PHY), link (MAC) and network (IP) layers with VLAN support and fields change capability
Cable testing	Copper cable testing for open circuit, short circuit, distance to open determination

D. Glossary

10Base-T:

Name of the data transmission standard at the rate of 10 Mbit/s over Ethernet network, using twisted pair cable.

100Base-T (100Base-TX):

Name of the data transmission standard at the rate of 100 Mbit/s over Ethernet network, using twisted pair cable.

1000Base-T:

Name of the data transmission standard at the rate of 1000 Mbit/s (1 Gbit/s) over Ethernet network, using twisted pair cable.

Back-to-back:

Data transmission unevenness. A test that determines quantity of frames in the longest transmission, that does not result in DUT loss of any frame.

ARP: Address Resolution Protocol . A network protocol that converts IP addresses (network level addresses) to MAC addresses (link level addresses) in TCP/IP networks. It is defined in RFC 826.

Auto-Negotiation:

the auto-negotiation function allows devices (adapters and hubs) to automatically adjust to the communication rate in the network.

DUT: Device Under Test .

Ethernet:

Local area networks implementation technology. Is defined in IEEE standard, group 802.3.

FTP: File Transfer Protocol . A protocol that supports file transmission in computer networks.

Full-duplex:

Duplex mode. A mode that supports data transmission and reception at the same time.

Half-duplex:

Semi-duplex mode. A mode that supports transmission in both directions, but with separation in time, i.e. at any moment of time transmission is performed in only one direction.

HTTP:

Hypertext Transfer Protocol . A protocol used for HTML documents transmission from Web server to Web browser.

ICMP:

Internet Control Message Protocol . A network protocol, a part of TCP/IP protocol stack. Is mainly used to transmit error notifications and in other exceptional cases that appear during data transmission.

IEEE 802.1Q:

A standard that defines changes in Ethernet frame structure, that allow for VLAN information transmission over network.

IP:

Internet Protocol. One of the main protocols of TCP/IP family, provides for non-guaranteed packet delivery without establishing a connection with recipient.

IP address:

Internet Protocol address. A unique identification (address) of a device connected to unified network based on the TCP/IP protocols family. Is represented in the form of 32 bits number.

IP datagram:

The main unit of information transmission in the unified network based on TCP/IP protocol. Each datagram has source and destination addresses and data.

IP network:

In this manual, IP network is treated as network that includes devices working at link and network levels, such as network switch, router.

LoT:

Latency over Time. Delay distribution in time.

MAC address:

Media Access Control address. A unique identification that is used to address network devices at physical level. Ethernet network uses 48-bit MAC address.

MDI:

Medium Dependent Interface . A port of an Ethernet device that enables network hubs and switches to connect to other hubs without using crossover cable.

MDI-X:

Medium Dependent Interface with Crossover . RJ-45 Ethernet interface used by network switches and hubs.

MPLS:

Multi-Protocol Label Switching . A technology that is used in high capacity switching devices to transfer IP datagrams. MPLS protocol is based on IP switching and label switching technology.

NUT: Network Under Test .**OSI:**

Open Systems Interconnection reference model . Hierarchical model

for network communication and network protocols interaction, adopted by International Standardization Organization (OSI).

RJ: Registered Jack. A standardized physical interface used to interconnect telecommunications equipment.

RJ-45:

One of the Registered Jack standard connectors, used in Ethernet networks to connect twisted pairs.

SFP: Small Form-factor Pluggable. A compact transceiver that interconnects Ethernet ports with the network by optical or copper cables.

PING:

Packet InterNet Groper . Name of a program that is used in unified networks based on TCP/IP protocol in order to assess reachability of a recipient.

RFC: Request For Comments. Name of a group of documents dedicated to TCP/IP protocols family (not limited to). RFC contains overviews, measurements data, concepts and methods descriptions, applied and adopted standards, and experimental results.

RTT: Round Trip Time. Characteristics of packet propagation delay between two network nodes. Total time needed to transmit a packet over network from sender to final recipient and to send it back to sender.

SSH: Secure SHell. An application level network protocol, that enables remote control of operations system and file transfer.

TCP: Transmission Control Protocol . A standard transport level protocol, member of the TCP/IP protocols family, that provides for reliable duplex flow data transmission.

Throughput:

A test that evaluates maximum rate at which quantity of test frames that pass through DUT is equal to the quantity of frames that were sent to it from the test equipment.

ToS: Type of Service. A set of four-bit flags in the IP packet header. Using ToS, an application that sends data, reports to the network the required type of network service.

Traceroute:

A program that supports data routes determination in TCP/IP networks, is based on the ICMP.

UDP: User Datagram Protocol . transport protocol to transmit data in IP networks. Provides for non-guaranteed message delivery without connection setup with recipient.

URL: Uniform Resource Locator . A test string that describes location of

information source. Line starts with the type of protocol used (for example, http://), followed by the source identification.

VLAN:

Virtual Local Area Network . A group of network devices that function as if they are connected to the same network segment.

VLAN ID:

VLAN Identifier (VID). A 12-bit VLAN identifier, defined in the 802.1Q standard. Uniquely identifies VLAN a frame belongs to.

VLAN Priority :

Three bits that carry information about frame priority. According to IEEE 802.3p, eight priority values are possible.

Link Layer :

Provides for network communication at physical level and error monitoring that may occur. Data link layer can communicate with one or several physical layers, monitors and controls this communication.

TCP/IP protocols family :

An official name of TCP/IP protocols group.

Network switch :

A device used for interconnection of several nodes of computer network. Sends data directly to recipient.

Network hub :

A device used for joining of several nodes of computer network. All devices connected to the hub ports receive same information.

Network Layer :

Provides for route determination for data transmission. Is responsible for logical to physical addresses and names mapping, for shortest routes determination, for switching and routing, network faults monitoring.

Transport Layer :

Ensures reliable transporting of packets between two network end points. Despite lower layer protocols check correctness of each data transmission operation, the task of this layer is to additionally check correctness of data being transmitted.

Physical network :

In this manual, physical network is treated as a network that contains devices working at data link layer, such as network switch.

Physical layer :

Its task is to directly transmit data flow. Transmits optical or electrical signals to the cable and receives them and converts into data bits according to coding methods of digital signals.

E. Technical support

Additional information on the **Bercut-MMT** device and new software can be found at the company site www.metrotek.ru. You also can send an email or call Technical Support Service (refer to **Contact Information**). Please provide problem description and device data that can be found in the device's menu item: ***Bercut-MMT Device Information*** (**O-menu** ⇒ **Configuring** ⇒ **Bercut-MMT Information**), and consist of the following information:

- device serial number (also present on the rear panel);
- version;
- pluggable modules information.

***Note:** prior to application to the technical support service it is recommended to update the firmware version of the device and to check its operability again.*

E.1 Contact Information

Metrotek
105082, Moscow,
26v/2, Bolshaya Pochtovaya street
Phone: (495) 961-0071
www.metrotek.ru

F. Troubleshooting

Table F.1: Possible faults

Fault main indication	Possible reason	Fault clearing method
Connection loss	Incorrect connection of a cable to the device	Check connected cable integrity and insert it again into the connector up to click

Bibliography

- [1] Introduction to TCP/IP
http://www.opennet.ru/docs/RUS/linux_base/node310.html
- [2] Ping and Traceroute
http://www.opennet.ru/docs/RUS/inet_book/4/45/ping_451.html
- [3] Address Resolution Protocol: ARP
http://www.opennet.ru/docs/RUS/inet_book/4/44/arp_446.html
- [4] ARP ping
<http://www.linux.com/feature/50596>
- [5] HTTP, RFC2616 materials
<http://tools.ietf.org/html/rfc2616>
- [6] FTP, RFC2228 materials
<http://tools.ietf.org/html/rfc2228>
- [7] Ssh, reference handbook
<http://www.openssh.org/>
- [8] Cooperation Agreement for Small Form-Factor Pluggable Transceivers
<http://schelto.com/SFP/>
- [9] IEEE Std 802.1Q, IEEE Standart for Local and metropolitan area networks — Virtual Bridged Local Area Networks.
- [10] RFC 791, Postel, J., "Internet Protocol", DARPA, September 1981.
- [11] RFC 1349, Almquist, P., "Type of Service in the Internet Protocol Suite", July 1992.