SG-17R User Manual

A. Kazantsev

SG-17R User Manual

A. Kazantsev

Abstract

This Manual concernes such aspects as adjustment and operation of the routers of the 17th series manufactured by LLC SIGRAND (SG-17R).

A brief description of characteristics, options, operational conditions, network interfaces settings and supported modules of the router is given.

Network interfaces and services adjustement procedures, and different operational modes of the router (multiplexing, bridging, bonding, VLAN, QoS, VoIP and others) are explained.

Table of Contents

List of Figures

List of Tables

Chapter 1. Description of the Router SG-17R

The Router SG-17R is a multifunctional device comprising an IP-router, DSL modem, E1/DSL multiplexer and VoIP gateway. The Router SG-17R has plugin architecture including E1, SHDSL, RS-232 and VoIP (FXO, FXS, VF) plugins, which permit the use of various protocols and physical links. There exist a possibility of use together with SG-17E signal regenerators, which allow to extend the operating distance on retention of the correct speed. Using the SHDSL equipment it is possible to obtain information about the communication lines for all the regenerators operating on line.

he software for the router is developed on the basis of the operational system GNU/Linux with the core ver. 2.6 and is distributed in accordance with the licence agreement GNU GPL.

Liability Restriction

The manufacturer, for obvious reasons, does not hold responsibility for the performance of the software developed by third parties which was not tested for compatibility with the basic software of the LLC SIGRAND device. We are not responsible for the outcomes of use of such software which can lead to disability or to limitatiton of device functionality.

The Router SG-17R has the following functional:

- Adjustement through web-interface.
- Configuration upload and failback.
- Saving of changeable interfaces settings with reference to slot number.
- Logging.
- Independent adjustement of Ethernet-ports forming parts of the base platforms.
- Additional Ethernet-services on the basis of VLAN technologies.
- Multiplexing of synchronous channels.
- Transfer of IP-traffic under bridging and routing modes.
- In multiplexing mode, if multi-pair connection is used, it is possible to agregate trace tails of E1 threads into one logical channel to transport the Ethernet.
- Banding of physical interfaces for data transport speeding.
- Supporting of network interfaces: SHDSL, E1, Ethernet, RS-232, FXO/FXS, VF (TFC).
- Working with SHDSL interfaces, providing rates up to 14 Mbit/s at one pair.
- Providing remote feed for regenerators SG-17E-P, modems SG-17B-P .
- Supporting network services: DHCP, DNS.
- Traffic control: NAT, Firewall, QoS.
- Built-in SHDSL track monitoring up to G.SHDSL (G.991.2) standard.

- Supporting SNMP: MIB-II, HDSL2-SHDSL-LINE-MIB.

Chapter 2. Distribution Kit

SG-17R

- Mounting of the router.
- Using DC 36-72V type of power supply— mating connector of power socket.
- Using 220V/50Hz type of power supply— power cord.
- Terminal cord DB-9M — DB-9F — a cord for terminal connection.
- CD with software and documentation.
- Warranty certificate.

Chapter 3. Technical Description

Characteristics and Parameters of the Device

Common Parameters

- *Processor* : 32-bit MIPS processor with 4KC core, performance 227 MIPS.
- *Core memory* : 64 MB SDRAM.
- *Disk memory* : 32 MB flash.
- *Interfaces* :
  - 4 Ethernet/Fast Ethernet, auto negotiations, auto MDI/MDI-X.
  - *RS-232C* — for router management.
  - 4 slots for optional modules.
- *Dimensions*, mm : 438x258x43.
- Power supply: 220 V/50 Hz or 36-72 V constant current (depending on the model and the delivery).
- *Base platform weight, kg* : 3,9 for 220V/50 Hz type and 3,3 for 36-72 V constant current type.

Parameters of RS-232C Interface (console port)

- *Connector type* : DB-9F.
- *Data transfer rate, bit/sec* : 115 200.
- *Protocol* : 8-N-1.
- *Traffic control* : no.

Parameters of SHDSL Line Interface (extension modules)

- *Connector type* : RJ-45 (socket).
- *Interface type* : G.SHDSL (recommended ITU-T G.991.2.bis).
- *Connection type* : point-to point.
- *Number of communication line cables* : 2 (one pair). Contacts in use 4 and 5.
- *Data transfer rate, Kbit/sec* : 192 to14080.
- Linear code : TCPAM.
- Connection type : full duplex.

- Distant feed (for models with distant feed option)
  - *Voltage, V* : 240.
  - *Maximum current, mA* : 70.
- *Number of interfaces depending on module modification* : 1, 2.

Parameters of E1 Interface (extension modules)

- *Connector type* : RJ-45 (socket).
- *Number of communication line cables* : 4 (two pairs). Contacts 4, 5 are used for transmission, 1, 2 — for reception.
- *Linear code (ITU-T G.703)* : HDB3, AMI.
- *Data transfer rate* : Nx64 Kbit/sec, where N=1:32, for each of E1 Interfaces (64:2048 Kbit/sec in incriments of 64 Kbit/sec).
- *Distance to Equipment (DTE), km* : 2,4 (for cable of 0,5 mm), 1,6 (for cable of 0,4 mm).
- *Cyclic structure (framing)* : G.704.
- *Supercycles (superframe)* : CRC4, CAS.
- *Cyclic structure shutdown option (unframed mode)* : yes.
- *Number of interfaces depending on module modification* : 1, 2, 4, 8.

Parameters of RS-232 Interface (extension modules)

- *Connector type* : DB-9F (DCE), DB-9M (DTE).
- Interface type: RS-232 (V.28).
- *Data transfer rate, bit/sec* : 300 to 230400.
- *Data capacity* : 7 or 8 bit.
- *Number of stop bits* : 1 or 2.
- *Evenness* : ODD, EVEN, NONE.
- *Commands* : DTR/DSR, RTS/CTS, CD, RI.
- Number of interfaces depending on module modification : 2, 4.

Parameters of Carrying Module for VoIP Interfaces (extension module)

- *Setup interface for submodules* : 2 slots: 40+10 contacts (system part and linear part).
- *Maximum of submodules* to install: 4.

- Supported submodules: FXO, FXS, FV in any combination.
- *Number of interfaces VoIP depending on the occupancy of the module with the submodules* : 2, 4, 6, 8.

Parameters of FXO Interfaces (extension submodule)

- *Connector type* : RJ-11.
- *Battery voltage, V* : 30-72.
- *Ring voltage range, V*: 30-120.
- *Ringing signal frequency, Hz* : 15-65.
- *Two wire termination total resistance, Ohm* : 600.
- *Codecs in use*
  - *High quality* : G711 (A-law).
  - *High speed* : G729.
  - Full VoIP codec stack support option.
- *Number of interfaces on one submodule* : 2.

Parameters of FXS Interfaces (extension submodule)

- *Connector type* : RJ-11.
- *Battery voltage, V* : 48.
- *Ring voltage range, V* : 65.
- *Maximum load, REN* : 3.
- *Two wire termination total resistance, Ohm* : 600.
- *Codecs in use*
- • *High quality* : G711 (A-law).
  - *High speed* : G729.
  - Full VoIP codec stack support option
- *Number of interfaces on one submodule* : 2.

Parameters of VF - signaling channels (extension submodule)

- *Connector type* : RJ-11.
- *Parameters of four wire termination*
  - Contacts: 3-4 - reception (output), 2-5 - transmission (input).

- *Input and output impedance, Ohm* : 600.
- *Channel input relative level, dBr* : minus 13.
- *Channel output relative level,* dBr : plus 4.
- *Channel input relative level in transit mode, dBr* : plus4.
- *Channel output relative level in transit mode,* dBr: plus 4.

- *Parameters of two wire termination*
  - Contacts: 3,4 - reception/transmission.
  - *Input and output impedance, Ohm* : 600.
  - *Channel input relative level, dBr* : 0.
  - *Channel output relative level, dBr* : minus 7.
  - *Channel input relative level in transit mode, dBr* : minus 3,5.
  - *Channel output relative level in transit mode, dBr* : minus 3,5.
- *Number of interfaces on one submodule* : 2..

Operation conditions

Router is meant for operation in a closed heated space under the following environmental conditions:

- *Air temperature, °C* : 10 .. 40.
- *Relative air humidity, %* : up to 85.
- *Air pressure, Kpa* : 84 .. 107.

SHDSL Characteristics

Operating Distance and Rate

Test Conditions

The information about operating distance and rate is given below. The results are obtained on lines of such length, where Bit Error Rate (BER) is equal to or less than 10^{-7} . The specified distance is estimated experimentally on the control communication line of the company`s laboratory.

The results obtained while operating a concrete communication line may differ from the indicated values due to differences in characteristics of this line and the reference line.

Different series of routers and different modules show different values of distance/rate.

Modules MR-17H

Table of distance/ratefor SHDSL modules MR-17H.

Table 3.1. Table of distance/rate for SHDSL modules MR-17H

Rate, Kbit/s	0.5 mm cable, km	0.9 mm cable, km (*)	1.2 mm cable, km (*)
15296 (**)	0,6		
14080	1,2	3,6	5,8
12800	1,2	3,8	6,4
11520	1,4	4,2	6,4
10240	2,0	4,6	7,2
9216	2,2	4,8	7,4
8192	2,4	5,0	8,0
7168	3,0	5,4	8,4
6144	3,4	6,0	9,0
5696	3,6	6,8	10,6
5120	3,8	7,2	12,0
4608	4,0	7,4	13,0
4096	4,4	8,0	14,0
3072	5,0	9,0	15,8
2304	5,4	10,6	17,0
2048	6,2	12,6	19,4
1536	7,0	14,8	22,2
1024	7,8	17,0	26,0
768	8,4	18,4	28,0
512	9,0	19,8	30,0
384	9,6	21,2	32,0
192	10,4	23,0	35,0

Note

(*) - not all data obtained expermentally

(**) - rate of 15296 Kbit/s is possible only for modulesMS-17H4 for SG-17S base platform.

Link connection

Warning

Make sure that the dedicated line does not have any electrical sources and is not connected to central office equipment. Non-observance of this rule may lead to the failure of the router or of the equipment installed on the line!

For normal performance of routers and maintenance of the set-up parameters, the communication line should comply with the following requirements:

- The use of thermal switches on communication line is not recommended. The presence of thermal switches lead to considerable decrease in rate. Operation on coil-loaded lines is also unpracticable.

- The cable should not have any closing wires and leakages to ground and to other conductors, including those not connected to something. There should not be any branching on line.
- In multipair cable, the wires should be taken from one and the same pair.
- Parallel connection of several pairs (e.g. to reduce the active resistance) is not allowed.

Non-compliance with the above-mentioned requirements may lead to the reduce of the performance or to the failure of the overall communication line.

In order to connect the line to the router, mount the plug RJ-45 on the cable. The router uses only one pair of wires, pins 4 and 5, other pins are not used.

Figure 3.1. Connector RJ-45

After that plug the cable into SHDSL port of the router.

Layout, functions of indicators and connectors of SG-17R

The router Sigrand SG-17R is supplied in shape form 19" to install into a communication box. The layout of the front panel without the attached modules is depicted in the figure below.

Figure 3.2. Front panel without plugged-in modules

Figure 3.3. Front panel

- *0,1,2,3* — slots for installation of replaceable modules.

  ## Important

  The slot 3 can be used only for installation of SHDSL and E1 modules in *multiplexing mode*. The relevant network interface will be visible within the system and will be adjustementable, however it will not have an option to transmit the network traffic (the traffic which is thansmitted via other lines, not multiplexing ones). It is due to the absence of DMA support for the given slot. The slot 3 does not impose any restrictions on the use of the RS-232 and VoIP modules.

- *Console* — RS-232C a port for router management.
- *Ethernet ports* — RJ-45 ports for Ethernet interface connection.
- *Ethernet ports indication* — each channel corresponds with two indicators:
  - Upper — *DPX* :
    - *On* — full duplex mode.
    - Off — half duplex mode.

    - *Flashing* — channel collision.
  - Lower — *LNK* :
    - *On* — connected with a remote device.
    - *Off* — no connection with a remote device.
    - *Flashing* — data exchange is in process.
- *Power button* — router start button.
- *Power indicator* — on when the router is switched on.

The layout of the back panel of the router with 36-72V direct current (DC) power supply is depicted below .

Figure 3.4. Back panel with 36-72V DC power supply

- *Power socket* — for electrical connection (36-72V DC).

The layout of the back panel of the router with 220V/50GHz is depicted below.

Figure 3.5. Back panel with 220V/50Hz power supply

- *Power socket* — for electrical connection 220V/50Hz.

The layout of the front panel with the mounted SHDSL and E1 modules is depicted below.

Figure 3.6. Front panel with mounted modules

- *Modules SHDSL* — two double-channel modules SHDSL with distant feed.
- *Modules E1* — two double-channel modules E1.

Changeable Interfaces

While operating a SG-17R router, there is a possibility to extend its functionality using changeable modules - at the moment these are SHDSL, E1, RS-232 and VoIP (FXO, FXS, VF - tone frequency channels).

SHDSL Modules

There are several types of SHDSL modules:

- One channel SHDSL no distant feed (MR-17H1).
- Two channels SHDSL no distant feed (MR-17H2).
- One channel SHDSL with distant feed (MR-17H1P2).
- Two channels SHDSL with distant feed (MR-17H2P2).

Figure 3.7. One SHDSL channel module without distant feed (MR-17H1)

Figure 3.8. One SHDSL channel module with distant feed (MR-17H1P2)

Figure 3.9. Two SHDSL channels module without distant feed (MR-17H2)

Figure 3.10. Two SHDSL channels module withdistant feed (MR-17H2P2)

- *SHDSL ports* — RJ-45 ports for SHDSL interface connection .
- *SHDSL indicators*
  - *ERR* :
    - Off — no jabbers.
    - *Flashing* — a jabber is received.
  - *LINK* :
    - *On* — connected with a remote device.
    - *Off* — no connection with a remote device.
    - Flashing — connection is in process.
  - *UNB* :
    - *On* — power supply balance is broken to earth. Norm is plus120 V at one wire, and minus120 V at the other. If the shift exceeds 30 V or the grounding is absent - it implies power imbalance.
    - *Off*— power balance is normal.
  - *OVL* :
    - *On* — power overload or short circuit on line. It is associated with an excess number (more than 4) of regeneraters on line, adjusted to get feed from this router.
    - *Off* — no power overload.

E1 Modules

There are several types of E1 modules:

- One channel E1 (MR-17G).
- Two channels E1 (MR-17G2).
- Four channels E1 (MR-17G4).
- Eight channels E1 (MR-17G8).

Figure 3.11. One E1 channel module (MR-17G)

Figure 3.12. Two E1 channels module (MR-17G2)

Figure 3.13. Four E1 channels module (MR-17G4)

Figure 3.14. Eight E1 channels module (MR-17G8)

- *Ports E1* — RJ-45 ports for E1 interface connection.
- *E1 Indicators*
  - *On* — connected with a remote device.
  - *Off* — no connection with a remote device.

RS-232 Modules

There are several types of RS-232 modules:

- Two channels RS-232 DCE (MR-17S2C).
- Two channels RS-232 DTE (MR-17S2T).
- Four channels RS-232 DCE (MR-17S4C).
- Four channels RS-232 DTE (MR-17S4T).

Figure 3.15. Two RS-232 DCE channels module (MR-17S2C)

Figure 3.16. Two RS-232 DTE channels module (MR-17S2T)

Figure 3.17. Four RS-232 DCE channels module (MR-17S4C)

Figure 3.18. Four RS-232 DTE channels module (MR-17S2T)

Modules for VoIP Submodules Mounting.

There are sevelar carrying modules meant for mounting of VoIP submodules (FXO, FXS, VF - tone frequency channels):

- For two submodules or four VoIP channels (MR-17V4).
- For four submodules or eight VoIP channels (MR-17V8).

Figure 3.19. Four VoIP channels module (MR-17V4)

Figure 3.20. Eight VoIP channels module (MR-17V8)

Installation of Changeable Interfaces

Important

For modules mounting slots 0, 1, 2, 3 of the router can be used (read "Important" in Section Layout, functions of indicators and connectors of SG-17R slot 3 usage restrictions).

Figure 3.21. Front panel without changeable modules

Mounting of a odule is performed as follows:

1. Switch off the router.
2. Remove the plug sealing the slot.
3. Place the module into the slot.
4. Fix it with the help of screw knobs.
5. Switch on the router and carry out the adjustment of the mounted module.

Chapter 4. Start of Work with Router

Getting ready for the first switch-on

Important

Make sure that there are no visible damages which could occur while transporting the device. If there are any, please, contact the LLC Sigrand guarantee service as soon as possible.

Warning

In case the device was transported or stored at temperatures below zero - the switch-on should be made after the device spend at least one hour at room-temperature!

Remove the packing and place the router on the table or other flat level surface. Connect the device to the appropriate power sourse (220V/50Hz or DC 36-72V).

In case the router management using console interface is needed, for example, for router weaving renewal (see Router firmware renewal), or for diagnostic of loading process, connect the console port of the router to the serial port of the computer via the terminal cable.

For router management via console interface any terminal program can be used — HyperTerminal or Putty for OS Windows and Minicom for OS GNU/Linux. Serial port settings are mentioned above in Section Parameters of RS-232C Interface (console port) (traffic rate, bit/sec: 115 200; protocol: 8-N-1; flow control: no).

For router adjustement via web-interface connect its eth0 interface to the network adapter of the computer or to the port of local network switchboard via conventional patch cord.

Switch-on of the router is carried out with the help of the power switch located on the front panel.

Loader

Work with the loader menu is carried out using console interface RS-232. After switching on the power, on the screen of the terminal emulator program you will see a statement offering to enter the loader menu. To do this you should quickly (within 3 seconds) press any button except 'q':

```
ADM5120 Boot:
CPU: Infineon 5120-175MHz
SDRAM: 64MB
Flash: NAND-32MB
Boot System: Linux-5120
Version: 2.3 (Feb  1 2011 - 17:53:29)

Press any key to enter boot menu or 'q' to boot OS immediately...
3
Checking flash......
```

If you pressed any button (except 'q') you will see the settings and the menu of the loader:

```
CPU: Infineon 5120-175MHz
SDRAM: 64MB
Flash: NAND-32MB
Boot System: Linux-5120
Version 2.3 (Feb  1 2011 - 17:53:29)

Press any key to enter boot menu or 'q' to boot OS immediately...
3

ADM5120 based router: Bootloader Menu
====================================

MAC address: 00-FF-11-22-3F-44
IP address: 192.168.2.100
TFTP Server IP address: 192.168.2.1
TFTP Server Gateway IP address: 192.168.2.1
Remote bootloader file name: sg5120boot_rom.bin
Remote Linux file name: sg.bin

[P] Set Parameters
[S] Update OS
[B] Update bootloader
[F] Flash operations
[R] Reset
Enter your option:
```

In the menu several actions are available:

- Set Parameters - enter to the menu of setting of all parameters of the loader
- *Update OS* — system update via TFTP-server.
- *Update Bootloader* — loader update via TFTP-server (available only in expert mode).
- *Flash* operations — Flash-memory management (available only in expert mode).
- Reset - processor reset and restart.

Router firmware renewal

Important

Save the configuration (see Configuration upload and failback) since the firmware renewal will initialize all the settings and reset all the MAC-addresses (see Chapter MAC-addresses of network interfaces) set by the manufacturer.

Firmware renewal is carried out via console interface RS-232. For the renewal you will need the following:

- A computer with serial interface port RS-232 (or with USB cable adapter -> RS232).
- TFTP-server, accessible via router.

For firmware renewal it is important to have a TFTP-server accessible via router where firmware image file is located.

If a local TFTP-server is used, it is necessary to copy the firmware file, which can be downloaded from www.sigrand.ru [http://www.sigrand.ru], to its (TFTP-server) root directory after adjustment. You can find the recent version of the firmware at: http://sigrand.ru:8280/downloads/firmware_sg17-r-cp1/ .

The process of preparation of the router to be managed via console interface is described in Chapter Getting ready for the first switch-on. Switch the router on after running of the terminal emulator program and setting parameters of the port. The information about the router and an offer to enter the loader menu will be displayed in the program window (see Chapter Getting ready for the first switch-on).

A configuration example is given below:

```
Parameters Menu
===================================
 [P] Pre-defined parameters menu
 [M] Local MAC address: 00-FF-0F-22-32-11
 [I] Local IP  address: 192.168.2.100
 [T] TFTP server IP address: 192.168.2.1
 [G] TFTP server gateway address: 0.0.0.0
 [B] Bootloader file name: sg5120boot_rom.bin
 [S] OS file name: sg.bin
 [E] Expert mode: Off
 [X] Save parameters and exit menu
Enter your option:
```

In the given example only the IP address of the router was changed, all other settings are left unchanged.

After the adjustment of network settings, choose Update OS menu item for system update.

```
Enter your option:s
Starting the TFTP download(ESC to stop) ..........................................
.................................................................................
.......................................................... PASS

Eraseing flash ...................................................................
.................................................................................
.................................................................................
.......................................................... PASS
Programming flash ................................................................
.................................................................................
.......................................................... PASS
```

PASS, corresponding with the lines "Eraseing flash" and "Programming flash" means that the updating was completed successfully. FAIL indicates that there exist some problem, usually they are:incorrect IP-address of the TFTP-server (the router and the TFTP-server are located in different networks) or incorrect file name on server. To start a new firmware updating process, it is necessary to reset the router by puching the 'R' key in top-level menu, or by switching the power on and off.

After the router loading is completed (in case of normal loading, it is not necessary to enter the loader menu; you should wait until timer runs out operating system loading begins), you can move forward to the adjustment via web-interface. The access to the console is not needed anymore, the cable can be disconnected and relevant software closed.

In case the following statement is displayed:

```
Starting the TFTP download(ESC to stop) ... FAIL
```

— it means that the loader failed to download the firmware file from the indicated TFTP-server. In this case check if the IP address of the TFTP-server and firmware file name are correct. If they are correct, check the settings in "Set Parameters". Another option is to chenge of MAC-address and checking whether the TFTP server is blocking the connection to the router.

Expert mode

In expert mode you can update the loader of the router and carry out some actions with the flash memory of the router.

Important

Use expert mode only if you are aware of your actions! These actions may lead to disability of the router!

Actuation of expert mode is carried out in configuration menu of the loader. Expert password - adm5120.

MAC-addresses of network interfaces

MAC-addresses for network interfaces (Ethernet, SHDSL, E1) are kept in configuration file with all other settings of the router.

At the moment there exist two ways of the initial allocation of MAC-addresses:

- The *first* is when after the firmware update random MAC-addresses generation for eth* and dsl0, dsl1 interfaces occurs. This way of MAC-addresses generation can not guarantee their uniquness for several routers - it means that two routers may generate similar MAC-addresses. To minimize the probability of MAC-addresses repetition, the initial loading should be carried out when the router is connected to the ethernet, preferably with intensive traffic - it will increase the randomness of address generation.

- Then runs the script instantiating the second way of MAC-addresses allocation - ##### ########## ######, ########## ###### ###### ########## MAC-####### — receiption of MAC-addresses list from the special-purpose server. The script checks whether the given server is accessible - if yes, than it downloads the list of unique MAC-addresses which then allocate to network interfaces.The second way of MAC-addresses allocation is available to and used only by the manufacturer of the router. In case the MAC-addresses are updated successfully, the following statement is displayed:

  ```
  Updating MAC addresses
  ```

  If the above mentioned server is not available, relevant message will be displayed, and the MAC-addresses update will not be carried out during the further loadings.

  ```
  MAC-address server is unreachable. You can update your MAC-address
  manually by running:
  /etc/init.d/updatekdb force
  ```

Thr router is delivered from the manufacturer with allocated MAC-addresses, received from a special-purpose server, which guarantees their uniqueness for all possible interfaces of the router.

Since MAC-addresses are kept in the configuration file, they will be lost after reflashing. To avoid this, please, save the configuration of the router (see Chapter Configuration upload and failback) before the reflashing, and then make a failback.

Device Management

With the manufacturer configuration and after the firmware update the router has an active eth0 interface with the IP-address 192.168.2.100, net mask 255.255.255.0.

To adjust the router connect the network adapter of the computer to the Ethernet-port eth0 via patch-cord. On the computer set an IP-address of the network where the router is located (192.168.2.0/24), for example, 192.168.2.1, with the net mask 255.255.255.0.

Management via web-interface

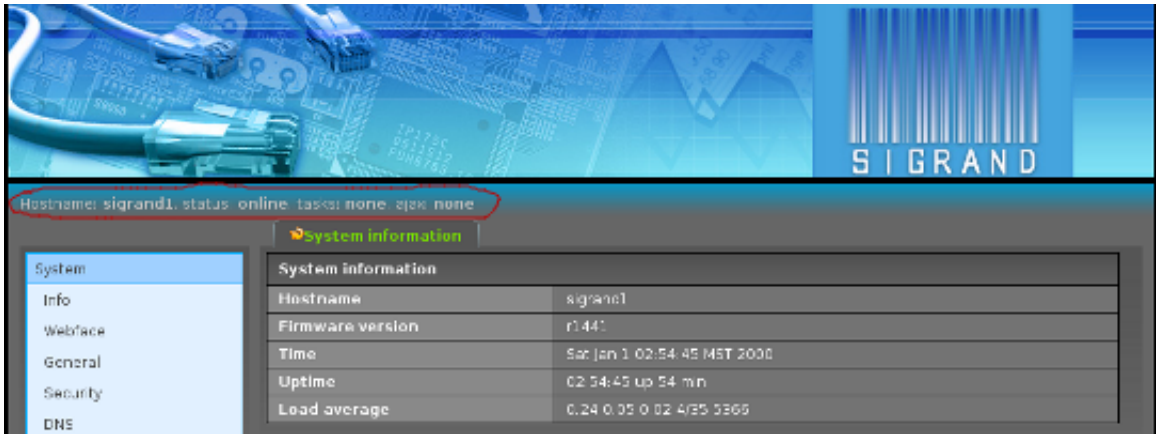
Router adjustment via web-interface is carried out using any web-browser supporting HTTPS protocol and JavaScript: Internet Explorer begining from Ver. 6, Opera, Mozilla Firefox. To forward to the adjustment page, type http://192.168.2.100 or https://192.168.2.100 in address line. After that several questions concerning encryption certificates, which should be answered positively. On default, login/password admin/1234.

When entering web-interface loading of all necessary files and the content of configuration file is done. Rendering of all elements of user interface is performed on client-side (in browser) by means of JavaScript, which allows to speed the work of the interface as it shifts resource-intensive operations from the router.

When saving changes, the page does not reset - only confuguration data is sent to the router (using AJAX technology). After saving the configuration parameters the relevant subsystem is restarted. All this performs as a background operation while the user may forward to the adjustment of other subsystems. In this case the number of active or queued tasks will be displayed in the web-interface (router can perform only one task at a time).

When enterring the web-interface, the page with general information about the device will be opened first: device name, firmware version, device local time, and information about the mounted modules. This page is shown below.

Figure 4.1. Page with general information



On the given page the status bar is highlighted which indicates the interaction between the web-interface and the device. It indicates the following parametres:

- *Hostname* — name of current device;
- *status* — whether the device is online or offline. For example, if you switch off the power supply of the router , the status will change to "offline" after a while (about 10-15 seconds). In this case it is impossible to make settings or poll the status of the router;
- *tasks* — number of active or queued tasks;

  ### Warning

  It is not allowed to switch off the router at a non-zero value of "tasks".

- *ajax* — how many AJAX-requests waiting for answer were transmitted to the router (these requests are not related to changes in device configuration).

Manageent via console interface

To perform the adjustement of the router via console interface, it is necessary to connect to it on serial interface using a terminal program, or using network through Ethernet-port and SSH protocol (port 22). There are several programs supporting SSH protocol, for example, Putty for OS Windows and ssh for OS GNU/Linux. Enter "root" as a login,and the password— 1234.

Note

It should be noted that the changes introduced in the router configuration via the console interface will be substituted with the parameters introduced via web-interface after the restart.

Summary

Table 4.1. Summary chart

Parameter		**Value**
IP-address(eth0)		192.168.2.100
Net mask		255.255.255.0
Web interface		
	Protocol	HTTPS
	Address	http://192.168.2.100
	Login	admin
	Password	1234
Console interface		
	Protocol	SSH
	Login	root
	Password	1234

Chapter 5. System settings and information

Language of the web-interface

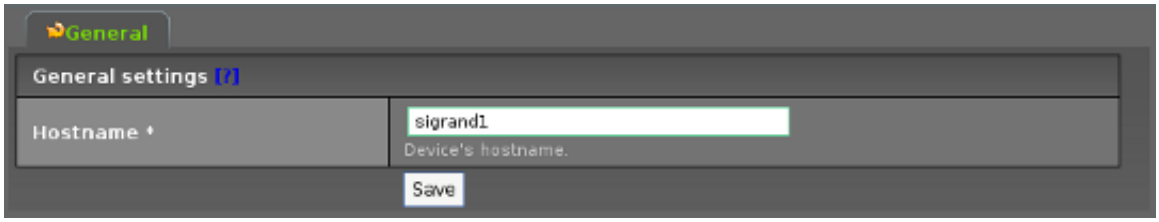
Language settings for the web-interface is carried out on page System/Webface.

Figure 5.1. Language settings for web-interface

Name of router

Change of the router name (hostname) can be performed on the page System/General, which is shown below.

Figure 5.2. Change of hostname



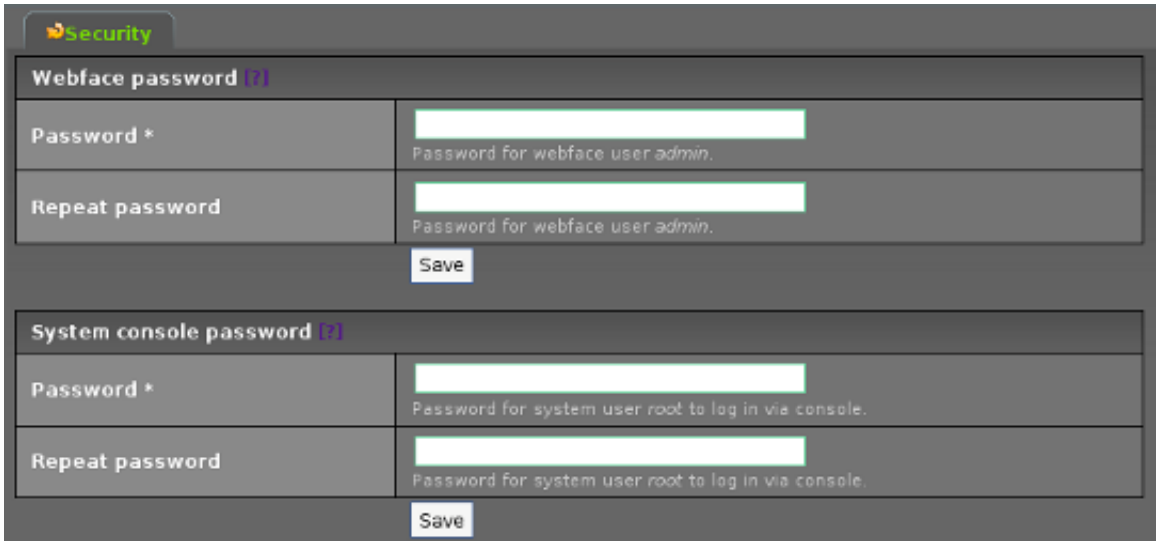
Password settings

Important

It is strongly recommended to change the password for the access to the router adjustment option, it can be done on page System/Security.

At the same page it is recommended to change the password on router management via the console interface. Password change page is shown below.

Figure 5.3. Change of password

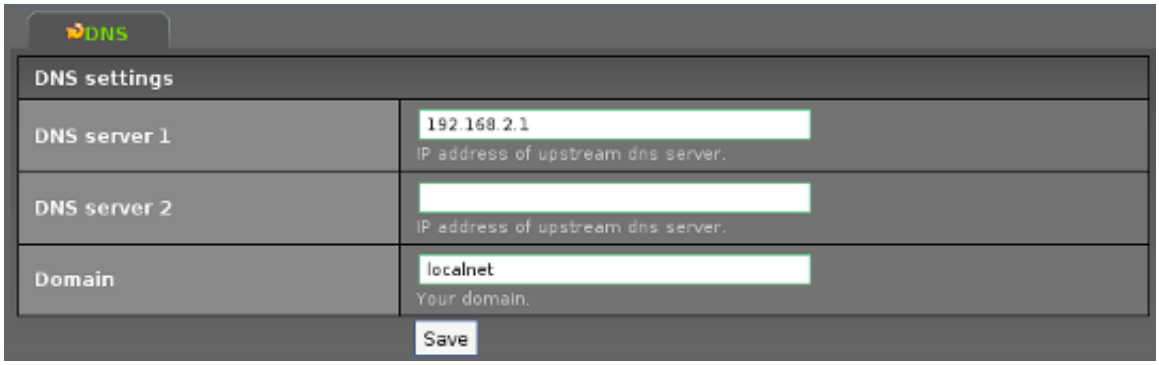


Webface password — password for web-interface access (user "admin"), *System console password* — password for access to device console (user "root").

DNS settings

Setting of DNS-server address, ton which the device will refer with DNS-requests and the name of the domain to which the device belongs can be set on page System/DNS.

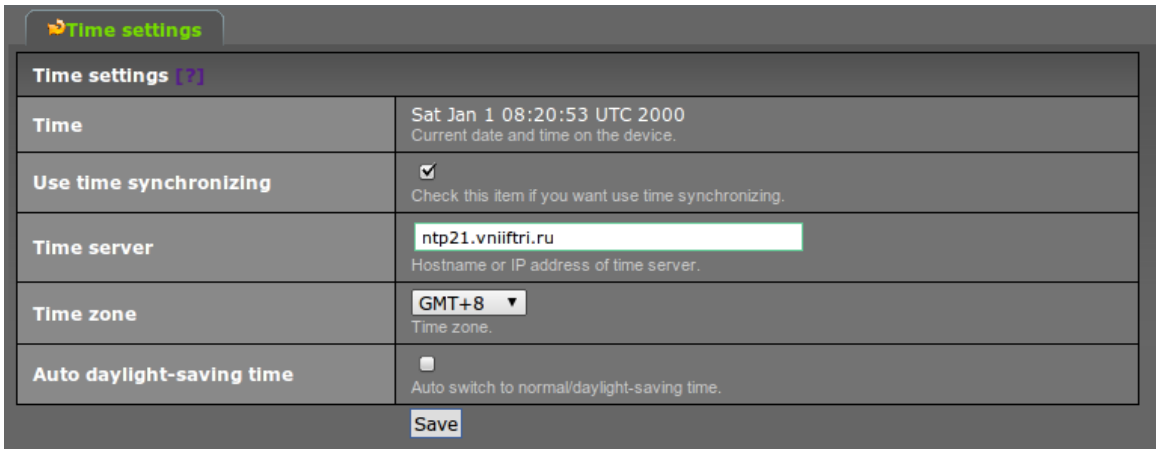
Figure 5.4. DNS settings



Time synchronization

Settings for local time synchronization can be found in the tab System/Time. Since the device does not have a battery for the timer, the system time drops each time the power is switched off.

Figure 5.5. Time synchronization



- *Time* — system time at the device;
- *Use time synchronizing* — enable time synchronization;
- *Time server* — NTP server, used time synchronization;
- *Time zone* — time zone of the device;
- *Auto daylight-saving time* — automatic adjustment for daylight saving time.

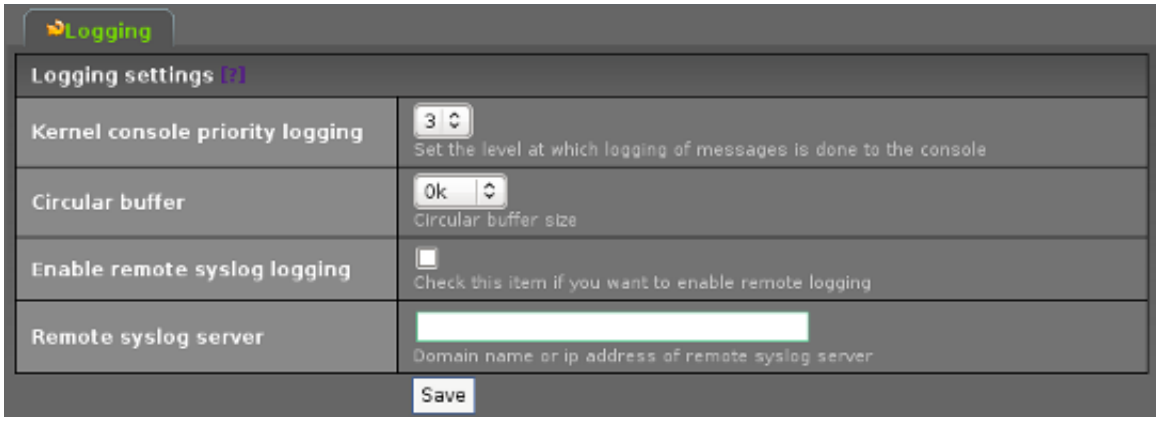
Note

Since the year 2011 daylight saving time principle is not applied in Russia.

Logging

Due to peculiarities of the embedded memory (flash-memory), system events (logs) cannot be saved locally on the router, they are written to a specialized buffer, browseable using special utilities (in console using the command "logread", on web-interface on page System/tools/syslog). The device has several parameters controlling the logging:

Figure 5.6. Logging



- *Kernel console priority logging* — priority grading of system messages at which they are displayed on the console.
- *Circular buffer* — buffer size.
- *Enable remote syslog logging* — enable logging to the remote syslog-server.
- *Remote syslog server* — address of the remote syslog-server.

Note

When enabling remote server logging, local buffer event recording continues.

Note

In order the remote syslog-server accept logs from the router it should be started with "-r" option. Logging is performed on udp protocol, 514 port.

Utilities

On page System/tools ofweb-interface various utilities are available which are used for the device performance analysis or functional check.

- *syslog* — grant access to the logs obtained from "logread" utility;
- *dmesg* — grant access to the logs obtained from "dmesg" utility;
- *ping* — allows checking the availability of the site using icmp protocol;
- *mtr* — allows checking the quality of connection between the device and the remote site.

Reboot

Reboot can be perfored by puching the "Reboot" button on page System/Reboot.

Configuration upload and failback

Web-interface allows saving of the current configuration or to back out saved or initial configuration of the router.

Configuration saving is performed on page System/Configuration/Backup:

Figure 5.7. Configuration backup

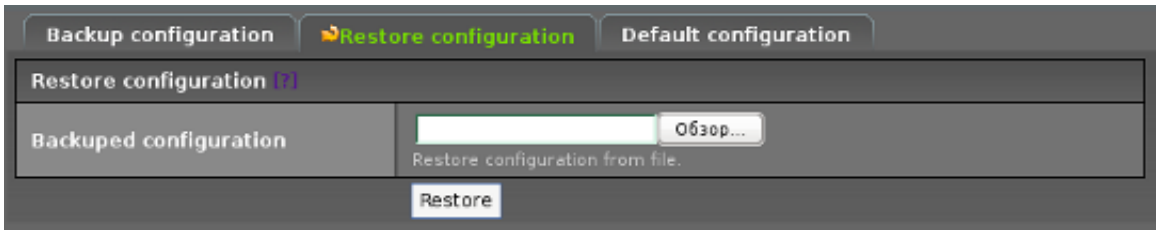
When clicking the "Backup" button there will be offered to save the configuration file, which can be loaded in future.

Important

After the failback the device will reboot automatically.

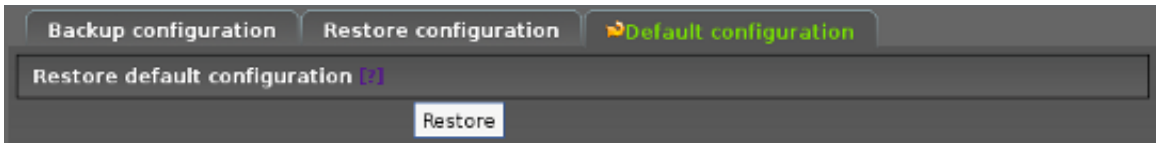
The failback is performed on page System/Configuration/Restore:

Figure 5.8. Failback



On the tap System/Configuration/default it is possible to back out the initial configuration by clicking the Restore default button.

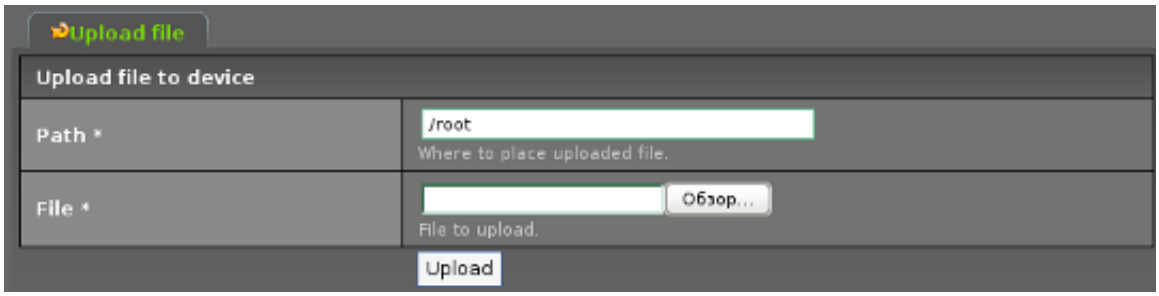
Figure 5.9. Back-out of factory default model



File download

In some cases it can be necessary to download a file in the device. For example, it can be a burst which needs to be installed on the device. For this purpose a downloader available in web-interface on page System/Upload file can be used.

Figure 5.10. File download



- *Path* — a directory in file system to which the file will be downloaded;
- *File* — a file on a local computer which needs to be downloaded.

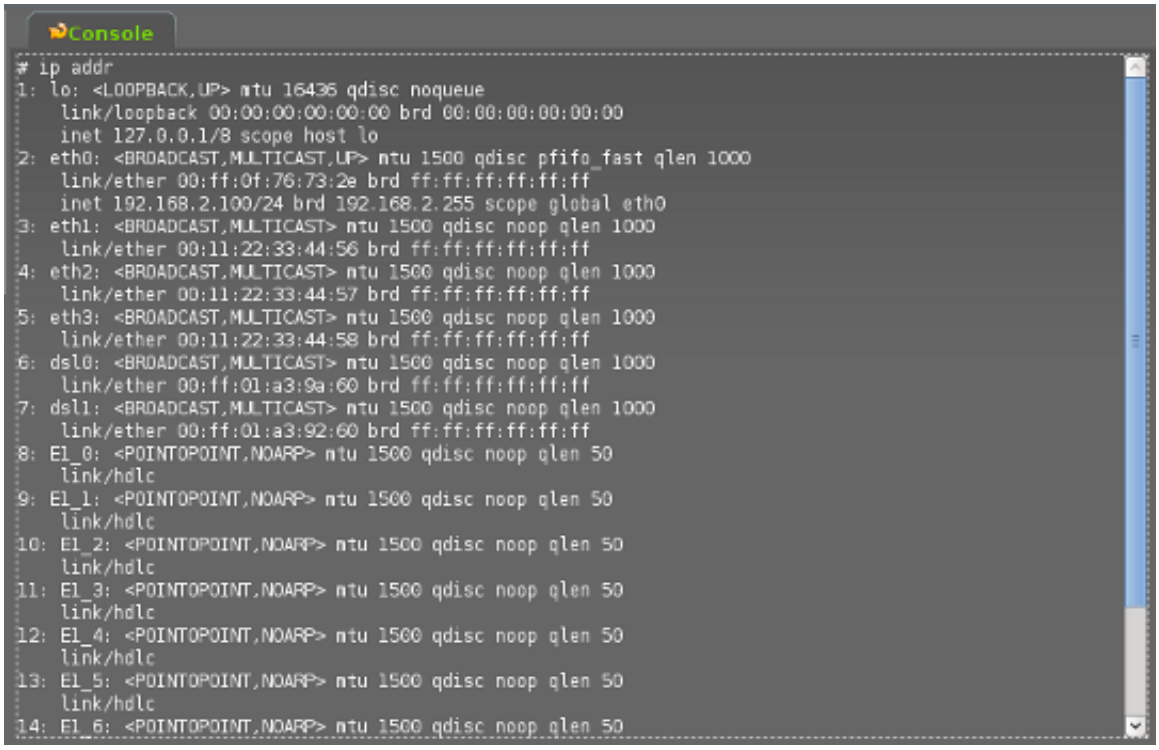
Console

In the absence or inhibited access to the console (SSH or via a serial port), it is possible to use the web-interface console which is accessible on page System/Console.

Important

This console hav a limited functionality! In particular, it does not support text pasting from the exchange buffer and launching of interactive programs (i.e. programs which interact with the user, for example, "top"). After the launching of an interactive program , for example "top", the console will display "executing command..." and stop. For the recovery it is necessary to reopen the page of the console by clicking on the menu or on the tap name.

Figure 5.11. Execution of "ip addr" command in console



Chapter 6. Equipment adjustment

Principle of module settings holding

In previous versions of firmware interface settings were attached to the interface name, which caused problems when working with modules, as with mounting of a new module interfaces names could change and the settings were applied to an incorrect module.

In current versions of firmwares, hardware settings are attached to PCI-slot, and network settings are copied in case of changes in the interface name. It means that if after mounting a new module the interface name changed from "*dsl0*" to "*dsl1"* , the network settings will be copied from the "dsl0" to the "dsl1".

The main difference in holding hardware settings and network settings consists in fact that if you remove a module for a while and switch the router on, network settings will be *deleted* , and hardware settings *will be preserved* . Therefore, when you return the module to its place and switch the router on, the module will be configured as before, but without network settings.

Besides, the use of settings for compatible modules is supported: for example, if a one-channel module was replaced by a two-channel one, the settings will be applied to the first channel of the new module.

If, vice versa, a instead of a two-channel module you mount a one-channel module, the settings (hardware and network) will be applied to the new module in the folllowing way: hardware settings for the second channel will be preserved, while its network settings *deleted* . Therefore, if the two-channel module is returned to its place, it will get its hardware settings (and network settings for the first channel).

The difference between hardware and network settings is made due to technical constraints.

Built-in Ethernet-commutator settings

Commutator adjustment can be done on page Hardware/Switch, where the binding of commutator physical ports to network interfaces is performed. Binding of several ports to one network interface creates a single physical environmebt for them, i.e. they begin functioning as ports of the same commutator. The adjustment window is shown in the picture below:Adjustment of

Figure 6.1. Adjustment of built-in commutator

Under the default settings each physical port corresponds to a separate network interface. Binding of Port 0 and Port 1 to the same interface, eth1 for example, makes possible a second-level traffic exchange between these interfaces, i.e. as in a standard commutator.

Note

Restart the router after implementation of alternations.

Bonding of interfaces states

To create complex interconnections between interfaces there was added an option of managing the states of the Ethernet or E1 port depending on the state of the correspondent SHDSL port.

Figure 6.2. Bonding of interfaces states

It is fixed under the given configuration that in case of link drop-out at dsl0 interface, the link at the interfaces eth3 and E1_0 will be subject to a despotic shutdown.

Note

SHDSL-interfaces may function as link-master, Ethernet and E1 - as link-slave.

SHDSL interface modules

Interface settings

For SHDSL connection one router should operate in "master", the other - in "slave" mode. Settings of SHDSL interface can be made on page Hardware/SHDSL/dsl*/Settings.

Settings of SHDSL modules

Note

SHDSL driver for the router SG-17R (and modules MR-17H*) is called MR17H, its name is displayed in the headline of the configuration window.

Important

Read Chapter Principle of module settings holding.

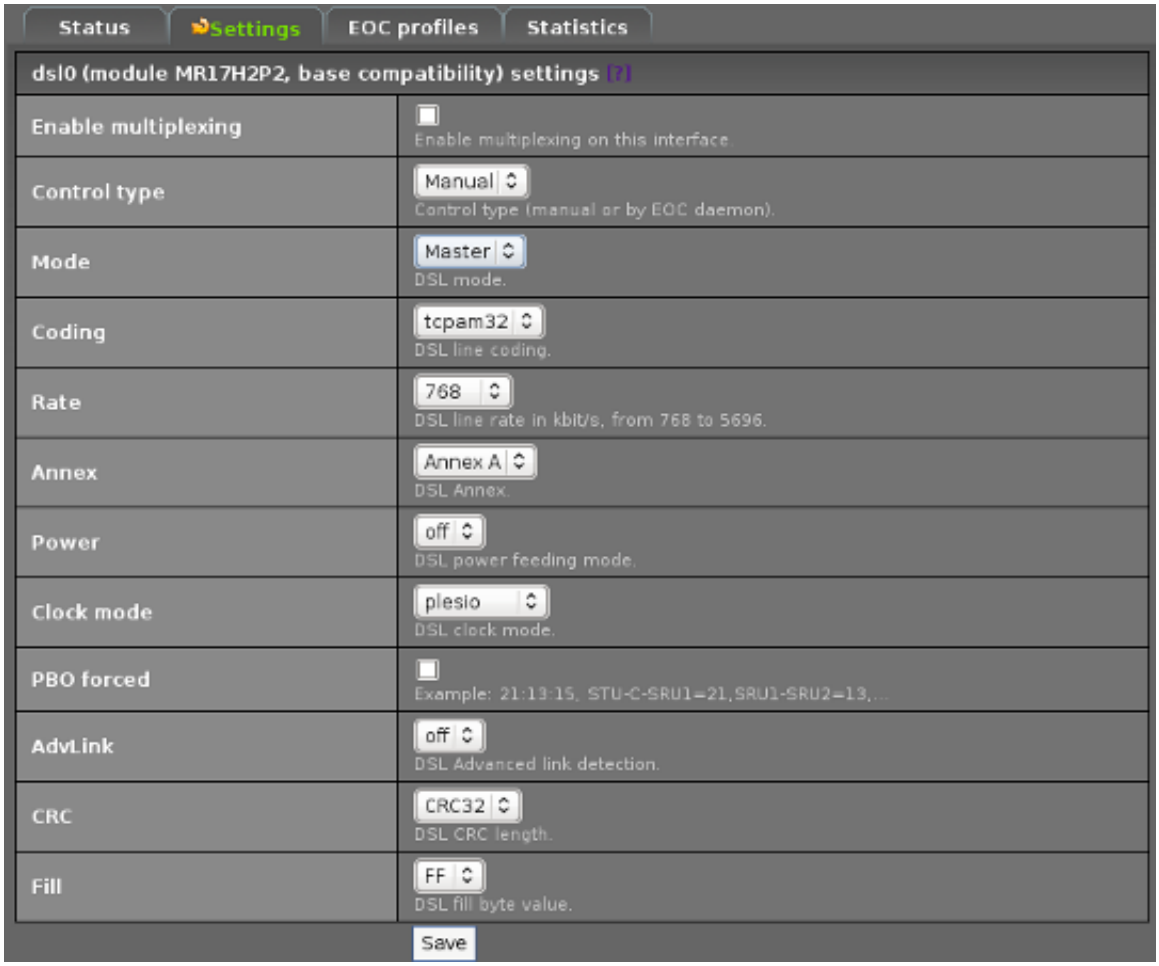
Important

If the given network interface refers to the module pluged into the fourth slot (*D slot*), it can be used only for operation in *multiplexing mode*. This netork interface cannot transfer the network

traffic (traffic transmitted not via multiplexing lines). It is associated with the absence of DMA support for the fourth slot.

Settings of *rate*, *clock mode*, *coding*, *annex*es and signal level reduction (*PBO Forced*) are made on the master device, "slave" receive these settings during connection initialization. Configuration window is shown below:

Figure 6.3. SHDSL Settings (MR17H)



- *Enable multiplexing* — enable the multiplexing mode at the given interface. This parameter reproduces the relevant parameter on the multiplexing settings page.
- *Control type* — interface management mode:
  - *Manual* — making settings on interface configuration page (on the current page).
  - *EOCd* — interface is managed by the daemon EOCd. It allows monitoring of different parameters of the interface and of the communication line in general. Further information on settings and operation of this mode is given in Chapter Interface management via EOCd.
- *Mode* — mode: master, slave.
- *Coding* — coding method. For information see ChapterSpecific features of TCPAM coding use.

- *Rate* — traffic rate, kbit/sec. The dropdown list does not include all the available bit rates - to set a voluntary bit rate, choose the value *other*, which will open an input box. After saving the input value will be rounded to the nearest correct value of the bit rate.

- *Annex* — amendments selection.

- *Power* — switch on the power supply for the regenerators on line.

- *Clock mode* — synchronization mode, on default *sync* (synchronic) mode is used. Make sure that all the equipment of the communication line (regenerators, routers) are operated in this mode.

- *PBO Forced* — reduction of the output signal to the set value (in dB). Used to reduce the impact on the ewuipment operating on the same cable.The given parameter influence on distance/rate of the connection.

  Signal level reduction can be carried out on all segments of the communication line - for this purpose the values of signal level reduction are input with colons. For example, "3:0:12" reduces the signal level in segmant STU-C — SRU1 by 3 dB, in segment SRU1 — SRU2 the signal level remains the same, in segment SRU2 — STU-R — by 12 dB. If the value of reduction is set not for all segments, there will be no signal level reduction in those segments.

- *AdvLink* — expanded mode of link statusing. In normal mode the link at the interface is considered advanced when there is a connection between the interface of the given device and the nearest device connected to it, whether it is a regenerator or the terminal device. It is not always correct when regenerators are operated on line, because the advanced state of the link at the interface should indicate the connection between the terminal devices, not between the device and a regenerator. For this purpose the parameter *AdvLink* is used — when it is active, a link at the interface is considered advanced only when there is a connection between the master device and the slave.

- *CRC* — batch total computation algorithm.

- *Fill* — byte selection for channel filling in the absence of batches to transmit.

Connection and status of the connection

When settings are saved, after a while the connection will be established, which will be indicated by light-emitting diodes on the front panel of the router. Connection status information can also be found in the status tab.

In case the connection is not made, the following information will be displayed:

Figure 6.4. Information about not-established SHDSL connection (MR17H)

- *Link state* — connection status: *offline* — connection is not established, *online* — connection is established.

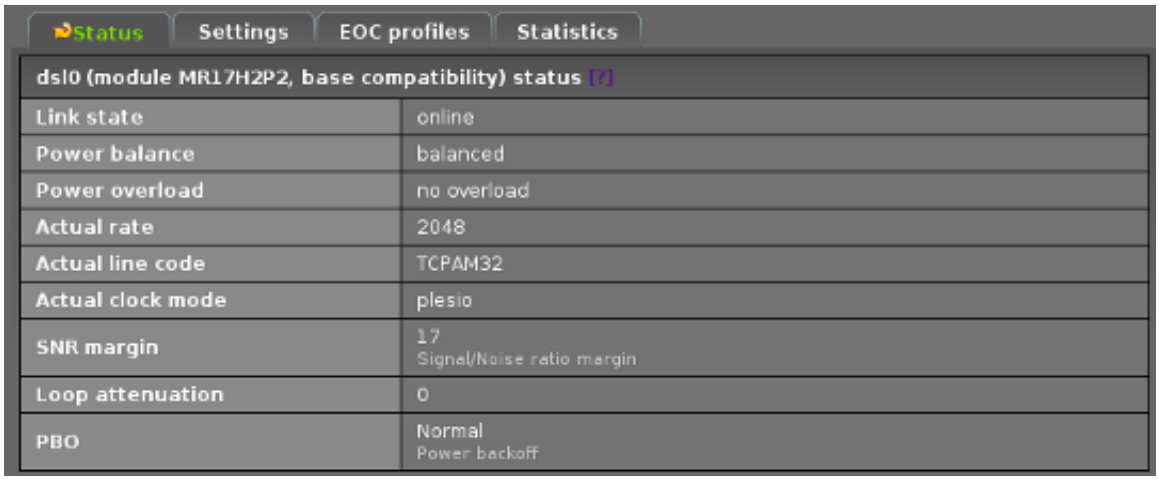
- *Power balance* — power supply balance to earth. Norm is plus120 V in one wire, and minus 120 V in the other. If the shift exceeds 30 V or earth is absent - it indicates power supply unbalance; in this case the "unbalanced" LED flashes on the SHDSL module. The value "*balanced"* of the parameter corresponds to normal operation, ,*"unbalanced*" — to unbalanced power supply.

- *Power overload* — excess power load. An excess number of regenerators operating on line which are set for power supply from the given router lead to power overload. In this case "overload" LED flashes on the SHDSL module. The value "*no overload*" of the parameter corresponds to normal operation, "*overload"* — to power overload.

- *PBO* — active settings for output signal level reduction.

When the connection is established the following information is added:

Figure 6.5. Information about the established SHDSL connection (MR17H)



- *Actual rate* — data transfer rate in the established connection, kbit/sec.

- *Actual line code* — coding method.

- *Actual clock mode* — synchronizing mode.

- *SNR margin* — signal to noise ratio margin in the communication line (the more the better).

- *Loop attenuation* — signal attenuation in the communication line (the less the better).

Interface management via EOCd

Interface adjustment for operating via EOCd means passing the control over the interface to a customized application which works with the devices on line via the service channel EOC. It allows to obtain information about the communication line from all segments, obtaining it from the regenerators and the terminal device - slave.

Interface adjustment for operating via EOCd

To manage the interface via EOCd it is necessary to set a relevant value of the parameter in interface settings (parameter *Control type*).

Figure 6.6. Interface adjustment for operating via EOCd

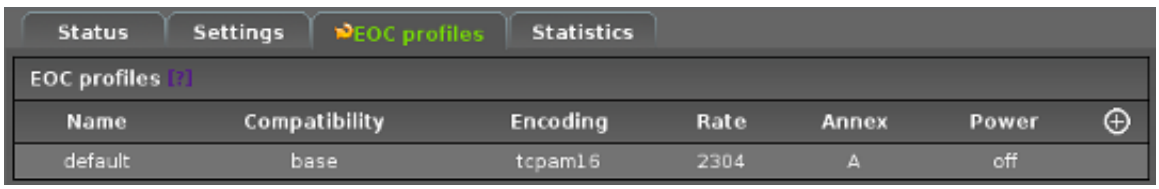
After selecting of EOCd mode in *Control type*, additional parameters will be displayed:

- *Config profile* — profile used for the given interface. Only those profiles are available for selection, compatibility level of which corresponds with the given interface.
- *Regenerators* — the number of regenerators installed. This value is informative and is meant for help to the network administrator. Actual number of regenerators on line may not coincide with the indicated value.

Profile creation and editing

The creation and editing of link profile is made in EOC Profiles tab which is shown below.

Figure 6.7. Creation and editing of link profiles



In EOCd the profile "default", the parameters of which cannot be changed, is available. The process of creation of a new profile or editing of the existing profile is shown below.

Figure 6.8. Creation of a new profile or editing of the existing one

- *Name* — profile name;
- *Compatibility* — compatibility level of the profile:
  - *base* — base combatibility, for modules operating at the rate of 5,7 Mbit/sec and 14 Mbit/sec.
  - *extended* — extended compatibility, can be used only for modules operating at the rate of 14 Mbit/sec.
- *Encoding, Rate, Annex, Power* — the given parameters correspond to the parameters on the interface configuration page (SHDSL settings).

SHDSL-channels monitoring

Note

Monitoring option is supported only by MR-17H* modules. Interfaces should be managed via EOCd. Browsing of the statistics of the communication line is available only on master device.

Monitoring via web-interface

SHDSL-channels monitoring allows to obtain information about different parameters and errors of the communication lines. If *SG-17E* regenerators are used in the communication line, it is possible to obtain information about their status and number.

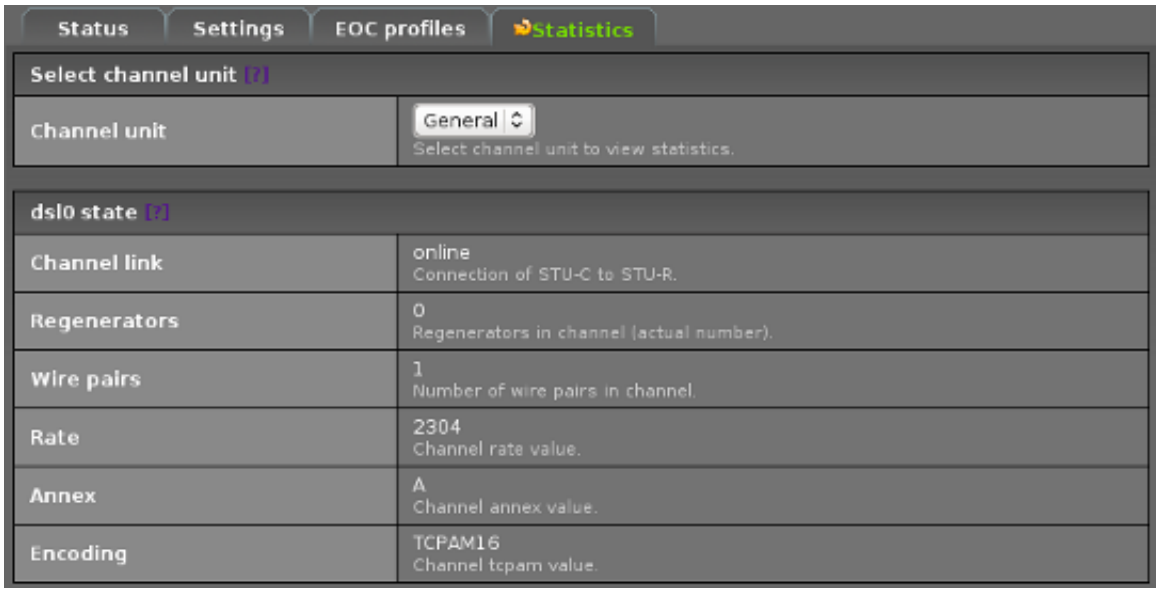
Browsing of statistics of the channel parameters is available in "Statistics" tab. On page information about the connection in general and about the devices operating on line is available. The name of the parameter - *Channel unit*:

- *General* — general information about the communication line;
- *STU-C* — master statistics;
- *STU-R* — slave statistics;

- *SRU1 - SRU8* — regenerator statistics.

When opening the page, general statistics of the connection is displayed:

Figure 6.9. General statistics of the connection



- *Channel link* — status of the connection between master device and slave, determined by the status of the connection between EOCd processes on the devices. If the connection is established but the parameter value is *"offline*", the EOCd processes failed to establish the connection between them. It can be associated with several reasons: one of the EOCd processes may not be launched, or a relative interface may not be managed via EOCd.

- *Regenerators* — actual number of regenerators on line.

- *Wire pairs* — number of pair in the channel.

- *Rate, Annex, Encoding* — transfer rate, amendments, coding mode.

When statistics for a concrete device is displayed, the following parameters of the performance characterizing the SHDSL channel are available:

- *Errored Second (ES)* — number of second intervals when one or more CRC anomalies were detected or more than one LOSW bug. When working with this parameter it is necessary to consider the rules of parameters priority (see parameters priority).

  ## Note

  Loss of Sync Defect (LOSW defect) – loss of synchronization. In plesiochronous mode loss of synchronization bug should be identified when not less than three successively received slides contain synchronization errors. These errors are indicated by a group of bits in a slide: Frame Sync Word, Stuff Bits and Stuff Bit Ids. LOSW indication clears after receiving at least two successive slides not containing any synchronization errors.

- *Severely Errored Second (SES)* — number of one-second intervals, in which not less than 50 CRC anomalies occured or more than one LOSW bug was found. (50 CRC anomalier per second corresponds

to 30% of incorrect slides for standard frame length). When working with this parameter it is necessary to consider the rules of parameters priority.

- *Code Violation (CV)* — number of CRC anomalies, found withing the monitoring period. When working with this parameter it is necessary to consider the rules of parameters priority which will be described below.
- *LOSW Second (LOSWS)* — number of one-second intervals in which more than one LOSW bug was found.
- *Unavailable Second (UAS)* — number of one-second intervals in which SHDSL-channel was not available. The channel after failure is considered available in 10 seconds without SES. These 10 seconds should be extracted from the number of seconds when the channel was unavailable.

Many parameters are set for different pairs and sides:

- *Side* — there are two sides, to which the communication settings may belong:
  - *NetSide* — master side (communication line to the master).
  - *CustSide* — customer side (communication line to the slave).
- *Pair* — number of wire pair.

The table "*state"* shows the current parameters of the line (SNR margin and LoopAttn) and errors found from the begining of channel monitoring.

Figure 6.10. Table "state"

dsl0 state [?]

Side	Pair	SNR margin	LoopAttn	ES	SES	CV	LOSWS	UAS
CustSide	Pair0	24	1	0	0	0	0	0

The table "*relative counters"* contains the same parameters that the table "*state"*, allowing to reset them in order to take samples in certain time intervals.

Figure 6.11. Table "relative counters"

dsl0 relative counters [?]

Start date	Start time	Side	Pair	ES	SES	CV	LOSWS	UAS	Reset
01 Jan 1999	05:23	CustSide	Pair0	0	0	0	0	0	reset

The table "*current intervals*" contains errors occured during the last 15 minutes and the previous day. The values, thus, are updated every 15 minutes and every day.

Figure 6.12. Table "current intervals"

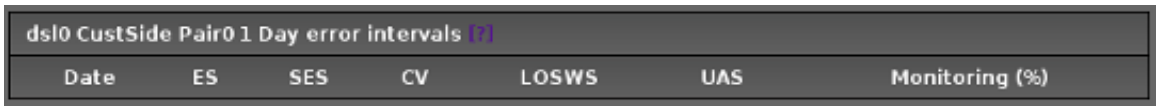
dsl0 current intervals [?]

Interval	Side	Pair	ES	SES	CV	LOSWS	UAS	Time elapsed
Curr 15 minutes	CustSide	Pair0	0	0	0	0	0	06m:38s
Curr 1 day	CustSide	Pair0	0	0	0	0	0	05h:36m:38s

Besides, tables are maintained for each wire pair and for each side (NetSide and CustSide), where 15-minutes and day-intervals when errors occured are kept. Tables keep the information about the last 96 15-minutes intervals and the last 30 day intervals.

Figure 6.13. Table of 15-minutes intervals for CustSide

Figure 6.14. Table of day intervals for CustSide



- *Monitoring* — ratio of time when the channel was being monitored.

Monitoring via console

For SHDSL-channel monitoring **eoc-info** utility is used; for further information about the utility functions use the key `--help`.

To get a aummary of channel status use the command **eoc-info** `-s`. It reflects the status of each channel: how many regenerators is found, is there a connection to slave (the router operating in *slave mode*). The "*offline*" status indicates that the connection with the second router is not established. In this case the number of regenerators shows the regenerator to which the connection is established.

For the detailed information type the name of the interface: **eoc-info** `-i dsl0`. The program output will contain full information about all units of the track - master, slave and all the regenerators. To get information about a specific unit use an option " `-u`"and unit`s name: STU-C, STU-R, SRU1..SRU8.

Rules of SHDSL -channel performance parameters priority

- No restrictions for *UAS* parameter.
- Parameters *ES* and *SES* are disabled if *UAS* indication is enabled.
- *CV* parameter is disabled if *SES* indication is enabled.

Specific features of TCPAM coding use

TCPAM Coding (Trellis-Coded Pulse Amplitude Modulation) used to data transfer under G.SHDSL Standard (G.991.2) has several versions with different degrees of complexity of coding algorithm. High rate data transfer corresponds to the mode with high number of modulation positions (TCPAM32), at lower transfer rates the mode with lower number of modulation positions is used (TCPAM16). Consequently, with the increase of coding algorithm complexity the noiseproof feature of the channel decreases ans vice versa.

Therefore it is necessary to pay special attention to the TCPAM coding algorithm when selecting a transfer rate, and change the linear code, if necessary, for the best result.

For SHDSL modules of MR-17H* series there exist own acceptable and recommended TCPAM coding values.

Table 6.1. Recommended values

Linear code	Bitrate range, kbit/sec
TCPAM128	8192..14080
TCPAM64	5760..8128
TCPAM32	2560..5696
TCPAM16	192..2496

Modules of E1 interface

The interface adjustment is made on page Hardware/E1/E1_*.

Important

Read Chapter Principle of module settings holding.

Important

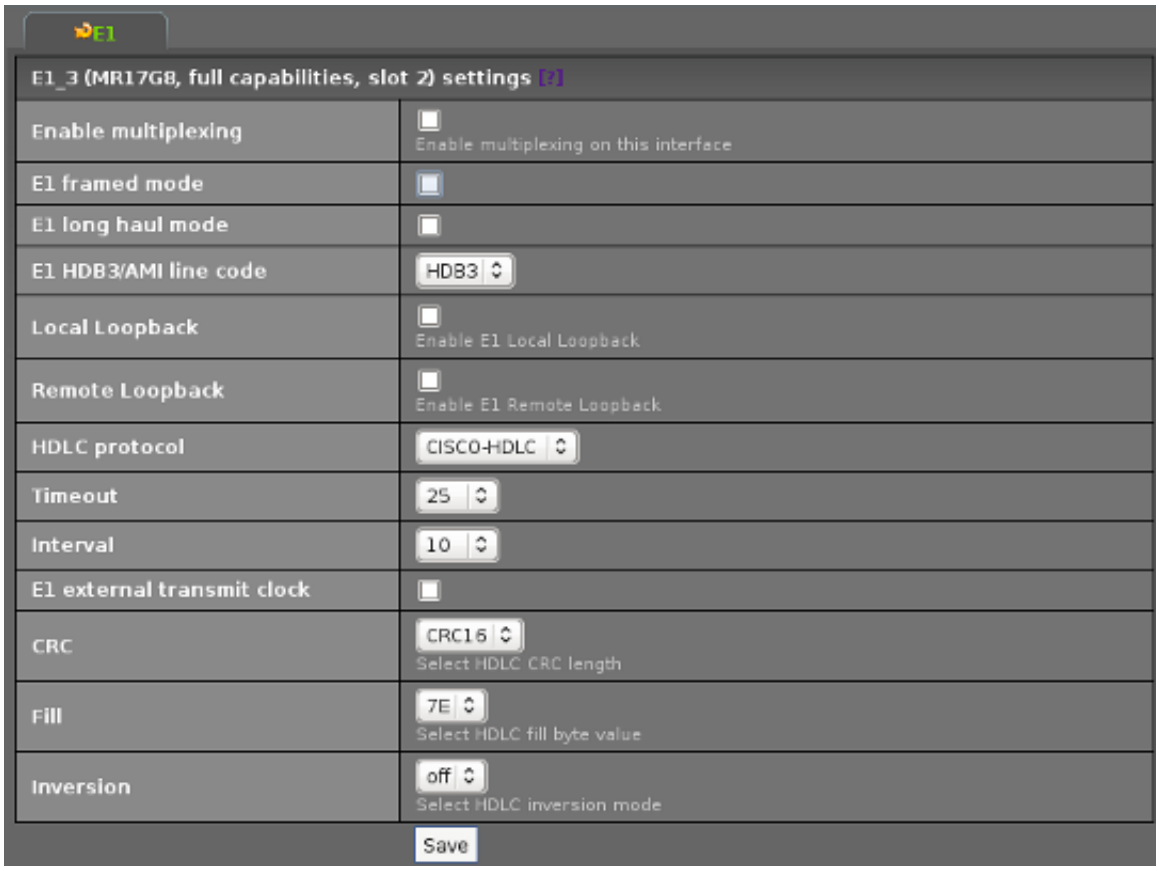
If the given network interface refers to the module pluged into the fourth slot (*D slot*), it can be used only for operation in *multiplexing mode*. This netork interface cannot transfer the network traffic (traffic transmitted not via multiplexing lines). It is associated with the absence of DMA support for the fourth slot.

Important

On some versions of 8-channel modules four higher ports may also be used only in *multiplexing mode*. In this case in the page headline near the name of the module it will be indicated: *MR17G8, multiplexing only, ...* It is associated with technical constrains of the module. Parameters related to transfer of IP-traffic are not available for configuration.

Setting of interface parameters

Figure 6.15. Setting of E1 interface parameters



- *Enable multiplexing* — enable the multiplexing mode at the interface. This parameter reproduces the correspondent parameter on the multiplexing adjustment page.

- *E1 framed mode* — enable the frame mode, when the channel is divided in time-slots. In this mode a map of time-slots is set which should coincide with the map on the other end of the connection. The time-slots which are set here are used for IP-traffic transfer and should not coincide with the time-slots used for multiplexing.

  ### Note

  The capacity of one time-slot is 64 Kbit/sec.

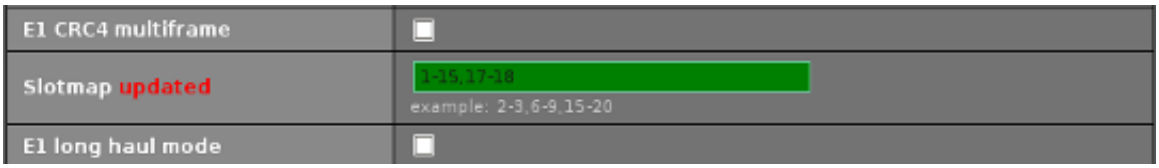
  In this mode there are additional parameters:

  - *Use time slot 16* — at E1 interface slots 0 and 16 are reserved on default, they can be used for control footing. Activation of this parameter allows to use the time-slot number 16 for data transfer (in multiplexing or IP mode).

  - *E1 CRC4 multiframe* — enable the CRC4 mode.

- *Slotmap* — time-slots map. Time-slots can be separated by commas or in ranges using a hyphen. The map should be updated by a driver after saving, in this case the background will change and near to the word "Slotamp" a word "*updated*" will be displayed.

Figure 6.16. Slotmap update



- *E1 CAS multiframe* (not available when *Use time slot 16* is on) — enable CAS mode, usually used with PBX equipment. In this mode slot number 16 is reserved for service use.

- *E1 long haul mode* — when activating long haul mode, the distance from the router to the DTE equipment connected to it can reach 1 600 meters with 0,4mm cable and 2 400 meters with 0,5 mm cable. When the mode is not active, the distance is limited by 400 meters.

- *E1 HDB3/AMI line code* — communication line signal coding mode.

Important

Recommendation ITU-T G.703 requires the use of HDB3 linear code!

- *Local Loopback, Remote Loopback* — used for connection diagnostics, see the next Chapter.

- *HDLC protocol* — protocol used for IP-traffec transfer. There can be additional parameters for some protocols:

  - *HDLC, ETHER-HDLC*:

    - *Parity* — ######## ######## ########.

    - *Encoding* — coding algorithm.

  - *CISCO-HDLC*:

    - *Timeout* — time in seconds after the last received connection maintenance packets upon the expiry of which the connection is cinsidered brocken.

    - *Interval* — time in seconds between keepalive packets.

- *E1 external transmit clock* — use the outer source of triggering. On default the internal source is used.

Note

If for the given interface multiplexing is on (MXEN=1), parameters from the table of multiplexing should be used (CLKM, CLKR). If multiplexing mode is off, the given parameter is used.

- *CRC* — ######## ########### ##### ######.

- *Fill* — selection of a byte for channel filling at the absence of packets for transfer.

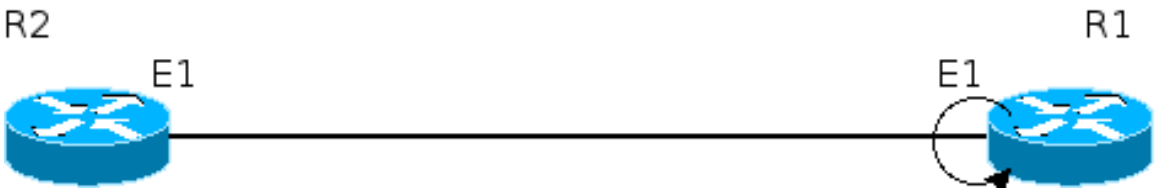
- *Inversion* — batch total value.

E1 connection diagnosting

For connection diagnosting "loop" can be used, i.e. to return the traffic instead of transferring it, simulating the traffic addressee response.

It is possible to create two types of loops - local and remote. In case of local loop, E1 module transfer data to physical line and immediately returns it to the sender, as shown in the figure below.

Figure 6.17. E1: local loop



To activate this type of loop select the parameter "Local Loopback" on the E1 nterface adjustment page of the router, on which you want to create the loop (in our figure - on router R1).

In case the second type of loop is used - remote loop - data is transferred to a physical line, it reaches the remote router which transfers it further and returns it to the sender.

Figure 6.18. E1: remote loop

To activate this type of loop select the parameter "RemoteLoopback" on the E1 nterface adjustment page of the router, on which you want to create the loop (in our figure - on router R2).

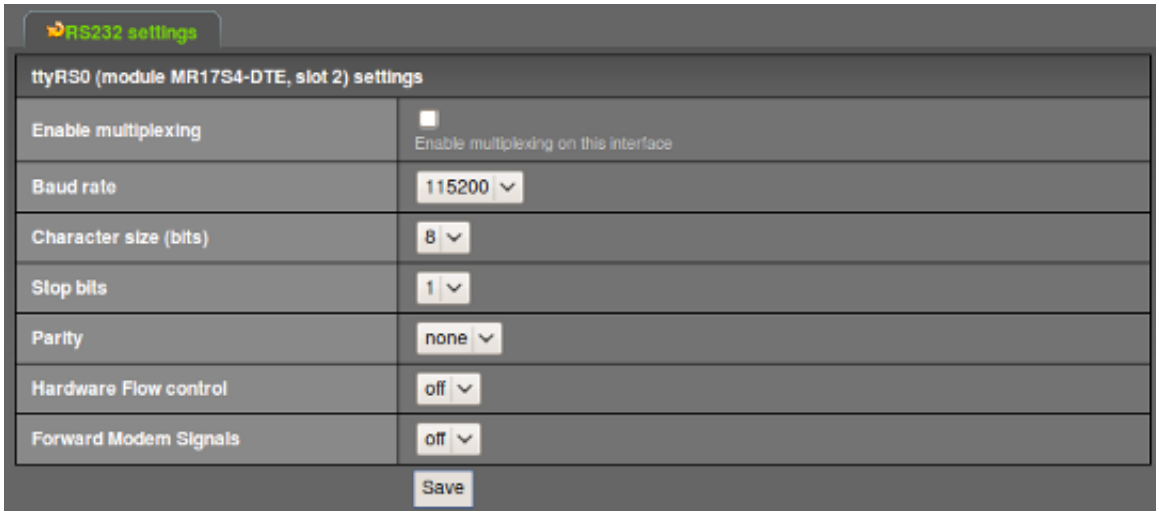
Thus, when two loop types are used, the data is still be transferred to the physical line and, at the same time, returns back, which allows configuration correctness control independent from the status of the communication line.

RS232 interface modules

Setting of interface parameters

Setting of RS232 interface parameters is made on page Hardware/RS232/ttyRS*.

Figure 6.19. Settings o RS232 interface parameters



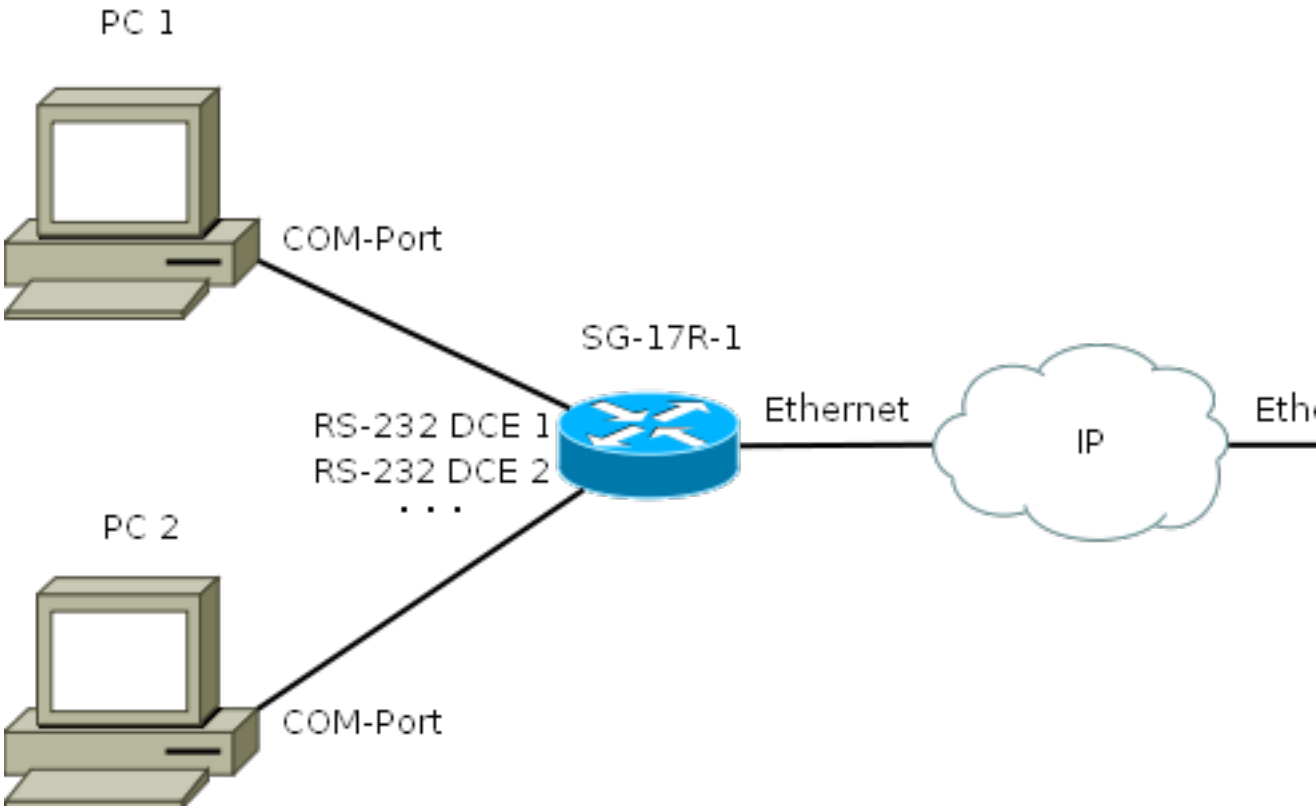
- *Enable multiplexing* — enable the multiplexing mode at the interface. This parameter reproduces the correspondent parameter on the multiplexing adjustment page.
- *Baud rate* — bit rate of the port.
- *Character size* — number of bits to transfer.
- *Stop bits* — number of stop bits.
- *Parity* — parity control.
- *Hardware Flow control* — hardware control of the data flow.
- *Forward modem signals* — transfer of control signals of the serial port, usually used when operating a modem.

RS-232 over TCP/IP

Description

This option allows to connect two routers with RS-232 ports (DTE andDCE) through IP networks, transferring data and control/modem lines statuses in both directions.

Figure 6.20. Scheme of the RS-232 extention cord via IP networks



Transmitting direction of control/modem lines:

```
Direct connecting cable:

    DTE    DCE
    ---    ---
    DTR -> DTR
    DSR <- DSR
    RTS -> RTS
    CTS <- CTS
    CD  <- CD
    RI  <- RI

null-modem:

    DTE    DTE
    ---    ---
    DTR -> DSR,CD
 CD,DSR <- DTR
    RTS -> CTS
    CTS <- RTS
```

Design and principles of operation

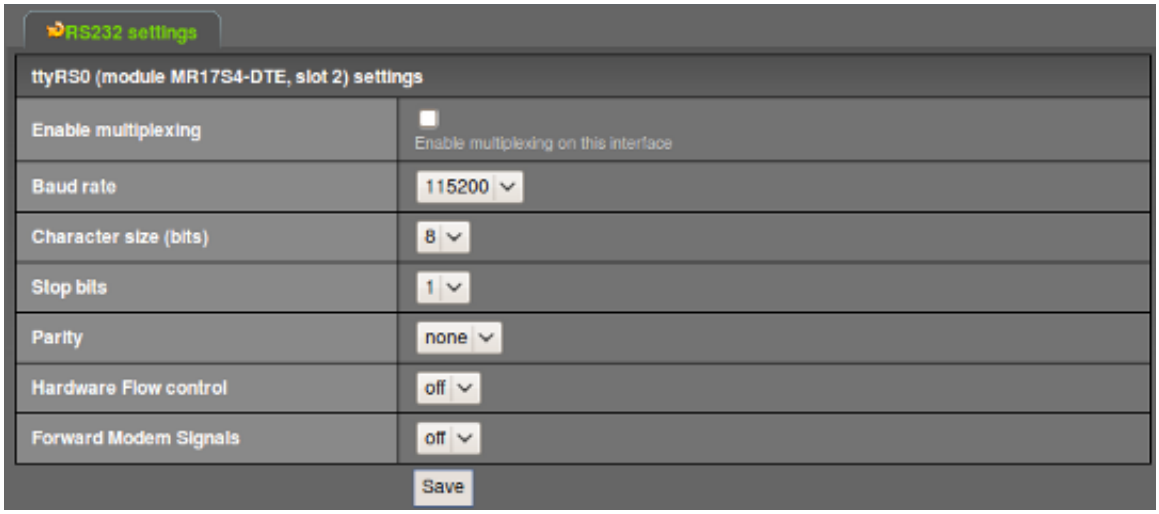
For each configured RS-232 port on both routers a separate version of rs232-tcpext daemon is launched - at the side of the router waiting for connection in passive mode, and at the side of the router initiating the connection, in active mode.

TwoTCP/IP connections are established: one for data transfer, the other - for control/modem lines statuses transfer. Control/modem lines status is requested in set periods, usually 1000 msec.

Architecture with separate daemons for each port provides the non-involvement of other ports in data flows while one port is being configured/restarted.

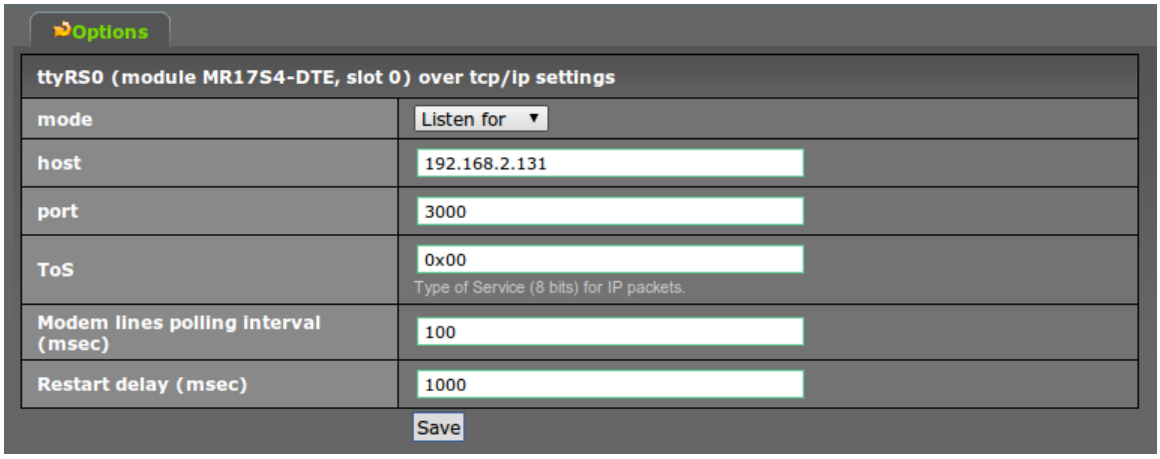
Setting instructions

Figure 6.21. Settings of RS232 port parameters



- Browse two tabs to management pages of both routers
- In tabs Hardware/ttyRS* set the parameters of the chosen ports and click "save".
- For each port deside which of the routers will be passive and which active side. Passive side waits for connection at a chosen network address from the active side.
- In tabs Services / RS-232 over TCP/IP / ttyRS* of both routers adjust the connecting sides.

Figure 6.22. Setting of RS-232 over TCP/IP



Selector "mode" defines the mode:

- "Disable" - service is disabled,
- "Listen On" - wait for connection at the set "host", "port" (passive mode)
- "Connect To" - connect to the set "host", "port" (active mode)

Boxes "host" and "port" define the network address and the port on which the passive side in waiting for the connection from the active side (see bind(2)) or to which the active side connects. Value on default - 0.0.0.0 - accept connections from all of the network interfaces.localhost (127.0.0.1) cannot accept connections from other nodes of the network.

Box "ToS" defines bits ToS for IP packets which will be transferred by the daemon rs232-tcpext.

Box "Modem lines polling interval (msec)" defines the time intervals between the requests for modem lines status, on default 1000 msec.

Box "Restart delay (msec)" defines the delay before the restart in case of any error, on default 1000 msec.

Click "save".

Make sure that the process is active on both routers: in tab System/Console enter the command "ps ax" and check that the rs232-tcpext process is launched:

```
ps ax
...
 728 ? S 0:00 rs232-tcpext /dev/ttyRS0 0.0.0.0 3000 listen /var/run/rs232-tcpext.t

3571 ? S 0:00 rs232-tcpext /dev/ttyRS0 192.168.2.101 3000 connect /var/run/rs232-t
```

Note

Take into account that the launching process over web system is rather slow.

In tabs System/Tools/Syslog you may see the daemon messages:

Passive side:

```
daemon.warn rs232-tcpext ttyRS0  listen : started up
daemon.info rs232-tcpext ttyRS0  listen : pid file '/var/run/rs232-tcpext.ttyRS0.p
daemon.info rs232-tcpext ttyRS0  listen : Waiting data connection...
```

After connection to the active side:

```
daemon.info rs232-tcpext ttyRS0  listen : Data connection from 192.168.3.102:2937
daemon.info rs232-tcpext ttyRS0  listen : Waiting state connection...
daemon.info rs232-tcpext ttyRS0  listen : State connection from 192.168.3.102:2938
daemon.info rs232-tcpext ttyRS0  listen : Recv modem state: 0x03, DTR:1 DSR:1 RTS:
daemon.info rs232-tcpext ttyRS0  listen : Send modem state: 0x03, DTR:1 DSR:1 RTS:
daemon.info rs232-tcpext ttyRS0  listen : Recv modem state: 0x03, DTR:1 DSR:1 RTS:
```

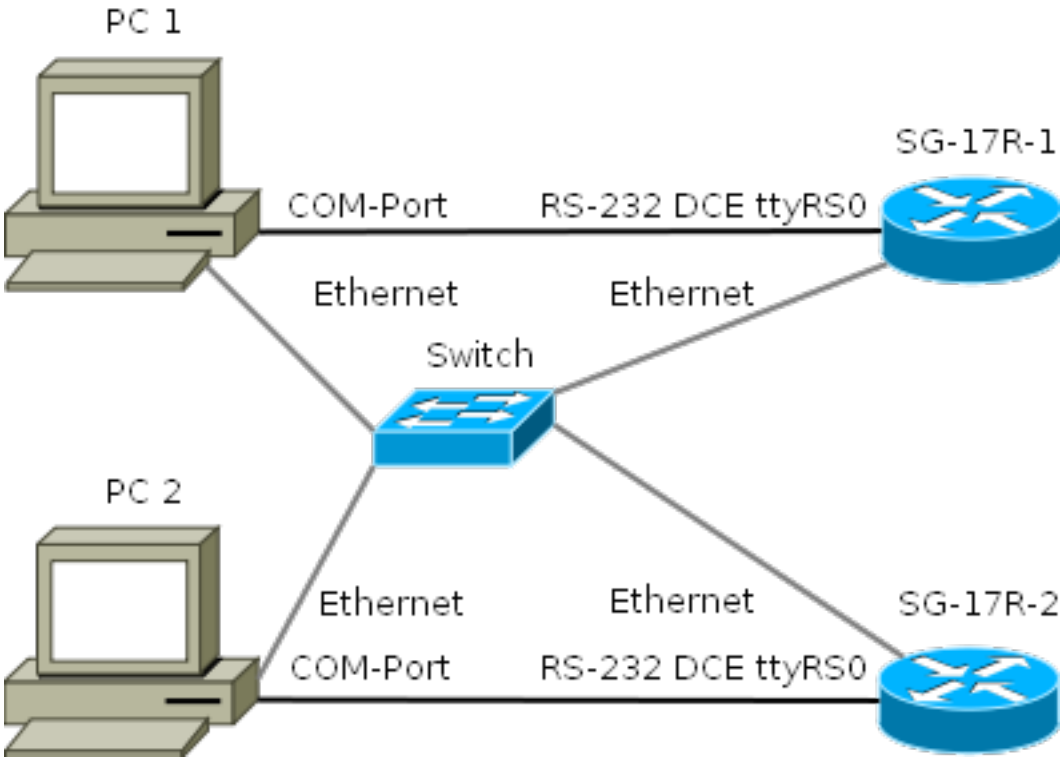
Active side:

```
daemon.warn rs232-tcpext ttyRS0  connect: started up
daemon.info rs232-tcpext ttyRS0  connect: pid file '/var/run/rs232-tcpext.ttyRS0.p
daemon.info rs232-tcpext ttyRS0  connect: Connecting (data) to 192.168.2.101:3000
daemon.err rs232-tcpext ttyRS0  connect: socket_connect(): Could not connect to 19
daemon.warn rs232-tcpext ttyRS0  connect: restart
daemon.info rs232-tcpext ttyRS0  connect: Connecting (data) to 192.168.2.101:3000
daemon.info rs232-tcpext ttyRS0  connect: Connecting (state) to 192.168.2.101:3000
daemon.info rs232-tcpext ttyRS0  connect: Send modem state: 0x03, DTR:1 DSR:1 RTS:
daemon.info rs232-tcpext ttyRS0  connect: Recv modem state: 0x03, DTR:1 DSR:1 RTS:
daemon.info rs232-tcpext ttyRS0  connect: Send modem state: 0x03, DTR:1 DSR:1 RTS:
```

Simple check of the RS-232 extention cord performance.

Connect the chosen RS-232 interfaces of the routers to the PC ports as shown below:

Figure 6.23. Scheme for RS-232 extention cord check over IP



Note

The given scheme can be configured on one PC if there are COM1, COM2 and two Ethernet ports. Adjust the RS-232 Interfaces PC (rate, 8n1, ...) in the same way as the router interfaces connected to them.

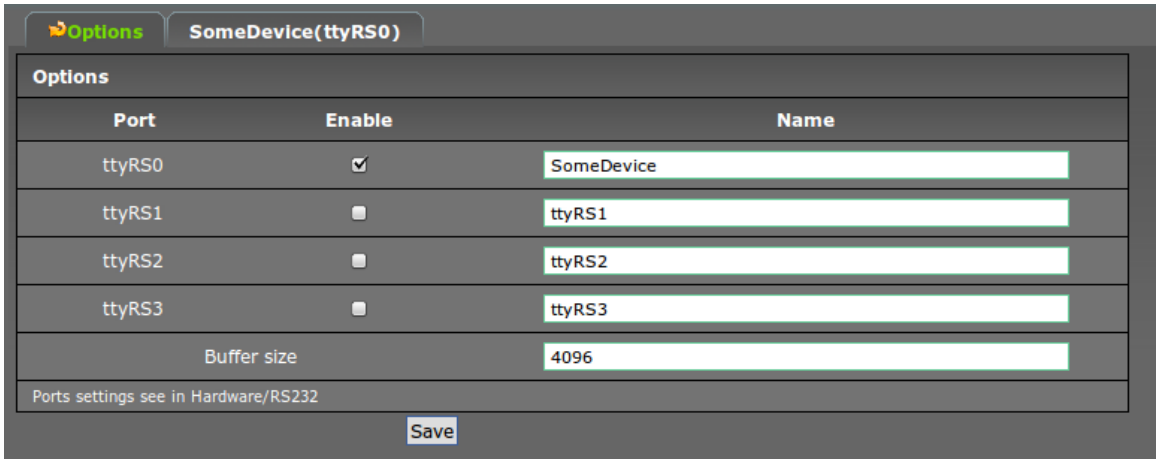
Launch terminal programs at the corresponding interfaces on both PCs and type something.

This scheme cannot be used to check the transfer of control signals/modem lines.

Terminal server

There exist many devices which can be adjusted and managed via the serial interface RS232. For remote management of such devices the terminal server of the router can be used.

Figure 6.24. Terminal server adjustement



In the tab "Options" you can activate/diasctivate this function for a specific port.

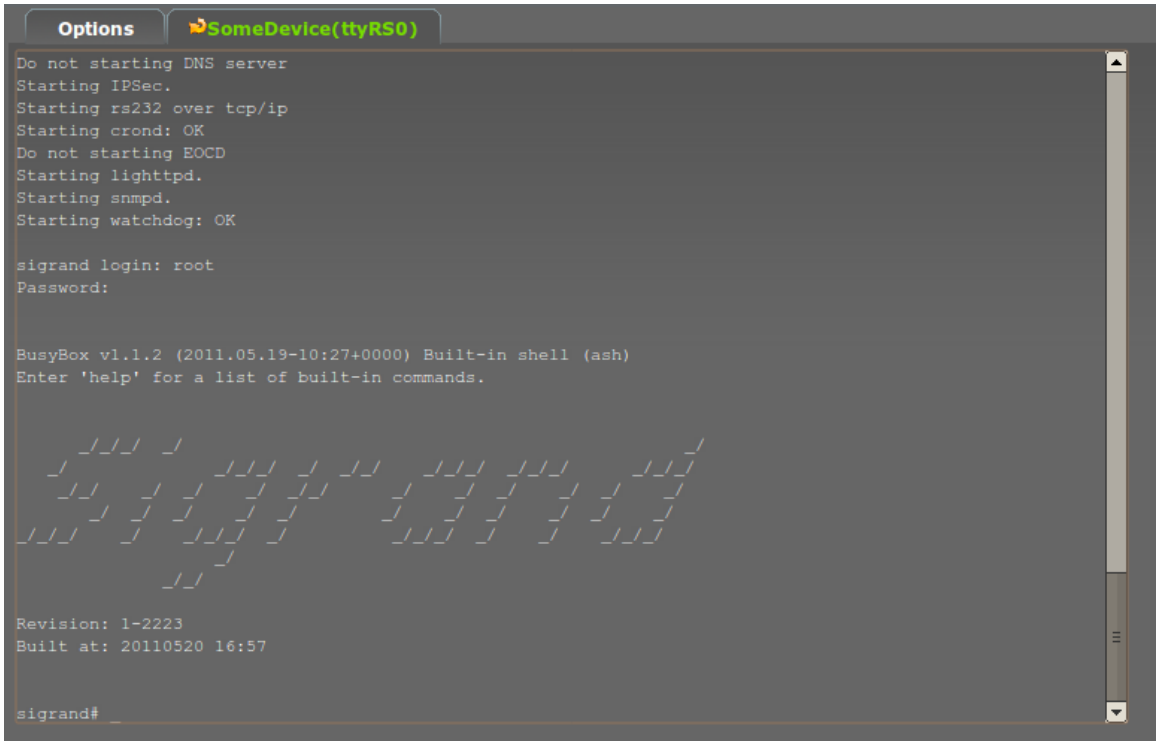
Important

Before activating this function for a port, make sure that other options (multiplexing, RS232-over-IP, Dial-in) are not active.

For the convenience each port can be given a name which will be indicated in the tab of the port.

"Buffer size" defines the size of the buffer for keeping the data from the port.

Figure 6.25. Terminal server console



Management of the remote device is carries out via web-interface.

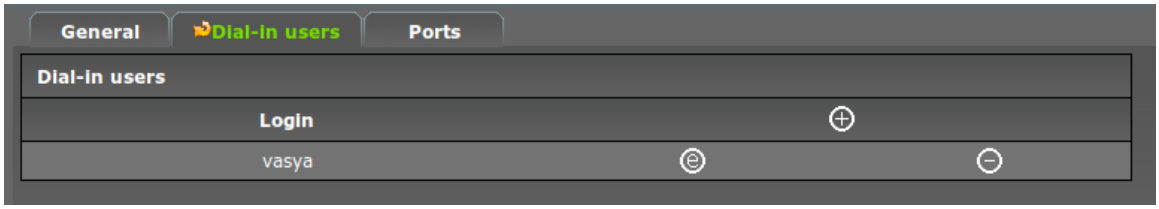
Dial-in server

Dial-in server allows to organize a spare or controlling data channel via wireless or switched connections. For this purpose different GSM and wired modems with RS232 interface can be used.

Figure 6.26. Tab General

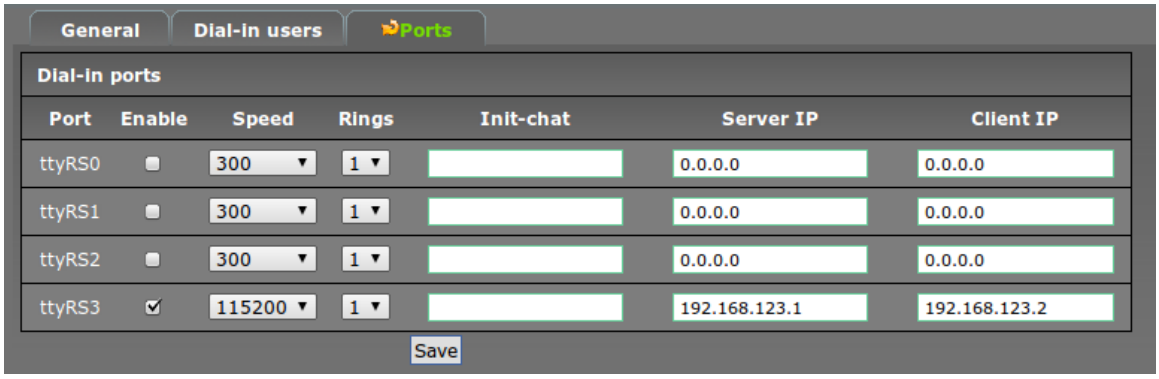
- *Enable terminal access* — enable access to the router console.
- *Authentification type* — PAP or CHAP.

Figure 6.27. Tab Users



In the tab "users" user and users password management is performed.

Figure 6.28. Tab Ports



- *Enable* — accept connections to the port.
- *Speed* — speed of connection.
- *Rings* — number of rings after which the connection will be accepted.

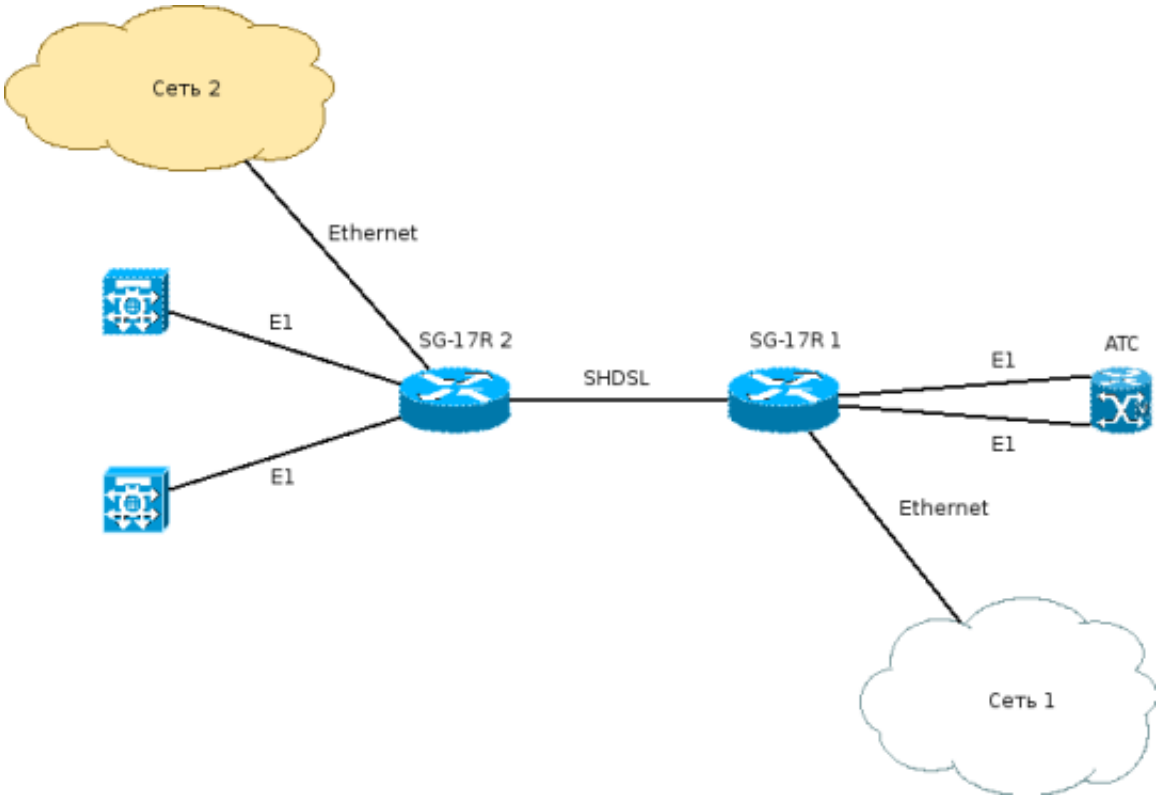
- *Init-chat* — modem initialization chart.
- *Server IP* — IP address of the PPP connection, router side.
- *Client IP* — IP address of the PPP connection, remote device side.

Multiplexing

Multiplexing is used for traffic transfer from one interface to another, by-passing the central processor. *SG-17R* allows simultaneous multiplexing and IP-traffic transferring.

Generally in can be represented as follows:

Figure 6.29. Network scheme



In the given example two E1 channels are connected to the SG-17R routers and there is also a TCP/IP network via Ethernet. The routers are interconnected over SHDSL. Maximum rate of SHDSL - 14080 kbit/sec, i.e. two E1 channels (2048 kbit/sec each) can be transferred via one SHDSL channel, 9984 kbit/sec remaining not used.

To transfer E1 flows, multiplexing is used: both E1 input flows are multiplexed into the SHDSL channel, by which they are transferred to the second router, where athey are de-multiplexed and the flows split to clients. The remaining SHDSL lane is used for the transfer of the IP-traffic between the two Ethernet networks.

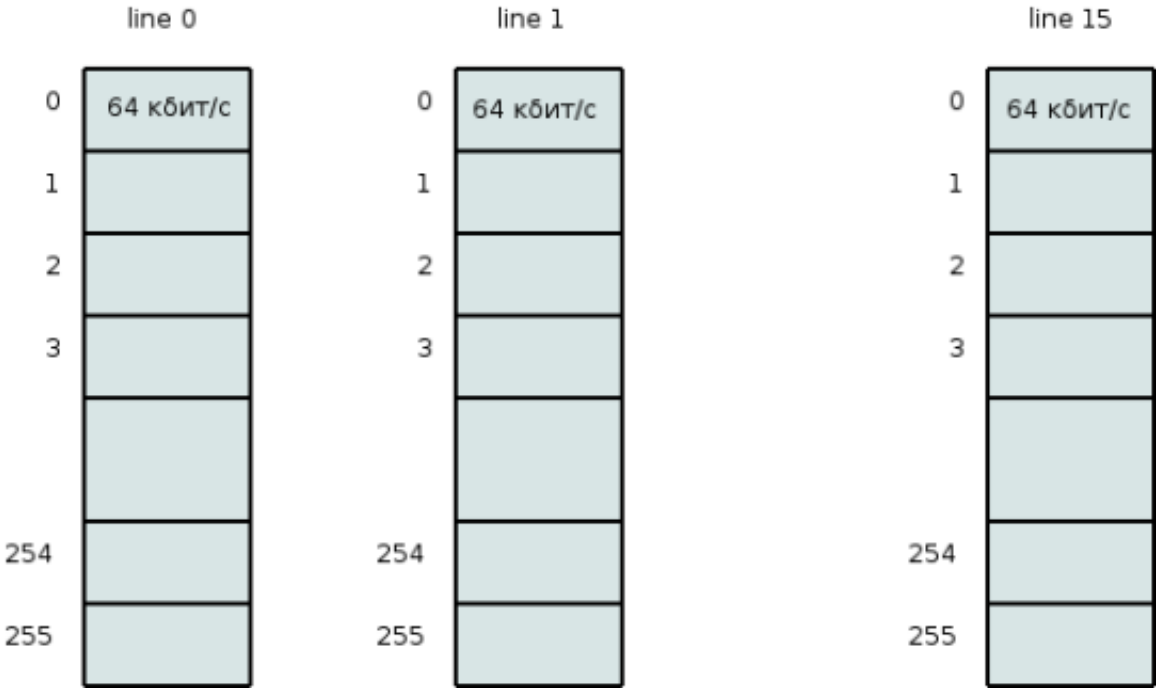
For purposes of multiplexing, the router has a strip which consists of 16 lines, each of which contains 256 time-slots. Each time-slot of the line corresponds to a time-slot in E1 or SHDSL, i.e. has a rate of 64

kbit/sec. E1 contains32 time-slots, SHDSL — depending on the interface speed. Interfaces E1 (E1) and SHDSL (dsl) may place data received from the physical line to the strip, and accept the data placed by another interface.

Note

Some modules may use only 8 lines.

Figure 6.30. Architecture of multiplexing



All the devices participating in traffic multiplexing should be triggered by one signal. For this purpose it is necessary to define which interface will determine the clock signal while multiplexing adjustment.

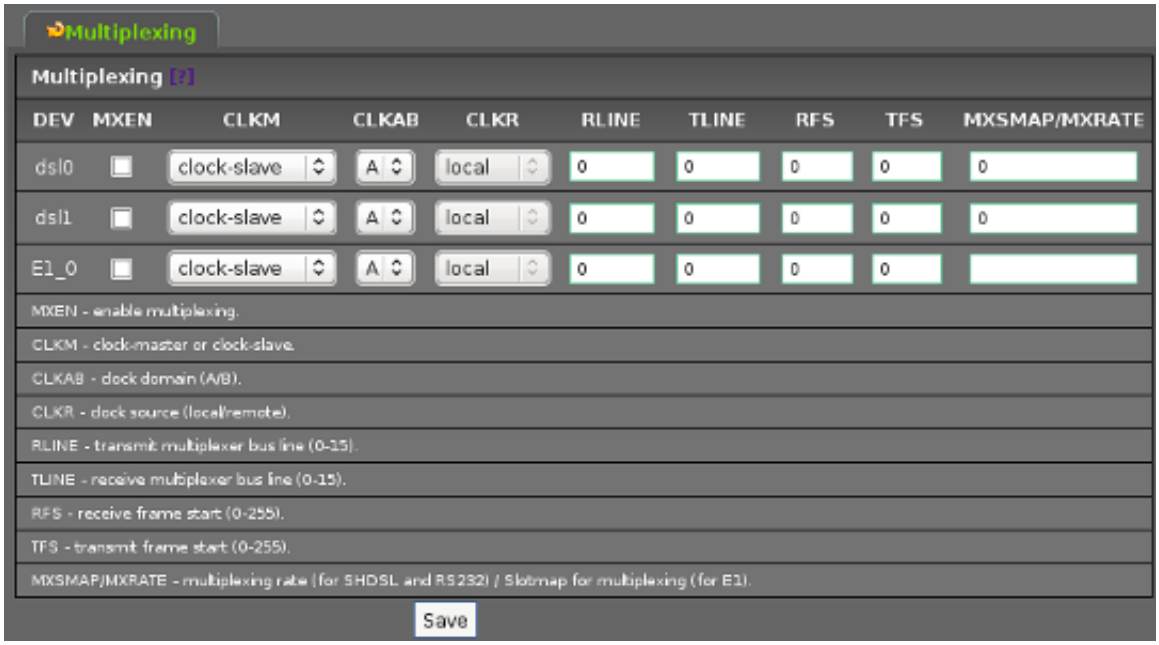
Router may have two sources defining the synchro-signal for multiplexing each of which defines a *domain*. Each line refers either to the domain A or to the domain B, and all the interfaces associated with this line also refer to one of the domains accordingly. Defining synchro-signal can be local or remote.

Important

One domain can have one and only one device (interface) controlling the clock signal! All other devices of the domain should be set in *clock slave* mode. Thus one device trigger all the devices of the given domain.

Below is a multiplexing confuguration page which is located at address Hardware/Multiplexing.

Figure 6.31. Multiplexing adjustment



- *MXEN* — interface participates in multiplexing.
- *CLKM* — synchronization of the interface:
  - *clock-master* — interface is the source of synchronization for the given domain.
  - *clock-slave* — interface functions as a receiver of synchronization.
- *CLKAB* — defines to which synchronizing domain the interface is related.
- *CLKR* — source of synchronization:
  - *local* — use local clock for timing.
  - *remote* — use external clock for timing.
- *RLINE* — number of line to which the interface will place the data received from the physical line.
- *TLINE* — number of line, from which the givn interface will take the data (placed by another interface participating in multiplexing) to transfer it to the physical line.
- *RFS* — number of the line time-slot starting from which the interface place the data on the line.
- *TFS* — number of the line time-slot starting from which the data can be taken from the line.
- *MXRATE* — number of time-slots for multiplexing (for SHDSL interfaces).
- *MXSMAP* — map of time-slots used for multiplexing (for E1 interfaces). This map should not be mixed with the map which is set while adjusting the E1 interface for IP-traffic transfer. The map should be set as "1-16", "16-31", ... type

Important

Time-slot in E1 can be used *only* for multiplexing or only for IP-traffic transfer. For this reason the time-slots map set for multiplexing using the parameter *mxsmap* should not coinside with the time-slots map set while E1 adjustment for use in IP-traffic transfer.

If while adjustment any mistakes were made, test information will be displayed:

```
Checking status:
Errors detected:

WARNING: Line2: timeslots 45 written but not read
WARNING: Line3: timeslots 55 read but not written
```

Chapter 7. Network interfaces adjustment

Common parameters

Network interfaces of web-interface are devided into two types: static and dynamic. To the group of static interfaces belong those which cannot be created or deleted, i.e. these are physical interfaces referred to certain hardware. To the dynamic interfaces belong those of bonding, bridging, VLAN, as these interfaces can be created and deleted, they are not physical, but use other interfaces for functioning.

This chapter considers common settings for all types of network interfaces.

Tip

At some interfaces there can be displayed the following statement on the top of the page: *This network interface is used for accessing the web interface*. This statement means that the access to the web-interface is performed via network interface, a page of which is open, and that the user should be careful while configuring in order not to lose control over the device.

Figure 7.1. Information message

Status tab

In the tab *Status* the basic information about the selected interface is given, and there is the option of shutdown/launching/restart of the interface.

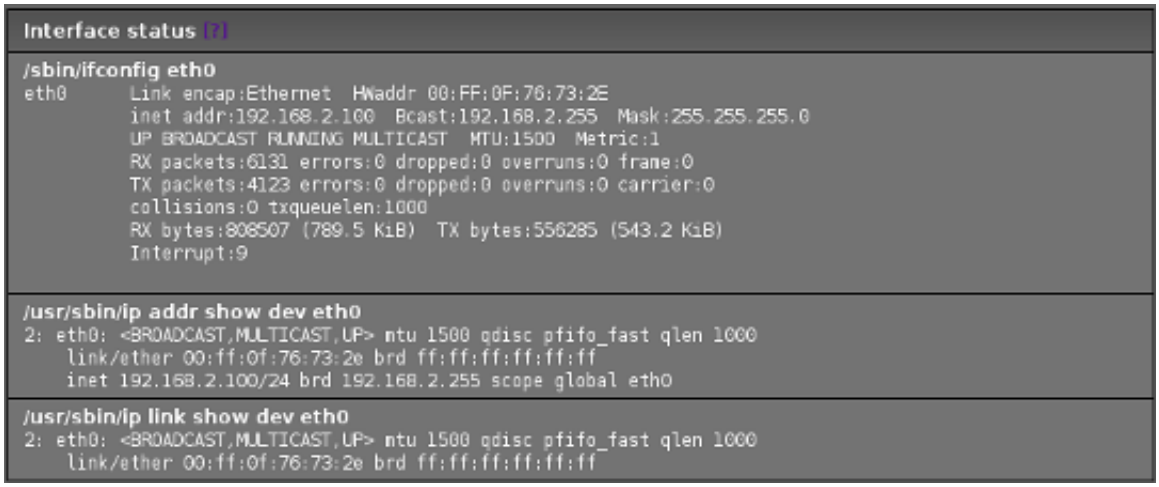
Interface management:

Figure 7.2. Interface management

- The button *Start* allows to launch ("advance") the interface, if the tab General is marked with "*enabled" flag*.
- The button *Stop* stops ("leave out") the work of the interface.
- The button *Restart* stops and then launch the interface.

Interface network settings information:

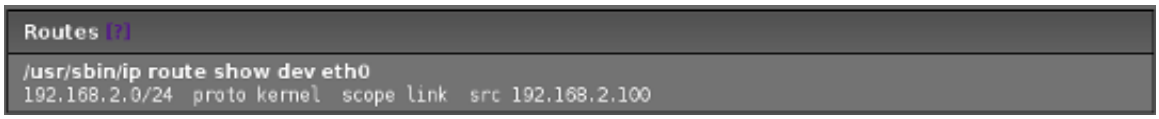
Figure 7.3. Network settings



Interface status (on/off) can be defined with the help of the flag row. If it contains the word *UP*, the interface is on (for example, *UP BROADCAST MULTICAST*).

Paths allocated to the interface:

Figure 7.4. Network paths

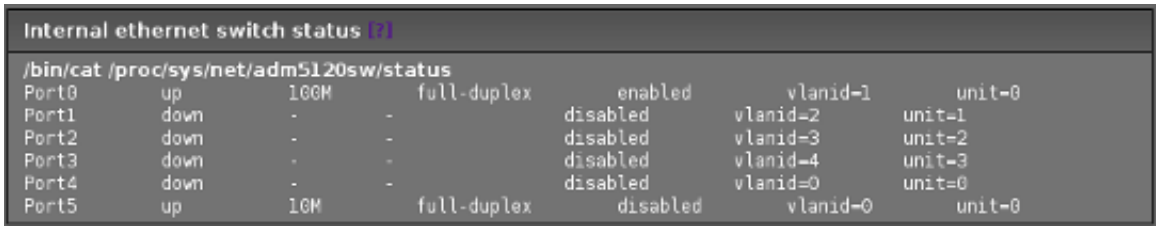


Data in ARP Table:

Figure 7.5. ARP Table

For Ethernet interfaces information about theinner switch performance:

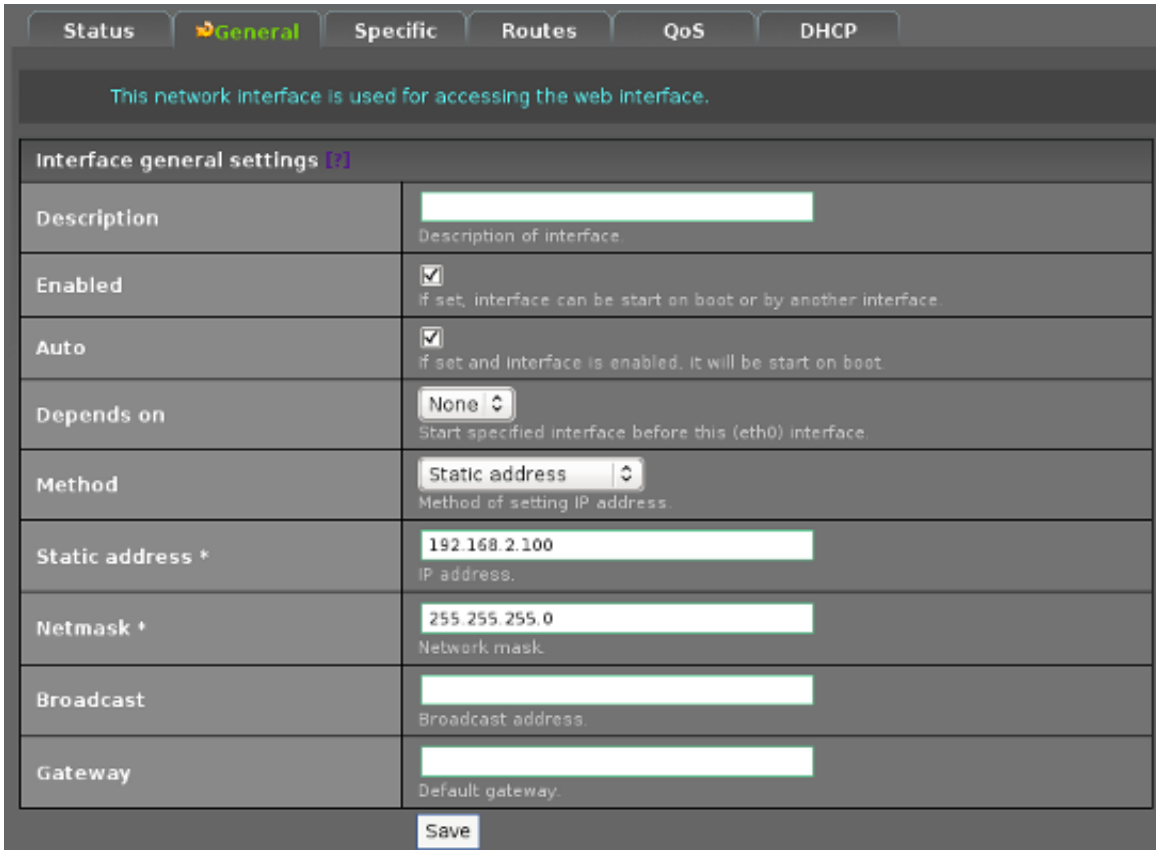
Figure 7.6. Inner switch



General tab

In the tab *General* you can activate a network interface, choose the way of IP-address setting, and, if necessary, set the IP-address.

Figure 7.7. Tab General



- *Description* — the description of the interface; used as a commentary to the interface..
- *Enabled* — the interface is active. It enables launching of the interface via another interface (bonding or bridging interface), but the interface will not be loaded while launching (for automatic launching of the interface select Auto). Particularly, the interface can be launched by clicking on *Start interface* in the tab *Status*.
- *Auto* — automatic launching of the interface. The interface will be launched while device loading or while saving the interface settings.
- *Depends on* — interface on which the given interface depends. When launching, the independable interface will be launched first.

  ## Note

  For VLAN interface this parameter is unavailable - for this interface its physical interface is always used.

- *Method* — IP-address allocation method.

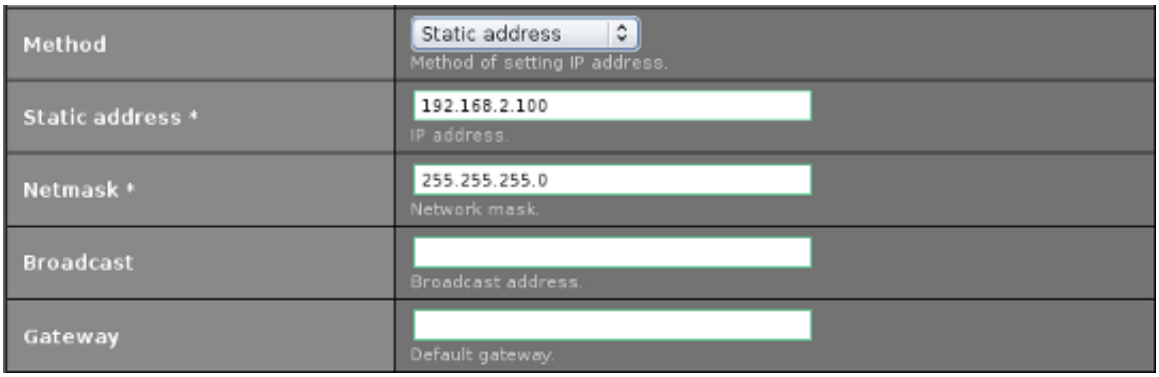
  ## Note

  For *E1* interface, when protocols other than *ETHER-HDLC* are used, there are only two available methods: none and Static address.

  - *None* — IP-address is not allocated.

- *Static address* — static, manual input.

Figure 7.8. Static method of IP-address allocation

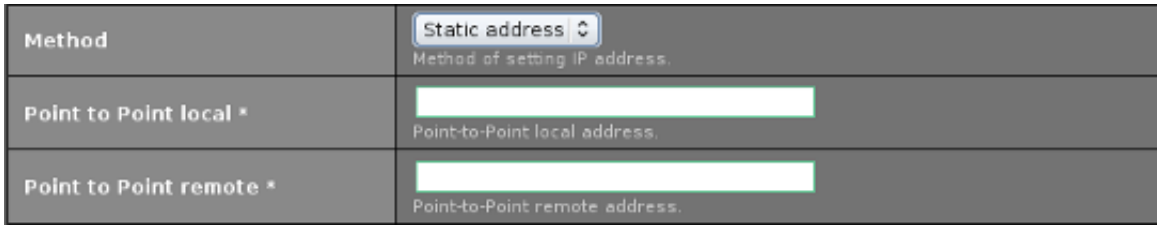


- *Static address* — the required IP-address in the following format xxx.xxx.xxx.xxx (for example, 192.168.2.100);
- *Netmask* — network mask in the following format xxx.xxx.xxx.xxx (for example 255.255.255.0);
- *Broadcast* — optional broadcast address of xxx.xxx.xxx.xxx format (192.168.2.255). If not specified, settled automatically while interface launching (browseable in the tab Status in the output of interface status);
- *Gateway* — path on default;

Note

For *E1* interface using protocols other than *ETHER-HDLC*, address is allocated in Point-to-Point format, i.e. IP-addresses of the local and the remote side are set.

Figure 7.9. Point-to-Point IP-address



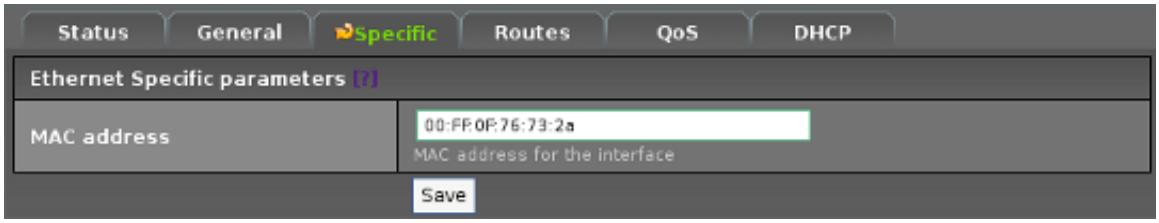
- *Point to Point local* —local IP-address (for the current device);
- *Point to Point remote* — remote IP-address (address of the device at the other end of E1 connection).

- *Zero configuration* — automatic way of ip-address allocation allowing configure a working network without manual allocation of IP-addresses and without DHCP servers. In this case the IP-address of the server will be chosen from the following diapason range: 169.254.*.
- *Dynamic address* — dynamic IP-address — allocated by DHCP server.

Tab Specific

This tab contains parameters specific for the given interface. For example, for the Ethernet-compatible interfaces (Ethernet, SHDSL, E1 in ETHER-HDLC mode etc.) here you can allocate a MAC-address. For bridging here there are settings specific for it.

Figure 7.10. Tab Specific

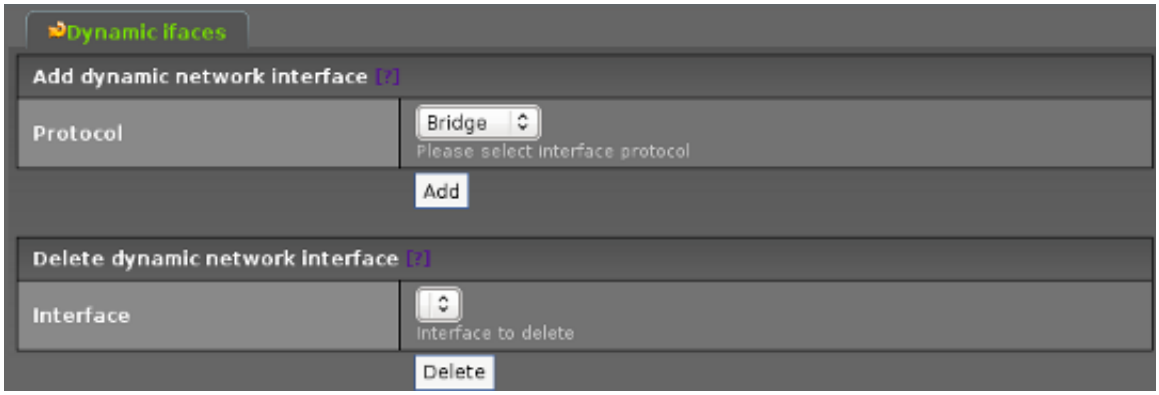


Dynamic interfaces

Work with dynamic interfaces

Dynamic interfaces managenets is carried out on page Network/Dynamic interfaces/Manage.

Figure 7.11. Dynamic interfaces

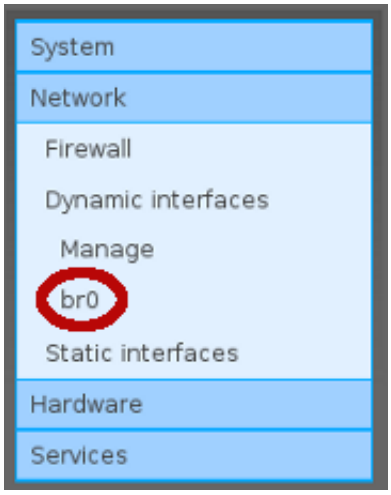


there exist the following types of the dynamic interfaces:

- *Bridge* — traffic transfer between interfaces at the second level;
- *Bonding* — increase of the connection capacity and reliability by means of using several interfaces;
- *VLAN* — interface of virtual networks: traffic isolation within the communication environment.

To create a new dynamic interface select its type and click *Add*. The added dynamic interface will be displayed in the list of network interfaces:

Figure 7.12. Dynamic interface in the list of the network interfaces



To delete the dynamic interface select its name in the list of interfaces and click *Delete*.

Settings of bonding

Bonding allows to band several physical connections into the logical one (by creating a dynamic interface - *bond*). For example, two SHDSL-channels can be banded into one, expanding the capacity and reliability of the connection.

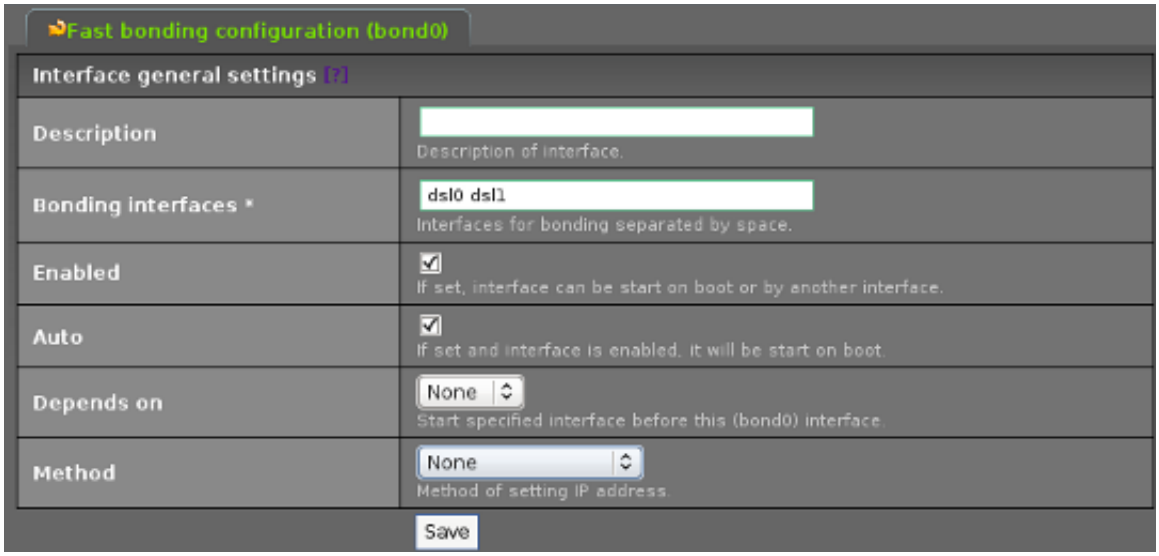
Important

In Bonding mode only ethernet-compatible interfaces can be banded. The Ethernet-compatible interfaces in the device are: Ethernet,SHDSL, E1 in ETHER-HDLC mode, and the interfaces of bonding, bridging, VLAN.

The dynamic interface of the bonding is created on page Network/Dynamic interfaces/Manage, where *the section Add dynamic network interface* the user should select "Bonding" and click *Add*.

After the interface is added, its name will be displayed in the menu Network/Dynamic interfaces/bond* (see the figure in the previous chapter). Besides, a window of the interface quick settings will be opened, where the user should set all the parameters necessary for interface launching:

Figure 7.13. Bonding quick settings window



In this window all the parameters, except one, were described in the previous chapter. The new parameter - *Bonding interfaces* - contains the interfaces enumerated with spacing which form the bonding.

Important

Physical interface can be added only to *one* interface of the bonding! For example, the interfaces bond0 (eth0, dsl0) and bond1 (eth1, dsl0) cannot be created because the dsl0 can be added only to one interface of the bonding. To break this limit use VLAN technology (see the relevant chapter with examples of use).

After the settings are saved, the interfaces, forming a bonding, will be adjusted automatically: for them *enabled=1 auto=0* is set. The IP-addresses of the existing interfaces, if they were set, will be reseted. One MAC-address corresponding to the MAC-address of one of the physical interfaces will be allocated to all the interfaces (dynamic and physical within it).

The settings can be altered on the interface adjustment page, in the tab General.

Note

The same settings should be made on the second router.

Note

When one of the physical connections is broken, traffic will be transferred via the remained connection.

Note

If you adjust several bondings, restart the device after setting. It is related to the fact that after the launching of the first bonding-interface, launching of new bonding-interfaces will be possible only after the restart.

Bridging settings

The operation of the device in bridging mode allows to transfer traffic between the interfaces transparently, simulating the function of a switch. For this purpose a special network dynamic interface with the name "*br"* is created, with which the network interfaces meant for traffic exchange are associated.

Important

In Bridge mode only ethernet-compatible interfaces are supported. The Ethernet-compatible interfaces in the device are: Ethernet,SHDSL, E1 in ETHER-HDLC mode, and the interfaces of bonding, bridging, VLAN.

Figure 7.14. Example of bridging

In the figure above the bridge is formed by two interfaces — Ethernet-interface eth0 and SHDSL-interface dsl0 — and joins PC1 and PC2 into a single network.

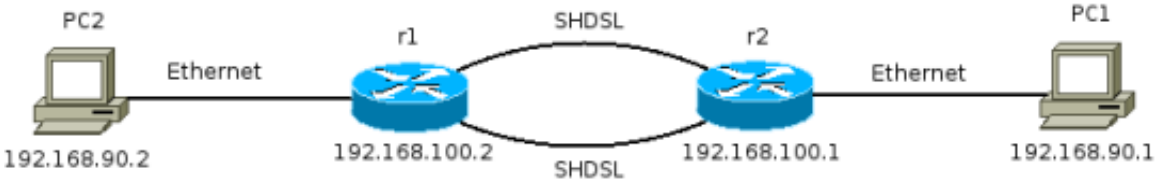
Note

It should be noted that the router operating in bridge mode and networks between which it transfers traffic do not need to be located in the same address space as it is required when traffic routing is being set.

Moreover, such router cannot have an IP-address. However, if the router management is needed, it is necessary to set an IP-address from the same network with the computer on which the management of the router will be performed. In our example the routers can have the following IP-addresses: 192.168.90.10 and 192.168.90.11.

The following figure shows a network analogous to the previous one, but with bonding that allows to expand the network capacity. In this case bridge is formed by the Ethernet-interface eth0 and bonded SHDSL-interfaces dsl0 and dsl1 into a single interface bond0:

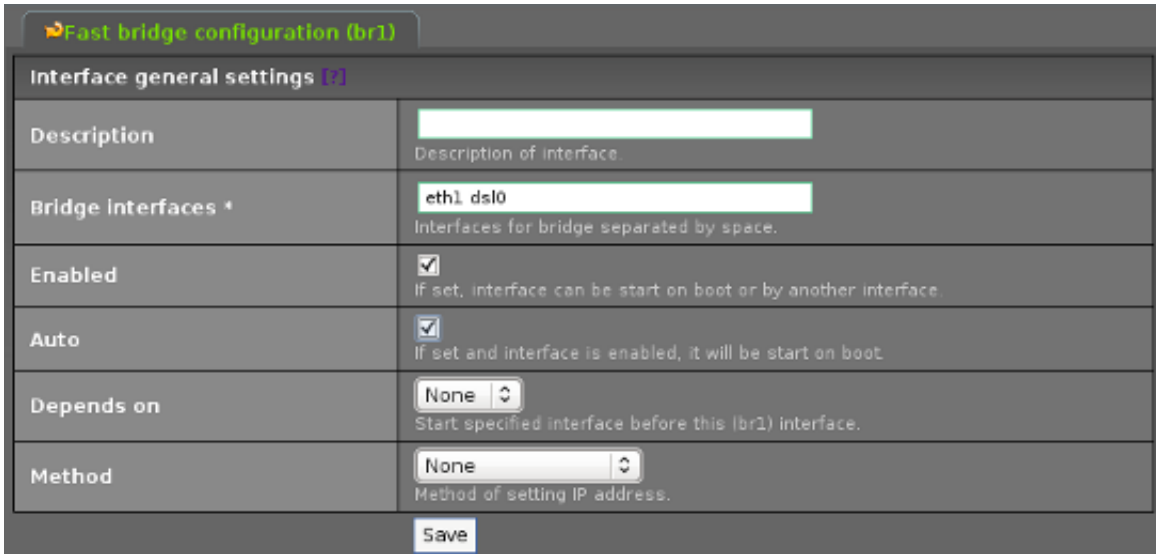
Figure 7.15. Example of a bridge with bonding



Creation of a dynamic interface of a bridge is performed on page Network/Dynamic interfaces/Manage, where "Bridge" should be selected as a protocol.

After the interface is added, its name will be displayed in the menu Network/Dynamic interfaces/br*. Besides, a window of the interface quick settings will be opened, where the user can set all the parameters necessary for interface launching:

Figure 7.16. Bridge quick settings window



In this window all the parameters, except one, were described in the previous chapter. The new parameter - *Bridge interfaces* - contains the interfaces enumerated with spacing which form the bridge.

Important

Physical interface can be added only to *one* interface of the bridge! For example, the interfaces br0 (eth0, dsl0) and br1 (eth1, dsl0) cannot be created because the dsl0 can be added only to one interface of the bridge. To break this limit use VLAN technology (see the relevant chapter with examples of use)

After the settings are saved, the interfaces, forming a bonding, will be adjusted automatically: for them *enabled=1 auto=0* is set. The IP-addresses of the existing interfaces, if they were set, will be reseted.

The settings can be altered on the interface adjustment page, in the tab General.

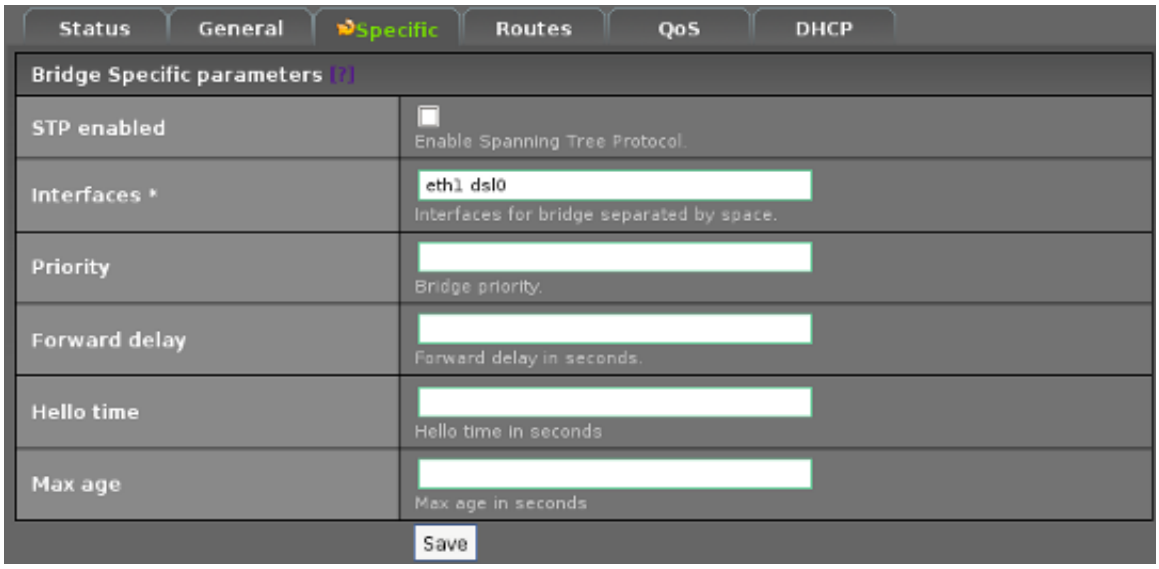
Important

Launching of *br** interface leads to reset of the IP-addresses of the physical interfaces which form the bridge. Therefore, if the setting is made via a physical interface which is a part of the bridge, the management of routers can be lost. To avoid this set an IP-address to the dynamic interface *br**.

The same procedure should be executed on the second device, and in a couple of minutes, during which the bridge recognizes the network topology and conduct a short procedure of self-learning, the packet-mode communication between the interfaces will begin.

Additional settings can be made for the bridge, which are available on page Network/Dynamic interfaces/ br*, tab Specific:

Figure 7.17. Additional parameters of bridge



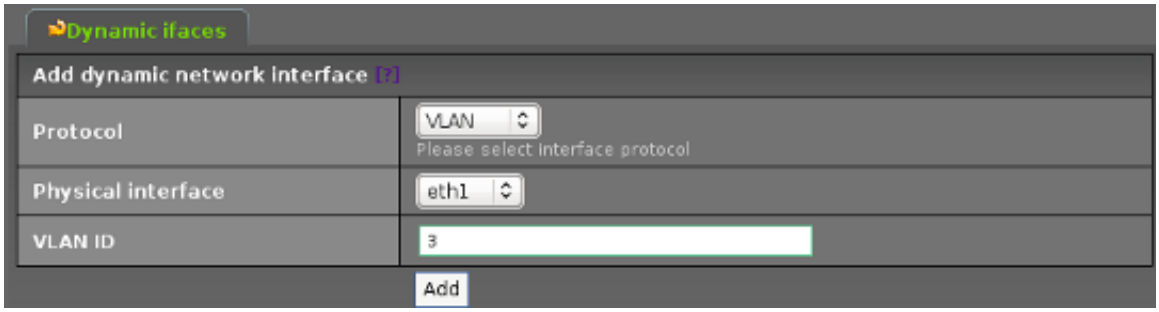
- *STP enabled* — enable Spanning Tree Protocol. The main target of the STP is to bring the Ethernet topology with its numerous interrelations to a state of a tree-type typology, eliminating the packet cycles. Is is performed by means of automatic blocking of redundant ports.
- *Interfaces* — interfaces forming the bridge.
- *Priority* — priority of the bridge, the less is the value, the higher is the priority. Used in STP.
- *Forward delay* — time which the bridge spends inListening and Learning modes before switching to Forwarding mode (working mode). In seconds. Used in STP.
- *Hello time* — time intervals between the sending of packets about the network topology. In seconds. Used in STP.
- *Max age* — if the hello packet does not come from the bridge after a *max age*, bridge is considered broken. In this case routes reconfiguration is possible. In seconds. Used in STP.

VLAN interfaces settings

The use of VLAN allows to divide traffic within a single communication environment. For this purpose in each Ethernet-slide a headline allocating the slide to this or that VLAN is added. Each VLAN is identified with its own number — *VLAN ID*, within the range from 0 to 4094. For work with VLAN networks a virtual interface VLAN is created on the base of a physical interface, having a certain VLAN ID.

In order to create a VLAN interface, it is necessary to create a dynamic interface VLAN at page Network/ Dynamic interfaces/Manage. For this purpose select the VLAN protocol, after which two parameters will be available:

Figure 7.18. Adding a VLAN interface



- *Physical interface* — physical interface on which basis the VLAN interface is created.
- *VLAN ID* — VLAN number.

Tip

VLAN interface may operate on physical interfaces (SHDSL, Ethernet), and on dynamic ones (Bonding, Bridge).

After the VLAN interface is added, it will be displayed in the list of interfaces as "InterfaceXvN", where InrefaceX — the name of the interface, N — VLAN number. For example, if the VLAN interface is created for the interface bond0 and VLAN ID 4, the name of the VLAN interface will be *bond0v4*. In the system the interface is desplayed as *bond0.4*.

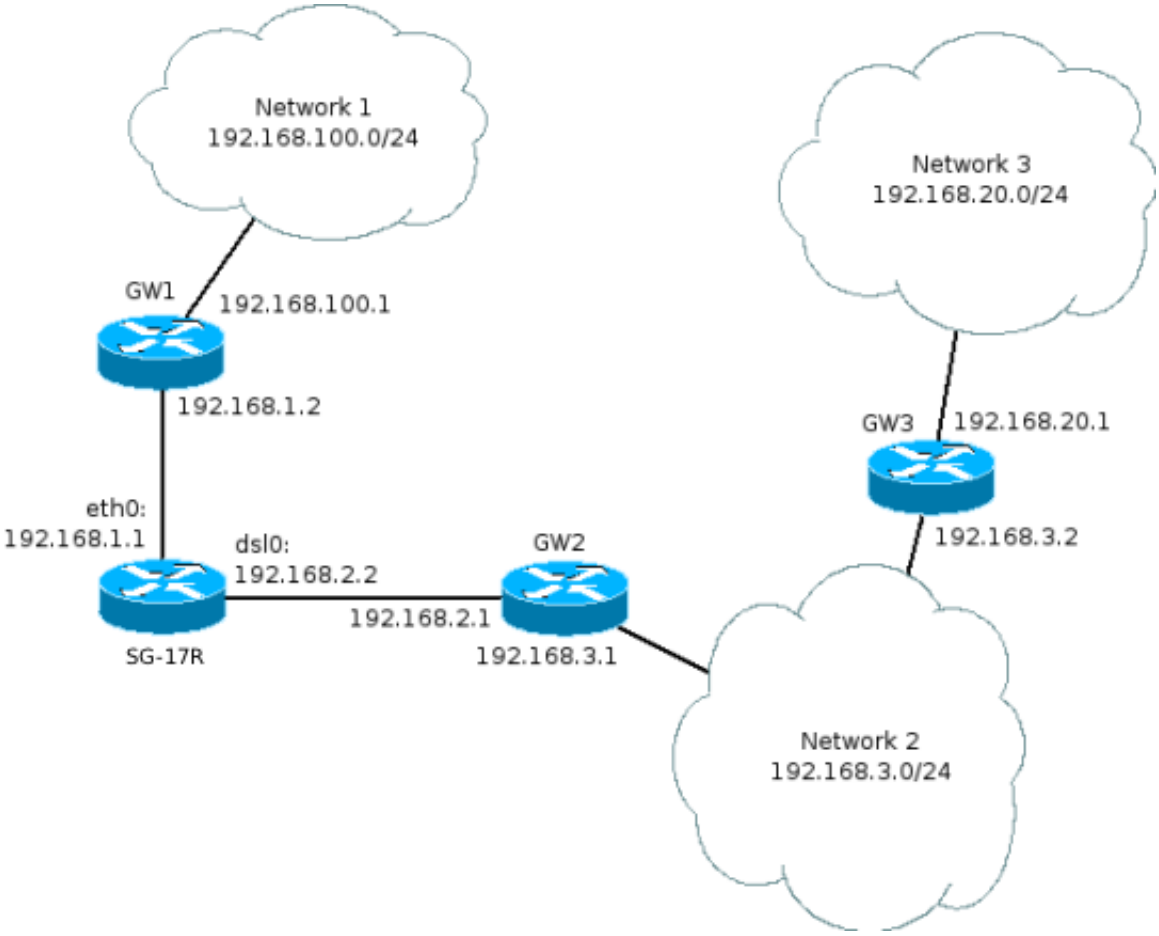
Now standard actions can be applied to the interface: set an IP-address, add it to bonding, bridge etc.

Chapter 8. Traffic control

Addition of network routes

Network routs define which routers give access to which network. Addition of network routes is made on adjustment page of the network interface through which it goes. For example, a network has the following structure:

Figure 8.1. Example: network structure



Our router has an identification name SG-17R, and is connected to two routers — GW1 and GW2 - over eth0 (Ethernet) and dsl0 (SHDSL) interfaces accordingly. It is obvious that the addition of the network routes will be the following:

- Network1: network 192.168.100/24 via the router 192.168.1.2 (interface eth0)
- Network2: network 192.168.3.0/24 via the router 192.168.2.1 (interface dsl0)
- Network3: network 192.168.20.0/24 via the router 192.168.2.1 (interface dsl0)

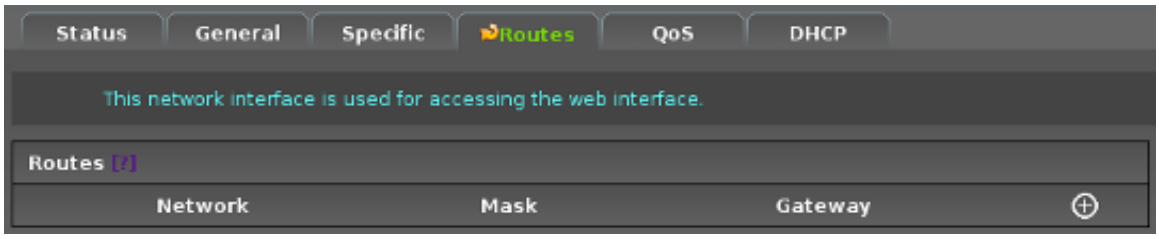
Analysing the routes we come to the conclusion that the route of the first network is referred to the interface eth0, of the second and the third — to dsl0. For this reason the addition of routes via web-interface will be made on the pages of the relevant interfaces.

Note

The route to the Network3 and Network 2 is added via the router GW2 as the router SG-17R does not have a direct connection to the router GW3 and is forced to address it via GW2.

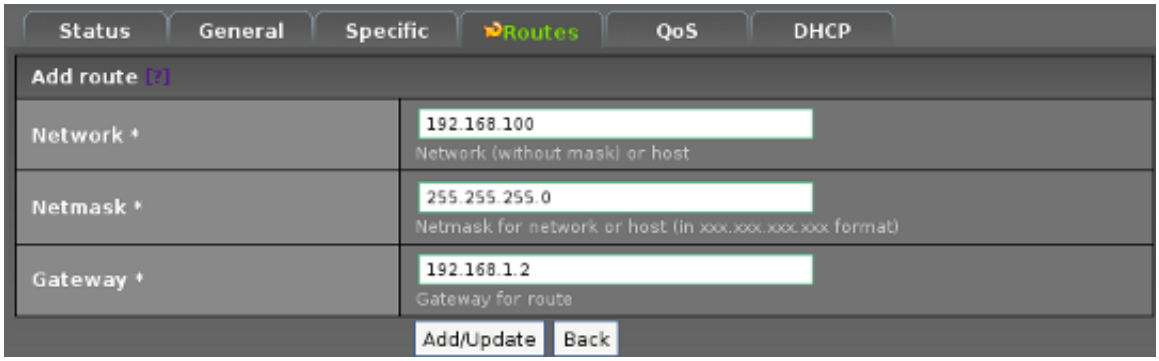
To add a route forward to the adjustment page of the interface corellating with the route (for example, Network/Static interfaces/eth0), where select the tab Routes:

Figure 8.2. Empty route list



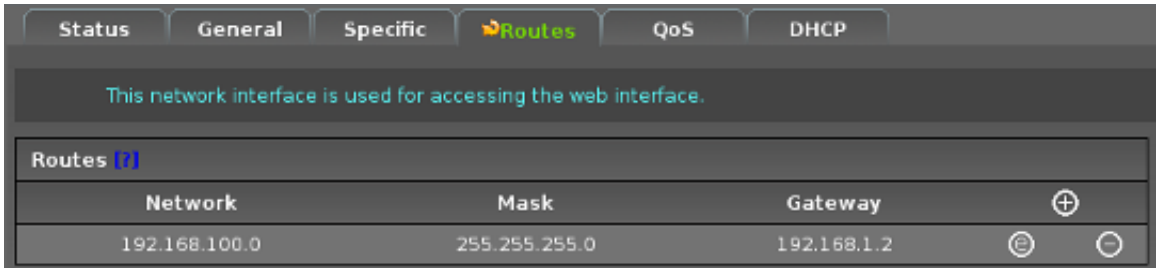
Initially the list is empty. To add a new route, click on "+" and fill the boxes in the new window:

Figure 8.3. Addition of a route



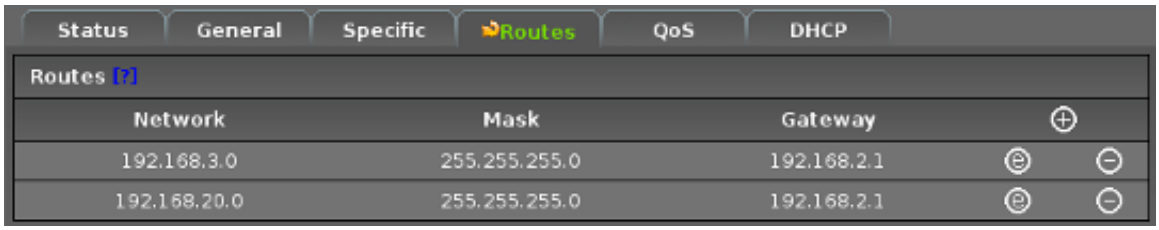
After the route is added, the information about it will be displayed in the table of routes:

Figure 8.4. List of routes for eth0 interface



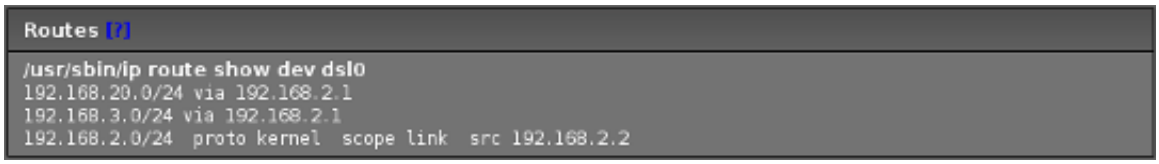
After the routes necessary for dsl0 interface will be added, its routes table will change to the following:

Figure 8.5. List of routes for dsl0 interface



The route registers in the system immediately after it is added. The user can check that the added routes are accepted correctly by the system on the tab Status, in the output Routes:

Figure 8.6. Check of the list of routes for dsl0 interface

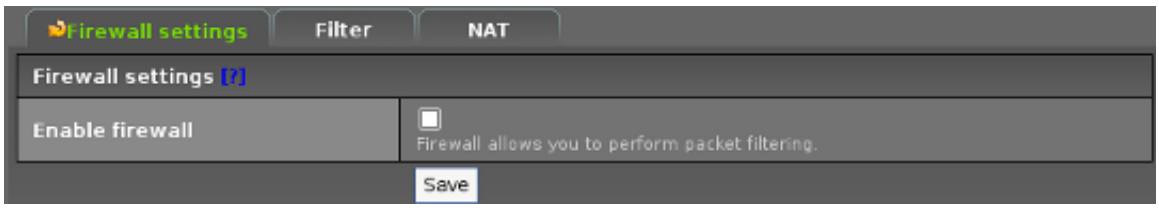


Firewall management

The firewall is used to limit the access to these or that network resources, basing on IP-addresses, ports of the sender and the addressee, or on the used protocol.

Firewall activation is made on the page Network/Firewall:

Figure 8.7. Firewall activation



Firewall functioning is based on the packet passing chains of rules, where each rule defines one of the action: packet accepting or dropping, basing on one or several criteria. Addition of the rules is carried out on the tab Filter. For each chain a default action is set - policy, i.e. in case if the packet does not complies with the criteria:

Figure 8.8. Policy of chains

Note

When implementing a policy in DROP value for the chain INPUT or OUTPUT, make sure that there are exist permitting rules, otherwise the router management can be lost.

The following actions are determined for a rule:

- *ACCEPT* — acception of a packet;
- *DROP* — dropping of a packet without notifying the source of the packet;
- *REJECT* — rejection of a packet with notification to the source;

The chain FORWARD is passed by transit packets, i.e. which are transferred from one interface of the router to another:

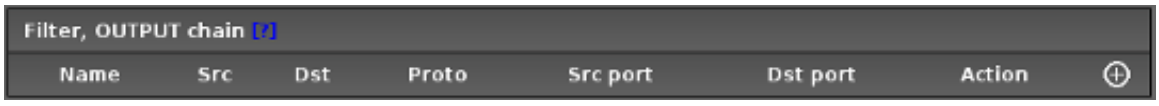
Figure 8.9. FORWARD chain

The chain INPUT is passed by packets addressed to the router :

Figure 8.10. INPUT chain

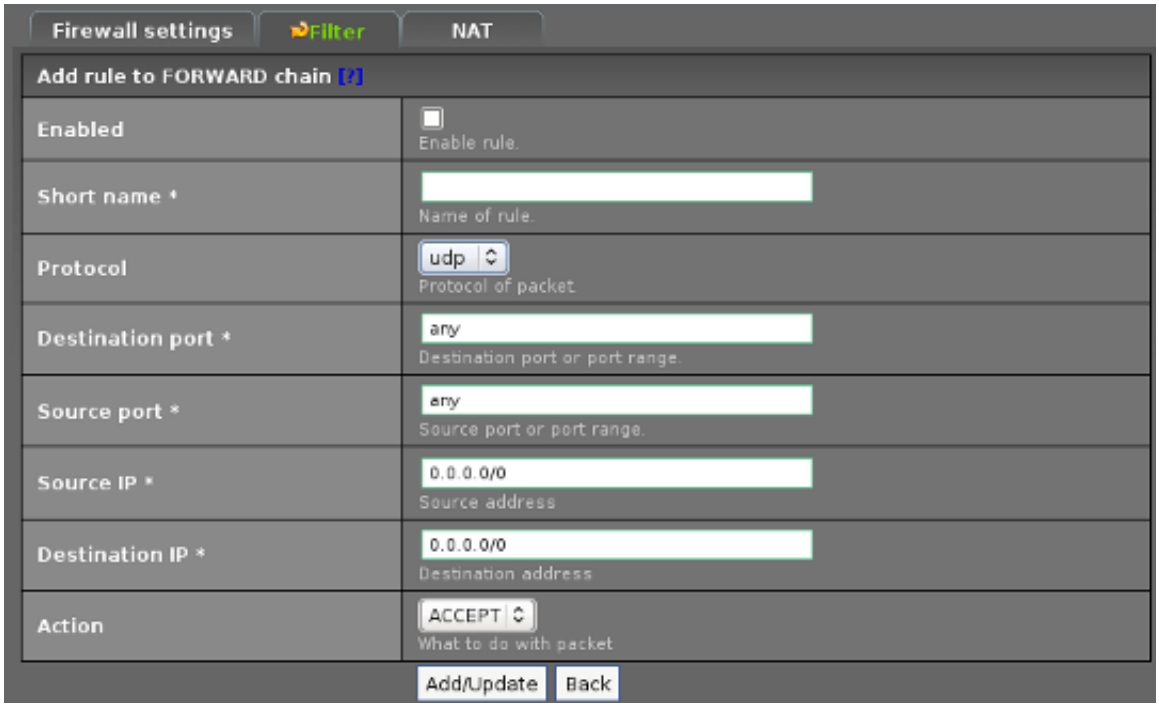
The chainOUTPUT is passed by packets which source is the router:

Figure 8.11. OUTPUT chain



Addition of rules is made by clicking on the"+" button, and filling the form opened in a new window:

Figure 8.12. Addition of a rule



- *Enabled* — the rule is active or not.
- *Short name* — the rule name. Should include only latin letters and cyphers.
- *Protocol* — For protocols *tcp*, *udp* additional settings are available:
  - *Destination port* — port of the packet addressee.
  - *Source port* — port of the packet sender.
- *Source IP* — IP-address or the network of the sender.
- *Destination IP* — IP-address or the network of the addressee.
- *Action* — action with the packet.

Note

If the changes were not implemented, check whether you have activated the firewall on page Network/Firewall.

NAT

NAT — network address translation — allows to change the source address or the destination address.

NAT is a part of the firewall, and the scheme of management is the same, only action is changed. For chains in NAT policies are set, i.e. actions for the packets satisfying none of the criteria:

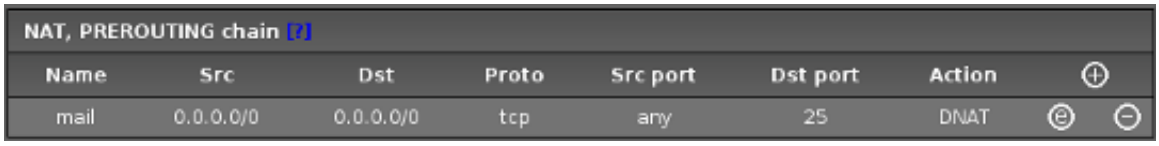
Figure 8.13. Policy of chains

Note

As far as in the PREROUTING chain go the packets intended for the router itself, before setting the DROP policy make sure that the chain contains a rule permitting the passage of packets for router management.

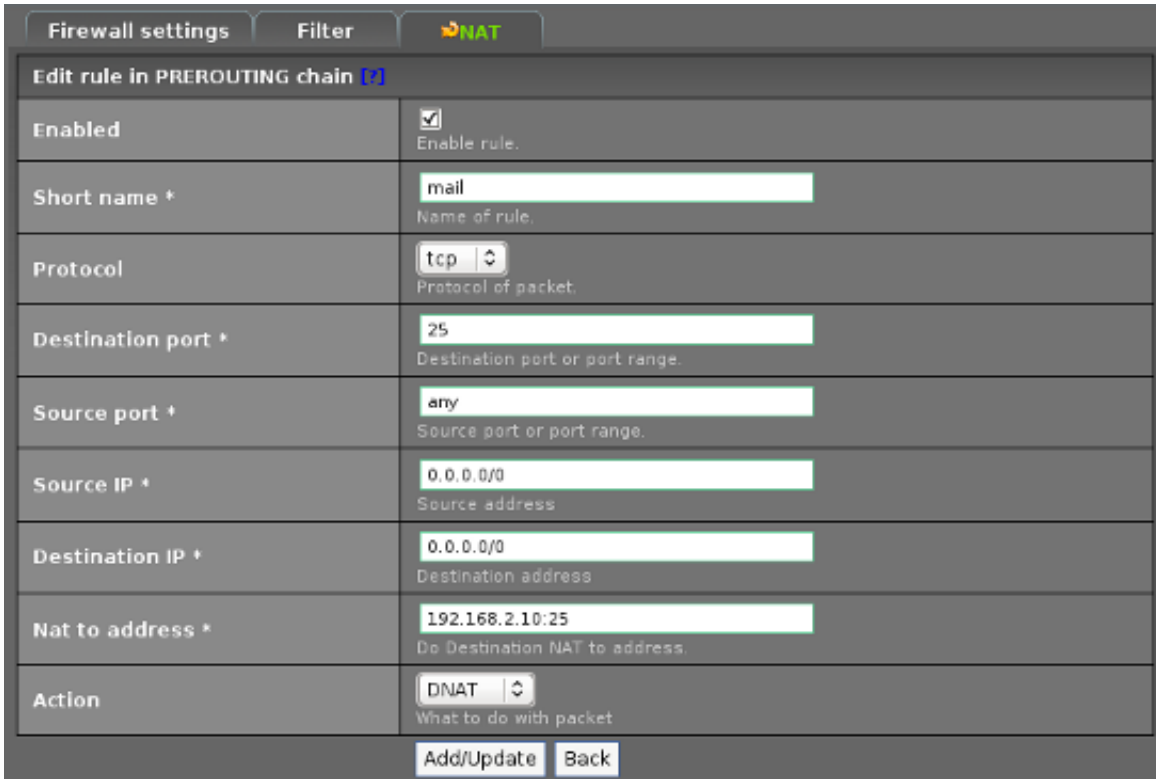
All the network packets, transit or intended for the router, go first to the PREROUTING chain, where several actions can be done to them. It is recommended to carry out a packet filtration procedure in this chain using the FORWARD chain for this purpose. The PREROUTING chain is intended for DNAT - destination NAT - performance, i.e. changing of the destination address .

Figure 8.14. PREROUTING chain



The window od addition is shown below.

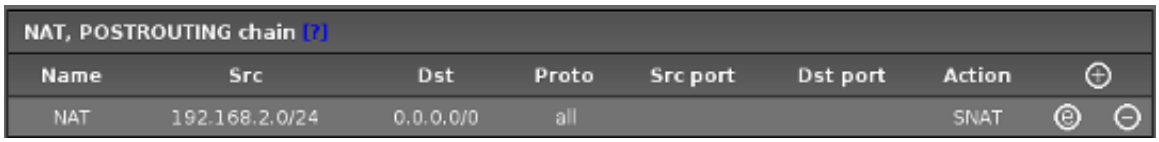
Figure 8.15. Addition of a rule to PREROUTING chain



When choosing the *DNAT* action, there appears a new option *Nat to address* — address to which the destination address of the packet should be changed. The user can either input the address only, or to indicate the address with the number of port separated with a colon (example 192.168.2.1:25).

The chain POSTROUTING is passed by the packets sourcing from the router, transit or generated on the router. In this chain a SNAT action can be performed - source NAT — change of the source address, or MASQUERADE — in which case the substitutional address will be generated automatically (useful for work with dynamic interfaces and IP-addresses).

Figure 8.16. POSTROUTING chain



Addition of a rule to the chain is similar to addition of a rule to the *PREROUTING chain*.

Note

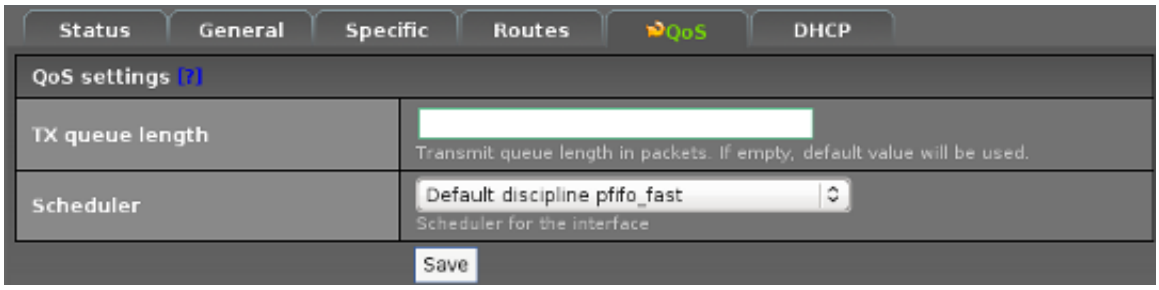
For NAT operation the firewall should be activated on page Network/Firewall.

Quality of service

Quality of service (QoS) allows to change the sequence of traffic pass at the interface. Different disciplines of service provide different opportunities of traffic classification and control.

QoS adjustment is done on the interface configuration page, QoS tab.

Figure 8.17. QoS setting



- *TX queue length* — outgoing queue of the interface, measured in packets. If no settings are made, the value on default is set for the interface automatically.
- *Scheduler* — discipline of traffic service.

Classless discipline pfifo_fast

Standard discipline of traffic servicing, realizing a simple mechanism First In First Out. Consists of three lines — 0, 1 and 2. The line 0 is served until it contains packets, queued for tranfer. Then lines 1 and two are serviced in the same way.

Traffic distribution along the lines can be performed by means of bit installation ToS — Type of Service, which is produced by the software generating the traffic or by means of the firewall. There exist fourToS bits:

- *Minimum Delay*;
- *Maximum Throughput*;
- *Maximum Reliability*;
- *Minimum Cost* — minimum channel cost;

Important

In currebt version of web-interface of the router installation of ToS bits by means of the firewall is not available. For this purpose the console interface of the router can be used.

Classless disciplines FIFO with bytes buffer (bfifo) and FIFO with packets buffer (pfifo)

The simpliest service disciplines. Do not have internal lines, all traffic is equal. Allow to obtain some statistics of their performance.

- *limit* — queue length, for bfifo — in bites, for pfifo — in packets.

Classless discipline SFQ

SFQ — Stochastic Fairness Queueing — fair planning discipline. It operates with such notions as "flow" — TCP session or UDP data flow, for each of which a separate pseudo-queue is created as a part of the

discipline. The discipline switches successively between the pseudo-queues (round robin), not allowing any of the flows to monopolize the channel.

For session distribution along the pseudo-queues hashes are used which need reconfiguration for the improvement of the discipline performance. The discipline is configured according to several parameters.

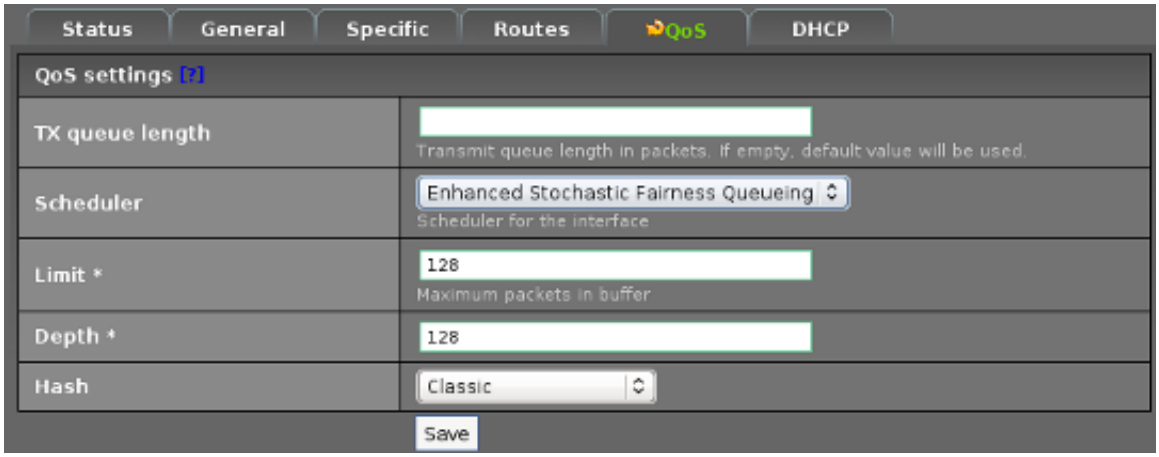
- *perturb* — time interval in seconds, in which hash reconfiguration is performed. Recommended value — 10.
- *quantum* — number of bytes, which are extracted from the queue during one "step" (before switching to another queue). On default equal to maximum transmission unit (MTU), and must not exceed it!
- *limit* — number of packets which can be queued. In case the number is exceeded, packets will be dropped.

When installing the SFQ discipline to web-interface, the above mentioned settings are made automatically taking into account the recommended values.

Classless discipline ESFQ

ESFQ — Enhanced Stochastic Fairness Queueing — improved SFQ discipline. It provides more opportunities for setting, which allows more equal distribution of the bandwidth. For example, if the user launches programs operating in several flows, the usual SFQ becomes ineffective, as it cannot divide the channel between the users. ESFQ discipline allows to choose another algorithm of hashing, for example, using the source IP-address or the destination IP-address, which allows to distribute different users to different pseudo-queues indepandable of the number of sessions for each user.

Figure 8.18. ESFQ configuration



- *Limit* — number of packets that can be queued. In case the number is exceeded, packets will be dropped.
- *Depth* — maximum number of pseudo-queues (in SFQ this number is strictly limited to 1024).
- *Hash* — hash type.
  - *Classic* — analogous of that used in SFQ.
  - *Source address* — address of the sender.
  - *Destination address* — address of the recepient.

- *perturb* — time interval in seconds in which the hash reconfiguration is performed. Recommended value - 10 (when installing the discipline via web-interface the recommended value is set automatically).

Classless discipline TBF

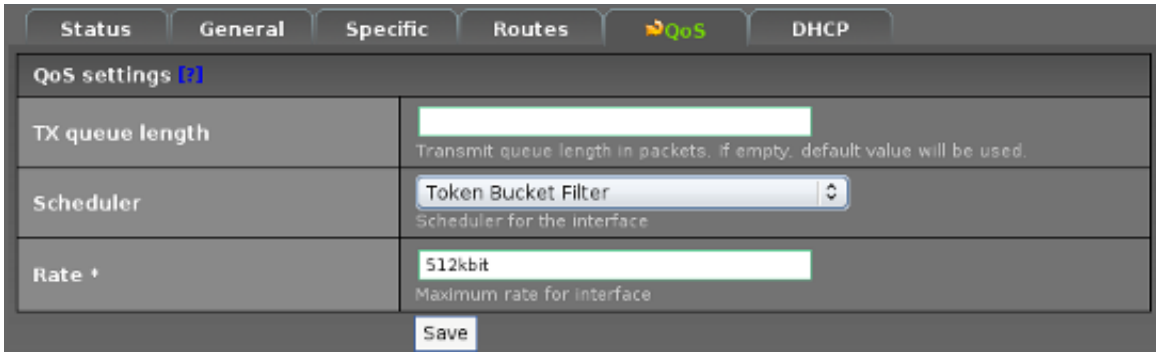
Token Bucket Filter (TBF) — a simple classless discipline, which transmits the coming packets at a bitrate not exceeding the set value. This discipline is very economical in terms of system resources, therefore it is a best choice when it is needed just to limit the speed of the outcoming traffic.

The essense of the discipline is the following. Packets coming for tranferring are capture in discipline buffer, from which they are transferred to the outgoing interface at a pre-set speed. The three situations are possible:

- Packets come at the speed equal to the speed of their transferring to the outgoing interface. In this case the packets go through the interface without any delays.
- Packets come at the speed less than the speed of their transferring to the outgoing interface. In this case during short periods of increase in the incoming traffic speed it will be accumulated in the incoming queue and then transmitted at the pre-set speed.
- Packets come at the speed exceeding the speed of their transferring to the outgoing interface. In this case the packets will begin to drop after a while.

Discipline has several parameters allowing to manage its performance:

Figure 8.19. TBF configuration



- *Rate* — speed at which the incoming traffic is transmitted to the outgoing interface.

Class-specific discipline HTB

The HTB discipline allows to separate different throughput of the channel for different types of traffic. It is done by means of traffic distribution along different classes, each of which has a pre-set throughput value. The traffic classification can be done on the basis of IP-addresses or source/destionation ports. This type of traffic processing (limitation of its speed) is called *shaping*.

First of all it should be noted that the user can control the speed only of the outgoing traffic (which is reasonable), therefore it is important to define the interface at which the traffic will be outgoing correctly, when adding the rules of shaping.

Realization of QoS on the basis of the class-specific discipline HTB consists of two steps — class definition and traffic distribution in classes according to certain criteria using filters. Classes defining the traffic speed can be added either to the root, or to other sublasses, forming a hierarchy of classes. Filters are added into the root of the hierarchy.

Tip

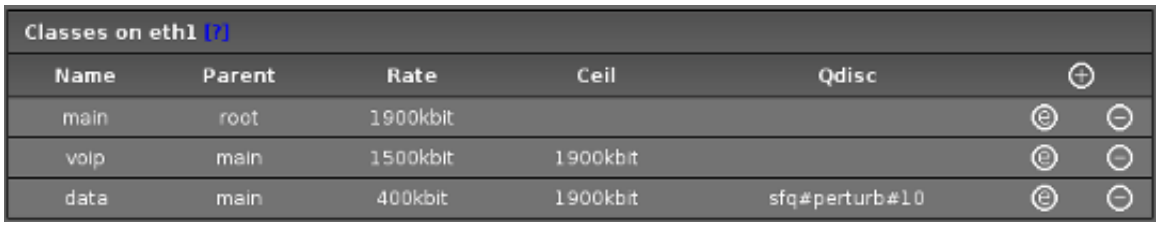
The peculiarity of classes consists in fact that the speed of one subclass can be increased (withing the value of the parent class speed) due to *unused* speed of another subclass.

For the discipline a class can be created to which all the traffic not complying with any filter will be transmitted.

Figure 8.20. Class on default

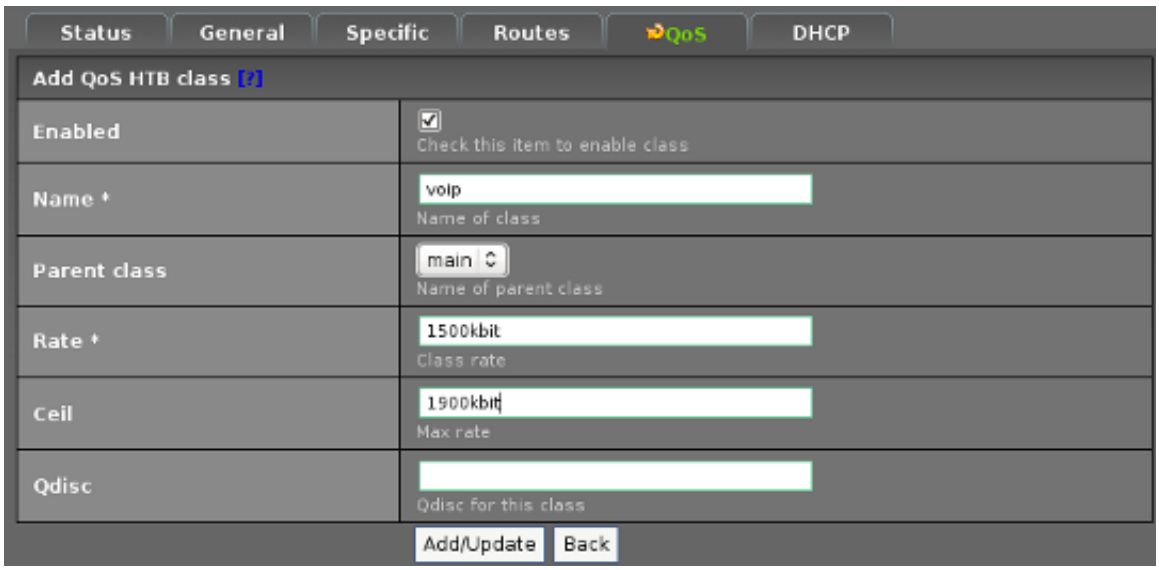
The table below contains information about classes. Optionally, for each class can be added own classless discipline of service described above.

Figure 8.21. Traffic classes



Class addition window is shown below.

Figure 8.22. Addition of a class



- *Enabled* — the class is active or not.
- *Name* — name of the class being added. Used for traffic classification in filter.
- *Parent class* - root class. When a class is added into a non-root class - it is called *subclass*.

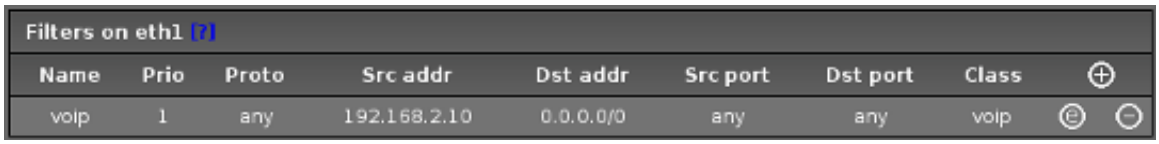
- *Rate* — throughput of a class. Should not exceed the speed of the parent class!
- *Ceil* — maximum throughput of a subclass (in case when another subclass of the same class does not use the full volume of the throughput given to it). Should not exceed the speed of the parent class!
- *Qdisc* — an optional classless discipline of class service. Here the name of the serviced discipline and its parameters can be indicated, for example: **esfq#limit#128#depth#128#divisor#10#hash#classic#perturb#15** or **sfq#perturb#10**, etc. Spacing should be substituted with # symbol. The detailed information about the classless disciplines and their parameters is given above.

To avoid the confusion, let`s pay attention to the abbreviations conventional for QoS which describes the rate:

- mbps = 1024 kbps = 1024 * 1024 bps => byte/s => 1024 kbytes/sec.
- mbit = 1024 kbit => kilo bit/s => 1024 kbit/sec.

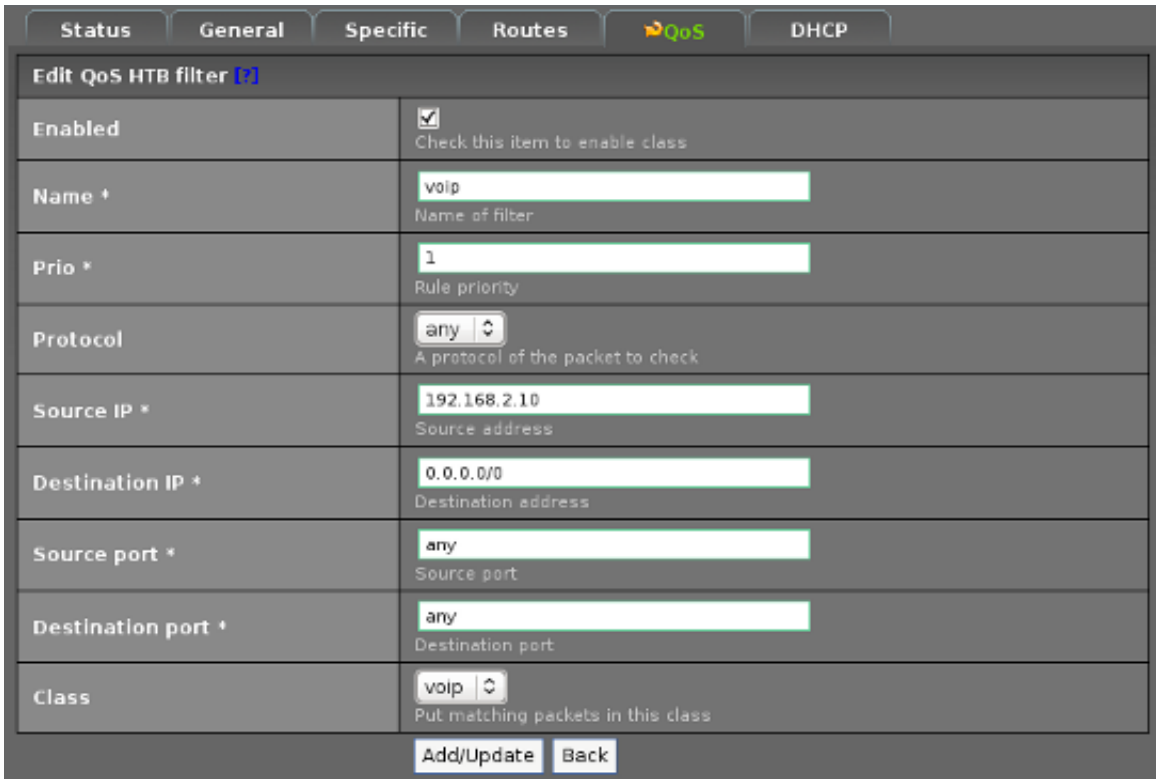
Table of filters dividing traffic into classes on the basis of certain criteria.

Figure 8.23. Filters dividing traffic into classes



A filter creation window is shown below.

Figure 8.24. Addition of a filter



- *Enabled* — the filter is active or not.
- *Name* — name of the filter.
- *Prio* — priority of the filter. The less is the value — the higher is the priority.
- *Protocol* — traffic classification according to protocol.
- *Source IP* — traffic classification according to source address.
- *Destination IP* — traffic classification according to destination address.
- *Source port* — traffic classification according to sourse port number.
- *Destination port* — traffic classification according to destination port number.
- *Class* — to which class the packet should be referred.

The configuration describes in the figures has one class - *main* - and two subclasses: *voip* and *data*. The subclass *voip* is used for high priority traffic, at the rate of 1500 to 1900 kbit/sec. The subclass *data* is used as a default class for all other traffic. Its rate value - 400 to 1900 kbit/sec.

All the traffic coming from the node 192.168.2.10 is transmitted to the *voip* subclass.

Chapter 9. Network services settings

DHCP server

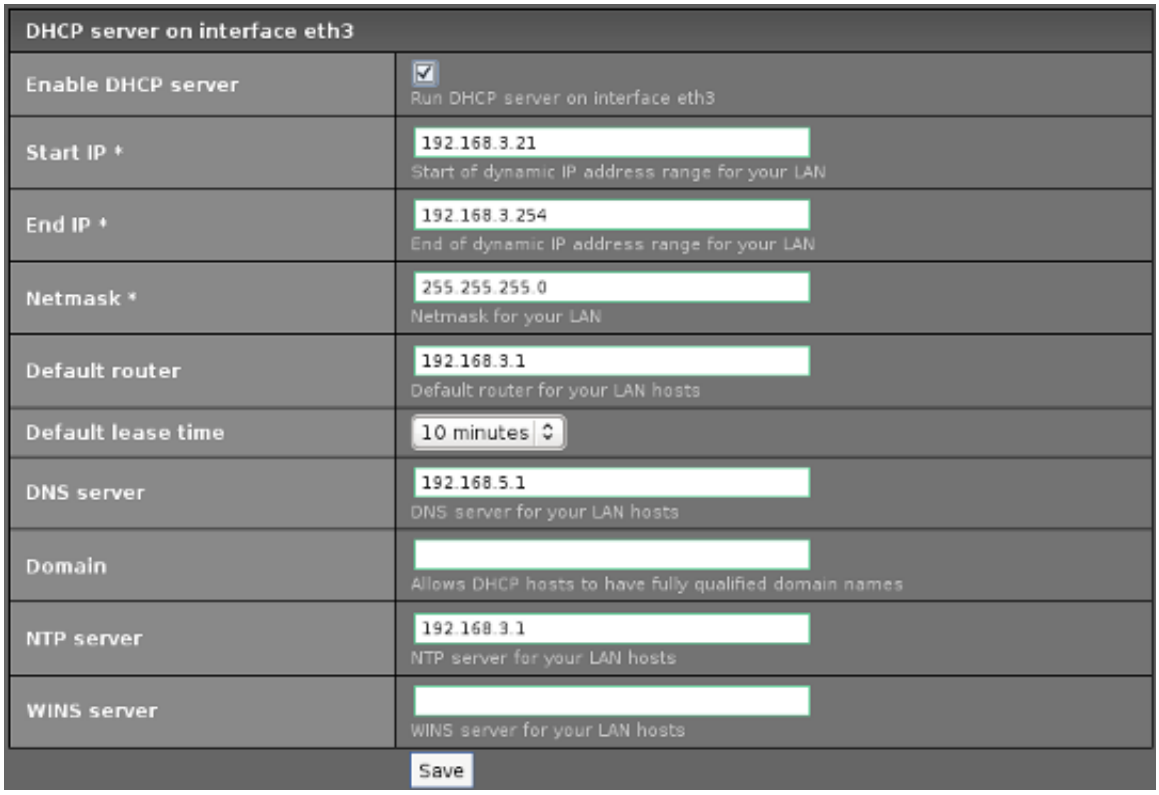
Adjustment of DHCP server is performed for each network interface independently, and is made at network interface adjustment page, DHCP tab, or Services/DHCP Server.

Important

Before DHCP server activation, it is necessary to launch the interface (select the flags *Enabled* and *Auto*) at which it will work, and set an IP-address for the interface.

DHCP server adjustment page is shown below.

Figure 9.1. DHCP-server adjustment



- *Enable DHCP Server* — activate a DHCP-server for the given interface.
- *Start IP, End IP* — the extremes of the diapason for allocation of IP-addresses for DHCP clients.
- *Netmask* — network mask, to which IP-addresses are allocated.
- *Default router* — route on default.
- *Default lease time* — time for which an IP-address is allocated. Upon the expiry of the time, the client should refer to the DHCP-server again to approve the previously given address or to get a new one.

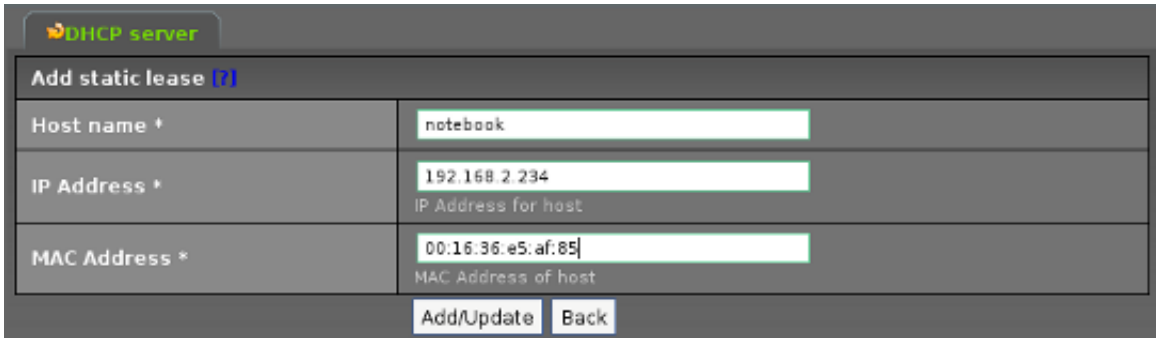
- *DNS server* — IP-ddress of the DNS-server, to which the client will refer to get domain names permission.
- *Domain* — domain to which the DHCP-server client will enter.
- *NTP server* — IP-address of the exact time server.
- *WINS server* — IP-address of the WINS-server.

Note

After the settings are saved, the DHCP-server will be started or restarted automatically.

There is a possibility of allocation of static IP-addresses to certain devices. The identification of the devices is done according to the MAC-address of the network adapter. The form of allocation of an IP-address to a MAC-address is located in the bottom of the adjustment page and is shown in the figure:

Figure 9.2. IP to MAC allocation form



- *Host name* — defines the name of the device to which the address in allocated. This value is of informational character and is used only in the rule, may not coinside with the actual name of the device.
- *IP Address* — IP-address which will be allocated to the device
- *MAC Address* — MAC-address of the network adapter of the device, to which an IP-address will be allocated.

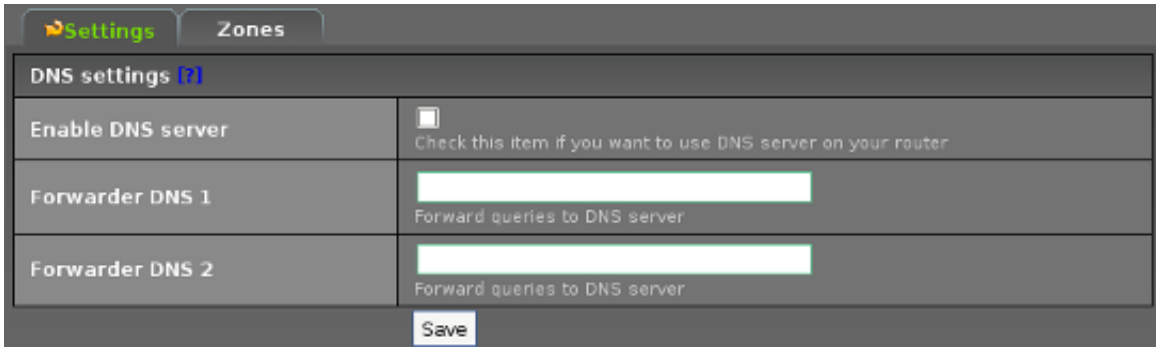
After the changes are saved, in the table of static addresses a new entry will appear.

Figure 9.3. Updated list of IP-addresses

DNS server

DNS server is responsible for the transformation of a domain name to an IP-address. Its setting is made at the page Services/DNS server.

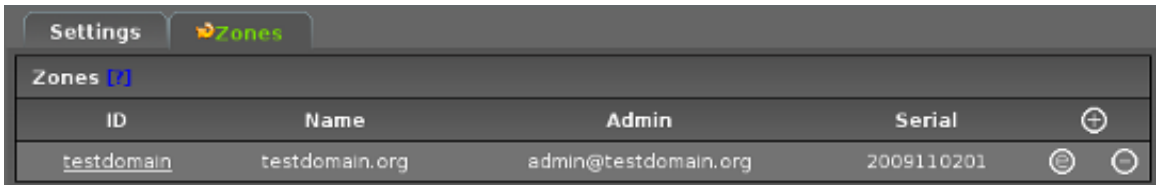
Figure 9.4. DNS server settings



- *Enable DNS server* — activate the DNS server.
- *Forwarder DNS 1* — server DNS 1, to which the queries should be redirected in case the local DNS server does not respond.
- *Forwarder DNS 2* — server DNS 2, to which the queries should be redirected in case the local DNS server or DNS server 1 do not respond.

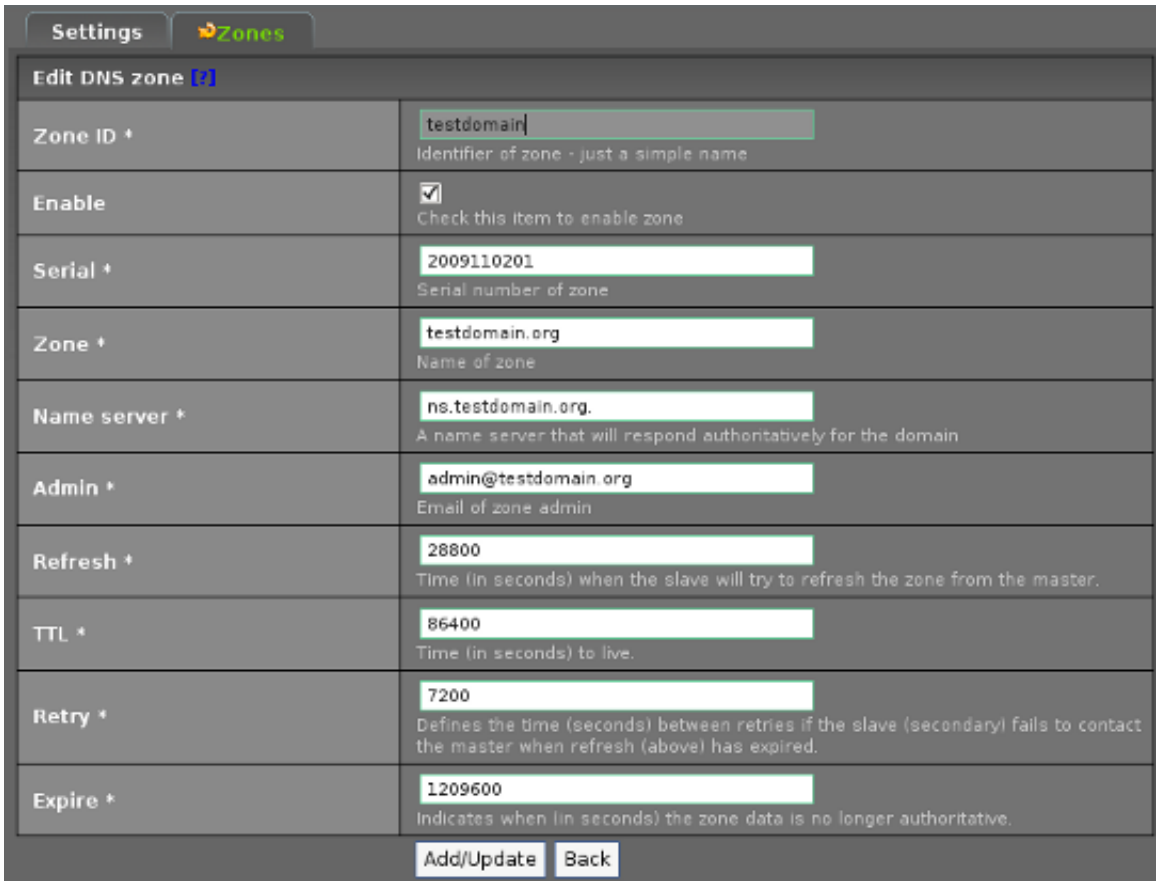
This DNS server can be used as an authoritative server of the domain, i.e. keep information about the domain records (NS, A, CNAME, ...). For this purpose there should be created a zone file, in which the information about the domain and its records would be kept.

Figure 9.5. DNS server zones



Creation and editing of the zone file is performed on the tab Zones with the help of relevant buttons.

Figure 9.6. Addition of a zone

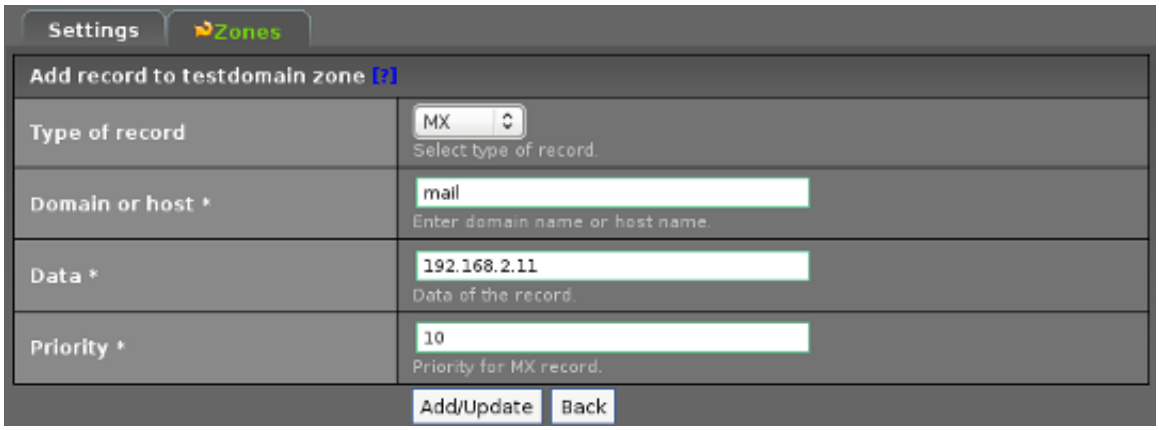


- *Zone id* — zone indentifier (the identifier names the file in which the zone is held). This parameter is set while zone creation, it cannot be edited after that.
- *Enable* — the zone is active or not.
- *Serial* — zone serial number. After evry edition of the zone file the serial number should be enlarged in order that DNS servers could see that the alternations were made in the zone. It is convenient to use a date of editing - year, month, day - plus a two-digit number denoting the number of the edition for this day.
- *Zone* — zone name (the domain name for which a zone is created).
- *Name server* — authoritative DNS server for the domain. If in this box the full domain name of the server is indicated, it should end with a dot: *ns.testdomain.org.*, otherwise a name of the current zone.
- *Admin* — zone administratoe e-mail address.
- *Refresh* — intervals in which DNS slave servers will update the zone.
- *TTL* — cach atorage period of a zone record.
- *Retry* — intervals in which the slave server will retry the zone update in case of failure.
- *Expire* — period after which the zone data is not considered actual any more.

After an addition of a zone, the relevant entry will appear in the table of zones.

Forwarding to the zone records creation page is made by clicking on the zone identifier whicn is underlined. As a result, a page with a table containing the records for the zone will be opened. The form of creation of a new record is given below.

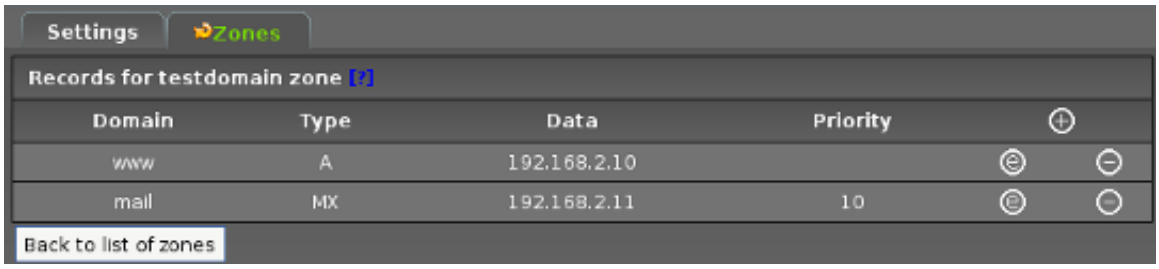
Figure 9.7. Addition of a record to the zone



- *Type of record* — The following values are available:
  - *A* — shows the IP-address corresponding to the name.
  - *CNAME* — a synonym of another name. In this case the corresponding name is indicated as the DATA.
  - *MX* — nae of mail server for the domain. If this record type is chosen an additional parameter is available.
    - *Priority* — priority of the MX record.
  - *NS* — indicates the authoritative DNS server of the domain (in point of fact - domain delegation).
  - *PTR* — indicates a name for the given IP-address. Used in the inverse zone.
  - *TXT* — additional textual information.
- *Domain or host* — domain name (or the IP-address, for inverse zones).
- *Data* — record data— domain name or IP-address, or some textual information.

After saving, a new record for the zone will be displayed in the table.

Figure 9.8. Table of zone records



In order to return to the list of zones click on *Back to list of zones*.

Chapter 10. VoIP

General information

The device allows to arrange the IP-telephony using modules MR-17V which can be complete with submodules having FXO (SMR-17Vo), FXS (SMR-17Vs) or Voice Frequency (SMR-17Vf) ports.

- *FXO* — connection to the public telephone network (PSTN) or to office PBX.
- *FXS* — commutation of telephone apparatuses.
- *VF* — commutation of voice frequency equipment.

When working with VoIP, the router must have a unique three-digit number which is used for addressing it from the side of other routers. For each router, the interfaces of the VoIP module (FXO/FXS/VF) have unique two-digit channel numbers which allow to identify it for call receiption and initiation.

Numbers used for calls via the router look as follows:

xxxyy[zzz...], where:

- *xxx* — the number of router.
- *yy* — the number of channel.
- *[zzz...]* — an additional number, for example, when calling via PBX.

For example, if the number of the router is 100, and we want to call to its second port, then dialling number from phone connected to this router or to another one looks as follws: 10002.

Also, when dialling number from phone connected to the router, the following codes are available:

- Instead of the router number you can dial:
  - * — calling to the own router;
  - # — calling to a number from the address book.
- Instead of the channel number you can dial:
  - * — calling to the first unoccupied FXO port;
  - # — calling via SIP-server (only for the abonents registered at SIP-server, indicated in settings. In order to call to an abonent of another SIP-server - it is necessary to add them to the address book and make calls through it).

For calls to other routers an IP-address of the router should be received according to its number. For this purpose the routing table is used, where the correlations between the router number and its IP-address are stored. The content of the table is usually similar for all the routers of the network.

In order to speed up the dialling of frequently used or long numbers, the address book is used. A short number for speed-dial (with «#» before the number) and the corresponding full number should be added to the address book.

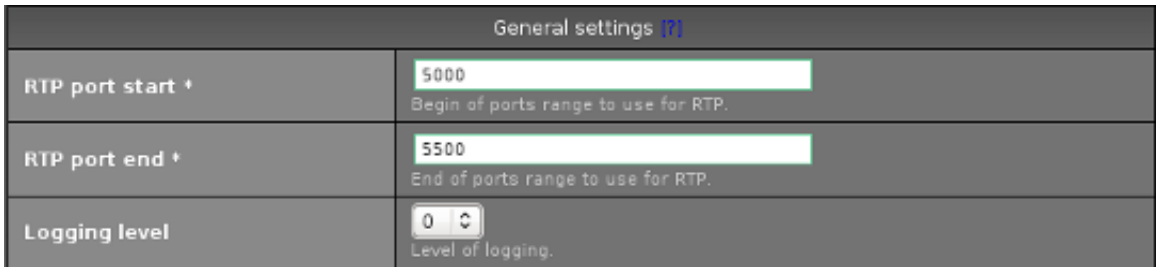
In the IP-telephony software the Hotline mode support is realized. The essence is the following: when answering the phone connected to a FXS port, a special background process (daemon) may start automatic dialling of the recorded number. When a call is incoming to a FXO port (connected to PSTN or PBX), daemon can redirect the call from one port to another or to a specified port of another router.

When adding full numbers to the address book table and Hotline table, the use of a special symbol «,» is accepted - it denotes a second delay when dialling the number.

Setting of basic parameters

Basic settings of VoIP are made at the page Hardware/VoIP/Settings. There are several groups of settings at the page. We will describe them one by one.

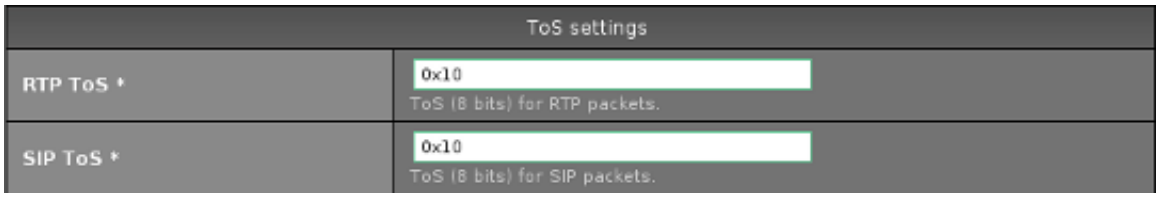
Figure 10.1. Basic settings of VoIP



- *RTP port start* — begining of the range of numbers of portes used by the device when sending RTP traffic (UDP protocol is used).
- *RTP port end* — end of the range of numbers of portes used by the device when sending RTP traffic (UDP protocol is used).
- *Logging level* — level of detailization of diagnostic messages.

As far as the VoIP traffic is sensitive to delays, there is a possibility of setting of the needed bit valuesType of Service. On default the value 0x10 is used meaning the minimal delay of traffic transfer.

Figure 10.2. ToS settings



- *RTP ToS* — value for 8 byte ToS field, allocated to RTP packets (actual voice traffic).
- *SIP ToS* — value for 8 byte ToS field, allocated to SIP packets(announcement).

The device allows making calls via SIP-proxy, providing the following settings.

Figure 10.3. SIP settings

- *Registrar* — IP-telephony server in the format *sip:server.domain*;
- *Username* — usenameon the server;
- *Password* — user password;
- *User SIP URI* — URI of the user in the format *sip:user@server.domain*;
- *FXS channel* — number of FXS channel, to which the incoming calls received from SIP-proxy are redirected.

Hotline mode

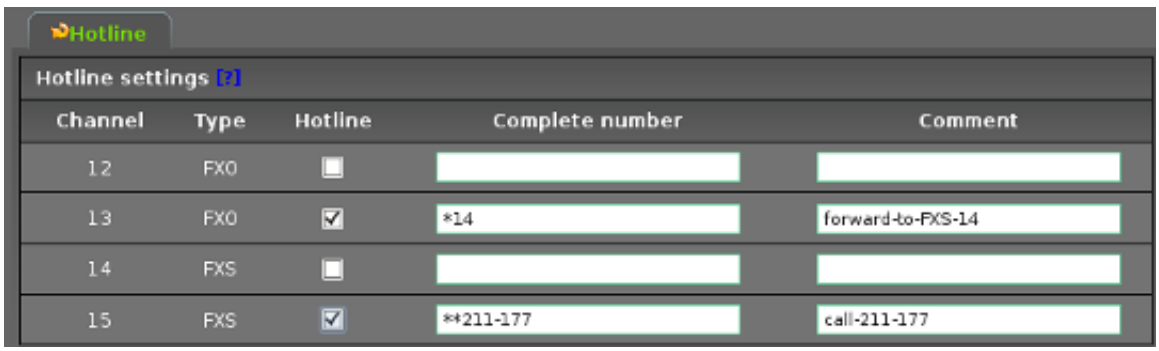
Hotline is adjusted at page Hardware/VoIP/Hotline. As far as theHotline settings are allocated to specific channels of a module and the performance depends on the channel type (FXO/FXS), the table contains the available channels and their types.

Hotline mode works with channels of FXO and FXS types, and has a separate working algorithm for each type.

- *FXO* — call redirection to another channel during the incoming call to a FXO channel (connected to PSTN or PBX).
- *FXS* — number dialling by the router when answerring a call, on the telephone apparatus connected to a FXS channel.

Let`s consider the parameters responsible for Hotline adjustment:

Figure 10.4. Hotline adjustment table



- *Channel* — channel number;
- *Type* — channel type;
- *Hotline* — Hotline mode in the channel when selected;
- *Complete number* — full number dialling by a router when finding a traceable event (answering an incoming call);
- *Comment* — comment (without spacing).

VF channels

VF channels allow to digitize the signal incoming from analogous equipment for the further transmission by means of IP-technology. VF channels adjustment is performed at the page Hardware/VoIP/VF, and consists in the adjustment of the connection between the two devices with VF modules which transmit signals from the analogous devices connected to them.

To establish a connection, the correspondence between the chosen local number of the channel and the identifier of the remote device and the number of its channel should be indicated. After that the codec parameters are indicated used for signal digitizing and other settings. Both, two-wire and four-wire, VF modes are supported.

Figure 10.5. VF channels setting

- *#* — the number of the active VF channel;
- *EN* — ativete the VF connection;
- *R.ID* — identifier of the remote device, should be displayed in VoIP routing table (see below);
- *Chan* — the number of VF channel at the remote device;
- *Codec* — VoIP codec in use;
- *P.time* — packetization time;
- *Pay-d* — Payload — identifier of the content of RTP packet;
- *Bitpack* —
- *JB type* — jitter buffer type;
  - *Fixed* ;
  - *Adapt.* — adaptable;
- *LAT* — Local Adaptation Type —

- *off* ;
- *on*;
- *SI* — with sample interpolaton

- *nScal* — average play out delay is equal to the estimated jitter times the scaling factor. Values: [1;16]
- *nInit* — initial size of the jitter buffer in ms. Values: JB Adaptive [nMin;nMax], JB Fixed: for aLaw [10; 150], for others [10; nMax]
- *nMin* — minimum size of the jitter buffer in ms. Values: [10; nMax]
- *nMax* — maximum size of the jitter buffer in ms. Values are depended on Codec and Pkt.time

Important

The same settings should be made on the second device.

Note

After the adjustment of the VF channel, the connection will be estabiliched and maintained automatically.

Adjustment of physical parameters of VF ports is performed in the tab Settings.

Figure 10.6. Adjustment of physical parameters of VF ports

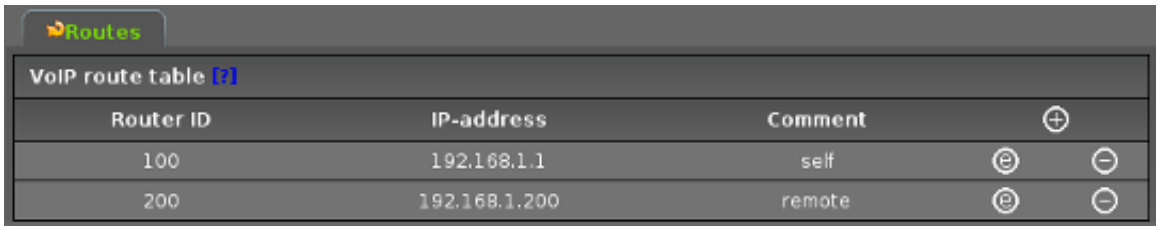
- *Wires* — connection type: two-wire or four-wire;
- *Transmit type* — signal level at transmission:
  - *4-Wire Normal*:
    - *Tx (In)*: -13 dBr
    - *Rx (Out)*: +4 dBr
  - *4-Wire Transit*:
    - *Tx (In)*: +4 dBr

- *Rx (Out)*: +4 dBr
- *2-Wire Normal*:
  - *Tx (In)*: 0 dBr
  - *Rx (Out)*: -7 dBr
- *2-Wire Transit*:
  - *Tx (In)*: -3,5 dBr
  - *Rx (Out)*: -3,5 dBr

Calls routing

Cals routing adjustment is performed at the page Hardware/VoIP/Routes. It includes the table reflecting the correspondence of the routers identifiers to their IP-addresses. The content of the tab is shown below.

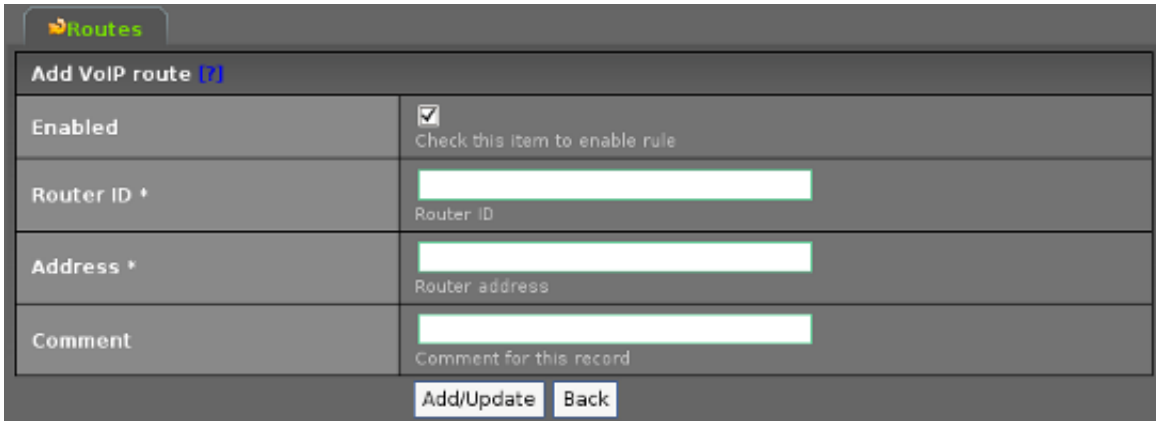
Figure 10.7. Calls routing



The table should include records with the identifier and the IP-address of the adjusted device. # ####### ###### ############### ###### # ################ # IP-####### ############### ##########. In this way the allocation of an identifier to the device and defining of the IP-address for work over VoIP is performed. As a comment to the record usually the word *"self"* is used.

Addition of a new record to the table is shown in the figure below.

Figure 10.8. Calls routing: addition of a new record



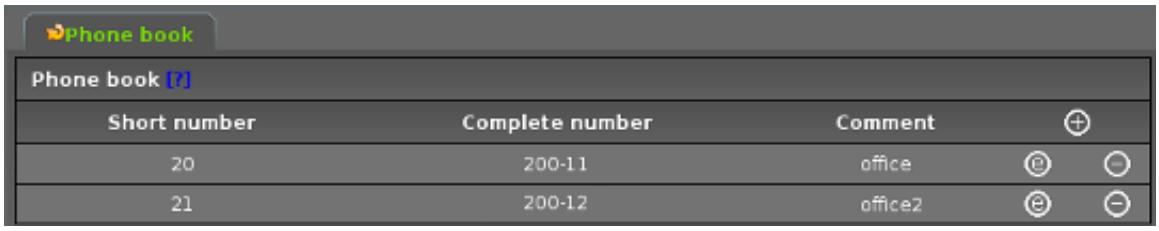
- *Enabled* — the record is active or not. If the recors is not active, it will not be added to the table of calls routing;

- *Router ID* — three-digit number of the router for which the record is added;
- *Address* — IP-address of the router;
- *Comment* — comment to the record.

Phone book

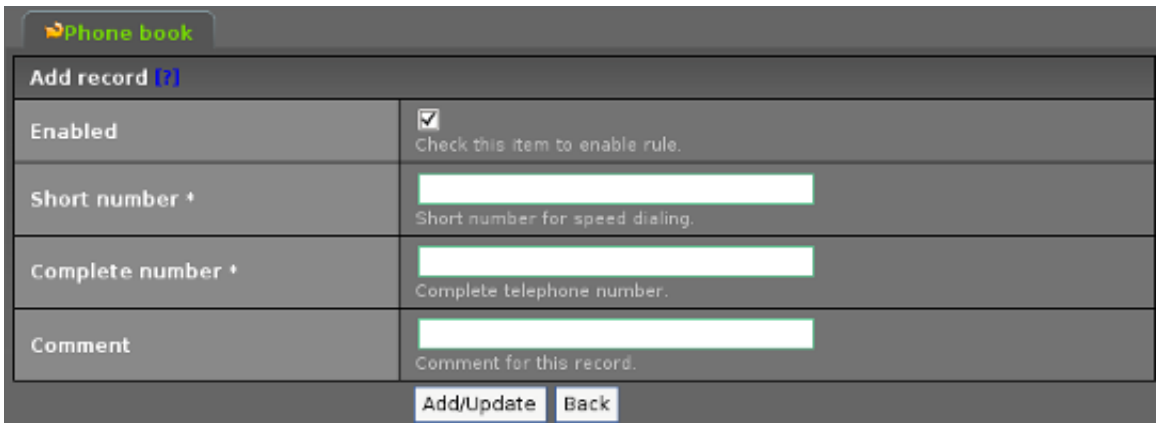
The phonebook is located at the page Hardware/VoIP/Phone book. It is used for speed-dial of telephone numbers. For example, for the number 100 02 833 the short number 10 can be set, and #10 can be used for dialling.

Figure 10.9. Phone book



Addition of a new record to the table is shown in the figure below.

Figure 10.10. Phone book: addition of a new record

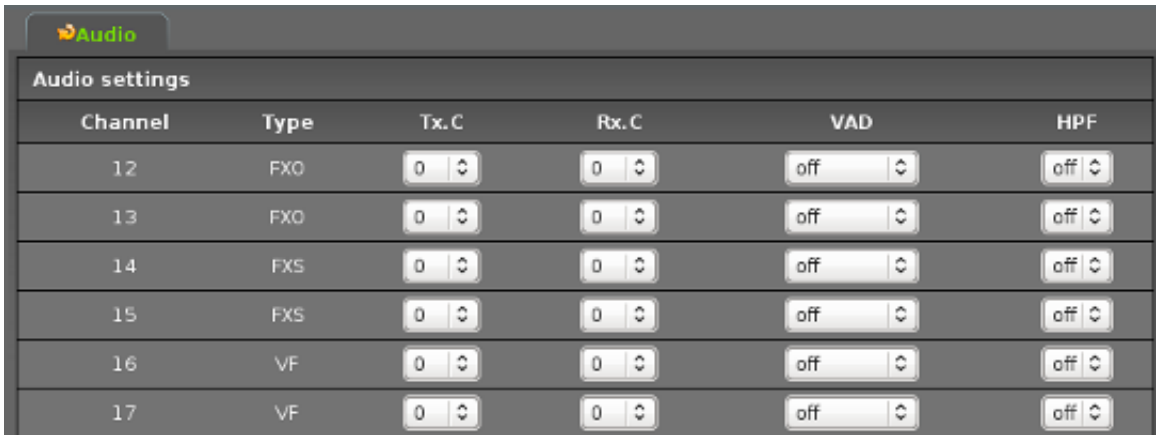


- *Enabled* — the record is active or not. If the record is not active, it will not be added to the configuration file.
- *Short number* — two-digit short number.
- *Complete number* — full number addressed when dialling "#short_number". When indicating the full number, the "_" symbol can be used to divide groupd of digits. Here a SIP-number can be indicated in the fromat: *#sip:user1@domain#.*
- *Comment* — comment to the record.

Audio settings

At the page Hardware/VoIP/Audio audio settings for FXO/FXS/VF channels can be made.

Figure 10.11. Audio settings



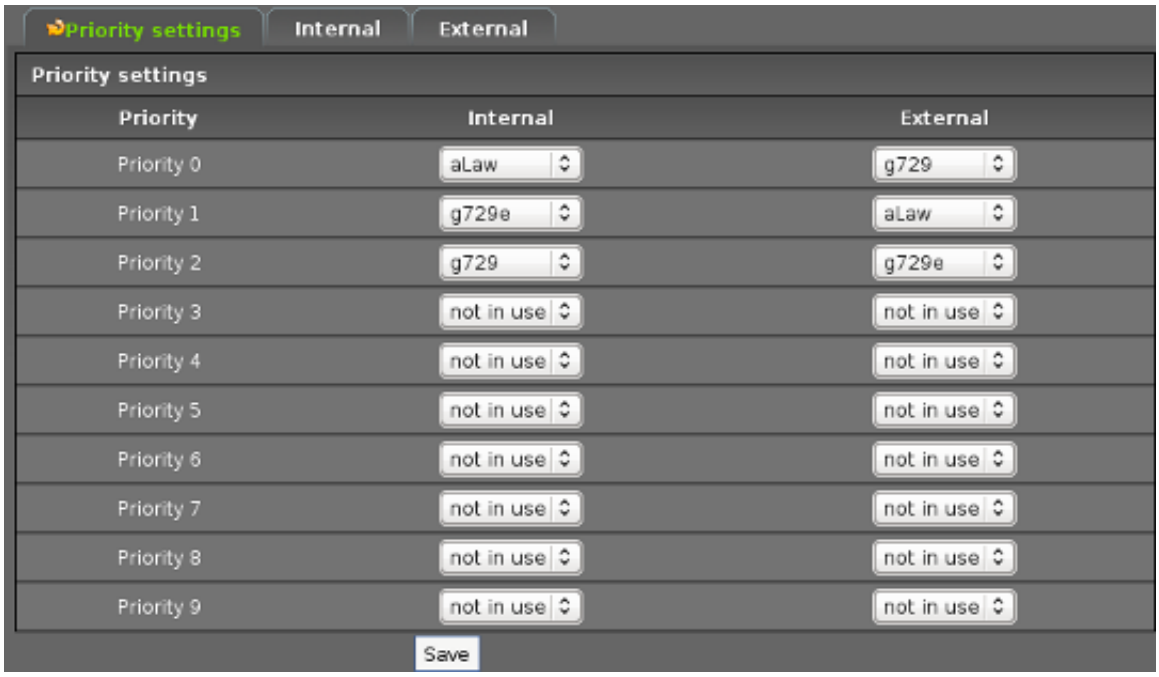
- *Tx.C* — outgoing signal volume level;
- *Rx.C* — incoming signal volume level;
- *VAD* — voice activity detector;
- *HPF* — income high-pass filter.

Codecs

The adjustment of the codecs in use can be performed at the page Hardware/VoIP/Codecs. Codec settings are available for two directions of calls: *Internal* — calls between the devices, and *External* — calls via SIP-proxy.

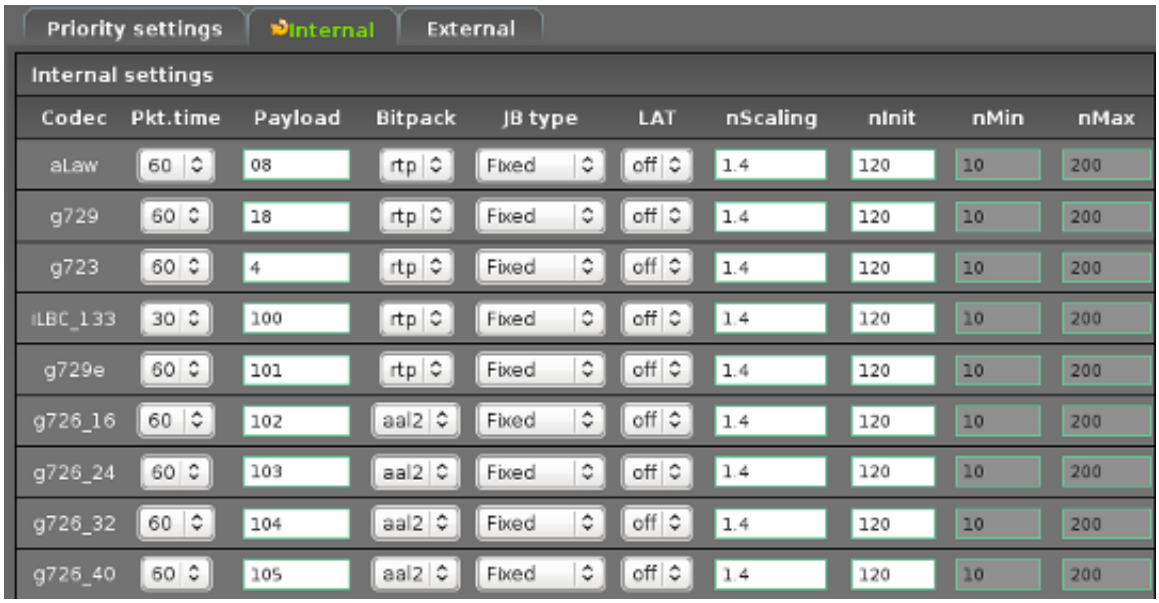
In the *Priority settings* tab the codec priority can be set. One codec can have only one priority level.

Figure 10.12. Codec priority



In the tabs *Internal* and *External* codec settings for the relevant call directions are made. Values on default are usually enough for most of the configurations.

Figure 10.13. Codec settings



- *Codec* — codec name;
- *Pkt.time* — packeting time;
- *Payload* — identifier of the content of an RTP packet;
- *Bitpack* —
- *JB type* — jitter buffer type;
  - *Fixed* ;
  - *Adaptive* — adaptable;
- *LAT* — Local Adaptation Type —
  - *off* ;
  - *on*;
  - *SI* — with sample interpolaton —
- *nScaling* —
- *nInit* —
- *nMin* —
- *nMax* —

Echo cancellation settings

Echo cancellation settings are made at the page Hardware/VoIP/Echo.

Figure 10.14. Echo cancellation settings

- *WLEC type* — echo cancellation type;
- *NLP* —
- *Near-end window* —
- *Far-end window* —

Dialing mode settings

Dialing mode settings are made at the page Hardware/VoIP/Dial mode. There is one setting — *PSTN type*. This parameter indicates which dialing mode is supported by the telephone station.

Figure 10.15. Dialing mode settings

Chapter 11. SNMP

Introduction to SNMP

SNMP — Simple Network Management Protocol. The protocol allows monitoring of network devices (routers, multiplexers, bridges etc.) and services (web-servers, mail servers, DNS-servers) and manage their configuration.

Management and monitoring is performed according to agent-manager scheme. Agent is the software operating at the network device which is a subject for monitoring or management; manager - is the software collecting the dats from agents for monitoring or management. The cooperation is usually performed over the UDP transport protocol, port 161. There is also a possibility of use the TCP protocol.

The objects to which the operations (reading or recording) can be applied have unique numbers. For example, 1.3.6.1.2.1.1.1 corresponds to the object SysDescr — system description, which may have the following value: *STRING Linux sigrand 2.6.16 #1 Tue Nov 7 21:37:48 NOVT 2007 mips* .

MIB — Management Information Base. MIB describes the objects and operations which can be applied to them. If the object is included in the MIB, it can be addressed by name and not by the digital index.

Authentification is performed on the basis of the "community" - each agent is referred to this or that community. At the command reception the checking whether the agent refers to the community indicated in the command is carried out. If yes - the command will be accepted and processed, if no - ignored. Community is a simple line; on default two communities are used - public, for object browsing, and private - for object editing.

SNMP support level of the router

For SNMP support the router uses an unbound software package *net-snmp* , supporting all the actual versions of SNMP, which includes the *snmpd* daemon functioning as an agent.

The router supports *MIB-2* which provides general information about the system (network interfaces, routing tables, system data), and *HDSL2-SHDSL-LINE-MIB* which includes the objects used for SHDSL channels monitoring and management.

MIB-2 is a standard MIB and is included in the majority of managers, while HDSL2-SHDSL-LINE-MIB is type-specific. This file can be downloaded from the Internet sources or by reference [http://sigrand.ru:8280/temp/HDSL2-SHDSL-LINE-MIB-rfc4319.txt] .

At the moment only monitoring of the router SNMP and SHDSL channels and regenerators is available, the management option will be added soon.

SNMPD settings

The settings of the *snmpd* daemon are stored in the file */etc/snmp/snmpd.conf* and consists in setting of tokens for receiving and editing of objects.

The content of the configuration file looks as follows:

```
com2sec ro default public
com2sec rw localhost private

group public v1 ro
group public v2c ro
group public usm ro
group
private v1 rw
group private v2c rw
group private usm rw

view all included .1

access public "" any noauth exact all none none
access private "" any
noauth exact all all all
```

The *com2sec* command establiches a correspondence between a community and a token, and defines the addresses which can be referred to these communities. In the configuration file above the first command defines that thecommunity "public" complies with the RO security, and that it is corresponds to all IP-addresses. The second command defines the compliance of the "private" community with the RW security, and limit the access to the router itself.

The *group* command defines which security corresponds to which group. In our example, RO security corresponds to the group "public", RW security - to the group "prvate". v1, v2c, usm define the security model. v1 refers to SNMP ver.1, v2c — to ver.2, usm — SNMPv3.

The *view* command defines the name of scope and what it includes. In our case, the scope name — all, and it includes the overall MIB tree.

The last command - *access* - defines the access rights for different groups. In our example for both groups access without authentification is allowed, but in case of "public" group - only for reading, "private" group - for reading and editing.

For further information visit the web site net-snmp, in particular the folowing reference [http://net-snmp.sourceforge.net/wiki/index.php/Vacm] .

Interaction of SNMPD with EOCD

SNMPD receives the SHDSL-channel status data from the daemon *EOCD* . Therefore, in order to receive data conserning the state of the SHDSL-channel via SNMP, the EOCD daemon should be adjusted. After the data is available via the **eoc-info** utility — the data can be received via SNMP. The detailed information about the functionality and adjustment of the EOCD daemon is given in chapter SHDSL-channels monitoring .

Usage example

As an example lets look at the router SHDSL-channel monitoring function. For this obtain data about the number of regenerators, signal attenuation and signal/noise ratio.

Digital name of the object corresponds to the number of regenerators installed on line (Hdsl2ShdslStatusNumAvailRepeaters), equal to1.1.3.6.1.2.1.10.48.1.2.1.1. For signal

attenuation (Hdsl2ShdslEndpointCurrAtn) the name is equal to 1.1.3.6.1.2.1.10.48.1.5.1.1.11.1.2.1 for the client-side (slave) and 1.3.6.1.2.1.10.48.1.5.1.1.11.2.1.1 for master, and for signal/noise ratio(Hdsl2ShdslEndpointCurrSnrMgn) — 1.3.6.1.2.1.10.48.1.5.1.2.11.1.2.1 and 1.3.6.1.2.1.10.48.1.5.1.2.11.2.1.1 accordingly. Values of these parameters are given below:

```
1.3.6.1.2.1.10.48.1.2.1.1.11 = Gauge32 0
1.3.6.1.2.1.10.48.1.5.1.1.11.1.2.1 = INTEGER 0
1.3.6.1.2.1.10.48.1.5.1.1.11.2.1.1 = INTEGER 0
1.3.6.1.2.1.10.48.1.5.1.2.11.1.2.1 = INTEGER 19
1.3.6.1.2.1.10.48.1.5.1.2.11.2.1.1 = INTEGER 17
```

I.e. the number of regenerators is 0, signal attenuation on both end of the connection — 0 dB, signal/noise ratio on client-side -19 dB, on master-side - 17 dB.

When using specialized software supporting MIB loading it is possible to obtain information in a more convenient form.

Supported software for management via SNMP

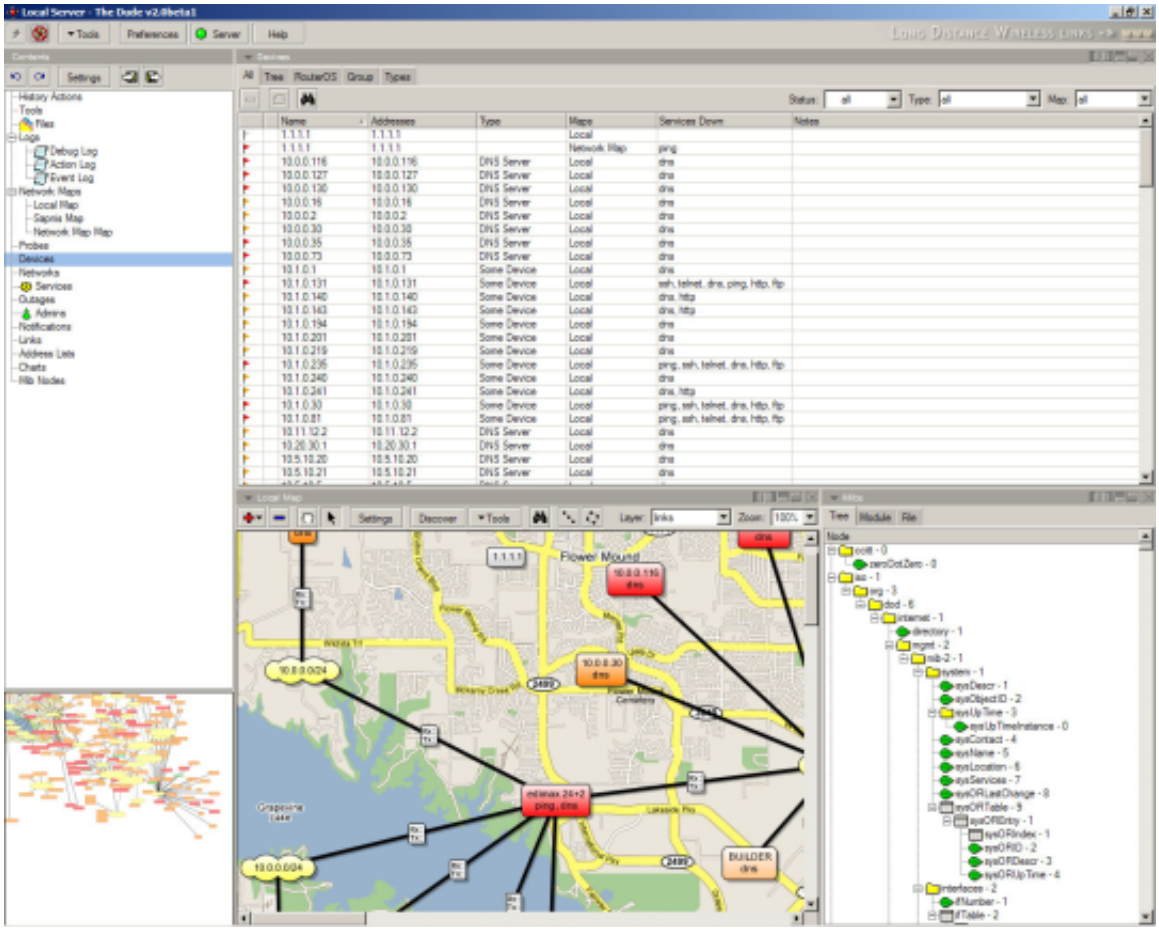
For the purpose of SNMP support an unbound software package *net-snmp* is used, which allows to work with all software solutions compatible with net-snmp.

In addition a brief review of the available software was made. The results are given below.

The Dude

The Dude — is a free software product for work at SNMP protocol, works in MS Windows OS.

Figure 11.1. The Dude



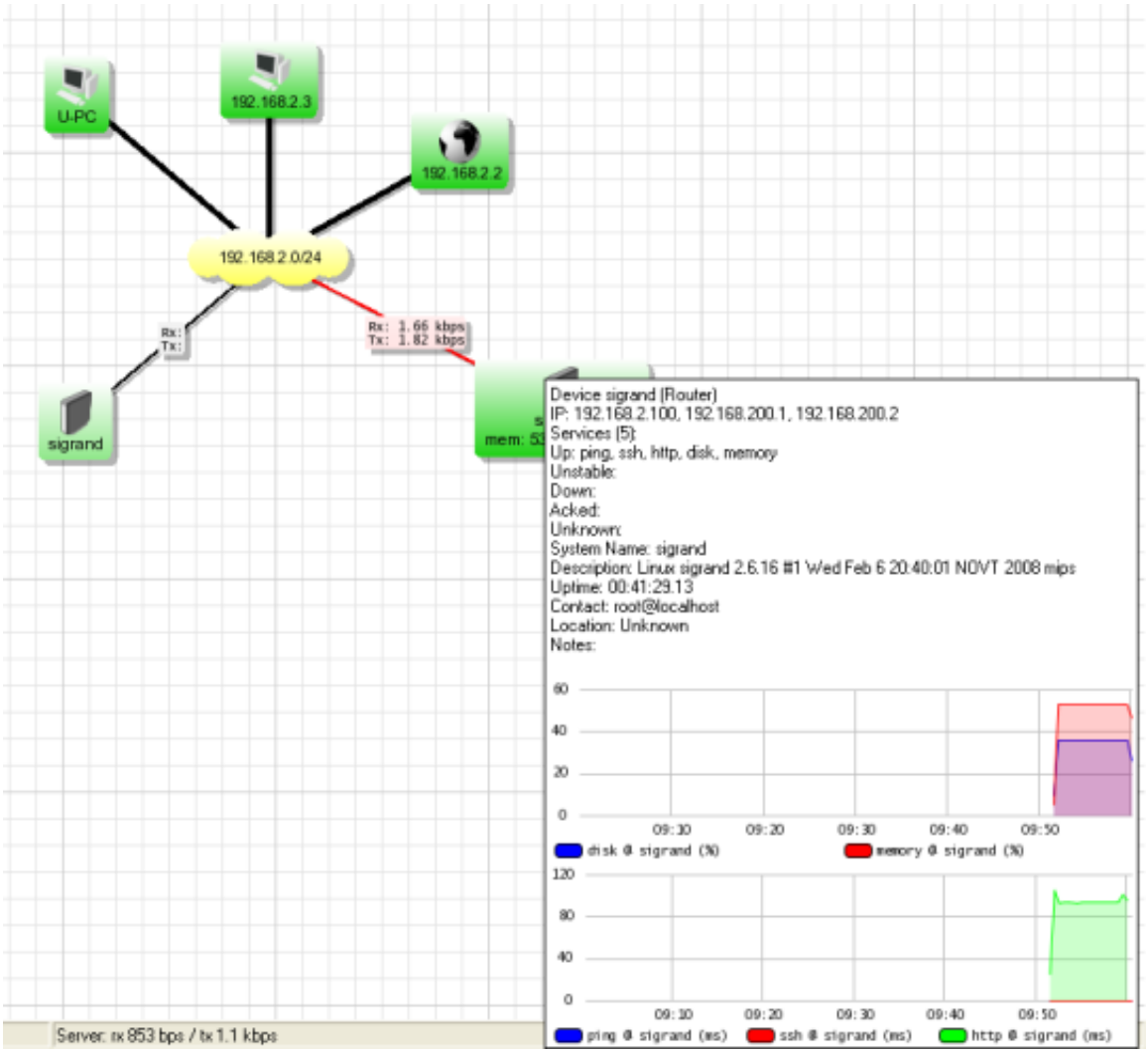
Advantages:

- Identifies the network devices automatically.
- Build network map, allows addition of new devices to the map, output the values of SNMP-variables.
- Performs the device monitoring, graphing in real-time mode.
- Has several friendly integrated utilities for network administration and monitoring (terminals, snmpwalk).
- Friendly modes of SNMP data browsing (list, tree, table).

Disadvantages:

- Interface indexes are displayed incorrectly in table view.
- Incorrect displaying of SnmpAdminString for SHDSL profiles names is possible.

Figure 11.2. The Dude: Sigrand routers

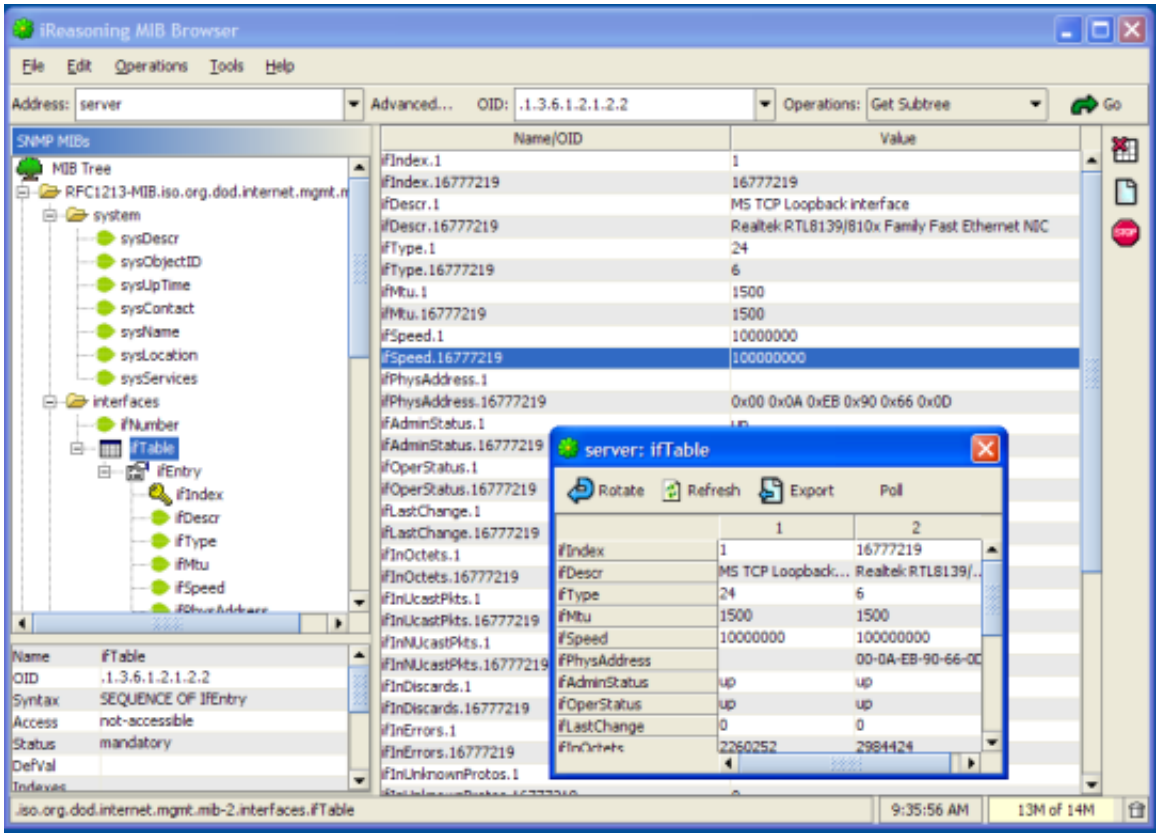


Homepage of the project: The Dude [http://www.mikrotik.com/thedude.php].

MIB Browser

MIB Browser , a product of the company iReasoning, available in pay and free versions which differ in license agreements and functionality. The support of Windows, Mac OS X and Linux OS is declared.

Figure 11.3. MIB Browser



Advantages:

- Friendly interface.
- Table view of SNMP tables.

Disdvantages:

- The free version does nor support SNMPv3, allows downloading no more than 5 MIBs to the existing.
- Incorrect displaying of SnmpAdminString is possible for SHDSL profiles names.

Homepage of the project: MIB Browser [http://www.ireasoning.com/mibbrowser.shtml].

OpenNMS

OpenNMS — a web application written in Java, uses DBMS PostreSQL and Apache Tomcat for operation, allows monitoring of industrial networks. It is a free software, available for the pletforms on which Apache Tomcat works (usually these are Linux servers).

Figure 11.4. OpenNMS

Advantages:

- OpenNMS, apparently, uses *net-snmp* for work under SNMP, which provides full compatibility with *Sigrand* devices.

Homepage of the project: OpenNMS [http://www.opennms.org/index.php/Main_Page].

Chapter 12. Configuration examples

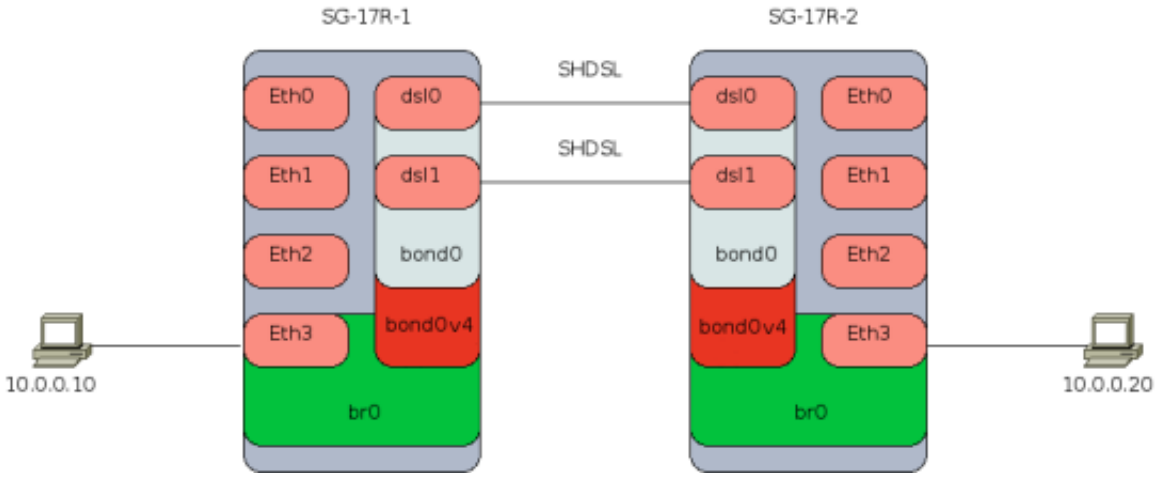
VLAN

Setting of independent channels between Ethernet-interfaces

The given example considers the setting of independent channels between the Ethernet-ports of the devices connected via SHDSL.

Let`s consider the arrangement of data communication fronm the port eth3 of one device to the port eth3 of another device via SHDSL connection. If necessary, all ports of the devices can be used (eth0, eth1, eth2). The pattern of interaction between the devices can be represented as follows:

Figure 12.1. Interaction pattern



The devices are connected via two SHDSL channels which are bonded. On the bonding there created a VLAN with VLAN ID 4. The bridge actualize packet-mode communication between the interfaces bond0v4 (VLAN interface) and eth3.

The adjustment begins from the adjustment od the physical connection between the routers (see SHDSL settings).

Then we create a bonding of the interfaces dsl0 and dsl1 (see Bonding settings). In the result we get the interface *bond0*.

After that we need to create a VLAN on the bonding. The number of VLAN interfaces depends on the number of ethernet-ports between which we are going to establish an independent data transfer - one VLAN for each port. The VLAN interface setting procedure is described in details in the relevant chapter. I.e. we need to create a VLAN interface with VLAN ID 4 on the bond0 interface. As a result, we have the interface *bond0v4*.

The final step is bridging (see bridge settings). Bridge consists of the interfaces *bond0v4* and *eth3*, between which the traffic transfer is performed. The number of bridges depends on the number of ports used for data exchange - one bridge for each port.

Thus, if we want to arrange the exchange between the ports eth2, we should create one more VLAN on the interface *bond0*, for example, with VLAN ID 3, create one more bridge interface and add the interfaces *bond0v3* and *eth2* to it.

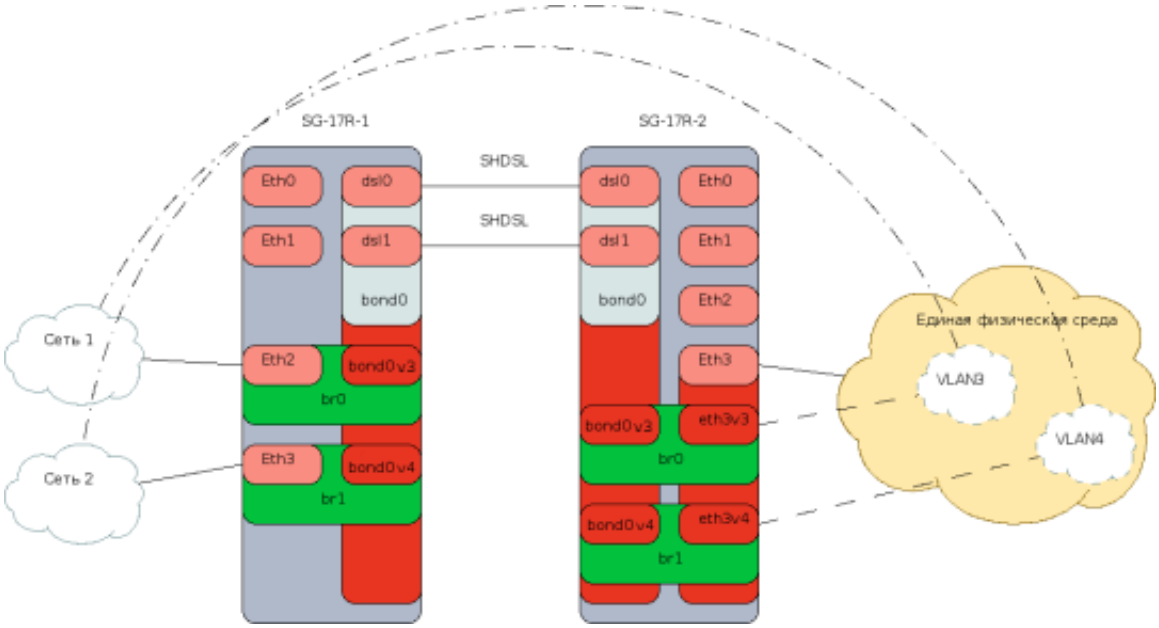
Note

If it is necessary to arrange a device management via the port which participates in data transfer (included in the bridge), its IP-address (at which the settings are made) should be allocated to the interface of the bridge. The detailed information is given in the relevant chapter.

Traffic distribution along Ethernet-ports according to VLAN ID

Suppose that we want to arrange a transfer of VLAN-traffic incoming to the trunk-port of one device via SHDSL-channel, and transfer traffic (without VLAN tag) to the relevant ethernet-port depending on the VLAN ID on the other device.

Figure 12.2. Structure chart



The idea of the given arrangement consists in that at the SG-17R-2 device, one of the ports of which functions as a trunk-port, we create VLAN interfaces which traffic should be transmitted to the relevant ports of the other device.

For example, to the SG-17R-2 device (let`s say to the 4th ethernet-port) there connected a network, in which there are functioning several VLAN networks with numbers 3 and 4. We need to connect the VLAN ID 3 network to the network connected to the 3rd ethernet-port of the SG-17R-1 device. We also need to connect the VLAN ID 4 network to the network connected to the 4th ethernet port of the SG-17R-1 device. It should be noted that the networks connected to SG-17R-2 are simple LAN networks, and therefore the traffic transmitted to them should not contain "VLAN" tags.

The adjustment of the given arrangement is divided onto two steps: adjustment of SG-17R-1 and adjustment of SG-17R-2. It is understood that the physical connection between the devices (for example, via SHDSL)is already adjusted. In our example we use bonding over SHDSL channels.

Adjustment of SG-17R-1

In general the adjustments consists in creation of VLAN interfaces over the bonding interface, and bridging of the relevant ethernet-interface and VLAN interface. Let`s consider it in more detail.

Create the VLAN interface with VLAN ID 4 on the interface *bond0* (see VLAN settings). The name of the new interface is *bond0v4*. Here we also create a bridge interface named, for example, *br0*. Integrate in it the interfaces between which the traffic will bw transferred: *bond0v4* and *eth3*.

If it is necessary to arrange the transmission of several VLAN to the ports of SG-17R-1, the gives procedure should be repeated for each VLAN. In the given configuration the maximum number of VLAN is 4,cas it is limited by the number of ethernet-ports of the device.

Adjustnment of SG-17R-2

Before starting we should deside which of the ethernet-ports of the device will function as a trunk-port, i.e. to which port the VLAN networks will be connected.

For the chosen trunk-port we create a VLAN interface and the corresponding VLAN interface on the basis of the interface of the bonding. Than we arrange a bridge between the existing interface of the trunk-port and the VLAN interface of the bonding. The thing is that each VLAN interface created on the trunk-port receives its own traffic and transmit it to its "own" bonding interface. On the second device (SG-17R-1) the bonding trasnfer it to the relevant ethernet-port. Let`s consider these actions in more detail.

The adjustment begins from the creation of VLAN interfaces with similar VLAN ID on the interfaces of the bonding (for example, *bond0*) and of the ethernet-port functioning as a trunk-port (*eth3*). Suppose the created interfaces have the names *bond0v4* and *eth3v4*. Here we also create the interfaces of the bridge, one for each pair of VLAN interfaces. For example, we add the interfaces *bond0v4* and *eth3v4* to the first interface.

Thus we have one or several bridge interfaces, trasmitting traffic between VLAN interfaces which were created on the trunk-port and on the bonding.

Device management access control via VLAN

For controlling the access to the device management VLAN technology can be used. For this purpose, on the basis of the interface trough which the management is conducted we create a VLAN interface to which we allocate an IP-address, deleting the IP-address of the underlying interface.

Management of device control via the interface integrated in a bridge or bonding

######, #### ####, ##### ####### ############## ########## ###########, ########## ######## # ###### ###### ### ########, IP-#####, ############ ### ##########, ####### ######### ##########, # ###### ######## ########## ####. For example, the port eth0 is used for device control and the allocated IP-address is 192.168.2.100. Than while intergating the port in the bridge (interface br0), the interface br0 gets the allocated IP-address 192.168.2.100.

Tip

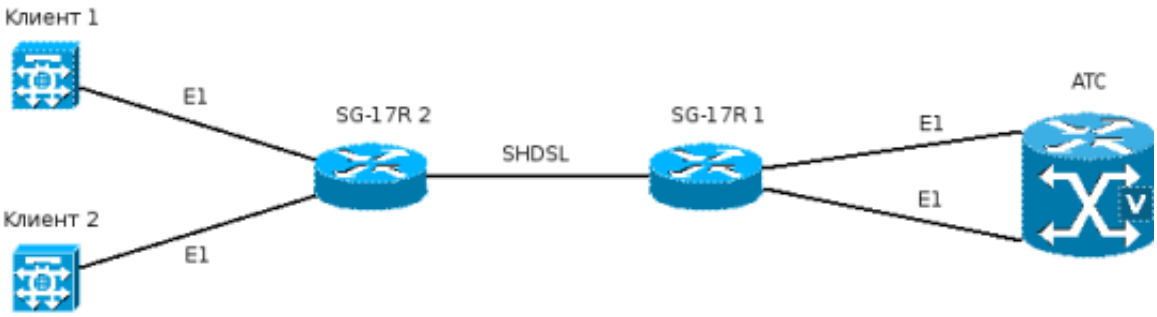
In case when the bridge interface gets the same IP-address which was allocated to the port interface, temporery loss of connection with the device is possible. It happens because the MSC-

address of the bridge is related to one of the interfaces it incorporates, and if the chosen MAC-address differs from that of the interface of the port to which the IP-address belonged, the correlation between the MAC-address and IP-address in the local APR-cach of the computer should be changed. It can be done manually by means of deleting the correspondent record from the APR-cach, of automatically after a while.

Multiplexing

Let`s consider multiplexing on the following example:

Figure 12.3. Network example



Two E1 channels (unframed mode) should be transmitted from PBX to Client 1 and Client 2 via SHDSL channel.

As far as the signal source is similar for both channelsE1 — #PBX, it does not matter which of the E1 interfaces will synchronize the multiplexing lines. We have 16 lines, 256 time-slots each. For convenience we will use two of them - one for traffic reception, the other - for traffic transmission.

The scheme of multiplexing will be the following:

- InterfaceE1 *E1_0* receives data from the physical line and transfer it to the line 0 (from 0 time-slot). The data for transmission to the physical line are taken from the line 1, from o time-slot. This interface also functions as a source of synchronization for the domain.

- Interface E1 *E1_1* functions as *E1_0*, but places and tekes data begining from the 32 time-slot (and does not transmit the synchro-signal, i.e. functions in *clock slave* mode).

- InterfaceSHDSL *dsl0* places the data obtained from the physical line to the line1 (from which they are taken by E1 interfaces), and the data for transmission to the physical line are taken from the line 0 (where E1 interfaces place it). The number of time-slots used by the interface for multiplexing - 64 (32 from each E1 interface).

The described arrangement id represented below:

Figure 12.4. Interface interaction, line 0

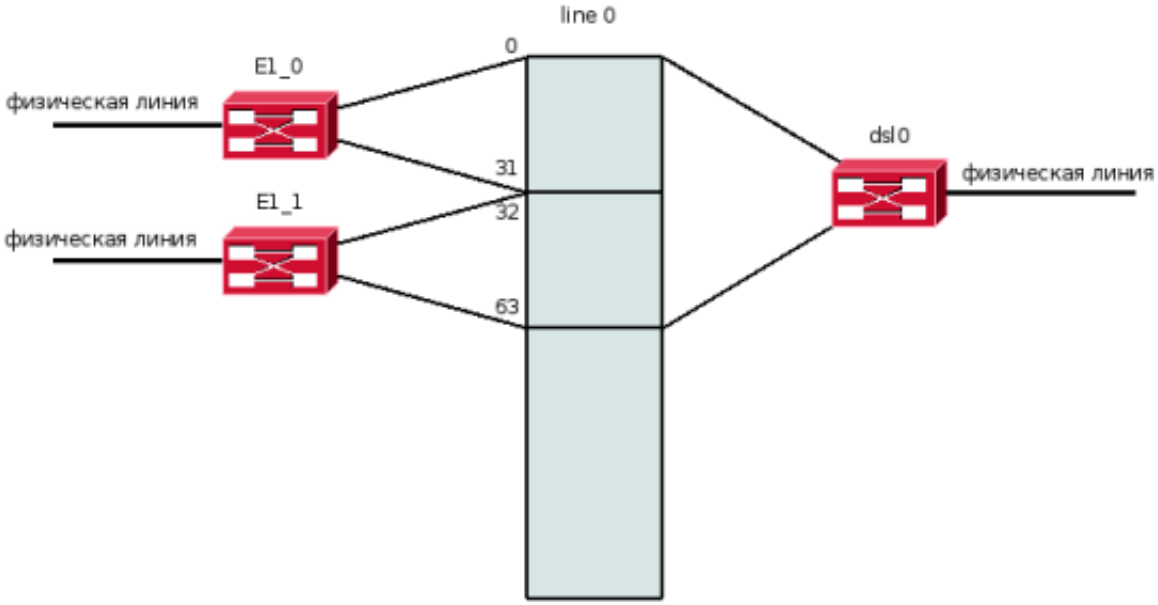
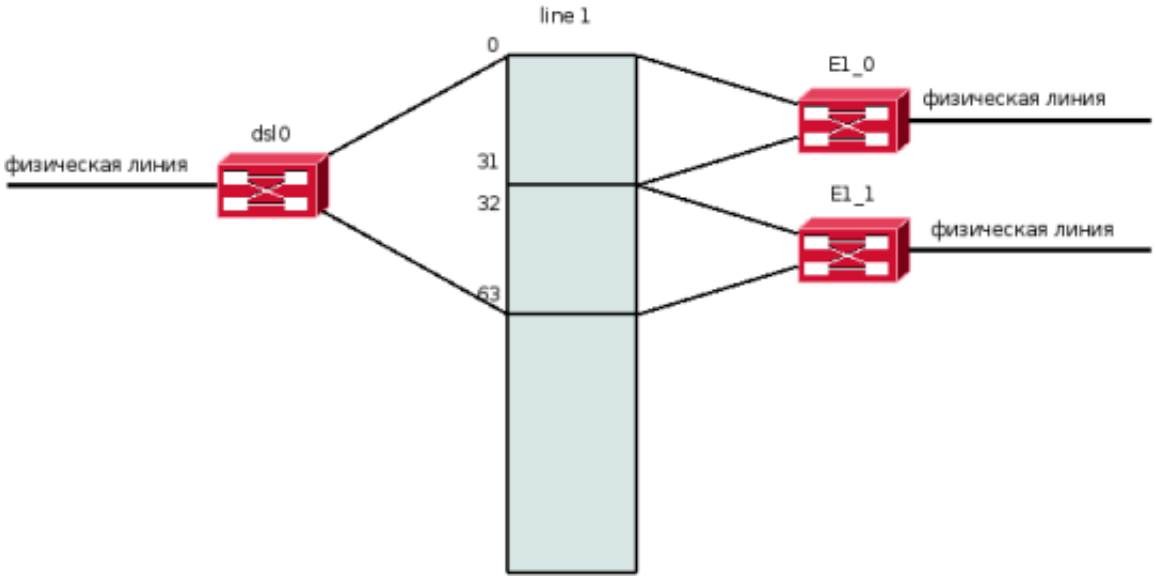


Figure 12.5. Interface interaction, line 1



For the realization of the scheme the following parameters should be set:

- Interface E1 *E1_0*
  - `rline = 0`
  - `rfs = 0`
  - `tline = 1`
  - `tfs = 0`
  - `mxsmap = "0-31"`

  - *clkm = 1*
  - *clkr = 1*
  - *clkab = 0*
- Interface E1 *E1_1*
  - *rline = 0*
  - *rfs = 32*
  - *tline = 1*
  - *tfs = 32*
  - *mxsmap = "0-31"*
  - *clkm = 0*
  - *clkr = 0*
  - *clkab = 0*
- Interface SHDSL *dsl0*
  - *rline = 1*
  - *rfs = 0*
  - *tline = 0*
  - *tfs = 0*
  - *mxrate = 64*
  - *clkm = 0*
  - *clkr = 0*
  - *clkab = 0*

Note

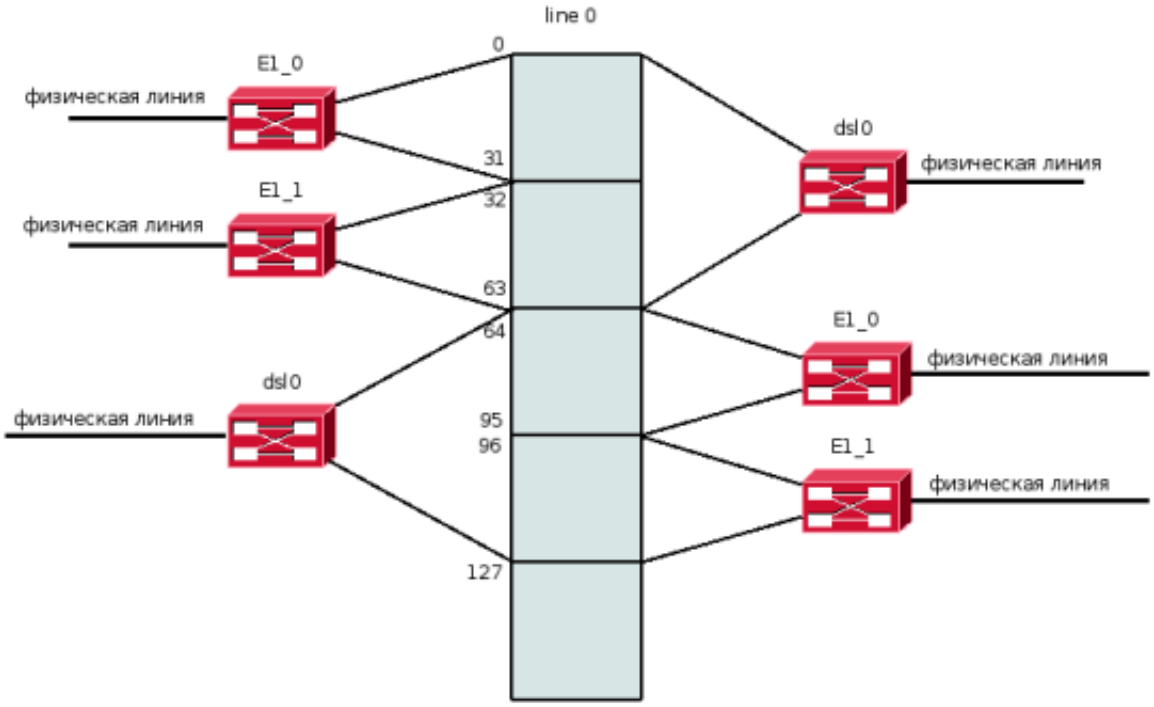
For these interfaces the multiplexing mode should be activated - set the parameter *mxen*.

The configuration on the second router can be set in the same way. The only difference in this case consists in change of the interface functioning as a source of synchronization. This function will be performed by the interface SHDSL *dsl0*, as far as it is the interface which receive the multiplexed flow from the first router connected to the PBX.

Tip

For traffic reception and transmission separate lines should not necessarily be used. For these purposes we can use one line under the condition that we correctly indicate the time-slots starting from which each interface places or takes data from the line. An example of such configuration is given below:

Figure 12.6. Usage of a single line for data transfer in both directions

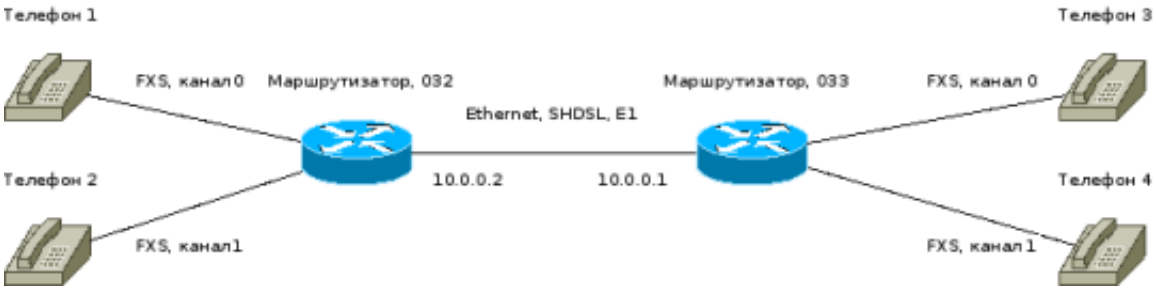


VoIP

Common telephones function as a pair of IP-telephones

Install on the router VoIP modules with FXS channels to which connect common POTS telephones. Using these telephones it is possible to make calls to the telephones connected to the given router or to other Singand routers. An example of connection pattern is given below.

Figure 12.7. Common telephone function as a pair of IP-telephones



In the given example in the network there are operating two routers with numbers 032 and 033 and addresses 10.0.0.2 and 10.0.0.1 accordingly. Each router is connected to a POTS telephone; the routers are interconnected via any technology — Ethernet, SHDSL or E1.

For IP-telephony adjustment it is necessary to put the data into the routing tables, address book and Hotline tables. For convenience the examples of settings are given in form of textual tables given below. .

The routing table has the same content at all the routers of the network, as you can see below.

Table 12.1. Routing table

Router #	Router address	Comment
032	10.0.0.2	Router 032
033	10.0.0.1	Router 033

Address book should be filled for each router seperately, as far as different short number can be used. Address books of the routers is given below.

Table 12.2. Address book of the router 032

Short number	Full number	Comment
00	* 01	Telephone 1 (###### ####### ###### ######)
01	032 02	Telephone 2 (###### ####### ###### ######)
02	033 01	Telephone 3
03	033 02	Telephone 4

Table 12.3. Address book of the router 033

Short number	Full number	Comment
00	032 01	Telephone 1
01	032 02	Telephone 2
02	* 01	Telephone 3
03	* 02	Telephone 4

In this configuration the following dialing modes are available:

- From telephone 1 to telephone 2:
  1. directly:
     a. * 02
     b. 032 02 (with indication of the own router number)
  2. via the address book: #01
- From telephone 1 to telephone 4:
  1. directly: 033 02
  2. via the address book: #03

In Hotline mode the configuration can be arranged in which there will be initiated an automatic dialling of the number pre-set for the FSX channel (to which the telephone is connected) by lifting of a hand-set. Hotline settings for the router 032 are given in the table below.

Table 12.4. Hotline table for the router 032

Channel #	Full number	Comment
01 (FXS)	033 01	Automatic call to telephone 3

Channel #	Full number	Comment
02 (FXS)	032 01	Automatic call to telephone 1

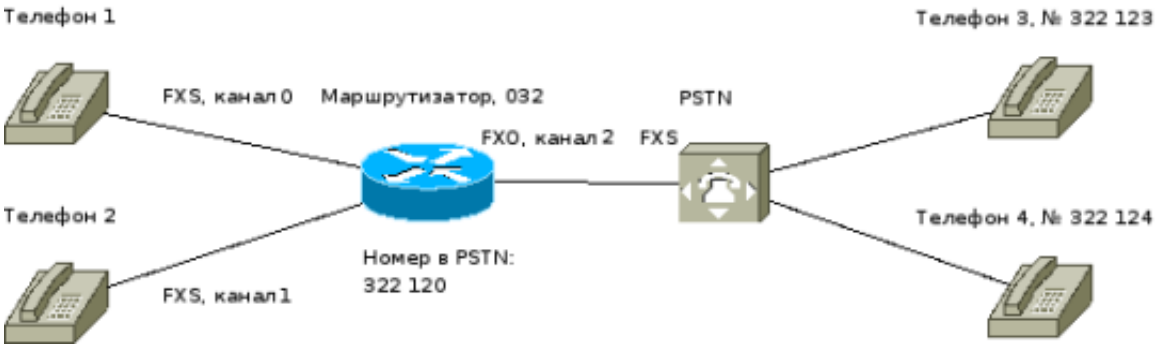
This configuration sets the following behavior:

- when lifting the hand-set of telephone 1 an automatic call to telephone 3 is made.
- when lifting the hand-set of telephone 2 an automatic call to telephone 1 is made.

Communication arrangement via PBX

Install on the router VoIP modules with FXS channels for connection to POTS telephones, and FXO for connection to PBX - for example, to a city network (PSTN). The port 322 120 of the PBX is reserved for the router. The scheme is given below.

Figure 12.8. Communication arrangement via PBX



In this case the routing table is not used; the address book can be adjusted for speed-dial. The settings for the address book are given in the table below.

Table 12.5. Address book

Short number	Full number	Comment
00	* 01	Telephone 1
01	032 02	Telephone 2
02	* * , 322 123	Telephone 3
03	032 * , 322 124	Telephone 4

Note

The «*» symbol instead of the channel number denotes the call via the first unoccupied channel FXO. In our case there is only one FXO, and we can always ude this symbol for the faster dialling.

In this configuration the following dialing modes are available:

- From telephone 1 to telephone 2:
  1. directly: * 02
  2. via the address book: #01
- From telephone 2 to telephone 4:

1. directly: * *, wait for a signal from PBX, 322 124
2. via the address book: #03

- From telephone 3 to telephone 1:
  1. directly:
     a. 322 120, wait for a signal from the router, * 01
     b. 322 120, wait for a signal from the router, 032 01

The Hotline mode allows realization of the behaviours given in the table below.

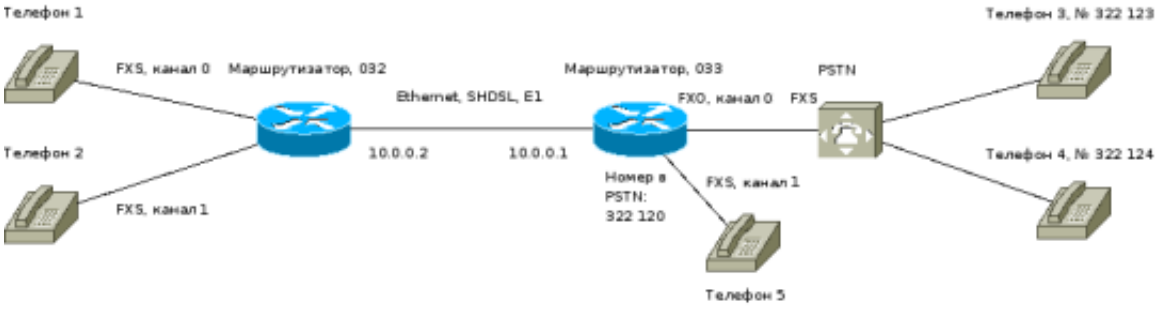
Table 12.6. Hotline table for the router

Channel #	Full number	Comment
01 (FXS)	* * , 322 124	Automatic call when the hand-set is lifted at the telephone 1 to telephone 4
03 (FXO)	* 01	Redirection of the incoming calls from PSTN to telephone 1

Arrangement of communication via PBX using two routers

Let`s consider a more complicated version of the network described in thr previous example. there are two routers operating on line to which POTS telephones are connected. The routers are interconnected by means of Ethernet/SHDSL/E1, and one of the routers is connected to the PBX. We need to realize the possibility of calls between the telephones, connected to the routers and between the routers and the PBX. The scheme is given below.

Figure 12.9. Arrangement of communication via PBX using two routers



As far as there are two routers operating in the network, we need to adjust the VoIP routing table (tab Routes), as shown below.

Table 12.7. Routing table

Router #	Router address	Comment
032	10.0.0.2	Router 032
033	10.0.0.1	Router 033

For speed-dial adjust the address book for each router as shown in tables below.

Table 12.8. Address book of the router 032

Short number	Full number	Comment
00	* 01	Telephone 1
01	* 02	Telephone 2
02	033 02	Telephone 5
03	033 * , 322 123	Telephone 3
04	033 * , 322 124	Telephone 4

Table 12.9. Address book of the router 033

Short number	Full number	Comment
00	032 01	Telephone 1
01	032 02	Telephone 2
02	* * , 322 123	Telephone 3
03	* * , 322 124	Telephone 4

In this configuration the following dialing modes are available:

- From telephone 1 to telephone 2:
  1. directly: * 02
  2. via the address book: #01
- From telephone 2 to telephone 4:
  1. directly: 033 *, wait for a signal from the PBX, 322 124
  2. via the address book: #04
- From telephone 2 to telephone 5:
  1. directly: 033 02
  2. via the address book: #02
- From telephone 3 to telephone 2:
  1. directly: 322 120, wait for a signal from the router, 032 02

Also adjust the Hotline mode as shown in tables below.

Table 12.10. Hotline table for the router 032

Channel #	Full number	Comment
01 (FXS)	033 02	Automatic call when the hand-set is lifted at the telephone 1 to telephone 5

Channel #	Full number	Comment
02 (FXS)	033 *, 322 124	Automatic call when the hand-set is lifted at the telephone 2 to telephone 4

Table 12.11. Hotline table for the router 033

Channel #	Full number	Comment
01 (FX0)	032 02	Redirection of the incoming calls from PSTN to telephone 2
02 (FXO)	* * , 322 123	Automatic call when the hand-set is lifted at the telephone 5 to telephone 3

Chapter 13. Warranty and liabilities

The Manufacturer guarantees the operability of the router under the condition that the user obliges the operating rules.

Warranty period - 5 years from the date of purchase indicated in the certificate, or, in the absence thereof, from the date of manufacturing indicated on the label.

Warning

Warranty is cancelled for routers used in overhead lines or in lines with a combined method of construction.